Computational Problems in Complex Cubic Fields

by

Gilbert Wai-Wing Fung

A thesis presented to

the University of Manitoba

in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

in

the Department of Computer Science

Winnipeg, Manitoba

ISBN 0-315-76910-6

COMPUTATIONAL PROBLEMS

IN COMPLEX CUBIC FIELDS

BY

GILBERT WAI-WING FUNG

A thesis submitted to the Faculty of Graduate Studies of
the University of Manitoba in partial fulfillment of the requirements
of the degree of

DOCTOR OF PHILOSOPHY

ABSTRACT

This thesis describes various algorithms for solving computational problems in cubic fields of negative discriminant.

A method for finding all the non-isomorphic complex cubic fields with discriminant $D > -10^6$ is described. Three different methods were used to find the class number of each of these fields. The speed of these techniques is discussed and several tables illustrating the computational results are presented.

Since the above method for constructing cubic fields is not suitable for a large absolute discriminant, a description is given as to how all the non-isomorphic cubic fields, which have the same given fundamental discriminant, can be computed by means of the CUFFQI algorithm of Shanks. A description is given of the implementation of this algorithm and its complexity is also discussed. The results of running this algorithm for certain discriminants are also presented.

An improved version of the Williams, Cormack and Schmid algorithm for evaluating the regulator of a pure cubic field is presented. By using this algorithm and the Open Architecture Sieve System (OASiS), some pure cubic fields which have large regulators were found. Furthermore, a brief description is given as to how OASiS can be used to find several values of D such that the cubic polynomial x^3+D has a large asymptotic density of prime values. The Hardy-Littlewood constants which characterize this density are also evaluated.

Finally, we show how the infrastructure idea of Shanks can be used to produce a fast algorithm for determining principal factors in pure cubic fields. This algorithm was implemented on a computer and was used to test a conjecture of Mayer by determining the existence of principle factors for certain pure cubic fields with large absolute discriminant.

Acknowledgements

I would like to acknowledge my advisor, Professor Hugh C. Williams, who first introduced me to computational number theory. In the last few years, he has taught me so much about solving research problems. The time, patience and commitment provided by Hugh are greatly appreciated. Not only did Hugh educate me within the scope of an advisor, he has also taught me to be a better person over the years, and I am very grateful for his valuable lessons. Through his NSERC operating grant, he financially supported me to attend a number of conferences and hired me as his research assistant on several occasions. Although it is not possible to express my deepest gratitude in words, I wish to thank him for everything he has done for me.

I would like to thank the members of the examining committee, Dr. Thomas Berry, Dr. Janet Hoskins, and Dr. Richard Mollin for expanding the large amount of time needed to read this thesis and for their valuable comments. I would also like to thank Dr. Daniel Shanks who suggested the problem discussed in Chapters 4 and 5, and kindly provided me with the unpublished manuscript version of his CUFFQI algorithm. His continued interest and encouragement are gratefully acknowledged. Furthermore, I was assisted by a number of individuals during the development of this thesis. Although it is not possible to name all of them, their efforts are deeply appreciated. In particular, I would like to thank Renate Scheidler, Dr. Allan Stephens, and Wendy White for their valuable assistance. I am also grateful to Dr. Daniel Mayer for pointing out an error in Chapter 2 and for providing me with several of his unpublished manuscripts.

Also, my doctoral studies were financially assisted by the Faculty of Graduate Studies of the University of Manitoba through a graduate fellowship.

The work required in the preparation of this thesis could not have been done without the support of my family. I would especially like to thank my parents, who provided me with encouragement from the beginning of my doctoral studies. The financial support from my parents and my brother, Alex, was of very great assistance on many

occasions. Finally, I would like to thank my other half, Theresa, who provided me with encouragement and support during the final stage of my doctoral program.

Table of Contents

Chapter 1.
An Introduction to Computing in Complex Cubic Fields

§1.1 Introduction.

Let $f(x) \in \mathbf{Z}[x]$ be any polynomial of degree n (≥ 2), which is irreducible over the rationals $\mathbf{Q}$. If ρ is any fixed zero of $f(x)$, denote by $\mathbf{K} = \mathbf{Q}(\rho)$ the algebraic number field of degree n formed by adjoining ρ to $\mathbf{Q}$. Let $f(x)$ have s real zeros $\rho_1, \rho_2, \rho_3, \cdots, \rho_s$ and $2t$ complex zeros $\rho_{s+1}, \bar{\rho}_{s+1}, \rho_{s+2}, \bar{\rho}_{s+2}, \cdots, \rho_{s+t}, \bar{\rho}_{s+t}$, where this ordering of the $n = s+2t$ is fixed. If $n = 2$, then the algebraic number field is either a real quadratic field or a complex quadratic field depending on the values of s and t. Also, if $n = 3$, we can only have the two cases of $t = 3$, $s = 0$ or $t = s = 1$. In the first case we say that the corresponding field is totally real; in the second case we say that the corresponding field is complex. Thus, if δ is the real zero of

$$f(a,b,c;x) = x^3 - ax^2 + bx - c\,,$$

an irreducible cubic polynomial with rational coefficients a, b, c and $s = t = 1$, then $\mathbf{Q}(\delta)$ is the complex cubic field formed by adjoining δ to the rationals. Furthermore, we say that $f(x;a,b,c)$ is a generating polynomial of $\mathbf{Q}(\delta)$. In the case when $a = b = 0$, we call $\mathbf{Q}(\delta)$ ($\delta = \sqrt[3]{c}$) a pure cubic field.

The purpose of this thesis is to develop efficient computational algorithms to solve certain problems which arise in the study of complex cubic fields. In this chapter, we give a brief description of the background material required for this thesis. In §1.2, we give a brief description on the topic of algebraic number theory. Since we make extensive use of Voronoi's algorithm in this thesis, we provide a short sketch of this algorithm in §1.3. We further note that most of the problems we deal with here involve the determination of ideal bases, the fundamental unit, and the class number of a complex cubic field. Thus, it is of

importance to discuss some previous developments on these topics here. Finally, a brief summary of this thesis is provided in §1.5.

§1.2 Definitions.

In this section we summarize many well-known properties concerning algebraic number fields. Most of these can be found in any standard text such as Stewart and Tall [ST79], Hua [Hua82] (also, see [Wil85]). If we define n mappings σ_i (i=1, 2, ⋯, n) of **K** into the set of complex numbers by $\sigma_i(\rho) = \rho_i$, $\sigma_i(\alpha+\beta) = \sigma_i(\alpha) + \sigma_i(\beta)$, and $\sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta)$, for any $\alpha, \beta \in \mathbf{K}$, then $\sigma_j(\rho) = \rho$, for some j, and the n-1 conjugates of $\alpha \in \mathbf{K}$ are given by $\sigma_i(\alpha)$, where $1 \le i \le n$, but $i \ne j$. In the case of n = 2 or 3, we use $\tilde{\alpha}$ or α', α'' respectively to denote the conjugates of α. We denote the trace of $\alpha \in \mathbf{K}$ to be

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

We also denote the norm of $\alpha \in \mathbf{K}$ to be

$$\mathrm{N}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

If $\alpha_i \in \mathbf{K}$ (i = 1, 2, 3, ⋯, k) are rationally independent, denote by $[\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k]$ the set $\{\sum_{i=1}^{k} x_i\alpha_i \mid x_i \in \mathbf{Z}\}$. If $GL_k(\mathbf{Z})$ is the group of all k × k matrices with entries from **Z** and determinant ±1, then $[\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k] = [\beta_1, \beta_2, \beta_3, \cdots, \beta_k]$ if and only if

(1.2.1) $$A = MB,$$

where A is the vector $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k)$, B = $(\beta_1, \beta_2, \beta_3, \cdots, \beta_k)$ and $M \in GL_k(\mathbf{Z})$. We will require the following result (see [Hua82] p.376).

Theorem 1.2.1. Let a be the gcd(a_{11}, a_{12}, a_{13}, ⋯, a_{1k}), where $a_{1j} \in \mathbf{Z}$ (j = 1, 2, ⋯, k). There is a matrix $M \in GL_k(\mathbf{Z})$ whose first row is made up of the entries a_{11}/a, a_{12}/a, a_{13}/a, ⋯, a_{1k}/a. ■

Let $\mathbf{O}_K$ be the ring of algebraic integers in **K**. There exist $\omega_1, \omega_2, \cdots, \omega_n \in \mathbf{O}_K$ such that $\mathbf{O}_K = [\omega_1, \omega_2, \cdots, \omega_n]$ and the set $\{\omega_1, \omega_2, \cdots, \omega_n\}$ is called a <u>basis</u> or <u>**Z**-basis</u> of $\mathbf{O}_K$. By virtue of Theorem 1.2.1 and (1.2.1) we may assume that there exists a basis of $\mathbf{O}_K$, where $\omega_1 = 1$. If we put $\gamma_{ij} = \sigma_i(\alpha_j)$ and define $\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n] = (\det(\gamma_{ij})_{n\times n})^2$, then the <u>discriminant</u> D of **K** is defined to be $\Delta[\omega_1, \omega_2, \cdots, \omega_n]$. Also, if α and α^{-1} are both in $\mathbf{O}_K$, then we call α a <u>unit</u> of **K**. In fact, a necessary and sufficient condition for an algebraic integer α to be a unit is that $N(\alpha) = \pm 1$. By the well-known theorem of Dedekind we know that the non-torsion part of the group of units of $\mathbf{O}_K$ has s + t - 1 generators, known as the <u>fundamental units</u> of $\mathbf{O}_K$. If $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s+t-1}$ is a system of fundamental units of $\mathbf{O}_K$, we define the <u>regulator</u> R of $\mathbf{O}_K$ to be $|\det(\log|\sigma_i(\varepsilon_j)|)|$. In the case of s+t-1=1, we use ε_0 (> 1) to denote the fundamental unit of $\mathbf{O}_K$ and $R = \log\varepsilon_0$.

Since $\mathbf{O}_K$ is a commutative ring, a subset **a** of $\mathbf{O}_K$ is an (integral) <u>ideal</u> of $\mathbf{O}_K$ if for any $\alpha, \beta \in \mathbf{a}$ we must have $\alpha + \beta \in \mathbf{a}$ and $\alpha\zeta \in \mathbf{a}$ for any $\zeta \in \mathbf{O}_K$. If $\beta_1, \beta_2, \cdots, \beta_m \in \mathbf{O}_K$ we denote by $(\beta_1, \beta_2, \cdots, \beta_m)$ the set $\{\sum_{i=1}^{m}\xi_i\beta_i \mid \xi_i \in \mathbf{O}_K\}$; we see that this set is an ideal of $\mathbf{O}_K$ and we say that $\beta_1, \beta_2, \cdots, \beta_m$ are <u>generators</u> of this ideal. Furthermore, if **a** is any ideal of $\mathbf{O}_K$, then $\mathbf{a} = (\beta_1, \beta_2, \cdots, \beta_m)$ for some $\beta_i \in \mathbf{O}_K$ (i = 1, 2, 3, ⋯, m) and m is finite. We also have the following

Theorem 1.2.2. If **a** is any ideal of $\mathbf{O}_K$, then there exist $\alpha_i \in \mathbf{O}_K$ (i = 1, 2, 3, ⋯, n) such that

$$\alpha_1 = a_{11}\omega_1$$

$$\alpha_2 = a_{21}\omega_1 + a_{22}\omega_2$$

$$\cdots\cdots\cdots\cdots$$

$$\alpha_n = a_{n1}\omega_1 + a_{n2}\omega_2 + \cdots + a_{nn}\omega_n,$$

where $a_{ij} \in \mathbf{Z}$, $a_{ii} > 0$ (i = 1, 2, 3, ⋯, n; j = 1, 2, ⋯, n) and

$$\mathbf{a} = [\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n]. \quad \blacksquare$$

Also, there exist $\beta_1, \beta_2, \beta_3, \cdots, \beta_n \in \mathbf{O}_K$ such that

$$\mathbf{a} = \left\{ \sum_{i=1}^{n} x_i \beta_i \mid x_i \in \mathbf{Z} \ (i = 1, 2, 3, \cdots, n) \right\}.$$

This set $\{\beta_1, \beta_2, \beta_3, \cdots, \beta_n\}$ is said to be a basis or **Z**-basis of **a**.

An ideal $\mathbf{a} = (\alpha)$, which is generated by the single generator α, is called a principal ideal. The ideal $(1) = \mathbf{O_K}$ is called the unit ideal. If $\mathbf{a} = [\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k]$ and $\mathbf{b} = [\beta_1, \beta_2, \beta_3, \cdots, \beta_m]$, we define the product **ab** to be that ideal generated by the km generators $\alpha_i\beta_j$ $(i = 1, 2, \cdots, k; j = 1, 2, \cdots, m)$. If **a** and **b** are two ideals of $\mathbf{O_K}$ and there exist non-zero $\alpha, \beta \in \mathbf{O_K}$ such that $(\alpha)\mathbf{a} = (\beta)\mathbf{b}$, then **a** and **b** are said to be equivalent and we write this as $\mathbf{a} \sim \mathbf{b}$. This is a true equivalence relation which partitions the set of ideals $\mathbf{O_K}$ into a finite number h (the class number) of distinct equivalence classes. If we denote these classes by $C_1, C_2, \cdots, C_h$ and define C_iC_j to be the class $\{ \mathbf{ab} \mid \mathbf{a} \in C_i, \mathbf{b} \in C_j\}$, then under this operation these equivalence classes form a group G called the class group of **K**. The identity of this group is the class of principal ideals. We also note that if $\mathbf{a} = [\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n]$ is an ideal of $\mathbf{O_K}$ and $\lambda A = \mu B$, where $\lambda, \mu \in \mathbf{O_K}$, $A = (\alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n)$, $B = (\beta_1, \beta_2, \beta_3, \cdots, \beta_m)$, then $\mathbf{b} = [\beta_1, \beta_2, \beta_3, \cdots, \beta_n]$ is an ideal and $\mathbf{a} \sim \mathbf{b}$.

We say that the ideal **a** divides the ideal **b** $(\mathbf{a} \mid \mathbf{b})$ if there exists an ideal **c** such that $\mathbf{b} = \mathbf{ac}$. It can be shown that $\mathbf{a} \mid \mathbf{b}$ if and only if $\mathbf{a} \supseteq \mathbf{b}$. If $\mathbf{a} \mid (\alpha)$, then we say that **a** divides α $(\mathbf{a}|\alpha)$. If $\mathbf{a} \mid \alpha - \beta$, when $\alpha, \beta \in \mathbf{O_K}$, then we say that α and β are congruent modulo **a** $(\alpha \equiv \beta \pmod{\mathbf{a}})$. If we denote by N(a) (the norm of **a**) the number of distinct residue classes modulo **a**, then

$$\Delta[\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n] = N(\mathbf{a})^2 D,$$

where $\mathbf{a} = [\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n]$. Also, if $\mathbf{a} = (\alpha)$, then $N(\mathbf{a}) = |N(\alpha)|$. Furthermore, $N(\mathbf{ab}) = N(\mathbf{a})N(\mathbf{b})$. Throughout this thesis, we will assume that the ideals we are considering are not the zero ideal (0).

It is an easy matter to see that we can always embed 1 into a **Z**-basis for $\mathbf{O_K}$. If $\omega_1 = 1$, we see from Theorem 1.2.2 that $\mathbf{a} = [a_{11}, \alpha_2, \alpha_3, \cdots, \alpha_n]$, where $a_{11} \in \mathbf{Z}$.

This value of a_{11} is unique for **a** and is the least positive rational integer in **a**. We denote it by L(**a**).

We say that, **a** is a primitive ideal if it has no rational integer divisors except 1. In other words, if (e) | **a**, where $e \in \mathbf{Z}$, then e must be ±1 if **a** is primitive. A reduced ideal is a primitive ideal **a** such that there does not exist any non-zero $\alpha \in \mathbf{a}$ that satisfies $|\sigma_i(\alpha)| < L(\mathbf{a})$ for i = 1, 2, ···, n. There are only a finite number of reduced ideals of O_K.

§1.3 Voronoi's algorithm.

In this section we briefly describe Voronoi's algorithm for determining the minima in a cubic lattice. For more details the reader is referred to Voronoi[Vor96], Delone and Faddeev [DF64], Williams, Cormack and Seah [WCS80] or Williams and Dueck [WD84].

Let **F** be a cubic field of negative discriminant. In order to find the fundamental unit of **F**, Voronoi's Continued Fraction algorithm is often used. This algorithm, which is particularly suited to the problem of finding the fundamental unit in a complex cubic field, is an extension of the Regular Continued Fraction algorithm, as used in real quadratic fields, to the case of cubic fields. It should be noted that Voronoi gave algorithms for application both in the complex cubic case and in the totally real case; however, we will focus our attention here on the complex cubic case only. Our discussion will be based on the description of the algorithm given in [DF64] (pp. 273-304).

If $\alpha \in \mathbf{F}$ and its congugates are α' and α'', define the point $A \in \mathbf{R}^3$ corresponding to α by

$$A = (\alpha, \eta_\alpha, \zeta_\alpha),$$

where $\eta_\alpha = (\alpha' - \alpha'') / 2i$, $\zeta_\alpha = (\alpha' + \alpha'') / 2$, $i^2 = -1$. Note that

$$\alpha'\alpha'' = |\alpha'|^2 = |\alpha''|^2 = \eta_\alpha^2 + \zeta_\alpha^2.$$

If $\lambda, \mu, \nu \in \mathbf{F}$ and λ, μ, ν are rationally independent, we define the lattice L ($\mathbf{R}^3 \supseteq L$) of **F** with basis $\{\lambda, \mu, \nu\}$ by

$$L = \{ a\lambda + b\mu + c\nu \mid a, b, c \in \mathbf{Z}\}.$$

When $\alpha \in \mathbf{F}$ and $A \in L$, for the sake of brevity we will often use the notation $\alpha \in L$ to denote that it is really the corresponding point A that is in L. We also use αL to denote the lattice with basis $\{\alpha\lambda, \alpha\mu, \alpha\nu\}$. If A (or α) is any point of L , we define the norm body NB(A) of A to be

$$NB(A) = NB(\alpha) = \{(x, y, z) \mid x, y, z \in \mathbf{R};\ |x| < \alpha;\ y^2 + z^2 \leq |\alpha'|^2\}.$$

Here, if $|\alpha'| = |\beta'|$ ($\alpha, \beta \in \mathbf{F}$), we must have $\alpha = \pm\beta$ (see p.274 of [DF64].). We say that ϕ ($\neq 0$) is a (relative) minimum of L if $NB(\phi) \cap L = \{(0, 0, 0)\}$. If ϕ and ψ are minima of L such that

$$0 < \phi < \psi,\ \ \phi'\phi'' > \psi'\psi''$$

and there does not exist a $\omega \in L$ such that $\phi < \omega < \psi$ and $\omega'\omega'' < \phi'\phi''$, we call ϕ the minimum of the first kind adjacent to ψ; and we call ψ the minimum of the second kind adjacent to ϕ.

Since the term "puncture" is mentioned in the subsequent chapters, we define the puncture of any $\Omega \in L$ to be a point $\omega = (\xi_\alpha, \eta_\alpha)$ in the x-y plane of $\mathbf{R}^3$, where

$$\xi_\Omega = (2\Omega - \Omega' - \Omega'') / 2,\ \ \eta_\Omega = (\Omega' - \Omega'') / 2i.$$

Consider now the sequence

(1.3.1) $$\theta_1, \theta_2, \theta_3, \cdots, \theta_n, \cdots,$$

where θ_1 is a minimum of L and θ_{i+1} is the minimum of the first kind adjacent to θ_i for $i = 1, 2, 3, \cdots$. We call such a sequence a chain of minima of the first kind. If θ_{i+1} is the minimum of the second kind adjacent to θ_i for $i = 1, 2, 3, \cdots$, we call (1.3.1) a chain of minima of the second kind. By Minkowski's theorem (see [DF64]) it can be shown that there always exist such chains in L. Voronoi actually gave two algorithms, one for finding chains of minima of the first kind and one for finding chains of minima of the second kind. However, he provided a detailed proof for the first of the two algorithms only. In this thesis we will confine our attention to a method for obtaining a chain of minima of the second kind for L.

It should be emphasized here that Voronoi's algorithm produces all the minima of L. For example, if μ is a minimum of L and $\mu > \theta_1$, then $\mu = \theta_n$ for some n in a chain of the second kind. Let $\mathbf{O_K} = [1, \omega_1, \omega_2]$ and let L be the lattice over **F** with basis $\{1, \omega_1, \omega_2\}$. Since $|N(\alpha)| \geq 1$ for all nonzero $\alpha \in \mathbf{O_K}$ ($N(\alpha) \in \mathbf{Z}$), we see that 1 must be a minimum of L. By using Voronoi's algorithm, we can find

$$\theta_1 = 1, \theta_2, \theta_3, \cdots, \theta_n, \cdots,$$

a chain of relative minima of the second kind for L. Since $\varepsilon_0 \in \mathbf{O_K}$ we must have $\varepsilon_0 \in L$ and since $N(\varepsilon_0) = \varepsilon_0\varepsilon_0'\varepsilon_0'' = \varepsilon_0|\varepsilon_0'|^2 = 1$, ε_0 must be a minimum of L; thus, at some point, we must find a minimal k (> 1) such that $N(\theta_k) = 1$. In this case we have

$$\varepsilon_0 = \theta_k$$

and

$$R = \log\theta_k.$$

We also point out that for a given ideal **a**, Voronoi's algorithm can be used to find all the reduced ideals which belong to the same ideal class as **a**. For a given reduced ideal $\mathbf{a}_1$, we can use Voronoi's algorithm to produce a sequence of equivalent reduced ideals

$$\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \cdots, \mathbf{a}_n, \cdots.$$

At some point we find $\mathbf{a}_1 = \mathbf{a}_i$ for some minimal i (i > 1). When this occurs we know that all the reduced ideals belonging to the same ideal class as $\mathbf{a}_1$ have been determined.

§1.4. Bibliographic Information.

In the course of conducting computational work in any algebraic number field, three important (and difficult) problems frequently have to be dealt with. These are: determination of ideals of $\mathbf{O_K}$ (usually in their **Z**-basis form), computation of a set of fundamental units of **K** (or at the very least the regulator of **K**), and the evaluation of the class number (and possibly the class group structure) of **K**. For a discussion of these topics in the context of a general **K** the reader is referred to the book of Pohst and Zassenhaus [PZ89]. As it will be necessary for us to deal with these problems as they relate

to complex cubic fields, we will provide, in this section, a brief description of the progress which has been made on them. Further bibliographic information on the particular problems addressed by this thesis will be provided in the introductions to the variuos chapters. In this section we will first discuss the problem of determining the ideals of $\mathbf{O_F}$. After that, we will recount the previous developments on finding the fundamental unit and class number of a general complex cubic field. This will then be followed by a lengthy summary of the progress of determining the fundamental unit and class number of a pure cubic field, a subject on which there is a surprising amount of literature. Our approach to the discussion of each of these topics will be chronological.

The problem of determining the ideals of $\mathbf{O_F}$ can be divided into two sub-problems. The first is the factorization of rational primes into prime ideals of $\mathbf{O_F}$, and the second is the calculation of the $\mathbf{Z}$-bases of the ideals of $\mathbf{O_F}$ with prime power norms. These two problems were completely solved by Voronoi. In his voluminous master's dissertation [Vor94] (also, see [DF64]), he worked out methods for determining the decomposition of the rational primes. He also determined $\mathbf{Z}$-bases not only for the prime ideals in any cubic field, but for products of certain prime ideal powers as well. From this information he was able to show how a $\mathbf{Z}$-bases for any ideal of $\mathbf{O_F}$ could be determined. Since the time of Voronoi, several papers have appeared which deal with the problem of determining how the rational primes factor into prime ideals of $\mathbf{O_F}$. In [Wah22], Wahlin gave a detailed table for the factorization of any rational prime in $\mathbf{O_F}$. This problem was further studied by Jaeger [Jae30], Hasse [Has30], Tornheim [Tor55], Arai [Ara81A] and [Ara81B]. Also, Martinet and Payan [MP67] dealt with this problem in a more general context. Finally, we mention that Llorente and Nart [LN83] presented a method which is very similar to the one given in [Wah22]. All these methods determine the factorization of a rational prime by making use of the generating polynomial of the cubic field. We note that there is a convenient table for practical use given in [LN83].

We now turn to a discussion of previous results on the problems of finding the fundamental unit and class number of a complex cubic field. A theory of units in cubic fields was outlined by Hermite [Her50] to Jacobi in 1850. His principle was applied by Charve [Cha80] to the calculation of a unit for cubic number fields. Charve utilized ternary quadratic forms with a single continously varying parameter for the calculation of a unit of a cubic field with negative discriminant. As a result, he was able to develop a method for finding a complete system of reduced forms, which consequently produces a unit of the cubic field. However, by neglecting the principle of Hermite's idea, Charve's method does not necessarily find the fundamental unit.

In 1893 a table of fundamental units of $Q(\sqrt[3]{c})$ for $c \leq 23$ was included in an unpublished manuscript of Voronoi (see Vol. 3, p.252 of [Vor52]). In the following January, Voronoi completed the work "On a certain modification of the algorithm of Jacobi" (see Vol. 1, pp. 121-180 of [Vor52]). In this unpublished manuscript, he gave an algorithm for finding the fundamental unit of a complex cubic field. In fact, his research on finding the fundamental unit of a cubic field with negative discriminant was in a complete state at this time (see Vol. 1, p.282 of [Vor52]). However, he delayed publication of his results until 1896 when his doctoral dissertation [Vor96] appeared. In this remarkable work he presented algorithms for finding the fundamental unit(s) in both complex and totally real cubic fields. We should mention here that these ideas were recently extended to other algebraic number fields by Buchmann [Buc82] (also, see[Buc85A] and [Buc85B]). Furthermore, as mentioned earlier, Voronoi provided two methods for finding the fundamental unit ε_0 of a complex cubic field; one finds ε_0 (> 1) and the other one finds ε_0^{-1} (< 1).

To the best of our knowledge, the first table of units and class numbers for general cubic number fields was given in 1899 by Reid [Rei99]. He found 161 cubic number fields having positive or negative discriminant. For each field, he gave the class number, the discriminant, a basis, and the factorization of certain rational primes into their ideal factors.

Units were also given for most of the fields. However, the units found are not necessarily fundamental.

In 1913, Berwick [Ber13] developed, from geometric considerations, a process for deriving the expansion of a cubic irrationality, for the case of a generating equation having one real root, so that periodicity ensues in every case. For a complex cubic field $\mathbf{F}$, he showed that an ideal of $\mathbf{O_F}$ can be linked up with an equivalent ideal by a substitution derived from the coefficients of the expansion, and that every ideal is equivalent to one of a finite number of reduced ideals. He then went on to give a method for linking up all the equivalent reduced ideals in one closed cycle. Hence, this closed cycle produces the fundamental unit of $\mathbf{F}$. We further point out that Berwick's method is very similar to Voronoi's algorithm for finding the chain of the second kind; that is it computes ε_0.

We should also mention the method discussed by Arwin [Arw29]. He presented some results concerning equivalent ideals and the construction of units in cubic fields. He then went on to sketch a method for finding two independent units in a totally real cubic field.

By using Voronoi's algorithm, Delone and Latyseva (see p.303 of [DF64]) calculated a table of fundamental units for all complex cubic fields with discriminant no larger than 379 in absolute value.

In [WZ72], Williams and Zarnke presented two tables of machine calculated fundamental units for various complex cubic fields. Instead of finding all the complex cubic fields with discriminant less than a given bound, they found the fundamental unit for those complex cubic fields having the absolute value of the coefficients of the generating polynomial less than a given bound. In one table they used 10 as the upper bound, and 50 was used in the other table. The fundamental unit and generating polynomial for each of the complex cubic fields were provided in both tables. The fundamental units were found by using Voronoi's algorithm. They also gave a description of the algorithm of Voronoi, which is useful for the purpose of programming this algorithm on a computer. In the

following year, Angell [Ang73] used a computer to produce a table of all complex cubic fields with negative discriminant greater than -20000. For each of the 3169 complex cubic fields that he found, he gave the generating polynomial, fundamental unit, and the class number. Again, Angell made use of Voronoi's algorithm in his computations.

In 1985, Dueck and Williams [DW85] presented a fast (assuming the Generalized Riemann Hypothesis) algorithm for finding the class number and class group of a complex cubic field. This method extends to the complex cubic case the ideas of Lenstra [Len82] and Schoof [Sch83] in the real quadratic case. The algorithm was implemented and used to determine the class number and class group structure for all pure cubic fields $\mathbf{Q}(\sqrt[3]{c})$, with $2 \leq c \leq 30000$.

Another recent development in finding the fundamental unit of a complex cubic field is that of Brentjes [Bre81]. By using arguments from plane geometry, Brentjes developed a two-dimensional continued fraction algorithm. He further showed how this algorithm can be applied to solve the unit problem in complex cubic fields. Also, he gave a table of fundamental units for some miscellaneous complex cubic fields.

At this point, we have listed all the paper, known to us at the time of writing, on the topics of finding the fundamental unit and class number of a general complex cubic field. We should also point out that there are serveral general methods for finding units in algebraic number fields. For examples of these, see Billevich [Bil56], Buchmann [Buc86], [Buc87], Buchmann and Pethö [BP89], Pohst and Zassenhaus [PZ77], [PZ82], [PZ89], Pohst, Weiler and Zassenhaus [PWZ82], Steiner and Rudman [SR76], [RS78], and Steiner [Ste76]. For the remainder of this section, we will focus on the problems of determining the fundamental unit and class number in a pure cubic field.

Besides their application to Charve's method, Hermite's ideas were also implemented by Zolotarev [Zor69] in 1869. Indeed, Zolotarev was the first to develop Hermite's suggestion in the case of a pure cubic field. In his little known master's thesis "On an indeterminate equation of the third degree" published in Russian in 1869, he

developed a method for finding the fundamental unit of a pure cubic field. His idea is based on the study of successive minima of a certain positive ternary form containing a continuously varying parameter. Although Zolotarev's method is remarkable, it requires further supplements in order to find all the successive minima. Because of the need to include these supplements in his method, the practical value of Zolotarev's method is reduced significantly.

In 1890, Mathews [Mat90] found a solution of the diophantine equation

$$F_c(x,y,z) = x^3 + cy^3 + c^2z^3 - 3cxyz = 1$$

for c = 2, 3, 4, 5, 7, 11. As

$$N(x+ \alpha y + \alpha^2 z) = F_c(x,y,z)$$

where $\alpha^3 = c$, this solution yields a unit of $\mathbf{Q}(\sqrt[3]{c})$ for c = 2, 3, 4, 5, 7, 11. However, Mathews was unable to show that these units are fundamental (in fact they are fundamental). In the following year, Meissel [Mei91] derived a new method for solving $F_c(x,y,z) = 1$. By using this method, he found solutions for all cube-free values of c where $c < 82$. Also, he admitted the uncertainly of his method for finding a solution which is fundamental. Although he illustrated the use of congruences in determining whether or not a given solution is fundamental, he was not able to show that all of his solutions were so.

In connection with his theoretical investigation of pure cubic fields, Markoff [Mar92] gave several units and a few class numbers for some pure cubic fields. He gave a table of units of $\mathbf{Q}(\sqrt[3]{c})$ for $2 \le c \le 70$. With the exception of those given for c = 28 and 55, the other units are fundamental. In 1900, Dedekind [Ded00] described a method for determining the class number of a pure cubic field $\mathbf{Q}(\sqrt[3]{c})$. He found some more values of the class number by using Markoff's table and incidentally proved certain of the units found by Markoff to be fundamental units.

With the exception of Voronoi and Berwick's methods, most of the other methods do not necessarily provide a fundamental unit. Instead, most of the existing methods tend to find a unit and then determine whether or not that unit is fundamental. General criteria

for a unit to be fundamental were developed by Nagell [Nag23]. In his paper [Nag23], he gave a list of units of $Q(\sqrt[3]{c})$, most of which are fundamental. Unfortunately, there are a few errors in his table; these occur when c = 41, 55, 180, 182. In the same year, Wolfe [Wol23] provided the minimum positive solutions of the equation $F_c(x,y,z) = 1$ for $c < 100$ which, in the case of c square-free and $c \not\equiv \pm 1 \pmod 9$, yields the fundamental unit for $Q(\sqrt[3]{c})$. There are several errors in his table, namely in the following cases: c = 72, 82, 85, 96, 97.

In 1928 Pocklington [Poc28] gave a method for finding units of $Q(\sqrt[3]{c})$ which he claimed to be practical and convenient. In his paper, little attention was given to the theoretical aspects of his method. He presented a table, containing the fundamental unit and its reciprocal of $Q(\sqrt[3]{c})$ for $c \leq 33$. Although he successfully calculated these fundamental units by using his method, he was unable to prove that his method always produces the fundamental unit. The basic idea of his method is similar to that of the algorithm of Voronoi. Besides Pocklington's paper, another method for finding a unit of a pure cubic field was also introduced at about this time. This is the method of Pierce [Pie26]. His technique makes use of approximations to the real zero of the generating equation in the determination of units in pure cubic fields. Unfortunately, this method does not necessarily produce the fundamental unit.

In [Usp31], Uspensky gave a method for finding units in pure cubic fields. He retained the basic principle of Zolotarev's method, but departed from Hermite's requirement to consider minima of a variable ternary form. According to the author, the main feature of his method is that it can be applied to numerical examples with comparative ease. However, his method does not necessarily find the fundamental unit. He pointed out, though, that if the unit found is not fundamental, then the fundamental unit can easily be obtained.

A complete and error-free table of the class number and fundamental unit of $Q(\sqrt[3]{c})$ for $c \leq 50$ was given by Cassels [Cas50]. Although Cassels did not show that all his units

are fundamental, Selmer [Sel55] later verified that the units are indeed fundamental. Furthermore, Selmer [Sel55] provided a table of class numbers and fundamental units of $Q(\sqrt[3]{c})$ for all $c \leq 100$. Later he [Sel] extended this table to $c \leq 250$.

It seems that Cohn [Coh57] was the first researcher who used a computer to find the class number of a pure cubic field. He implemented Dedekind's method on a computer and obtained class numbers for some pure cubic fields for which he could easily determine the regulator.

After computers became widely available, it became possible to do much more work in this area of research. In [Wad70], Wada used the computer TOSBAC-3300 to compute a table of fundamental unit of $Q(\sqrt[3]{c})$ for $2 \leq c \leq 250$. In the same year, Sved [Sve70] used the algorithm of Szekeres [Sze70] to calculate units of $Q(\sqrt[3]{c})$ for $2 \leq c \leq 199$. She did not stop after finding one unit, but tried to obtain more. Her reason was that if all units are powers of the first one that she found, then it would be reasonable to suppose the first one to be fundamental. Some of the big units found by Sved were later checked by te Riele (see [Bre81]), and they were proved to be fundamental. On the other hand, there is no mathematical certainly that the Szekeres algorithm will always produce the fundamental unit.

In 1971, Beach, Williams and Zarnke [BWZ71] computed a table of the fundamental units and class numbers for all $Q(\sqrt[3]{c})$ $(1 \leq c \leq 998)$. We also mention that they used Voronoi's algorithm for determining the fundamental unit and Dedekind's formula [Ded00] for calculating the class number, an idea which they got from [Coh57].

In [BWB76], Barrucand, Williams and Baniuk gave two different computational techniques for determining the class number of a pure cubic field. The first technique made use of a transformation of the Dirichlet series, and the second made use of the Euler product to estimate the Artin L-function at 1. This second technique is similar to the method used in [Sha74]. Both techniques are much faster than the computational technique of [Coh57] and [BWZ71]. They were implemented on an IBM computer, and the class

number for each pure cubic field $Q(\sqrt[3]{c})$ for $c \leq 9999$ was obtained. The authors noted that the second method appears to be faster than the first. However, the second method is not mathematically rigorous. In [Wil76], Williams used the Euler product method to determine the class number of each of the pure cubic fields $Q(\sqrt[3]{q})$, where q ($\equiv$ -1 (mod 3)) is a prime and $q < 35100$. He also examined the stability of the percentage of these fields having class-number one.

In [JH78], Jeans and Hendy presented a method for determining whether or not a known unit of a pure cubic field is fundamental. The main feature of this method is that if the unit tested is not fundamental, then the method can be used to produce the fundamental unit. Jeans and Hendy used this method to prove that Sved's units for c = 167, 177 are fundamental.

In 1978, Eisenbeis, Frey and Ommerborn [EFO78] used a modification of an algorithm of Birch and Swinnerton-Dyer to develop a technique for computing the 2-rank of the class group of $Q(\sqrt[3]{c})$. Using this method and the class number table of [BWB76], the 2-rank of the class group of $Q(\sqrt[3]{c})$ was computed for $c < 10000$. They noticed that for those fields $Q(\sqrt[3]{c})$ such that $c \equiv 8 \pmod 9$ the percentage having class number one was surprisingly high (about 60%). In order to test this further, Williams and Shanks [WS79] used an improved version of the Euler product method, as described in [BWB76], to determine all those pure cubic fields $Q(\sqrt[3]{c})$ having $c \equiv 8 \pmod 9$, $c < 2\text{x}10^5$ and h = 1. They also suggested a few interesting ideas for improving their algorithm. We should also mention that these computations were extended to values of $c < 10^6$ by Tennenhouse and Williams in [TW86]. These computations added further confirmation of the phenomenon noticed in [EFO78].

At an AMS meeting held in San Fransisco, Atkin [Atk81] discussed a new technique for finding a unit of $Q(\sqrt[3]{c})$. Atkin's method, which is reminiscent of that used in the real quadratic case by Pohst and Zassenhaus [PZ76], is almost entirely distinct from Voronoi's algorithm. His method is to factorize algebraic integers of small norm, and use

the Chinese remainder theorem to find the positive fundamental unit less than unity. He also suggested that his method appears to be faster than Voronoi's algorithm. However, its main weakness is its dependence on some luck in order to obtain the fundamental unit. Indeed, he admitted that his method did not produce the fundamental unit in a few instances.

Although it cannot be proved at this time, the coefficients of the fundamental unit for a complex cubic field tend to increase exponentially as the absolute value of the discriminant increases. In order to avoid the large amount of precision required for the computation of the fundamental unit, it is now customary to compute the regulator of a complex cubic field instead, when the absolute value of the discriminant is large. In [WCS80], Williams, Cormack and Seah gave a modified version of Voronoi's algorithm for obtaining the regulator of a pure cubic field $\mathbf{Q}(\sqrt[3]{c})$. This new algorithm has the advantage of executing relatively rapidly for large values of c. It also eliminates a computational problem which occurs in almost all algorithms for finding units in algebraic number fields: this is the problem of performing calculations involving algebraic irrationals by using only approximations of these numbers. A table of regulators and class numbers of $\mathbf{Q}(\sqrt[3]{c})$, where $c \leq 10^5$, and the class number of $\mathbf{Q}(\sqrt[3]{c})$ is not divisible by 3, was computed. This method was subsequently improved by Williams [Wil80] for certain pure cubic fields.

In [Sha72], Shanks discussed a technique for finding the regulator of a real quadratic field rapidly when the discriminant is large. His idea allows one to improve the speed of the continued fraction scheme by allowing one to proceed almost directly from the n^{th} step to the m^{th} step in the continued fraction, where m is approximately equal to 2n. A few years later, Lenstra [Len82] and Schoof [Sch83] presented another version of the ideas in [Sha72]. Both Shanks (see [Sha76] and [WS79]) and Lenstra (in [Len82]) pointed out that it should be possible to extend Shanks' ideas to the cubic case. In [WDS83], Williams, Dueck and Schmid showed how Shanks' idea could be extended to Voronoi's algorithm.

They also discussed at length an algorithm for finding the regulator and class number for pure cubic fields $Q(\sqrt[3]{c})$. Unfortunately, there is a major deficiency of the algorithm. The problem is that there is no mathematically rigorous proof to show that the value of h, the class number, produced by the algorithm is correct. On the other hand, the authors suggested that if h is small, then their method is very likely to find h correctly. In spite of the slight lack of confidence in h, however, the regulator found by the algorithm is correct. Assuming a Generalized Riemann Hypothesis, it was shown that the new algorithm can find the regulator and class number correctly in $O(c^{2/5+\varepsilon})$ operations. Consequently, when h is small, the new algorithm is a significant improvement over Voronoi's $O(c^{1+\varepsilon}/h)$ algorithm for finding R.

In [WD84], Williams and Dueck used an analogue of the nearest integer continued fraction algorithm to determine the regulator of a pure cubic field. This method can be used to find the regulator in about 75 percent of the time needed by Voronoi's continued fraction algorithm. They implemented the method and determined the regulator of $Q(\sqrt[3]{c})$ for $c \leq 91000$.

Recently, Nakamula [Nak88] presented a table of fundamental units and class numbers for all the pure cubic fields having discriminant between -300 and -270000. The method used by Nakamula is based on [Nak81] and [Nak82]. For a pure cubic field **F** with discriminant D, we define the elliptic unit to be ε_0^h, where ε_0 is the fundamental unit of **F** and h is the class number of **F**. The method utilizes the elliptic unit for the simultaneous determination of the fundamental unit and class number of **F**. The significance of the method is that no calculation in **F** is needed. Indeed, this method is completely different from Voronoi's algorithm. In fact, it computes the fundamental unit and class number by performing some arithmetic in an imaginary quadratic field $Q(\sqrt{D})$ and approximating the value of the Dedekind eta function.

Before we leave the topic of finding the fundamental unit of a pure cubic field, we should mention some other algorithms for finding units or the fundamental unit in $Q(\sqrt[3]{c})$.

The major weakness of these methods is that they are only suitable for certain pure cubic fields; thus, little emphasis is placed on these techniques here. One such technique utilizes the Jacobi-Perron algorithm on which there is a lengthy literature. As an example, we mention the paper of Bernstein [Ber74]. The Jacobi-Perron algorithm is periodic (and therefore useful in computing units) for certain values of c only. For most other c values, the Jacobi-Perron algorithm does not seem to be periodic. Thus, this method appears to be of limited utility. We should also remark that the fundamental unit of some pure cubic fields can be found by using the method given by Stender [Ste69]. The basic idea behind this method is some inequalities given by Nagell [Nag23]. However, it is also only suitable for pure cubic fields $Q(\sqrt[3]{c})$ in which c has a certain parametric form. Later, Rudman [Rud73] extended Stender's results. Finally, Williams [Wil76] extended Rudman's results by developing a method for finding the fundamental unit of certain pure cubic fields explicitly in terms of solutions to the Diophantine equations $x^2 - 3y^2 = -2$ and $t^2 - 3u^2 = 1$.

§1.5 Summary.

Terms used here, which have not yet been defined, are discussed in the introduction to the relevant chapter. In Chapter two, we present an algorithm which can produce all the non-isomorphic complex cubic fields with discriminant less than a given bound. This algorithm is implemented and used to find all the distinct complex cubic fields with discriminant $D > -10^6$. In the following chapter we discuss three different methods for finding the class number of a complex cubic field. The class number is computed for each of the fields generated from the previous chapter. Also, the regulator and class group structure are determined for each of these fields.

In Chapters 4 and 5, we describe a different method for finding all the non-isomorphic complex cubic field for a given large fundamental discriminant. This method is an automated version of the CUFFQI algorithm of Shanks. Chapter 4 deals with the

theoretical aspects of the CUFFQI algorithm. The computational aspects of CUFFQI, including a detailed description of the algorithm, are discussed in Chapter 5.

In Chapter 6, we give a fast computational technique for finding the regulator of a pure cubic field. This technique is a modified version of the method given in [WDS83]. This method was implemented and tested on some pure cubic fields with large regulators. In Chapter 7, we present a method of finding cubic polynomials of the form $x^3 + c$ ($c \in \mathbf{Z}$) which have a high asymptotic density of prime values.

In Chapter 8, we describe a new computational technique for finding the principal factors for a pure cubic field. This algorithm was implemented and applied to some pure cubic fields with large discriminant.

Chapter 2.
Construction of Complex Cubic Fields.

§2.1 Introduction.

In the last 10 years, there has been a series of new developments in the construction of totally-real cubic fields. Llorente and Oneto [LO82] first produced a complete table of totally-real cubic fields with discriminant $D < 10^5$. By using a different method, Ennola and Turunen [ET85] computed a table with discriminant $D < 5 \times 10^5$. Recently, with an improved version of the method developed in [LO82], Llorente and Quer [LQ88A] produced a table with discriminant $D < 10^7$. However, since the work of Angell [Ang73] little work seems to have been done on the tabulation of complex cubic fields. In this chapter, we will describe an algorithm which was used to produce all the non-isomorphic complex cubic fields with discriminant $D > -10^6$. This method is a modification of the method used in [LQ88A]. We further point out that the previously mentioned table of Angell (see also Shanks [Sha75]) only dealt with fields with discriminant $D > -20000$.

§2.2 Definitions.

Any cubic field **F** can be generated by the zero of an irreducible (over the rationals **Q**) polynomial

$$f(a,b,c;x) = x^3 - ax^2 + bx - c, \tag{2.2.1}$$

where $a,b,c \in \mathbf{Z}$. The discriminant of the polynomial $f(a,b,c;x)$ is given by

$$D(a,b,c) = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2. \tag{2.2.2}$$

Further, the discriminant D of the field **F** is given by

$$D(a,b,c) = DI^2, \tag{2.2.3}$$

where $I = I(a,b,c)$ is the index of the polynomial $f(a,b,c;x)$. We further point out that a field generated by the polynomial $f(a,b,c;x)$ is also generated by the polynomial

$$f(a',b';x) = x^3 - a'x + b', \tag{2.2.4}$$

where

$$a' = 3a^2 - 9b,$$

$$b' = 9ab - 2a^3 - 27c.$$

The discriminant D(a',b') of this polynomial is given by

$$D(a',b') = 4a'^3 - 27b'^2 = DI'^2 = D(27I)^2$$

for I given by (2.2.3).

For every prime $p \in \mathbf{Z}$ and integer m, $v_p(m)$ denotes the greatest integer k such that p^k divides m. If there exists a prime p such that $v_p(a') \geq 2$ and $v_p(b') \geq 3$, then we replace the coefficients a' by a'/p^2 and b' by b'/p^3. These replacements do not change the field **F** generated by f(a',b';x) but they reduce the size of the index of the polynomial f(a',b';x).

It should also be mentioned (see [LQ88A]) that

(2.2.5) $$D = dT^2,$$

where d is the fundamental discriminant of the quadratic field $Q(\sqrt{D})$,

(2.2.6) $$T = 3^m T_0 \quad (0 \leq m \leq 2),$$

and T_0 is a square free integer such that $GCD(T_0,3d) = 1$.

§2.3 Bounds on the coefficients and the index of the polynomial f(a,b,c;x).

The basis of our construction of the complex cubic fields is the following Theorem of Angell [Ang73] (misprint corrected).

Theorem 2.3.1. Let **F** be a cubic number field with discriminant $D < 0$. There is at least one polynomial which generates **F** such that if the zeros of the polynomial are $\alpha, \beta \pm i\gamma$ (α, β and γ are real numbers), then $0 < \alpha < 1$, $\beta > 0$ and

$$S = S(\alpha,\beta,\gamma) = (\alpha-\beta)^2 + 3\gamma^2 \leq \sqrt{|D|}. \blacksquare$$

Since a,b,c are given by

$$a = \alpha + 2\beta,\ b = 2\alpha\beta + \beta^2 + \gamma^2,\ c = \alpha(\beta^2 + \gamma^2),$$

we deduce the following Lemma from Theorem 2.3.1, (2.2.2) and (2.2.3).

Lemma 2.3.1. Let **F** be any cubic field with discriminant $D < 0$. Then **F** is generated by some polynomial $f(a,b,c;x)$ such that $a,b,c \in \mathbf{Z}$,

$$0 < a < 3 + 2|D|^{1/4},\ 0 < b < (a^2 + \sqrt{|D|}) / 3,$$

and $$0 < c < (a^2 - 3 + 2\sqrt{|D|}) / 6.$$

Also, the index $I = I(a,b,c)$ must satisfy $3\sqrt{3}I < (124a^2 + 432a + 4\sqrt{|D|} + 729)^{1/2}$.

Proof. We know that

$$S > (\alpha - \beta)^2$$

and $\beta = (a - \alpha) / 2$; hence

$$S > (a-3\alpha)^2/4.$$

We know that $0 < \alpha < 1$ and $\sqrt{|D|} > S$; therefore, we have

$$3 + 2|D|^{1/4} > a.$$

By putting $\gamma^2 = b - 2\alpha\beta - \beta^2$ and $\beta = (a-\alpha) / 2$ into the equation

$$S = (\alpha - \beta)^2 + 3\gamma^2,$$

we get

$$S = (3\alpha - a)^2/2 - (a^2 - 3b).$$

But $(3\alpha - a)^2/2 > 0$ and $\sqrt{|D|} > S$; thus, we can conclude that

$$S > 3b - a^2$$

and $$(\sqrt{|D|} + a^2) / 3 > b.$$

By using the substitutions for γ^2 and β, we can write

$$c = \alpha(b - a\alpha + \alpha^2),$$

and
$$\begin{aligned} S &\geq (\alpha - \beta)^2 + \gamma^2 \\ &\geq \alpha^2 - 3a\alpha - a^2/2 + 3b \\ &\geq 3(b - a\alpha + \alpha^2) + 3\alpha^2/2 - a^2/2. \end{aligned}$$

However,

$$b - a\alpha + \alpha^2 = c/\alpha;$$

thus we get

$$S \geq 3c/\alpha + 3\alpha^2/2 - a^2/2$$

and $$\sqrt{|D|}/3 + a^2/6 - 1/2 > S/3 + a^2/6 - 1/2 > c.$$

As for the index I, we know that

$$DI^2 = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2.$$

Since a, b and c are positive integers, we have

$$4b^3 + 4a^3c + 27c^2 > |D|I^2.$$

By using the upper bounds on a, b and c, we can easily deduce the bound for the index I.■

As a consequence of Lemma 2.3.1 we see that if we wish to determine all the possible complex cubic fields with discriminant D satisfying $|D| \leq B$, where B is some bound, we need to examine only a finite number of triplets (a,b,c) as possible coefficients of the generating polynomials of the form (2.2.1). The integers in these triplets must satisfy

$$0 < a < 3 + 2B^{1/4},$$

(2.3.1) $$0 < b < (a^2 + \sqrt{B})/3,$$

$$0 < c < (a^2 - 3 + 2\sqrt{B})/6,$$

and the index I(a,b,c) must satisfy

(2.3.2) $$I(a,b,c) < I_B = (124a^2 + 432a + 4\sqrt{|B|} + 729)^{1/2}.$$

§2.4 The algorithm to construct complex cubic fields.

As mentioned earlier, our algorithm for determining all the complex cubic fields with discriminant D satisfying $|D| \leq B$ is, with some minor modifications, very similar to the algorithm employed in §3 of [LQ88A]. The first modification occurs in step 1(a). Instead of eliminating the pair (a',b') when there is a prime p with $v_p(a') \geq 2$ and $v_p(b') \geq 3$, we replace a' by a'/p^2, and b' by b'/p^3 and then return to the beginning of step 1. In the case considered by [LQ88A] the pair $(a'/p^2, b'/p^3)$ will already be among the finite number of pairs being considered; hence, $(a'/p^2, b'/p^3)$ would be a duplication. In our case,

however, we do not have the same situation since our (a',b') is obtained via the transformation in (2.2.4). The second modification occurs in step 2. During the process of determining the irreducibility of f(a',b';x) over **Z**, if none of (11), (12) or (13) in part A of [LQ88A] §2 holds, then if f(a',b';x) is reducible it must have a zero $m \in \mathbf{Z}$ such that $m \mid b'$ and $|m| < \sqrt{|a'| + |b'|}$. This change must be made because, in this instance, either or both of a' and b' can be negative. This is not the case in [LQ88A].

Before we present our version of the construction of complex cubic fields, we first present a theorem of Llorente and Nart [LN83] which is the basis of our algorithm.

Theorem 2.4.1. Let a and b be the coefficients of the generating polynomial $f(a,b;x) = x^3 - ax + b$, Δ be the discriminant of the polynomial f(a,b;x) and D be the field discriminant of the generating polynomial f(a,b;x). Also, we define $S_p = v_p(\Delta)$ and $\Delta_p = \Delta/p^{S_p}$ for every prime p. The value of $v_p(D)$ for a prime p can be obtained as follows (Since in some cases not all entries are needed in the determination of $v_p(D)$, we use '---' to denote that this entry is not germane):

For p = 2 we have the following:

$v_2(a),v_2(b)$	S_2	$\Delta_2 \equiv 3 \pmod 4$	$v_2(D)$
---	odd	---	3
$v_2(a) \geq v_2(b) \geq 1$	even	yes	2
$v_2(a)=0$ or $v_2(b)=0$	even	---	0

For p = 3 we have the following:

$v_3(a),v_3(b)$	$a\equiv 3 \pmod 9$	b^2	S_3	$v_3(D)$
$v_3(a)>v_3(b)\geq 1$	---	---	---	5
$v_3(a)=v_3(b)=2$	---	---	---	4
$v_3(a)\geq 1, v_3(b)=0$	yes	$\not\equiv 4 \pmod 9$	---	4
$v_3(a)=v_3(b)=1$	---	---	---	3
$v_3(a)\geq 1, v_3(b)=0$	no	$\not\equiv a+1 \pmod 9$	---	3
---	yes	$\not\equiv a+1 \pmod{27}$ and $\equiv 4 \pmod 9$	---	3
$v_3(b)>v_3(a)=1$	---	---	---	1
$v_3(a)\geq 1, v_3(b)=0$	no	$\equiv a+1 \pmod 9$	---	1
---	yes	$\equiv a+1 \pmod{27}$	odd	1
$v_3(a)=0$	---	---	---	0
---	yes	$\equiv a+1 \pmod{27}$	even	0

For every prime p > 3 we have the following:

$v_p(a),v_p(b)$	S_p	$v_p(D)$
$v_p(a)\geq v_p(b)\geq 1$	even	2
$v_p(a)=0$ or $v_p(b)=0$	odd	1
$v_p(a)=0$ or $v_p(b)=0$	even	0

We now present Algorithm 2.4.1 for determining all the complex cubic fields with discriminant $D \geq -B$.

Algorithm 2.4.1.

For each triplet (a,b,c) satisfying (2.3.1), perform the following steps to determine if f(a,b,c;x) is a generating polynomial of a complex cubic field with discriminant D satisfying $|D| \leq B$. If this is the case, the discriminant D and the index I of the field are computed. Also, during the computation, divisors I_0 of I and D_0 of D are determined. If, during this process, we find that $I_0 \geq I(a')$ or $|D_0| \geq B$, then the pair (a',b') is eliminated.

1) Compute $a' = 3a^2 - 9b$, $b' = 9ab - 2a^3 - 27c$ and $S(a',b') = 27I_B$, where $27\ I_B$ is given by (2.3.2) as the bound on the index of f(a',b';x).

2) In the case of a' = 0, determine whether or not the pure cubic cubic field $\mathbf{F} = \mathbf{Q}((b')^{1/3})$ has its discriminant in the correct range. Eliminate (a',b') if it is out of range. Otherwise, go to step 10.

3) Initialize $I_0 = T_0 = D_0 = 1$.

4) Compute M = GCD(a',b'). For each prime factor p of M, do the following:

   a) If $v_p(a') \geq 2$ and $v_p(b') \geq 3$, then replace a' by a'/p^2 and b' by b'/p^3. Go to the beginning of this step.

   b) Compute $v_p(D)$ and $v_p(I)$ by using Theorem 2.4.1.

   c) If $v_p(D)$ is even, then compute $T_0 \leftarrow T_0\, p$ and $D_0 \leftarrow D_0\, p^2$ (T_0 is as defined in (2.2.6)).

   d) If $v_p(D)$ is odd, then compute $D_0 \leftarrow D_0\, p$.

   e) If p = 3 then determine T by using Theorem 2.4.1 (T is defined in (2.2.5)).

   f) Compute $I_0 \leftarrow I_0\, p^{v_p(I)}$.

   g) If $1 \leq v_p(b') \leq v_p(a')$, then f(a',b';x) is irreducible.

5) If irreducibility of f(a',b';x) has not been established in step 4 (g), then test whether f(a',b';x) = 0 for all possible values of x such that $x \mid b'$ and $|x| < \sqrt{|a'| + |b'|}$. If

$f(a',b';x) = 0$ for some x, then $f(a',b';x)$ is reducible and the pair (a',b') is eliminated.

6) If 2 is not a factor of M, then do the following:
   a) Compute $v_2(D)$ and $v_2(I)$ by using Theorem 2.4.1.
   b) If $v_2(D) > 0$ then $D_0 \leftarrow D_0 2^{v_2(D)}$.
   c) Compute $I_0 \leftarrow I_0 2^{v_2(I)}$.

7) If 3 is not a factor of M, then do the following:
   a) Compute $v_3(D)$ and $v_3(I)$ by using Theorem 2.4.1.
   b) If $v_3(D) > 0$ then $D_0 \leftarrow D_0 3^{v_3(D)}$.
   c) Compute $I_0 \leftarrow I_0 3^{v_3(I)}$.
   d) Determine T by using Theorem 2.4.1.

8) Let $I_1 = S(a',b') / I_0$. For every prime p where $p^2 > I_1 > p > 3$, p is not a factor of M and $D(a',b') \equiv 0$ (modulo p^2), do the following:
   a) Compute $v_p(D(a',b'))$.
   b) If $v_p(D(a',b'))$ is odd then $v_p(D) = 1$ and $D_0 \leftarrow D_0 p$.
   c) Compute $v_p(I) = [v_p(D(a',b'))/2]$ and $I_0 \leftarrow I_0 p^{v_p(I)}$.
   d) Compute the new value of I_1 where $I_1 = S(a',b')/I_0$.
   e) If $I_0 > S(a',b')$ then the pair (a',b') is eliminated.

9) Let $D_1 = D(a',b') / I_0^2$. If $B \geq |D_1|$ the pair (a',b') is eliminated. Indeed, in this case it is either $|D| \geq B$ or $I \geq S(a',b')$.

10) Let $D_2 = (D_1/D_0)T^2$. The pair (a',b') is eliminated in the following cases:
   a) If D_2 is not square free (in this case $I \geq S(a',b')$).
   b) If $D_2 = D_0 = 1$ (in this case $d = 1$).

11) If the pair (a',b') has not been eliminated in the preceding steps, **F** is a complex cubic field with discriminant $D = D_1$. During this process, $d = D_0D_2$ (d is defined in (2.2.5)), T and $I = I_0$ have been computed and they are recorded in a data file.

12) Stop.

After this algorithm has been executed we will have discovered all the fields with $|D| < B$; however, for any given D we may have several fields which are isomorphic. There are many methods that we can apply to eliminate isomorphic fields; for example, see Pohst [Poh87]. However, such algorithms were not needed in our case. We found that by using the algorithm given in §13 of Delone and Feddeev [DF64], we could effectively and rapidly eliminate all the isomorphic fields generated by Algorithm 2.4.1.

§2.5. Computational results and tables.

The entire procedure described in §2.4 was programmed in FORTRAN with some assembly language subroutines and run on the Amdahl 5870 computer in the University of Manitoba Computer Centre. We first tested our programs by putting B = 20000. In about 30 CPU seconds we produced a table of fields which agreed with that of [Ang73]. When we put $B = 10^6$, it required 4 hours and 11 minutes of CPU time to find all the non-isomorphic complex cubic fields with discriminant $D < -10^6$. Of this time, about 63 CPU seconds were needed to eliminate the isomorphic fields.

A large table, giving the values of D, a, b, T, R, h for each of the 182417 non-isomorphic complex cubic fields with negative discriminant $> -10^6$, has been deposited in the UMT (Unpublished Math. Tables) file. In this table, we use the symbols a, b to represent the coefficients of a generating polynomial of the form $x^3 - ax + b$ for the field F. Also, T^2 is the value of the largest square which divides the discriminant D of F (note that this is not the same T as in (2.2.5)), R is the regulator and h is the class number of F (the computation of R and h will be discussed in the following chapter). In this section we will give a brief discussion of some of the information provided by these computations.

In Table 2.5.1, we give the number of fields that were constructed for values of |D| within certain intervals and the number of these that were non-isomorphic. The intervals were selected in such a way that the upper bound on each interval is a perfect square. In Table 2.5.2 we present the number of the discriminants in our range for which there are

exactly k non-isomorphic fields having that discriminant. In Table 2.5.3 we give those discriminants that have 9 non-isomorphic fields with the same discriminant. In Table 2.5.4 we present the distribution of Table 2.5.2 for certain intervals.

Interval for |D|	Number of Fields	Number of Non-isomorphic Fields
1 - 100489	69471	17140
100490 - 200704	46762	17946
200705 - 300304	42431	18004
300305 - 400689	41879	18329
400690 - 501264	41096	18493
501265 - 600625	39414	18317
600626 - 700569	38992	18441
700570 - 801025	39049	18617
801026 - 900601	38196	18471
900602 - 1000000	38641	18659
		182417

Table 2.5.1.

k	Number of Discriminants
1	149204
2	1683
3	5510
4	3216
5	0
6	56
7	0
8	0
9	13
>9	0

Table 2.5.2.

Discriminant	k	Discriminant	k
-274348	9	-738575	9
-301676	9	-795199	9
-414511	9	-821464	9
-429679	9	-864244	9
-659263	9	-941016	9
-677487	9	-957427	9
-706547	9		

Table 2.5.3.

Interval for $\lvert D \rvert \setminus k$	1	2	3	4	5	6	8	9
1 - 100000	14564	167	422	216	0	2	0	0
100001 - 200000	14863	170	521	287	0	2	0	0
200001 - 300000	14870	161	559	291	0	4	0	1
300001 - 400000	14893	170	528	348	0	5	0	1
400001 - 500000	14897	180	556	349	0	9	0	2
500001 - 600000	15109	161	569	318	0	5	0	0
600001 - 700000	14905	170	564	362	0	5	0	2
700001 - 800000	15028	182	576	337	0	10	0	3
800001 - 900000	15000	160	591	348	0	7	0	2
900001 - 1000000	15075	162	624	360	0	7	0	2

Table 2.5.4.

In Table 2.5.5, we present the number of fields of which the discriminant is exactly divided by 3^n where n = 0,1,3,4,5.

n	Number of fields
0	126542
1	41213
3	9785
4	3247
5	1630
	182417

Table 2.5.5.

§2.6. On Davenport and Heilbronn's densities.

The total number of non-isomorphic complex cubic fields with discriminant less than -10^6 is 182417, giving the empirical density 0.182417. In Table 2.6.1, we exhibit the density of the non-isomorphic cubic fields for which $-L < D < 0$.

L	Density	L	Density
100489	.170566	600625	.180194
200704	.174815	700564	.180810
300304	.176788	801025	.181376
400689	.178240	900601	.181832
501264	.179371	1000000	.182417

Table 2.6.1.

Davenport and Heilbronn [DH71] have proved a theorem which says that this density should approach the asymptotic limit of $(4\zeta(3))^{-1} \approx 0.20798$. If, however, one were to plot the density versus L, ie would be seen that this density increases so slowly that the first impression would be that it will not achieve the Davenport-Heilbronn (D-H) limit. Thus, it remains a challenging problem, assuming that the D-H limit is not in error, to explain the origin of this very slow convergence. This problem was indicated by Shanks in [Sha76] and [Sha75] and, on the real side, in [Sha76] and [LQ88A], where the problem is further aggravated by even slower convergence. To date and to our knowledge, no good quantitative explanation of this phenomenon has been given.

Chapter 3.
Computation of the Class Number in Complex Cubic Fields.

§3.1. Introduction.

Once the table of complex cubic fields with discriminant $D < -10^6$ had been constructed, the next step was to evaluate the class number for each of the fields. In order to do this we made use of the analytic class number formula

(3.1.1) $$2\pi Rh = \sqrt{|D|}\Phi(1),$$

where h is the class number, R is the regulator, and D is the discriminant of F. Further,

$$\Phi(s) = \zeta_F(s)/\zeta(s)$$

is the Artin L-function at s and

$$\Phi(1) = \lim_{s \to 1} \Phi(s),$$

where $\zeta_F(s)$ is the Dedekind zeta function and $\zeta(s)$ is the Riemann zeta function.

The purpose of this chapter is to describe three different techniques for evaluating the class number of a complex cubic field. Two of these methods involve the use of the Euler product to estimate the Artin L-function at 1, and the third makes use of a transformation of the Dirichlet series. These techniques were implemented and run on the Amdahl 5870 computer in the University of Manitoba Computer Centre. Each obtained the same results, but with rather different timings. We also provide several tables illustrating some of the results of these computations. These tables describe the distribution of the various fields, their regulators, their class numbers, and their class group structures.

§3.2. Computation of the regulator.

In order to compute the class number by (3.1.1) we were required to obtain the regulator. We adapted the algorithm of Voronoi as modified in Williams, Cormack, Seah

[WCS80] to the general (negative D) cubic case with the minor modification that, instead of using the formulae as given in §4 of [WCS80], we used different formulae for ξ_ω, η_ω and ζ_ω. Let $\omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$, where q_1, q_2 and $q_3 \in \mathbf{Z}$, and δ is the real zero of the generating polynomial $x^3 - ax + b$, and let ω' and ω'' denote the conjugates of ω. Also, $(\xi_\omega, \eta_\omega)$ is the puncture of ω. As in [WCS80], we note that

$$\xi_\omega = (2\omega - \omega' - \omega'')/2,$$

$$\eta_\omega = (\omega' - \omega'')/2i \qquad (i^2 = -1),$$

and

$$\zeta_\omega = (\omega' + \omega'')/2.$$

Hence, we have the following formulae:

$$\xi_\omega = (-2aq_3 + 3q_2\delta + 3q_3\delta^2)/2\sigma_r,$$

$$\eta_\omega = \sqrt{-a + 3\delta^2/4}\,(q_2 - q_3\delta)/\sigma_r,$$

and

$$\zeta_\omega = (2q_1 + 2aq_3 - q_2\delta + q_3\delta^2)/2\sigma_r,$$

where a is the coefficient of the generating polynomial $x^3 - ax + b$. Since $|D|$ is small ($|D| < 10^6$) we found that a double precision FORTRAN program was sufficient for the evaluation of a very good approximation to R. All of the regulators were evaluated in about 89 minutes of CPU time. The largest regulator that we found has an approximate value of 1609.6035. In Table 3.2.1, we provide the number of fields for which the regulators lie within certain intervals.

Interval	Number of fields	Interval	Number of fields
0<R<200	137746	1000<R<1200	286
200<R<400	31558	1200<R<1400	103
400<R<600	9042	1400<R<1600	16
600<R<800	2771	1600<R<1800	1
800<R<1000	894	1800<R	0

Table 3.2.1.

§3.3. Computation of the class number via the Euler product.

From (3.1.1) we see that, in order to evaluate h, we need to find an approximation to $\Phi(1)$ which is sufficiently good that we can evaluate h (an integer) unequivocally. There are two basic approaches that can be used: $\Phi(1)$ can be estimated by using the Euler product formula or it can be estimated by using the Dirichlet series. In this section, we will discuss the Euler product techniques.

We first remark that we can write $\Phi(1)$ as the Euler product

$$\Phi(1) = \prod_{p} f(p), \tag{3.3.1}$$

where the product is taken over all the rational primes, and, for each such prime p, the value of f(p) depends upon how the principal ideal (p) splits or factorizes in **F**. These values are given in Table 3.3.1.

Type	Factorization of (p)	f(p)
A	$\mathbf{pp'p''}$	$p^2/(p^2 - 2p + 1)$
B	(p)	$p^2/(p^2 + p + 1)$
C	$\mathbf{pq}$	$p^2/(p^2 - 1)$
D	$\mathbf{p^2q}$	$p/(p - 1)$
E	$\mathbf{p^3}$	1

Table 3.3.1.

Here we use **p**, **p'**,**p"**, **q** to denote distinct prime ideals in **F**.

In order to determine the splitting type of (p), we used the following theorem of Llorente and Nart [LN83].

Theorem 3.3.1. Let a and b be the coefficients of the generating polynomial $f(a,b;x) = x^3 - ax + b$, Δ be the discriminant of the polynomial f(a,b;x), $S_p = v_p(\Delta)$ and $\Delta_p = \Delta / p^{S_p}$.The principal ideal (p) factorizes in **F** as follows (Since in some cases not all

entries are needed in the determination of $v_p(D)$, we use '---' to denote that this entry is not germane):

Factorization of (2).

$v_2(a),v_2(b)$	S_2	Δ_2	Type
$1\le v_2(b)\le v_2(a)$	---	---	E
$1=v_2(a) < v_2(b)$	---	---	D
$1<v_2(a),\ 0=v_2(b)$	---	---	C
$0=v_2(a),\ 1<v_2(b)$	odd	---	D
$0=v_2(a),\ 1<v_2(b)$	even	$\equiv 3 \pmod 4$	D
$0=v_2(a),\ 1<v_2(b)$	even	$\equiv 5 \pmod 8$	C
$0=v_2(a),\ 1<v_2(b)$	even	$\equiv 1 \pmod 8$	A
$0=v_2(a),\ 0=v_2(b)$	---	---	B

Factorization of (3).

$v_3(a),v_3(b)$	a	b	S_3	Δ_3	Type
$1\le v_3(b)\le v_3(a)$	---	---	---	---	E
$1=v_3(a)<v_3(b)$	---	---	---	---	D
$0=v_3(a),\ 0\le v_3(b)$	$\equiv -1 \pmod 3$	---	---	---	C
$0=v_3(a)=v_3(b)$	$\equiv 1 \pmod 3$	---	---	---	B
$0=v_3(a),\ 1\le v_3(b)$	$\equiv 1 \pmod 3$	---	---	---	A
$1\le v_3(a),\ 0=v_3(b)$	$\not\equiv 3 \pmod 9$	$\equiv a+1 \pmod 9$	---	---	D
$1\le v_3(a),\ 0=v_3(b)$	$\not\equiv 3 \pmod 9$	$\not\equiv a+1 \pmod 9$	---	---	E
$1\le v_3(a),\ 0=v_3(b)$	$\equiv 3 \pmod 9$	$\equiv a+1 \pmod{27}$	odd	---	D
$1\le v_3(a),\ 0=v_3(b)$	$\equiv 3 \pmod 9$	$\equiv a+1 \pmod{27}$	even,	$\equiv -1 \pmod 3$	D
$1\le v_3(a),\ 0=v_3(b)$	$\equiv 3 \pmod 9$,	$\equiv a+1 \pmod{27}$	=6,even	$\equiv 1 \pmod 3$	B
$1\le v_3(a),\ 0=v_3(b)$	$\equiv 3 \pmod 9$,	$\equiv a+1 \pmod{27}$	>6,even	$\equiv 1 \pmod 3$	A
$1\le v_3(a),\ 0=v_3(b)$	$\equiv 3 \pmod 9$	$\not\equiv a+1 \pmod{27}$	---	---	E

Factorization of (p) (p > 3).

$v_p(a),v_p(b)$	p (mod 3)	$(b/p)_3$	(a/p)	S_p	(Δ_p/p)	f(a,b;x)*	Type
$1\le v_p(b)\le v_p(a)$	---	---	---	---	---	---	E
$1=v_p(a)<v_p(b)$	---	---	---	---	---	---	D
$1\le v_p(a),0=v_p(b)$	$\equiv -1$	---	---	---	---	---	C
$1\le v_p(a),0=v_p(b)$	$\equiv 1$	$=1$	---	---	---	---	A
$1\le v_p(a),0=v_p(b)$	$\equiv 1$	$\neq 1$	---	---	---	---	B
$0=v_p(a),0<v_p(b)$	---	---	$=1$	---	---	---	A
$0=v_p(a),0<v_p(b)$	---	---	$=-1$	---	---	---	C
$0=v_p(a)=v_p(b)$	---	---	---	odd	---	---	D
$0=v_p(a)=v_p(b)$	---	---	---	even	$=1$	y	A
$0=v_p(a)=v_p(b)$	---	---	---	even	$=1$	n	B
$0=v_p(a)=v_p(b)$	---	---	---	even	$=-1$	---	C

In the case where it was necessary to determine whether or not f(a,b;x) has some root (mod p), we used the Lucas function technique mentioned in Williams and Zarnke [WZ74], with the algorithm for determining the value of the appropriate Lucas function (mod p) being that of Williams [Wil87]. Theorem 3.3.1 was implemented in assembly language.

Set

$$F(Q,D) = \prod_{p\le Q} f(q),$$

where the product is evaluated over the rational primes. Since $\Phi(1)$ in (3.2.1) is given as an infinite product, we must determine how large to make Q such that

---

* We use y to denote that f(a,b;x) has some root (mod p), and n to denote that f(a,b;x) has no roots (mod p).

$$H(Q,D) = \sqrt{|D|}F(Q,D)/(2\pi R)$$

is within 1/2 of h. When this occurs, h = Ne(H(Q,D)), where we denote the nearest integer to x by Ne(x).

One way of determining Q in the computation of h is to use the heuristic of Shanks mentioned in [Sha76A]. H(Q,D) can be evaluated by using the first 500, then 1000, 1500, 2000 etc. primes until H(Q,D) is within 0.1 of the same integer H for 6 successive evaluations. When this occurs, it is declared that h = H. This heuristic is easy to implement and executes fairly rapidly; but, unfortunately, it is not a mathematically rigorous method of computing h.

Another method which can be used is that of Buchmann and Williams [BW89]. The details of the method are discussed in [BW89]; we only mention here that in our case we have D given by (2.2.5) $n_L = 6$, $C(t) = 2\bar{C}(t)/3$, and $c_1 + 2c_2^2 = 3$. Given a known divisor h^* of h, this technique makes use of the Euler product to determine h in $O(|D|^{1+\varepsilon}/(h^*R)^2)$ elementary operations for any $\varepsilon > 0$. However, the truth of the Riemann Hypothesis on ζ_L, where L is the normal closure of **F**, must be assumed in order to be able to assert that the class number is correct.

Further, in cases for which R is small, a value for h^* must be found which is large enough that our technique does not take much time in executing. To do this we simply produced (by trial) a non-principal reduced ideal **a** in **F** such that the least value of m (>0) for which

(3.3.2) $$\mathbf{a}^m \sim (1)$$

is sufficiently large. We then put $h^* = m$. In order to do this we started m at 1 and increased it until we found a value for which (3.3.2) holds. Further, for ideals **a** and **b**, where **b** is a reduced ideal equivalent to $\mathbf{a}^j$, we found **c**, where **c** is an ideal equivalent to the ideal $\mathbf{a}^{j+1}$, in the following manner: If the norms of **a** and **b** were relatively prime, then the theorem of Voronoi [Vor94] for multiplying two ideals, as given in Williams, Dueck and Schmid [WDS83], was used to find **c**. However, if the norms of the two ideals were

not relatively prime, we used the Voronoi algorithm as described in [WCS80], to obtain some $\mathbf{a}'$, where $\mathbf{a}' \sim \mathbf{a}$ and the norms of $\mathbf{a}'$ and $\mathbf{b}$ were relatively prime. The theorem of Voronoi [Vor94] for multiplying ideals $\mathbf{a}'$ and $\mathbf{b}$ could then be applied to find $\mathbf{c}$. The process of finding m was not very time consuming because the fairly small value of $|D|$ guarantees that h will not be large. We used the algorithm of Voronoi to find all the reduced principal ideals in $\mathbf{F}$, and the reduction technique described in Williams [Wil85] to determine whether or not (3.3.1) holds for a particular m value. In our application, we found that a value of h^* could be found such that $h^* > \tilde{h}/6$, where $\tilde{h}$ is our first approximation to h (using 500 primes in the Euler product, say). We are now able to present the entire algorithm of Buchmann and Williams which was used in our computation.

Algorithm 3.3.1.

1) Compute F(500,D) and set $\tilde{h} = Ne(H(500,D))$.
2) Initialize $h^* = 1$.
3) Pick a non-principal ideal $\mathbf{a}$ and find the least m such that $\mathbf{a}^m \sim (1)$.
4) $h^* \leftarrow h^* (m/GCD(m,h^*))$.
5) If $h^* < \tilde{h}/6$, then go to step 3.
6) Initialize Q = 5000.
7) Compute F(Q,D) and set $\tilde{h} = Ne(H(Q,D)/h^*)$.
8) Compute C(Q) and $A(Q,D) = C(Q)(4+3\log Q)/\sqrt{Q} + 3/Q$.
9) Compute $\tau = \sqrt{|D|}F(Q,D)/2R\pi - \tilde{h}$.
10) Compute $Y = |\tau| + (|D|)F(Q,D)(e^{A(Q,D)}-1)/2R\pi$.
11) If $\tilde{h} - Y/h^* - [\tilde{h} + Y/h^*] > 1$, then stop.
12) Otherwise, set $Q \leftarrow Q + 5000$ and go to step 7.
13) Stop.

Both of these methods of utilizing the Euler product to compute h were implemented in FORTRAN (with some assembly language subroutines) and run. The Shanks heuristic method required 8 hours and 16 minutes of CPU time to find all the class numbers, whereas the method of Buchmann and Williams with the assumption of the truth of the Riemann Hypothesis required 14 hours and 10 minutes of CPU time. The large difference in these times is a result of the fact that the Shanks heuristic usually (80% of the time) required that no more than 3000 primes for the evaluation of H(Q,D) and only rarely required that more than 5000 primes be used. On the other hand the use of Algorithm 3.3.1 demanded that 5000 or more primes be used in most cases.

§3.4. Determination of h from the Dirichlet Series.

As noted in [BLW87], we can write

$$\Phi(1) = \sum_{j=1}^{\infty} \alpha(j) j^{-1}, \tag{3.4.1}$$

where $\alpha(j)$ is a multiplicative function, $\alpha(1) = 1$, and the value of $\alpha(p^n)$, where p is any rational prime, is given in the table below (see Barrucand, Loxton, Williams [BLW87]).

Type	n	$\alpha(p^n)$
A	any	n + 1
B	$n \equiv 0 \pmod 3$	1
B	$n \equiv 1 \pmod 3$	-1
B	$n \equiv 2 \pmod 3$	0
C	$n \equiv 0 \pmod 2$	1
C	$n \equiv 1 \pmod 2$	0
D	any	1
E	any	0

Table 3.4.1.

It can be noted that $\alpha(p^n) \leq d(p^n)$, where we represent the number of divisors of k by d(k). It follows that $\alpha(k) \leq d(k)$.

Also, the formula (3.4.1) can be transformed into

$$\Phi(1) = \sum_{j=1}^{\infty} \alpha(j) j^{-1} e^{-jC} + C \sum_{j=1}^{\infty} \alpha(j) E(jC),$$

where $C = 2\pi/\sqrt{|D|}$ and $E(y) = \int_{y}^{\infty} e^{-x} x^{-1} dx$.

Before we proceed any further, we now must define the function M(m) as follows:

(3.4.2) $$M(m) = \max\{d(j)j^{-1} \mid m < j \leq 3m\}.$$

We will show how this function can be utilized in the sequel; hence, but first require some results concerning it.

Lemma 3.4.1. Given any integer $n \geq 2$, there exists an integer m such that

$n/3 < m \leq n/2$ and $d(m)/m \geq d(n)/n$.

Proof. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$,

where $\alpha_i \geq 1$, and p_1 is the smallest prime factor of n.

Let

$$p_1 = 2k + r \qquad \text{where } r = 0 \text{ or } 1.$$

By using the multiplicative property of d and the fact that $k < p_1$ we can easily deduce the following:

$$\frac{d(n)}{n} = \frac{k(\alpha_1+1)d(kn/p_1)}{\alpha_1 p_1 d(k)(kn/p_1)}.$$

Thus, if $m = kn/p_1$, then

$$\frac{d(m)}{m} = \frac{d(n)\alpha_1 p_1 d(k)}{nk(\alpha_1+1)}.$$

Also, since $p_1 = 2k + r$, it is easy to show that $n/3 \leq m \leq n/2$.

But

$$\frac{\alpha_1 p_1 d(k)}{k(\alpha_1+1)} \geq \frac{\alpha_1 p_1}{k(\alpha_1+1)}$$

$$\geq \frac{2\alpha_1}{(\alpha_1+1)}$$

$$\geq 1.$$

So we have

$$\frac{d(m)}{m} \geq \frac{d(n)}{n}. \qquad \blacksquare$$

From this result it is a simple matter to deduce

Theorem 3.4.1. Let $n > 3m$. Then

$$M(m) = \max \{d(j)j^{-1} \mid m < j \leq n\}.$$

Proof. Suppose $M(m) = d(n)/n$, when $n > 3m$.

We define

$$S(n) = kn/p_1$$

as defined in Lemma 3.4.1.We also define

$$S^r(n) = S(S^{r-1}(n)).$$

Since $$S^{r-1}(n)/3 \leq S^r(n) \leq S^{r-1}(n)/2,$$

the value of $S^r(n)$ decreases monotonically as r grows larger. Let $S^t(n)$ be the first number in the sequence

$$n, S(n), S^2(n), \ldots, S^r(n), \ldots$$

such that

$$S^t(n) \leq 3m.$$

Also,

$$\frac{d(S^t(n))}{S^t(n)} \geq \frac{d(S^{t-1}(n))}{S^{t-1}(n)} \geq \frac{d(n)}{n}.$$

Hence the theorem holds. $\blacksquare$

By using Theorem 3.4.1 and (3.4.2), and replacing n by 3m, we can conclude that only the numbers between m and 3m+1 are needed to be inspected in the calculation of M(m). Now, if we put

$$A(m) = \sum_{j=1}^{m} \alpha(j) j^{-1} e^{-jC} + C \sum_{j=1}^{m} \alpha(j) E(jC),$$

then, by using the reasoning of [BLW87], we get

(3.4.3) $$|\Phi(1)/C - A(m)/C| < (2M(m)e^{-mC}) / C(e^{C} - 1).$$

Thus, by (3.4.3) and (3.1.1), we get

(3.4.4) $$|h - A(m)/CR| < (2M(m)e^{-mC}) / CR(e^{C} - 1).$$

It follows that, if m is sufficiently large that

(3.4.5) $$(2M(m)e^{-mC}) < CR(e^{C} - 1)/2,$$

then

(3.4.6) $$h = Ne(A(m)/CR).$$

Under the assumption (later verified) that we would never require a value for m in (3.4.5) that exceeds 2000 (for values of $|D| < 10^6$), we found by, using Theorem 3.4.1 to tabulate M(m), that

$$M(m) < 7.4(\log m)/m \qquad (m < 2000).$$

Thus, in order to determine h, we can use any value of m in (3.4.6) such that

(3.4.7) $$(\log m)m^{-1}e^{-mC} < 0.0338CR(e^{C} - 1),$$

provided that such a value of $m \leq 2000$. In fact, for the range of D values that we considered we never needed a value for m which exceeded 1109, in order for (3.4.7) to hold. We are now able to present Algorithm 3.4.1.

Algorithm 3.4.1.

1) Use Newton's method to solve the equation

$$(\log m)m^{-1}e^{-mC} = 0.0338CR(e^{C} - 1).$$

2) Compute A(m).

3) Compute h = Ne(A(m)/CR).

4) Stop.

This technique is not only mathematically rigorous but, surprisingly, is very much faster than both of the techniques based on the Euler product. To find all the class numbers by this method required only 60.8 minutes of CPU time, using a program written in FORTRAN and supplemented by assembly language routines for evaluating $\alpha(k)$ and $E(y)$. In view of the complexity of the Dirichlet series method ($O(D^{1/2+\varepsilon})$), one would expect the methods of §3.3 to be faster; however, these complexity measures have more relevance when $|D|$ is large rather than when $|D|$ has the small values which we were considering. It turned out that, for these values, the asymptotically faster method was actually considerably slower than the Dirichlet series method. For much larger values of $|D|$, of course, this situation would be reversed.

§3.5 Results.

In Table 3.5.1, we give the number of non-isomorphic fields that we found with class number h within a certain range. The largest class number found (162) occurs for discriminant -885871. In Table 3.5.2, we present a more complete picture for values of $h \leq 20$. In Table 3.5.3, we give the number of fields of which the class number is divisible by p where p = 2,3,5,7,11,13,17,19,23,29. In Table 3.5.4, we provide all the fields that have class number bigger than 100.

Range of h	Number of Fields
1 - 10	172789
11 - 20	6380
21 - 30	1897
31 - 40	691
41 - 50	324
51 - 60	148
61 - 70	91
71 - 80	36
81 - 90	29
91 - 100	14
>100	18

Table 3.5.1

h	Number of Fields	h	Number of Fields
1	97451	11	844
2	26335	12	1652
3	22586	13	601
4	7746	14	515
5	4477	15	843
6	5950	16	477
7	2134	17	312
8	2100	18	642
9	2931	19	273
10	1079	20	221
	172789		6380

Table 3.5.2

P	Number of Fields
2	48327
3	36322
5	7146
7	3309
11	1210
13	828
17	414
19	333
23	179
29	101

Table 3.5.3

D	A	B	h
-386855	7	2394	108
-456231	711	-7462	109
-499359	1911	-35350	123
-529444	-726	-700	104
-606279	-171	260	145
-703364	442	-3924	118
-714932	-17	4068	103
-719911	329	-2320	104
-814575	135	2170	129
-885871	-91	140	162
-893252	-861	11068	103
-930719	-1419	21940	144
-960456	894	32240	129
-968228	535	-4944	156
-968359	553	-5352	102
-978715	-528	2149	104
-983528	217	5670	141
-999431	253	-1596	134

Table 3.5.4

§3.6. The Cohen and Martinet heuristics.

In Table 3.6.1 we give the density of fields with $|D| < L$ and class number $h = 3^v h_0$, where $3 \nmid h_0$ and $h_0 \leq 10$. According to the heuristics of Cohen and Martinet (C-M) [CM87], we would expect the asymptotic densities to be 0.518642, 0.259321,

0.086440, 0.025932 and 0.012349 for $h_0 = 1, 2, 4, 5, 7$, respectively. If, once again, the densities given in Table 3.6.1 were to be plotted then, in the case of $h_0 = 1, 2, 4$, an aggravated case of what occurred for the Davenport-Heilbronn (D-H) theorem, as discussed in §2.6, would be noticed, and it might reasonably be conjectured that the C-M heuristic limits are inaccurate. However, in view of the fact that we do not have an explanation of the similar situation with D-H, we do not consider it wise to invalidate the C-M heuristic limits. We do not know where they are going, or how fast, in the case $h_0 = 1, 2, 4$. We are pleased to put these facts before the reader and urge him to conduct his own investigation. However, it should be noted that the columns for $h_0 = 5, 7$, which seem to be increasing, have already passed the C-M prediction; this is also a problem which needs further investigation.

$L \setminus h_0$	1	2	4	5	7	8	10
100000	0.73499	0.16050	0.03838	0.02770	0.01209	0.00833	0.00423
200000	0.71319	0.16955	0.04396	0.02740	0.01253	0.01018	0.00532
300000	0.70309	0.17207	0.04682	0.02805	0.01322	0.01058	0.00572
400000	0.69635	0.17330	0.04843	0.02863	0.01359	0.01140	0.00591
500000	0.69051	0.17498	0.04961	0.02918	0.01390	0.01179	0.00606
600000	0.68584	0.17713	0.05037	0.02913	0.01373	0.01247	0.00635
700000	0.68252	0.17788	0.05102	0.02943	0.01399	0.01281	0.00641
800000	0.67957	0.17926	0.05165	0.02943	0.01396	0.01306	0.00648
900000	0.67706	0.18006	0.05202	0.02941	0.01394	0.01337	0.00651
1000000	0.67521	0.18072	0.05228	0.02945	0.01381	0.01341	0.00675

Table 3.6.1

§3.7. Class group structure.

Once we had calculated the class number of our 182417 fields, it was a relatively simple matter to determine the structure of each class group. Only 3959 of these class groups are non-cyclic. In Table 3.7.1 we give the number of these non-cyclic class groups for a given n-rank.

n	n-Rank	Number of Occurrences
2	2	3055
2	3	12
3	2	868
3	3	3
4	2	16
5	2	4
6	2	5
		3963

Table 3.7.1

Finally, in Table 3.7.2 we present those fields that have the most interesting class group structures. Here C_n denotes the cyclic group of order n and the values of a and b are those for which f(a,b;x) generates the corresponding cubic number field.

D	a	b	Class Group Structure
-300551	49	-169	C_2 x C_2 x C_2
-421423	453	-5015	C_2 x C_2 x C_2
-421423	-276	-3395	C_2 x C_2 x C_2
-542251	19	151	C_2 x C_2 x C_2
-841304	741	-9110	C_2 x C_2 x C_2
-864023	91	-379	C_2 x C_2 x C_2
-344411	139	1914	C_2 x C_2 x C_4
-379591	-159	3107	C_2 x C_2 x C_4
-433243	-229	1526	C_2 x C_2 x C_4
-612263	31	606	C_2 x C_2 x C_4
-562123	228	4115	C_2 x C_2 x C_6
-694543	473	-4272	C_2 x C_2 x C_6
-894348	0	182	C_3 x C_3 x C_3
-936684	84	-350	C_3 x C_3 x C_3
-936684	-42	154	C_3 x C_3 x C_3
-280468	795	-9056	C_4 x C_4
-393828	-285	2684	C_4 x C_4
-532463	37	-165	C_4 x C_4
-555976	899	-10626	C_4 x C_4
-655483	-28	145	C_4 x C_4
-716131	-133	2538	C_4 x C_4
-751819	98	-409	C_4 x C_4
-787663	-267	-4295	C_4 x C_4
-898175	175	1275	C_4 x C_4
-989156	-149	310	C_4 x C_4

D	a	b	Class Group Structure
-359131	44	-161	C_4 x C_8
-375387	498	-10465	C_4 x C_8
-653971	-46	99	C_4 x C_8
-749723	40	-193	C_4 x C_8
-804443	52	-225	C_4 x C_8
-865851	516	-6613	C_4 x C_8
-173287	-55	32	C_5 x C_5
-304196	2307	-43508	C_5 x C_5
-383827	-240	22489	C_5 x C_5
-746287	1443	41650	C_5 x C_{15}
-641196	-6	154	C_6 x C_6
-782648	19	342	C_6 x C_6
-864243	60	-253	C_6 x C_6
-914683	-28	175	C_6 x C_6
-939843	30	197	C_6 x C_6

Table 3.7.2

Chapter 4.
Introduction to CUFFQI

§4.1 Introduction.

In Chapter 2, we presented an algorithm for finding all non-isomorphic complex cubic fields with discriminant larger than a given bound. However, this algorithm is impractical for determining all the non-isomorphic cubic fields for a given large discriminant, D. The major problem with this algorithm is that there are too many possible generating polynomials to be inspected; therefore, a different approach is needed. Over 60 years ago, Berwick[Ber25] presented one such method for obtaining all distinct cubic fields having discriminant D. Although this method is sound, it is somewhat inefficient and was not really designed for actual implementation. After Daniel Shanks [Sha72] described the idea of the infrastructure in real quadratic fields, he (see [Sha76B], [Sha87], [Sha88] and [Sha89]) introduced a different method, Cubic Fields From Quadratic Infrastructure (CUFFQI), to construct all the non-isomorphic complex cubic fields having the same fixed fundamental discriminant D. Unfortunately, no complete description of the CUFFQI algorithm exists, as yet in the current literature. In his preliminary write-up of the algorithm [Sha87], Shanks did not present his algorithm in a form which is suitable for implementation on a large computer. Indeed, the work done here was initiated at Shanks' request to render his algorithm into a form which can be easily automated. We will discuss the size of the intermediate calculations which are produced and the complexity of the algorithm. These are issues that Shanks did not address fully in his work. Thus, the purpose of this, and the following chapter is to present a computational version of the CUFFQI algorithm. As in [Sha87], we will also restrict our discussion to the construction of the complex cubic fields having a fundamental discriminant.

A fundamental discriminant is the discriminant D of the quadratic field $\mathbf{K} = \mathbf{Q}(\sqrt{n})$, where n is a square-free integer and D is given by

$$D = \begin{cases} n & n \equiv 1 \pmod 4 \\ 4n & n \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Also, for $\alpha, \beta \in \mathbf{K}$, denote the module $\alpha\mathbf{Z} + \beta\mathbf{Z}$ by $[\alpha, \beta]$. Put

$$\sigma = \begin{cases} 1 & D \equiv 2 \text{ or } 3 \pmod 4 \\ 2 & D \equiv 1 \pmod 4. \end{cases}$$

For $\omega = (\sigma - 1 + \sqrt{D}) / \sigma$, we have

$$\mathbf{O}_K = [1,\omega],$$

where $\mathbf{O}_K$ is the maximal order of $\mathbf{K}$.

For a given D (< 0), our task is to find a generating polynomial

(4.1.1) $$x^3 - ax^2 + bx - c, \qquad (a,b,c \in \mathbf{Z})$$

for each of the non-isomorphic complex cubic fields having discriminant D. Also, it is important to keep the coefficients and the index of the generating polynomial as small as possible. The number of distinct cubic fields of discriminant D can be determined by using a well known theorem by Hasse [Has80].

Theorem 4.1.1. (Hasse) If the discriminant of a quadratic field $\mathbf{Q}(\sqrt{n})$ is D and the 3-rank of the class group of $\mathbf{Q}(\sqrt{n})$ is r, then there are precisely

$$m = \frac{(3^r-1)}{2}$$

non-isomorphic cubic fields of discriminant D. ■

Hasse did not provide an efficient method of determining these m fields. Our objective here was to develop an algorithm which could construct all the non-isomorphic cubic fields having discriminant D by performing computation in the quadratic field $\mathbf{Q}(\sqrt{D'})$.

One of the bases of Shanks' algorithm is a theorem of Scholz[Sch32]. In order to present this theorem, it is necessary to introduce the idea of dual discriminants. We say that D and D' are dual discriminants if

(4.1.2) $$D' = \frac{-3D}{\gcd(3,D)^2},$$

where D and D' are both fundamental discriminants. Clearly, D' = -D/3, in the event that $3 \mid D$, and D' = -3D when $3 \nmid D$. For the rest of this chapter and the following chapter, D' is the dual discriminant of D. The relationship between the 3-ranks of $Q(\sqrt{D})$ and $Q(\sqrt{D'})$ is given by

Theorem 4.1.2.(Scholz) If D < 0 and the 3-rank of $Q(\sqrt{D})$ is r, then the 3-rank of its dual field $Q(\sqrt{D'})$ is either r or r-1. ■

The first case is called non-escalatory, whereas the second case is called escalatory. For example, the complex quadratic field $Q(\sqrt{-4027})$ has a 3-rank of 2 and its dual field $Q(\sqrt{12081})$ has a 3-rank of 1. Hence, this field belongs to the escalatory case.

In [Sha87], Shanks wrote the following:

> "We may assume our algorithm as a constructive version of Scholz's theorem with attention paid to the infrastructure of the real quadratic field."

Shanks' idea is that we can construct all the non-isomorphic cubic fields having a given discriminant D by performing all the computations in the field $Q(\sqrt{D'})$ (D'>0) which has discriminant D'. For example, there are 4 distinct complex cubic fields having discriminant -4027. These fields can be constructed by performing the CUFFQI algorithm in the quadratic field $Q(\sqrt{12081})$. Generating polynomials with coefficients a,b,c (see (4.1.1)) of these fields are shown in Table 4.1.1.

a	b	c	index
0	-8	-15	1
1	7	-8	1
0	10	-1	1
1	27	76	7

Table 4.1.1

The algorithm we used to produce the polynomials in Table 4.1.1 is the CUFFQI algorithm modifier to make it suitable for automation. Also, our approach was to use ideals rather than binary quadratic forms. In the remainder of this chapter, we present the theoretical aspects of CUFFQI which show that all the complex cubic fields with discriminant D can be found in the real quadratic field $\mathbf{Q}(\sqrt{D'})$. The computational aspects of this algorithm, including a detailed description of its implementation, are given in the following chapter.

§4.2. Quadratic Generators.

We first mention the following simple lemma.

Lemma 4.2.1.Given any cubic field $\mathbf{Q}(\rho)$ where ρ is a zero of an irreducible cubic polynomial, there exists an equation of the form

(4.2.1) $$x^3 - 3Qx + A = 0,$$

where $Q, A \in \mathbf{Z}$, and a zero of this equation ξ such that $\mathbf{Q}(\rho) = \mathbf{Q}(\xi)$.

Proof. We may assume that ρ is the real zero of

(4.2.2) $$a_0y^3 + a_1y^2 + a_2y + a_3 = 0$$

for some $a_0, a_1, a_2, a_3 \in \mathbf{Z}$. By performing the simple linear transformation $\xi = 3a_0\rho + a_1$ on (4.2.2.), we can easily deduce that $\mathbf{Q}(\rho) = \mathbf{Q}(\xi)$. ■

As in §2.2, without loss of generality, we may assume that

(4.2.3.) $$\text{if } p^3 \mid A, \text{ then } p^2 \nmid Q \text{ for any prime } p.$$

It is well known that the polynomial discriminant Δ of (4.2.1) is given by

$$\begin{aligned}\Delta &= 27(4Q^3 - A^2)\\ &= I(\xi)^2D,\end{aligned}$$

where $I(\xi)$ ($\neq 0$) is the index of ξ in $\mathbf{Q}(\xi)$. Since D is a fundamental discriminant, we either have $3 \nmid D$ or $3 \parallel D$. Thus, we can easily deduce that if $3 \nmid D$, then $9 \mid I(\xi)$; whereas if $3 \mid D$, then $3 \mid I(\xi)$.

Put

$$B = \begin{cases} I(\xi)/3 & 3 \mid D \text{ and } D' = -D/3 \\ I(\xi)/9 & 3 \nmid D \text{ and } D' = -3D \end{cases}$$

We have

$$\Delta = -27D'B^2,$$

where $B \in \mathbf{Z}$ and

$$4Q^3 = A^2 - B^2D' \qquad (B>0).$$

If we put $\lambda = \frac{A + B\sqrt{D'}}{2}$, then we have $\lambda + \bar{\lambda} = A$ and $\lambda\bar{\lambda} = Q^3$, where $\bar{\lambda}$ is the conjugate of λ in the field $\mathbf{K}$. Also, since $B \neq 0$, we have $\lambda - \bar{\lambda} \neq 0$. For this reason, we can see that $\lambda \in \mathbf{O}_K$. Thus we have proved the following lemma.

Lemma 4.2.2. Let $\mathbf{K} = \mathbf{Q}(\sqrt{D'})$. Given any cubic field $\mathbf{Q}(\rho)$ of fundamental discriminant D, there exists a

$$\lambda = \frac{A + B\sqrt{D'}}{2} \qquad (A,B \in \mathbf{Z})$$

such that $\lambda \in \mathbf{O}_K$, $\lambda \neq \bar{\lambda}$, $Q^3 = N(\lambda)$ $(Q \in \mathbf{Z})$ and $\mathbf{Q}(\rho) = \mathbf{Q}(\xi)$ for some zero ξ of

$$x^3 - 3Qx + A = 0.$$

We call such a λ a quadratic generator for the cubic field $\mathbf{Q}(\rho)$. ■

If we let $(\lambda) = \mathbf{a} = (u)\mathbf{h}$, where $\mathbf{h}$ is a primitive ideal of $\mathbf{O}_K$ and $u \in \mathbf{Z}$, we can prove

Lemma 4.2.3. For $\mathbf{a}$ and λ defined as in Lemma 4.2.2, we have $(\lambda) = \mathbf{a} = (u)\mathbf{h}$, where u is a square-free integer, $u \mid D'$ and $\mathbf{h}$ is a primitive ideal of $\mathbf{O}_K$.

Proof. Here, we will show that u must be a factor of D' and square-free. We describe the prime factors of u through the use of the following cases.

Case 1. $p > 3$. If $p^\alpha \parallel u$, then we have $p^\alpha \parallel \gcd(A,B)$ and it follows that $p^{2\alpha} \mid Q^3$. By (4.2.3), we can see that $\alpha = 1$ or 2.

Subcase 1.1. $\alpha = 2$. In this subcase, we get $p^2 \mid A$ and $p^2 \mid Q$. Hence, we have $p^2 \parallel A$ and $v_p(3Q) \geq v_p(A) = 2$. By using Theorem 2.4.1, we have $p^2 \mid D$. (For the rest of this

proof, Theorem 2.4.1 is used without reference.) However, D is a fundamental discriminant, so we get a contradiction.

Subcase 1.2. $\alpha = 1$. In this subcase, we have either $p \parallel A$ or $p^2 \mid A$. In the first case, we have $v_p(3Q) \geq v_p(A) = 1$ and we must have $p^2 \mid D$. Once again, we get a contradiction. In the second case, we have $p^3 \mid D'B^2$. Since $p \parallel \gcd(A,B)$, we have $p \parallel B$ and it follows that $p \mid D'$.

Case 2. $p = 3$. We have the same situation as in Case 1, α is either 1 or 2.

Subcase 2.1. $\alpha = 2$. In this subcase, we have $3^2 \mid A$ and $3^2 \mid Q$. This also implies that we have $v_3(3Q) \geq v_3(A) = 2$. Hence, we have $3^5 \parallel D$, and we get a contradiction.

Subcase 2.2. $\alpha = 1$. In this subcase, we have either $3 \parallel A$ or $3^2 \mid A$. In the former case, we have $v_3(3Q) \geq v_3(A) = 1$, and $3^5 \mid D$ follows, again, a contradiction. In the latter case, we have $27 \mid D'B^2$ and, since $3 \parallel B$, it follows that $3 \mid D'$.

Case 3. $p = 2$. In this case, we must consider two subcases: $4 \mid u$ and $2 \parallel u$.

Subcase 3.1. $4 \mid u$. Since $4 \mid u$, we have $4 \mid Q$; also, $2 \mid \gcd(A,B)$. According to (4.2.3), we know that $8 \nmid A$. Now, if $2 \mid A$, then we get $v_2(3Q) \geq v_2(A) \geq 1$, therefore $4 \mid D'$ and $4 \mid A$. In the event that $D'/4$ is even, because

$$(A/4)^2 - (D'/4)(B/2)^2 \equiv 0 \pmod 2,$$

we would have $8 \mid A$, a contradiction. In the event that $D'/4$ is odd, we get

$$A/4 \equiv B/2 \equiv 1 \pmod 2.$$

As a result, we have $\frac{A+B\sqrt{D'}}{8} \in \mathbf{O}_K$ and $\frac{A+B\sqrt{D'}}{16} \notin \mathbf{O}_K$. This implies that $4 \parallel u$ and $4 \mid N(\mathbf{h})$, and therefore, since 2 ramifies in $\mathbf{K}$, we have $(2) \mid \mathbf{h}$. Again, this is not possible because $\mathbf{h}$ is a primitive ideal. Thus, we have shown that $4 \nmid u$.

Subcase 3.2. $2 \parallel u$. In this case we have $2 \mid Q$. If D' is odd, then the assumption that $2 \nmid A$ implies that $\frac{A+B\sqrt{D'}}{4} \notin \mathbf{O}_K$ and $2 \nmid u$. Now, we have either $2 \parallel A$, $4 \parallel A$ or

$8 \mid A$. In the first case, $v_2(3Q) \geq v_2(A) = 1$ and we have $2 \mid D'$. If $4 \mid A$, we have $4 \mid B$ and

$$(A/4)^2 - D'(B/4)^2 = 2(Q/2)^3.$$

If $Q/2$ is odd, then we get

$$(A/4)^2 - D'(B/4)^2 \equiv 2 \pmod 4,$$

and this is not possible. Hence, $Q/2$ is even. If $4 \parallel A$, we get $v_2(3Q) \geq v_2(A) = 2$ and $2 \mid D'$. If $8 \mid A$, then, because $4 \mid Q$, we get a contradiction.

Summarizing these results, we have shown that, if $p \mid u$, then $p \parallel u$ and p is a factor of D'. Thus, we have proved the lemma. ■

By Lemma 4.2.2 we know that, for every distinct complex cubic field with discriminant D, there exists a quadratic generator λ of this cubic field in the real quadratic field $Q(\sqrt{D'})$. Thus, if we wish to construct a generating polynomial of a complex cubic field having discriminant D, we need only find a suitable quadratic generator. Hence, the quadratic generators will be of considerable interest to us throughout this chapter. We next show that if λ is a quadratic generator, then the ideal $\mathbf{a} = (\lambda)$ is the cube of another ideal of $\mathbf{O}_K$.

Theorem 4.2.1. If $\mathbf{a}$ is an ideal of $\mathbf{O}_K$, $N(\mathbf{a}) = Q^3$, $\mathbf{a} = (u)\mathbf{h}$, where $\mathbf{h}$ is a primitive ideal of $\mathbf{O}_K$ and $u \mid D'$, then there exists a primitive ideal $\mathbf{b}$ of $\mathbf{O}_K$ such that $\mathbf{b}^3 = \mathbf{a}$.

Proof. Certainly, we can write $\mathbf{a}$ as

$$\mathbf{a} = \prod_{i=1}^{m} \mathbf{p}_i^{\alpha_i}$$

where $\mathbf{p}_i$ $(i = 1, 2, \ldots, m)$ are distinct prime ideals of $\mathbf{O}_K$, and α_i are positive integers. We also have

$$Q^3 = \prod_{i=1}^{m} N(\mathbf{p}_i)^{\alpha_i}.$$

Now, there are 3 possibilities for each $\mathbf{p}_i$; where p_i is used, here, to denote a rational prime.

Case 1. $\mathbf{p}_i = (p_i)$. In this case, we have $p_i \mid u$, and by Lemma 4.2.3 we get $p_i \mid D'$. Since D' is the discriminant of the field **K** and p_i is inert in **K**, this is impossible.

Case 2. $\mathbf{p}_i^2 = (p_i)$. In this case, we have $N(\mathbf{p}_i) = p_i$ and $p_i^{\alpha i} \parallel Q^3$. Hence, we get $3 \mid \alpha_i$. Further, $\alpha_i = 3$ as $\alpha_i \geq 6$ implies that $p_i^2 \mid u$, which is impossible.

Case 3. $\mathbf{p}_i\bar{\mathbf{p}}_i = (p_i)$. $(\mathbf{p}_i \neq \bar{\mathbf{p}}_i)$. In this case, no $\bar{\mathbf{p}}_j \neq \mathbf{p}_k$ for any $j, k \in \{1,..., m\}$. (Otherwise, we have $(p_i) \mid (u)\mathbf{h}$ and $p_i \mid u$. By Lemma 4.2.3 it follows that $p_i \mid D'$ and we get a contradiction.) Consequently, since $N(\mathbf{p}_i) = p_i$, we know that $p_i^{\alpha i} \parallel Q^3$, and therefore $3 \mid \alpha_i$.

By putting

$$\mathbf{b} = \prod_{i=1}^{m} p_i^{\alpha_i/3}$$

our result follows. We can further say that **b** must be a primitive ideal. ■

Before proceeding any further, we introduce a theorem of Hasse[Has30]. This theorem is of some importance in the proof of the second property of λ. We should point out that a different proof of Hasse's theorem is given in [LN83].

Theorem 4.2.2.(Hasse) Let D" be the discriminant of a cubic field. If d" denotes the discriminant of $Q(\sqrt{D''})$ we have

$$D'' = d''3^{2m}E^2,$$

where

(a) $E = p_1p_2...p_g$ is a square-free integer (p_i denotes a rational prime), $\gcd(E,3d'') = 1$ and $p_i \equiv \left(\frac{d''}{p_i}\right) \pmod 3$ for all i.

(b) $0 \leq m \leq 2$; if $3 \nmid d''$, then $m \neq 1$ and if $d'' \equiv 3 \pmod 9$, then $m \neq 2$. ■

We have seen that, if $\lambda \in \mathbf{O_K}$ is a quadratic generator of some cubic field, then $(\lambda) = \mathbf{b}^3$ for some primitive ideal $\mathbf{b}$ of $\mathbf{O_K}$. We now present a result which gives us some information about <u>any</u> $\lambda \in \mathbf{O_K}$ such that the ideal (λ) is a cube of a primitive ideal of $\mathbf{O_K}$.

Theorem 4.2.3. Let D be a fundamental discriminant of a cubic field. For $\mathbf{K} = Q(\sqrt{D'})$, let $\mathbf{b}$ be any primitive ideal of $\mathbf{O_K}$ such that $\mathbf{b}^3 = (\lambda)$ for some $\lambda \in \mathbf{O_K}$, and put $\lambda = \frac{A+B\sqrt{D'}}{2}$; then if $Q^3 = N(\lambda)$ and ξ is a root of

$$\xi^3 - 3Q\xi + A = 0,$$

then $Q(\xi)$ is either a cubic field of discriminant D or a cubic field of discriminant -27D'

Proof. Let D'' be the discriminant of $Q(\xi)$. The polynomial $x^3 - 3Qx + A$ has discriminant

$$\Delta = I(\xi)^2 D'' = -27D'B^2 = 4(3Q)^3 - 27A^2 \tag{4.2.4}$$

where $I(\xi)$ is the index of ξ. Since D' = -3D or -D/3, we have

$$\Delta = I(\xi)^2 D'' = -27D'B^2 = \begin{cases} 3^4 DB^2 & 3 \nmid D \\ 3^2 DB^2 & 3 \mid D. \end{cases} \tag{4.2.5}$$

If $\mathbf{a} = (\lambda)$, then $\mathbf{a} = (u)\mathbf{h}$, where $\mathbf{h}$ is a primitive ideal of $\mathbf{O_K}$ and $u \in \mathbf{Z}$. Let $\mathbf{p}$ denote a prime ideal. If p is any prime such that $p \mid u$, there are 3 possibilities and they are as follows:

Case 1. $(p) = \mathbf{p}$. In this case we have $\mathbf{p} \mid \mathbf{b}^3$. Hence, we have $\mathbf{p} \mid \mathbf{b}$ and this contradicts the fact that $\mathbf{b}$ is a primitive ideal.

Case 2. $(p) = \mathbf{p}\bar{\mathbf{p}}$ $(\mathbf{p} \neq \bar{\mathbf{p}})$. In this case, we have $\mathbf{p} \mid \mathbf{b}^3$ which implies that $\mathbf{p} \mid \mathbf{b}$ and $\bar{\mathbf{p}} \mid \mathbf{b}^3$ which implies that $\bar{\mathbf{p}} \mid \mathbf{b}$. Thus, we have $(p) \mid \mathbf{b}$ and this is a contradiction because $\mathbf{b}$ is a primitive ideal.

Case 3. $(p) = \mathbf{p}^2$. In this case, we have $p \mid D'$. Also, if $p^2 \mid u$, then $\mathbf{p}^4 \mid \mathbf{b}^3$. Thus, we have $\mathbf{p}^2 \mid \mathbf{b}$ and it follows that $(p) \mid \mathbf{b}$. Again, we have a contradiction.

Thus, as before, we find that $u \mid D'$ and u is square free. Furthermore, we can easily deduce that the condition $p^2 \mid Q$ and $p^3 \mid A$ is not satisfied for any prime p.

By Theorem 4.2.2 we know that

(4.2.6) $$D'' = D3^{2m}E^2$$

where $(E, 3D) = 1$, E is square-free integer and $0 \le m \le 2$.

Suppose $p > 3$. If $p^2 \mid D''$, then, by Theorem 2.4.1, we have

$$v_p(3Q) = v_p(Q) \ge v_p(A) \ge 1.$$

By (4.2.4), we get $p^2 \mid D'B^2$ and $p \mid B$ follows. Since $p \mid A$ and $p \mid B$, we get $p \mid u$ which implies $p \mid D'$. On the other hand, we have $p \mid E$ and $p \nmid D$ by (4.2.6). Hence, we get $p \nmid D'$ by (4.2.5) and this is a contradiction. If $p \parallel D''$, then $p \parallel D$ by (4.2.6). Similarly, if $p \parallel D$, then $p \parallel D''$. Also, if $p \nmid D''$, then $p \nmid D$. Again, if $p \nmid D$, then $p \nmid D''$. It follows that

$$p \parallel D'' \Leftrightarrow p \parallel D.$$

Suppose $p = 2$. If $2^3 \mid D$, then $2^3 \mid D''$ by (4.2.6). On the other hand, if $2^3 \mid D''$, then $2^3 \mid D$ by (4.2.6).

If $2^2 \parallel D$, then $2 \nmid E$ and $2^2 \parallel D''$ by (4.2.6); whereas, if $2^2 \parallel D''$, we have either $2^2 \parallel D$ or $2 \nmid D$. If $2 \nmid D$, then $2 \nmid D'$. It follows from Theorem 2.4.1 that $2 \mid A$ and $2 \mid Q$; hence, we have $2 \mid B$. Now, by (4.2.4), we have $A/2 \equiv B/2 \pmod 2$, which means that

$$\frac{(A/2) + (B/2)\sqrt{D'}}{2} \in \mathbf{O}_K.$$

Therefore we deduce that $2 \mid u$ and $2 \mid D'$, but this is impossible. Hence,

$$2^2 \parallel D'' \Leftrightarrow 2^2 \parallel D$$

and

$$2^3 \parallel D'' \Leftrightarrow 2^3 \parallel D.$$

Further, by (4.2.6), we see that $2 \nmid D$ if and only if $2 \nmid D''$. Thus we have shown that $E = 1$ and $D'' = D3^{2m}$, where $m = 0, 1$ or 2.

We are now left with the case of $p = 3$. If $3 \nmid D$, then we have $D' = -3D$. Also, we know $m \neq 1$, by Theorem 4.2.2. Thus, we have

$$D'' = \begin{cases} D & m = 0 \\ -27D' & m = 2. \end{cases}$$

If $3 \mid D$, then $D' = -D/3$ and $3 \nmid D'$. We have

$$D'' = -3^{2m+1}D'.$$

If $m = 2$, then $3^5 \mid D''$. We either get $3 \mid Q$ and $27 \mid A$ or by Theorem 2.4.1, $v_3(3Q) > v_3(A) \geq 1$. In either case, it follows that $3 \mid A$ and $3 \mid Q$. If $9 \mid A$, then $27 \mid D'B^2$, and hence $9 \mid B$ and $9 \mid u$. Since u is square-free, we get a contradiction. On the other hand, in the case where $3 \parallel A$ we get $3 \mid B$ and $3 \mid u$; it follows that $3 \mid D'$, which is impossible. Thus, we have shown that $m \neq 2$ when $3 \mid D$. Hence, we can only have

$$D'' = \begin{cases} D & m = 0 \\ -27D' & m = 1. \end{cases} \quad \blacksquare$$

We now summarize the above results. We have shown that for every cubic field of discriminant D, there exists a quadratic generator λ of this field. Also, for a given quadratic generator λ, we have $(\lambda) = \mathfrak{b}^3$, where $\mathfrak{b}$ is a primitive ideal of $\mathbf{O}_K$. Furthermore, if $\lambda = \frac{A+B\sqrt{D'}}{2}$ is any algebraic integer of $\mathbf{K}$ such that $\lambda \neq \tilde{\lambda}$ and $(\lambda) = \mathfrak{b}^3$, where $\mathfrak{b}$ is a primitive ideal, then the field $Q(\xi)$, where $Q^3 = N(\lambda)$ and ξ is a zero of

$$x^3 - 3Qx + A = 0,$$

has discriminant D or -27D'. We will say that this is the cubic field produced by λ. Thus, our objective will now be to find a quadratic generator for each distinct cubic field of discriminant D by searching for those values $\lambda \in \mathbf{O}_K$ such that $(\lambda) = \mathfrak{b}^3$. We will also want our values of λ to be small. (ie. $|A|$ and $|B|$ are small for $\lambda = \frac{A+B\sqrt{D'}}{2}$).

§4.3 Quadratic generators and ideal classes of order 3.

Suppose that λ_1 and λ_2 are quadratic generators of cubic fields of discriminant D and that $(\lambda_1) = \mathfrak{b}_1^3$ and $(\lambda_2) = \mathfrak{b}_2^3$, where $\mathfrak{b}_1$, $\mathfrak{b}_2$ are primitive ideals of $\mathbf{O}_K$ and $\mathfrak{b}_1 \neq \mathfrak{b}_2$. We have yet to discuss the possibility that two quadratic generators, λ_1 and λ_2, generate

the same complex cubic field. In this section, we present a theorem which shows that λ_1 and λ_2 generate two distinct complex cubic fields if $b_1 \not\sim \bar{b}_2$. Before we do so, we must present the following results.

Lemma 4.3.1. (Berwick[Ber25]) Let ξ be a zero of the polynomial

$$x^3 - 3Qx + A,$$

then if λ is as defined in Lemma 4.2.2, we have

$$\lambda(-Q\xi + \bar{\lambda})^3 - \bar{\lambda}(-Q\xi + \lambda)^3 = 0. \quad \blacksquare$$

Lemma 4.3.2. If ξ is a zero of an irreducible cubic polynomial

$$x^3 - 3Qx + A$$

and

$$\xi^3 - a\xi + b\xi - c = 0$$

then we can only have $a = 0$, $b = -3Q$ and $c = -A$. $\blacksquare$

Let $\mathbf{F}_1$ and $\mathbf{F}_2$ be two complex cubic fields with the same discriminant D. By Lemma 4.2.2, we know that there exists a quadratic generator λ_1 for $\mathbf{F}_1$ and a quadratic generator λ_2 for $\mathbf{F}_2$, where $\lambda_1, \lambda_2 \in \mathbf{O}_K$. We also know that $N(\lambda_i) = Q_i^3$ $(i = 1,2)$. Further, by Lemma 4.3.1, we know that

$$\lambda_1(-Q_1\xi_1 + \bar{\lambda}_1)^3 - \bar{\lambda}_1(-Q_1\xi_1 + \lambda_1)^3 = 0,$$

(4.3.1)
$$\lambda_2(-Q_2\xi_2 + \bar{\lambda}_2)^3 - \bar{\lambda}_2(-Q_2\xi_2 + \lambda_2)^3 = 0.$$

We can now prove

Theorem 4.3.1. (Berwick[Ber25]) $\mathbf{F}_1 = \mathbf{F}_2$ if and only if there exists $\beta \in \mathbf{K}$, such that

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \text{ or } \frac{\bar{\lambda}_2}{\lambda_2}.$$

Proof. Without loss of generality we may assume that ξ_1 and ξ_2 are both real. Put $\rho_i = -Q_i\xi_i$ and $\mathbf{F}_i = Q(\xi_i)$ $(i = 1,2)$. Clearly, $Q(\xi_1) = Q(\xi_2)$ if and only if $Q(\rho_1) = Q(\rho_2)$. Also, $Q(\rho_1) = Q(\rho_2)$ if and only if there exist p, q, r,s $\in \mathbf{Q}$ such that

$$\rho_1 = \frac{p\rho_2 + q}{r\rho_2 + s}.$$

If

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2},$$

then because

$$\frac{\lambda_1}{\bar{\lambda}_1} = \left(\frac{\rho_1 + \lambda_1}{\rho_1 + \bar{\lambda}_1}\right)^3 \qquad \text{(from (4.3.1))}$$

and

$$\frac{\lambda_2}{\bar{\lambda}_2} = \left(\frac{\rho_2 + \lambda_2}{\rho_2 + \bar{\lambda}_2}\right)^3 \qquad \text{(from (4.3.1))}$$

we get

(4.3.2) $$\frac{\rho_1 + \lambda_1}{\rho_1 + \bar{\lambda}_1} = \frac{\bar{\beta}}{\beta}\left(\frac{\rho_2 + \lambda_2}{\rho_2 + \bar{\lambda}_2}\right)$$

(since ρ_1, ρ_2, λ_1, λ_2 are all real).

We now write (4.3.2) as

$$1 + \frac{\lambda_1 - \bar{\lambda}_1}{\rho_1 + \bar{\lambda}_1} = \frac{\bar{\beta}}{\beta}\left(\frac{\rho_2 + \lambda_2}{\rho_2 + \bar{\lambda}_2}\right) .$$

If we solve for ρ_1, we get

$$\rho_1 = \frac{(\lambda_1\beta - \bar{\lambda}_1\bar{\beta})\rho_2 + \lambda_1\bar{\lambda}_2\beta - \bar{\lambda}_1\lambda_2\bar{\beta}}{\rho_2(\bar{\beta} - \beta) + \lambda_2\bar{\beta} - \bar{\lambda}_2\beta} .$$

Putting

$$r = 1,$$

$$p = \frac{\lambda_1\beta - \bar{\lambda}_1\bar{\beta}}{\bar{\beta} - \beta},$$

$$q = \frac{\lambda_1\bar{\lambda}_2\beta - \bar{\lambda}_1\lambda_2\bar{\beta}}{\bar{\beta} - \beta},$$

$$s = \frac{\lambda_2\bar{\beta} - \bar{\lambda}_2\beta}{\bar{\beta} - \beta},$$

we see that $\bar{p} = p$, $\bar{q} = q$, $\bar{s} = s$; hence $p, q, r, s \in \mathbf{Q}$. Therefore, we can conclude that $\mathbf{F}_1 = \mathbf{F}_2$. By using similar reasoning we can also obtain the same result when

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\bar{\lambda}_2}{\lambda_2}.$$

Now suppose that $\mathbf{F}_1 = \mathbf{F}_2$. We must have

$$\left(\frac{\rho_2 + \bar{\lambda}_2}{\rho_2 + \lambda_2}\right)^3 = \frac{\bar{\lambda}_2}{\lambda_2},$$

$$\left(\frac{\rho_1 + \bar{\lambda}_1}{\rho_1 + \lambda_1}\right)^3 = \frac{\bar{\lambda}_1}{\lambda_1},$$

and $\rho_1 = \dfrac{p\rho_2 + q}{r\rho_2 + s}$ where p, q, r, s $\in \mathbf{Q}$ and r,s not both zero.

Hence,

$$\frac{\bar{\lambda}_1}{\lambda_1} = \left(\frac{p\rho_2 + q + \bar{\lambda}_1 r\rho_2 + \bar{\lambda}_1 s}{p\rho_2 + q + \lambda_1 r\rho_2 + \lambda_1 s}\right)^3$$

$$= \left(\frac{p + \bar{\lambda}_1 r}{p + \lambda_1 r}\right)^3 \left(\frac{\rho_2 + \bar{\gamma}}{\rho_2 + \gamma}\right)^3,$$

where $\gamma = \dfrac{q + \lambda_1 s}{p + \lambda_1 r}$. Put $\mu = (p + \bar{\lambda}_1 r)^3 \lambda_1$ and we get

(4.3.3) $$\mu(\rho_2 + \bar{\gamma})^3 - \bar{\mu}(\rho_2 + \gamma)^3 = 0.$$

We can write (4.3.3) as

$$(\mu - \bar{\mu})\rho_2^3 + 3(\mu\bar{\gamma} - \bar{\mu}\gamma)\rho_2^2 + 3(\mu\bar{\gamma}^2 - \bar{\mu}\gamma^2)\rho_2 + (\mu\bar{\gamma}^3 - \bar{\mu}\gamma^3) = 0,$$

a cubic equation in ρ_2 with rational coefficients. If $\mu = \bar{\mu}$, then we must also have

$$\gamma\bar{\mu} = \bar{\gamma}\mu$$

and

$$\gamma = \bar{\gamma}\ .$$

Thus, we have $\lambda_1 = \bar{\lambda}_1$, which is a contradiction to the definition of a quadratic generator.

If $\mu \neq \bar{\mu}$, then put

$$a_1 = \frac{\mu\bar{\gamma} - \bar{\mu}\gamma}{\mu - \bar{\mu}},$$

$$a_2 = \frac{\bar{\gamma}^2\mu - \bar{\mu}\gamma^2}{\mu - \bar{\mu}},$$

$$a_3 = \frac{\mu\bar{\gamma}^3 - \bar{\mu}\gamma^3}{\mu - \bar{\mu}}.$$

We see that $a_1, a_2, a_3 \in \mathbf{Q}$. Since ξ_2 is a zero of the irreducible cubic polynomial

$$x^3 - 3Q_2x + A_2$$

and by definition $\rho_2 = -Q_2\xi_2$, we can see that ρ_2 is a zero of the irreducible cubic polynomial

$$x^3 - 3Q_2^3x - A_2Q_2^3.$$

Hence, by Lemma 4.3.2 we have

$$a_1 = 0,\ a_2 = -Q_2^3,\ a_3 = -A_2Q_2^3.$$

Since $\frac{\mu}{\bar{\mu}} = \frac{\gamma}{\bar{\gamma}}$, we have

$$\begin{aligned} -Q_2^3 = -a_2 &= \frac{\bar{\gamma}^2(\mu / \bar{\mu}) - \gamma^2}{(\mu / \bar{\mu}) - 1} \\ &= \frac{\bar{\gamma}^2(\gamma / \bar{\gamma}) - \gamma^2}{(\gamma / \bar{\gamma}) - 1} \\ &= -\gamma\bar{\gamma}. \end{aligned}$$

Thus, we get $Q_2^3 = \gamma\bar{\gamma}$. Further, we know

$$\begin{aligned} -A_2Q_2^3 = a_3 &= \frac{(\mu / \bar{\mu})\bar{\gamma}^3 - \gamma^3}{(\mu / \bar{\mu}) - 1} \\ &= -\gamma\bar{\gamma}(\gamma + \bar{\gamma}). \end{aligned}$$

Since $Q_2^3 = \gamma\bar{\gamma}$, we get $A_2 = \gamma + \bar{\gamma}$. We can now conclude that $\gamma = \lambda_2$ or $\bar{\lambda}_2$, which implies that

$$\left(\frac{\rho_2 + \bar{\gamma}}{\rho_2 + \gamma}\right)^3 = \begin{cases} \left(\frac{\rho_2 + \bar{\lambda}_2}{\rho_2 + \lambda_2}\right)^3 = \frac{\bar{\lambda}_2}{\lambda_2} & \text{or} \\ \left(\frac{\rho_2 + \bar{\lambda}_2}{\rho_2 + \lambda_2}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \end{cases}.$$

Our result follows, on putting $\beta = p + \lambda_1 r$. ■

Corollary 4.3.1. Let $(\lambda_1) = b_1^3$ and $(\lambda_2) = b_2^3$, where b_1, b_2 are primitive ideals of $\mathbf{O_K}$. If $b_1 \neq b_2$, $\bar{b}_2$, then $\mathbf{F_1} \neq \mathbf{F_2}$.

Proof. From Theorem 4.3.1, we know that if $\mathbf{F_1} = \mathbf{F_2}$ then there exists some $\beta \in \mathbf{K}$ such that

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \text{ or } \frac{\bar{\lambda}_2}{\lambda_2} \ .$$

We may assume with no loss of generality that $\beta \in \mathbf{O_K}$.If

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\bar{\lambda}_2}{\lambda_2} \ ,$$

then $b_1^3 b_2^3(\beta^3) = \bar{b}_1^3 \bar{b}_2^3(\bar{\beta}^3)$. It follows that we have $b_1 b_2(\beta) = \bar{b}_1 \bar{b}_2(\bar{\beta})$ and $b_1 \sim \bar{b}_2$. Similarly, we can show that if

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \ ,$$

then $b_1 \sim b_2$. ■

If r is the 3-rank of $\mathbf{K} = \mathbf{Q}(\sqrt{D'})$, then $\mathbf{K}$ processes precisely $3^r - 1$ non-principal ideal classes of order 3. By using the above results, we can eliminate half of those ideal classes since they are the conjugate ideal classes of the other half. Hence, there are exactly $1 + \frac{(3^r - 1)}{2}$ ideal classes, counting the principal class, which are required in the generation of distinct complex cubic fields. In the next section we discuss the number of distinct cubic fields that can be generated in each of the distinct, non-conjugate ideal classes of order 3 and in the principal ideal class.

§4.4 Number of distinct cubic fields from each ideal class of order 1 or 3.

We now want to determine the number of non-isomorphic cubic fields that can be generated from each of the ideal classes of order 1 or 3, excluding the conjugate ideal classes. We divide these ideal classes into two categories: the principal ideal class and the

non-principal ideal classes. In order to present our theorem, we introduce the following lemmata.

Lemma 4.4.1. Let ε_0 be the fundamental unit of **K**. If $b_1^3 = (\lambda_1)$, $b_2^3 = (\lambda_2)$ and $b_2 \sim b_1$, then there exist $\mu \in \mathbf{K}$ and $i \in \mathbf{Z}$ such that $0 \le i \le 2$ and $\lambda_1 = \mu^3 \varepsilon_0^i \lambda_2$. (For the rest of this chapter and the following chapter, we use ε_0 to denote the fundamental unit of the real quadratic field **K**.)

Proof. Since $b_1 \sim b_2$, there exist non-zero $\alpha, \beta \in \mathbf{O_K}$ such that

$$(\alpha)b_1 = (\beta)b_2.$$

By raising both sides to the 3rd power, we get

$$(\alpha^3)b_1^3 = (\beta^3)b_2^3.$$

Consequently, we have

$$\alpha^3\lambda_1 = \eta\beta^3\lambda_2,$$

where η is some unit of **K**. Since $\eta = \pm\varepsilon_0^n$ for some $n \in \mathbf{Z}$ and $n = 3j + i$ ($0 \le i \le 2$, and $n,i,j \in \mathbf{Z}$), we have

$$\lambda_1 = ((\beta / \alpha)\varepsilon_0^j)^3 \varepsilon_0^i \lambda_2.$$

We can write $\mu = ((\beta / \alpha)\varepsilon_0^j)^3$, and the result follows. ■

Lemma 4.4.2. If $\dfrac{\varepsilon_0^i}{\bar{\varepsilon}_0^i} = \left(\dfrac{\nu}{\bar{\nu}}\right)^3$ where $\nu \in \mathbf{K}$, then $3 \mid i$.

Proof. Without loss of generality, we may assume $\nu \in \mathbf{Z} + \sqrt{D}\,\mathbf{Z}$. Put $\gamma = \dfrac{\varepsilon_0^i}{\nu^3}$. Since

$$\frac{\varepsilon_0^i}{\bar{\varepsilon}_0^i} = \left(\frac{\nu}{\bar{\nu}}\right)^3,$$

we have $\gamma = \bar{\gamma}$; hence $\bar{\gamma} \in \mathbf{Q}$. Now

$$N(\gamma)N(\nu)^3 = \pm 1,$$

so we have

$$\gamma^2 = \frac{\pm 1}{N(\nu)^3}.$$

Since $N(\nu) \in \mathbf{Z}$, we have $|N(\nu)| = t^2$, where $t \in \mathbf{Z}$ and $\gamma = 1 / t^3$. Put $\nu = a + b\sqrt{D'}$ where $a, b \in \mathbf{Z}$. Then $\varepsilon_0^i = (\frac{\nu}{t})^3$ and

$$t^3 \mid 2(a^3 + 3ab^2D').$$

If $|t| > 1$, let $p^\alpha \| t$. If $p^\beta \| 2a$ and $\beta < \alpha$, then

$$a^2 + 3b^2D' \equiv 0 \pmod{p^{3\alpha-\beta}}.$$

But $a^2 - b^2D' \equiv 0 \pmod{p^{2\alpha}}$ and $\beta < \alpha$; hence

$$4b^2D' \equiv 0 \pmod{p^{2\alpha}}.$$

If $p \neq 2$, then $p^{2\alpha} \mid b^2D'$, and $p^{2\alpha} \mid a^2$. Hence, we have $p^\alpha \mid a$ and we get a contradiction. If $p = 2$, then $p^{2\alpha-2} \mid b^2D'$, and we see that $p^{2\alpha-2} \mid a^2$. Consequently, we have $p^{\alpha-1} \mid a$ and a contradiction. Thus, we have $t \mid 2a$ and $| \nu / t | \in \mathbf{O_K}$. Since $\varepsilon_0^i = (\nu / t)^3$, we can conclude that $3 \mid i$. ■

Lemma 4.4.3. Under the conditions of Lemma 4.4.1, if $\mathfrak{b}_1$ is not a principal ideal, λ_1 and λ_2 produce the same cubic field if and only if $i = 0$.

Proof. By Lemma 4.4.1, we have

$$\frac{\lambda_1}{\bar{\lambda}_1} = \frac{\mu^3\varepsilon_0^i\lambda_2}{\bar{\mu}^3\bar{\varepsilon}_0^i\bar{\lambda}_2} .$$

Thus, if $3 \mid i$, we see that λ_1 and λ_2 produce the same cubic field by Theorem 4.3.1. Also, if λ_1 and λ_2 produce the same cubic field, then for some $\beta \in \mathbf{K}$, we get

$$\frac{\lambda_1}{\bar{\lambda}_1}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \text{ or } \frac{\bar{\lambda}_2}{\lambda_2} \quad ;$$

hence,

$$\frac{\mu^3\varepsilon_0^i\lambda_2}{\bar{\mu}^3\bar{\varepsilon}_0^i\bar{\lambda}_2}\left(\frac{\beta}{\bar{\beta}}\right)^3 = \frac{\lambda_2}{\bar{\lambda}_2} \text{ or } \frac{\bar{\lambda}_2}{\lambda_2} .$$

If

$$\frac{(\mu\beta)^3\lambda_2}{(\bar{\mu}\bar{\beta})^3\bar{\lambda}_2} = \frac{\bar{\varepsilon}_0^i\lambda_2}{\varepsilon_0^i\bar{\lambda}_2},$$

then

$$\frac{\varepsilon_0^{\,i}}{\bar{\varepsilon}_0^{\,i}} = \frac{\nu^3}{\bar{\nu}^3}$$

where $\nu = \bar{\mu}\,\bar{\beta}$ and $\nu \in \mathbf{K}$. Hence, by Lemma 4.4.2, $3 \mid i$.

On the other hand, if

$$\frac{(\mu\beta)^3\lambda_2}{(\bar{\mu}\bar{\beta})^3\bar{\lambda}_2} = \frac{\bar{\varepsilon}_0^{\,i}\bar{\lambda}_2}{\varepsilon_0^{\,i}\lambda_2} \quad ,$$

then

$$\bar{\lambda}_2^{\,2}(\bar{\mu}\bar{\beta})^3\bar{\varepsilon}_0^{\,i} = \varepsilon_0^{\,i}\lambda_2^{\,2}(\mu\beta)^3$$

or

$$\left(\frac{\lambda_2}{\bar{\lambda}_2}\right)^2 = \left(\frac{\bar{\varepsilon}_0}{\varepsilon_0}\right)^i \left(\frac{\bar{\mu}\bar{\beta}}{\mu\beta}\right)^3 .$$

Putting $\rho = \lambda_2^{\,2} / (\bar{\varepsilon}_0^{\,i}(\bar{\mu}\bar{\beta})^3)$, we have $\rho = \bar{\rho}$; hence $\rho \in \mathbf{Q}$. Since $N(\lambda_2)$ is the cube of a rational integer, then ρ is the cube of a rational, i.e. $\rho = t^3$ and $t \in \mathbf{Q}$. Putting $\gamma = \bar{\mu}\bar{\beta}t \in \mathbf{K}$, we see that $\gamma^3 = \lambda_2^{\,2} / \varepsilon_0^{\,i} \in \mathbf{O_K}$. By using the reasoning employed in Lemma 4.4.3, we get $\gamma \in \mathbf{O_K}$. Now

$$(\lambda_2)^2 = (\gamma)^3.$$

and $(\lambda_2) = \mathbf{b}_2^{\,3}$, so this gives $\mathbf{b}_2^{\,2} = (\gamma)$. Since $\mathbf{b}_2^{\,2}$ and $\mathbf{b}_2^{\,3}$ are principal ideals, we know that $\mathbf{b}_2$ must also be a principal ideal and we get a contradiction. By combining the above results, we have proved Lemma 4.4.3. ■

Lemma 4.4.4. If $\lambda = \nu^3$, where $\nu \in \mathbf{O_K}$, then λ does not produce a cubic field.

Proof. Let

$$\lambda = \frac{A + B\sqrt{D'}}{2} = \left(\frac{a + b\sqrt{D'}}{2}\right)^3 .$$

Put $Q^3 = N(\lambda) = N(\nu^3)$. We have

$$Q = \frac{a^2 - b^2D'}{4}$$

and

$$4A = a^3 + 3ab^2D'.$$

Therefore, we have

$$x^3 - 3Qx + A = (x + a) (x^2 - ax + (a^2 + 3b^2D') / 4) .$$

Since this is a reducible polynomial, λ cannot produce a cubic field. ■

Lemma 4.4.5. Only one cubic field can be produced from all λ such that $\mathbf{b}^3 = (\lambda)$, where $\mathbf{b}$ is a principal ideal.

Proof. Suppose λ_1 and λ_2 generate distinct fields and $(\lambda_1) = \mathbf{b}_1^3$, $(\lambda_2) = \mathbf{b}_2^3$, where $\mathbf{b}_1$ and $\mathbf{b}_2$ are principal ideals. It follows that

$$\lambda_1 = \eta_1\mu_1^3 = \varepsilon_0^{i1}\nu_1^3 ,$$

where $\nu_1, \mu_1 \in \mathbf{O}_K$ and $0 \le i_1 \le 2$. Similarly, we also have

$$\lambda_2 = \eta_2\mu_2^3 = \varepsilon_0^{i2}\nu_2^3 ,$$

where $\nu_2, \mu_2 \in \mathbf{O}_K$ and $0 \le i_2 \le 2$. By Lemma 4.4.4, if $i_j = 0$, where $j \in \{1,2\}$, then λ_j does not produce a cubic field. For this reason, $i_1 , i_2 \in \{1,2\}$. We now have

$$\frac{\lambda_1\lambda_2}{\bar{\lambda}_1\bar{\lambda}_2} = \frac{\varepsilon_0^{i1 + i2}}{\bar{\varepsilon}_0^{i1 + i2}}\left(\frac{\nu_1\nu_2}{\bar{\nu}_1\bar{\nu}_2}\right)^3 .$$

If $i_1 + i_2 \equiv 0 \pmod 3$, then the fields generated by λ_1 and λ_2 are identical by Theorem 4.3.1. Also,

$$\frac{\lambda_1\bar{\lambda}_2}{\bar{\lambda}_1\lambda_2} = \frac{\varepsilon_0^{i1 - i2}}{\bar{\varepsilon}_0^{i1 - i2}}\left(\frac{\nu_1\bar{\nu}_2}{\bar{\nu}_1\nu_2}\right)^3 ;$$

thus, if $i_1 - i_2 \equiv 0 \pmod 3$, then the fields generated by λ_1 and λ_2 are identical. Therefore, if λ_1, λ_2 generate different fields, we have $i_1 \not\equiv i_2$ or $i_2 \not\equiv -i_2 \pmod 3$. Since $3 \nmid i_1$ or i_2, this is not possible, hence, we can conclude that there is only one cubic field produced from all values of λ such that $\mathbf{b}^3 = (\lambda)$ and $\mathbf{b}$ is a principal ideal. ■

By using the above lemmata, we have shown that the following theorem holds.

Theorem 4.4.1. Let $\mathbf{C}$ be any ideal class such that $\mathbf{C}^3 = \mathbf{PI}$, where $\mathbf{PI}$ denotes the principal ideal class. If $\mathbf{C} = \mathbf{PI}$, all the values of $\lambda \in \mathbf{O}_K$ such that $\lambda \neq \bar{\lambda}$ and $\mathbf{b}^3 = (\lambda)$ for primitive $\mathbf{b} \in \mathbf{C}$ produce the same cubic field. Further, if $\mathbf{C} \neq \mathbf{PI}$, all the values of $\lambda \in \mathbf{O}_K$ such that $\lambda \neq \bar{\lambda}$ and $\mathbf{b}^3 = (\lambda)$ for primitive $\mathbf{b} \in \mathbf{C}$ produce only 3 distinct cubic fields. ■

Note that, in the case where $\mathbf{b} \notin \mathbf{PI}$ and $\mathbf{b}^3 = (\lambda)$, then λ_i (i = 0,1,2) produce the 3 distinct cubic fields which can be produced where

$$\lambda_i = \mu^3 \varepsilon_0^{\,i} \lambda \quad (i = 0,1,2).$$

For any $\mu \in \mathbf{K}$ such that λ_i (i = 0,1,2).$\in \mathbf{O_K}$. Of course, λ and $\tilde{\lambda}$ always generate the same field.

Suppose that the 3-rank of the class group in $Q(\sqrt{D'})$ is r' and the 3-rank of $Q(\sqrt{D})$ is r. By Hasse's theorem, there are exactly $\frac{(3^r - 1)}{2}$ complex cubic fields. On the other hand, by Theorem 4.2.1 we know that we can generate precisely

$$1 + \frac{3(3^{r'} - 1)}{2} = \frac{3^{r'+1} - 1}{2}$$

distinct cubic fields. For this reason, if r = r'+1 (escalatory case), then all the fields generated by the CUFFQI algorithm are distinct and have discriminant D. None of the fields generated in this case can have discriminant -27D'. If r = r' (non-escalatory case), then we get all the cubic fields of discriminant D and an additional $3^{r'}$ cubic fields of discriminant -27D'. In this case, a criterion for determining whether the generating polynomial has field discriminant D or -27D' is needed. By using Theorem 2.4.1, we have a simple such criterion. In the case where 3 | D, the generating polynomial x^3-3Qx+A has field discriminant D if and only if one the following conditions holds:

i) $3 \nmid Q$, $9 \mid A$,

ii) $Q \not\equiv 1 \pmod 3$, $A^2 \equiv 3Q+1 \pmod 9$,

iii) $Q \equiv 1 \pmod 3$, $A^2 \equiv 3Q+1 \pmod{27}$.

In the case where $3 \nmid D$, the generating polynomial x^3-3Qx+A has field discriminant D if and only if

$$Q \equiv 1 \pmod 3 \text{ and } A^2 \equiv 3Q+1 \pmod{27}.$$

Chapter 5.
Computational Aspects of CUFFQI

§5.1. Introduction.

We have seen in the preceding chapter that, if we want to find all of the non-isomorphic cubic fields which have a given fundamental discriminant D, we need only find their quadratic generators. For each given ideal class of order 3 (excluding conjugate classes), only 3 of the generators need be computed, and for the principal class only one need be found. Thus the problem now becomes one of determining each of the ideal classes of order 3 and then, in each of these classes, determining 3 quadratic generators $\lambda_1, \lambda_2, \lambda_3$ such that $(\lambda_i) = \mathbf{b}_i^3$, where $\mathbf{b}_i$ is some ideal in the class, λ_i is not large, and $\lambda_i / \lambda_j \neq \mu^3$ for some $\mu \in \mathbf{K}$ when $i \neq j$ $(i,j \in 0, 1, 2)$. We must also determine some small λ such that $(\lambda) = \mathbf{b}^3$, and $\mathbf{b}$ is principal.

In this chapter, we show how the CUFFQI algorithm determines these λ values. We discuss an algorithm to find an ideal $\mathbf{a}$ such that $\mathbf{a}^3 = (\lambda)$ and λ is small. We then present an algorithm to find this small λ when only $\mathbf{a}$ is given. In addition, the complexity of the CUFFQI algorithm is analyzed. The results of running the CUFFQI algorithm on a main frame computer for certain D, where it is known that $\mathbf{Q}(\sqrt{D})$ has a large 3-rank of its class group, including 3 fields with a 3-rank of 6 given in Quer[Que87], are also presented. Since this algorithm attempts to find a small λ, we also discuss the bounds on the coefficients and the index of a generating polynomial which the algorithm produces.

§5.2. Continued fractions, ideals and infrastructure.

In order to implement the CUFFQI algorithm, we require a number of results concerning the continued fraction expansion of an expression of the form $(P + \sqrt{D'})/Q$, where $P, Q, D' \in \mathbf{Z}$ and $D'(>0)$ is not a perfect square. These results are well known and are presented here for the convenience of the reader.

As in Stephens and Williams[SW88], we let $P_0, Q_0 \in \mathbf{Z}$ be such that $Q_0 \mid D' - P_0^2$ and put

$$\phi = \phi_0 = (P_0 + \sqrt{D'}) / Q_0.$$

By putting $q_0 = [\phi_0]^*$ and using the well-known formulae

$$P_{k+1} = q_k Q_k - P_k,$$

$$Q_{k+1} = (D' - P^2_{k+1}) / Q_k,$$

$$q_{k+1} = [(P_{k+1} + \sqrt{D'}) / Q_{k+1}] \geq 1 \quad (k = 0,1,2,\ldots), \tag{5.2.1}$$

we can expand ϕ into the simple continued fraction

$$\phi = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots \cfrac{1}{q_{m-1} + \cfrac{1}{\phi_m}}}} \tag{5.2.2}$$

where $\phi_m = (P_m + \sqrt{D'}) / Q_m$. Here, we call the above formulae the Forward Single-Step Continued Fraction Algorithm. We now proceed to introduce the Backward Single-Step Continued Fraction Algorithm for a given ϕ_{k+1}. We first require the following lemma.

Lemma 5.2.1.(Williams and Wunderlich[WW87]) If, in the continued fraction of $\phi = \phi_0$, we have $-1 < \bar{\phi}_1 < 0$, then

$$q_k = [(P_{k+1} + \sqrt{D'}) / Q_k]$$

for all $k \geq 1$. ■

Hence, if $-1 < \bar{\phi}_1 < 0$, then, for a given pair (P_{k+1},Q_{k+1}), we can find P_k and Q_k by using the following formulae:

$$Q_k = (D' - P^2_{k+1}) / Q_{k+1},$$

$$q_k = [(P_{k+1} + \sqrt{D'}) / Q_k],$$

$$P_k = q_k Q_k - P_{k+1}. \tag{5.2.3}$$

If we put $\theta_1 = 1$ and define

---

*We use $[\alpha]$ to denote that integer such that $\alpha - 1 < [\alpha] \leq \alpha$.

(5.2.4) $$\theta_n^{-1} = \prod_{i=1}^{n-1} \phi_i \ (> 1),$$

then

(5.2.5) $$\theta_n \bar{\theta}_n = (-1)^{n-1} Q_{n-1} / Q_0$$

and

(5.2.6) $$\theta_n = (-1)^{n-1}(A_{n-2} - \phi B_{n-2}) = (-1)^{n-1}(G_{n-2} - \sqrt{D'} B_{n-2}) / Q_0$$

where

(5.2.7) $$G_k = Q_0 A_k - P_0 B_k = P_{k+1} B_k + Q_{k+1} B_{k-1}.$$

Here $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$, and

(5.2.8) $$A_{i+1} = q_{i+1} A_i + A_{i-1},\ B_{i+1} = q_{i+1} B_i + B_{i-1} \quad (i = -1,0,1,2,\ldots).$$

If we put $\psi_i = |(\bar{\phi}_i)^{-1}|$ and $\rho_n = |\bar{\theta}_n|$, then by (5.2.1)

$$\psi_i = |(P_i + \sqrt{D'}) / Q_{i-1}|$$

and

(5.2.9) $$\rho_n = \prod_{i=1}^{n-1} \psi_i = \frac{Q_{n-1}}{Q_0} \prod_{i=1}^{n-1} \phi_i = \frac{Q_{n-1}}{(\sigma \theta_n)}.$$

Also, by (5.2.6) and (5.2.7) we have

$$\rho_n = | (G_{n-2} + B_{n-2}\sqrt{D'}) / Q_0 |$$
$$= | (B_{n-2} (P_{n-1} + \sqrt{D'}) + Q_{n-1} B_{n-3}) / Q_0 |.$$

It is known that there is a connection between the continued fraction expansion of $(P + \sqrt{D'}) / Q$ and the ideals in the real quadratic field $\mathbf{Q}(\sqrt{D'})$. Here, we briefly describe some of the results which are relevant to our work. A detailed description of these theorems, proofs and results is given in [WW87]. We first give an important definition.

Definition 5.2.1. We say that $\mathbf{j}$ is a reduced ideal in $\mathbf{O_K}$ if $\mathbf{j}$ is primitive and there does not exist any nonzero $\alpha \in \mathbf{j}$ such that both $|\alpha| < N(\mathbf{j})$ and $|\bar{\alpha}| < N(\mathbf{j})$ hold.

With the above definition, we are now able to present some of the well-known properties of reduced ideals.

Theorem 5.2.1. Let $\mathfrak{j}$ be a primitive ideal; then $\mathfrak{j}$ is a reduced ideal in $\mathbf{O}_K$ if and only if there exists some $\beta \in \mathfrak{j}$ such that $\mathfrak{j} = [N(\mathfrak{j}), \beta]$, $\beta > N(\mathfrak{j})$, and $-N(\mathfrak{j}) < \overline{\beta} < 0$. ■

Corollary 5.2.1. If $\mathfrak{j}$ is a reduced ideal in $\mathbf{O}_K$, then $N(\mathfrak{j}) < \sqrt{D'}$. ■

Theorem 5.2.2. If $\mathfrak{j}$ is a primitive ideal in $\mathbf{O}_K$ and $N(\mathfrak{j}) < \sqrt{D'}/2$, then $\mathfrak{j}$ is a reduced ideal in $\mathbf{O}_K$. ■

If $\mathfrak{j}$ is any reduced ideal in $\mathbf{O}_K$, then $\mathfrak{j} = [N(\mathfrak{j}), c + \omega]$, where $c \in \mathbf{Z}$ and $\omega = (\sigma - 1 + \sqrt{D'})/\sigma$, and we may certainly assume that $0 < c < N(\mathfrak{j})$. Since $N(\mathfrak{j}) < \sqrt{D'}$, we see that there can only be a finite number of reduced ideals in $\mathbf{O}_K$. We further point out that, if $\mathfrak{j}$ is a reduced ideal, then the conjugate of ideal $\mathfrak{j}$ is also a reduced ideal.

Now, given an ideal $\mathfrak{j}$ $(= \mathfrak{j}_1)$, we can use the Forward Single-Step Continued Fraction Algorithm, as given above, (applied to $\beta / N(\mathfrak{j}_1) = (P_0 + \sqrt{D'}) / Q_0$) to produce a sequence of ideals

$$\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \ldots, \mathfrak{j}_n$$

such that

$$\mathfrak{j}_k = [Q_{k-1} / \sigma, (P_{k-1} + \sqrt{D'}) / \sigma] \quad (k = 1,2,3,\ldots,n),$$

$$(N(\mathfrak{j}_1)\theta_s)\mathfrak{j}_s = (N(\mathfrak{j}_s))\mathfrak{j}_1$$

where $1 < s \leq n$. Also, $\rho_s = \theta_s^{-1} N(\mathfrak{j}_s)$, $\rho_s \in \mathbf{O}_K$ $(\rho_s > 1)$ and we have

$$(N(\mathfrak{j}_1))\mathfrak{j}_s = (\rho_s)\mathfrak{j}_1.$$

We mention further (Theorem 4.2 in [WW87]) that, for some $m = O(\log N(\mathfrak{j}))$, we get $\mathfrak{j}_n$ reduced for any $n \geq m$.

Theorem 5.2.3. ([WW87]) If, by developing $\phi_0 = (P_0 + \sqrt{D'}) / Q_0$ into a continued fraction, we find the least m (≥ 1) such that $0 < Q_{m-1} < \sqrt{D'}$ then $\mathfrak{j}_m$ $(= [Q_{m-1}/\sigma, (P_{m-1}+\sqrt{D'})/\sigma])$ is a reduced ideal in $\mathbf{O}_K$ and

$$1 < \theta_m^{-1} < 2Q_0 / Q_{m-1} = 2N(\mathfrak{j}_1) / N(\mathfrak{j}_m)$$

or

$$N(\mathfrak{j}_m) < \rho_m < 2N(\mathfrak{j}_1). \quad ■$$

Let $\mathbf{j}_1$ (= $[Q_0 / \sigma , (P_0 + \sqrt{D'}) / \sigma]$) be any reduced ideal. The Forward Single-Step Continued Fraction Algorithm applied to $\mathbf{j}_1$ ($\phi_0 = (P_0 + \sqrt{D'}) / Q_0$) yields a purely periodic sequence of all the reduced ideals $\sim \mathbf{j}_1$, with a minimal $p \in \mathbf{Z}^+$ such that $\mathbf{j}_{p+1} = \mathbf{j}_1$ and $\theta_{p+1} = N(\mathbf{j}_1)\varepsilon_0$ (ε_0 is the fundamental unit of $Q(\sqrt{D'})$, due to the following results.

Theorem 5.2.4. If $\mathbf{j} = \mathbf{j}_1$ is a reduced ideal in $\mathbf{O}_K$, then $-1 < \bar{\phi}_1 < 0$. ■

Corollary 5.2.2. If $\mathbf{j}_1$ is a reduced ideal in $\mathbf{O}_K$, then so is $\mathbf{j}_m$ for any $m \geq 1$. ■

We define the <u>distance</u> between two equivalent reduced ideals $\mathbf{j}_n$ and $\mathbf{j}_1$ ($\mathbf{j}_n \sim \mathbf{j}_1$) as

$$\delta_n = \delta(\mathbf{j}_n , \mathbf{j}_1) = \log (\sqrt{\rho_n \bar{\rho}_n}) = \log (\rho_n / \sqrt{N(\mathbf{j}_1)N(\mathbf{j}_n)}).$$

We note that, since $P_n + \sqrt{D'} > \sqrt{Q_n Q_{n-1}}$, we have $\delta(\mathbf{j}_{n+1} , \mathbf{j}_1) > \delta(\mathbf{j}_n , \mathbf{j}_1) > 0$ for any $n > 1$, and $\delta(\mathbf{j}_n , \mathbf{j}_1) = 0$ if and only if $n = 1$. The notion of distance was first discussed by Shanks[Sha73] and later refined by Lenstra[Len82] and Schoof[Sch83]. In this chapter, we use Lenstra's distance definition. Notice that distance is only defined between ideals of $\mathbf{O}_K$ that are equivalent and reduced. Furthermore,

$$\delta(\mathbf{j}_{p+1} , \mathbf{j}_1) = \log \varepsilon_0 = R,$$

where $\mathbf{j}_{p+1}$ is defined as above and R is the regulator of $Q(\sqrt{D'})$. We also note that

$$\delta(\bar{\mathbf{j}}_n , \mathbf{j}_1) = R - \delta(\mathbf{j}_n , \mathbf{j}_1).$$

Let $\mathbf{i}_1$ (= (1)), $\mathbf{i}_2, \mathbf{i}_3, \ldots , \mathbf{i}_n, \ldots$ be the sequence of reduced principal ideals in $\mathbf{O}_K$ and suppose that $\mathbf{j}_1$ is any reduced ideal in $\mathbf{O}_K$. Let

$$(u)\mathbf{h} = \mathbf{j}_1\mathbf{i}_n,$$

where $u \in \mathbf{Z}$ and $\mathbf{h}$ is a primitive ideal in $\mathbf{O}_K$. If $\mathbf{j}_1$ and $\mathbf{i}_n$ are known, then the algorithm of Shanks as given in Section 6 of [MW87] can be used to find u and $\mathbf{h}$. Also,

$$\mathbf{h} \sim \mathbf{j}_1.$$

Let $\mathbf{h}_m$ be a reduced ideal equivalent to $\mathbf{h} = \mathbf{h}_1$, which we find by using the Forward Single-Step Continued Fraction Algorithm on $\mathbf{h}_1$, with m defined as in Theorem 5.2.3.

Since $\mathbf{h}_m \sim \mathbf{j}_1$, and $\mathbf{h}_m$ is reduced, we have $\mathbf{h}_m = \mathbf{j}_t$ for some t. Hence, we now present a modified version of a theorem of Williams and Wunderlich[WW87].

Theorem 5.2.5 If $\delta_s = \delta(\mathbf{j}_s, \mathbf{j}_1)$, $\delta_n = \delta(\mathbf{i}_n, \mathbf{i}_1)$, $\delta_t = \delta(\mathbf{j}_t, \mathbf{j}_1)$, then

$$\delta_t \equiv \delta_s + \delta_n + \eta \pmod{R}$$

where $|\eta| < \log 2D'$.

Proof. Let $\mathbf{i}_n = (\rho_n)$, $(N(\mathbf{j}_1))\mathbf{j}_s = (\rho'_s)\mathbf{j}_1$, $(N(\mathbf{h}_1))\mathbf{h}_m = (\rho''_m)\mathbf{h}_1$. Since $(u)\mathbf{h}_1 = \mathbf{j}_s\mathbf{i}_n$, we get $u^2N(\mathbf{h}_1) = N(\mathbf{j}_s)\,N(\mathbf{i}_n)$.

Also,

$$(N(\mathbf{j}_s)N(\mathbf{i}_n))\mathbf{h}_m = (\rho''_m u)\mathbf{j}_s\mathbf{i}_n\ ;$$

hence,

$$(N(\mathbf{j}_s)N(\mathbf{j}_1)N(\mathbf{i}_n))\mathbf{h}_m = (\rho_n\rho'_s\rho''_m u)\mathbf{j}_1,$$

and

$$(N(\mathbf{j}_1))\mathbf{h}_m = \left(\frac{\rho_n\rho'_s\rho''_m u}{N(\mathbf{j}_s)N(\mathbf{i}_n)}\right)\mathbf{j}_1.$$

Also,

$$\delta_t = \delta(\mathbf{h}_m, \mathbf{j}_1) = \log\left(\frac{\varepsilon\rho_n\rho'_s\rho''_m u}{N(\mathbf{j}_s)N(\mathbf{i}_n)\sqrt{N(\mathbf{j}_1)N(\mathbf{h}_m)}}\right)$$

$$= \log\left(\frac{\rho'_s}{\sqrt{N(\mathbf{j}_1)N(\mathbf{j}_s)}}\right) + \log\left(\frac{\rho_n}{\sqrt{N(\mathbf{i}_n)}}\right) + \log\left(\frac{\rho''_m u}{\sqrt{N(\mathbf{j}_s)N(\mathbf{i}_n)N(\mathbf{h}_m)}}\right) + \log\varepsilon.$$

where ε is a unit of $\mathbf{K}$. Putting

$$\eta = \log\left(\frac{\rho''_m u}{\sqrt{N(\mathbf{j}_s)N(\mathbf{i}_n)N(\mathbf{h}_m)}}\right),$$

we have

$$\delta_t \equiv \delta(\mathbf{j}_s, \mathbf{j}_1) + \delta(\mathbf{i}_n, \mathbf{i}_1) + \eta \pmod{R}.$$

By Theorem 5.2.3, we have $\rho''_m < 2N(\mathbf{h}_1) = \dfrac{2N(\mathbf{j}_s)N(\mathbf{i}_n)}{u^2}$, and it follows that

$$\eta < \log\left(\frac{2\sqrt{N(\mathbf{j}_s)N(\mathbf{i}_n)}}{u\sqrt{N(\mathbf{h}_m)}}\right).$$

Since $\sqrt{N(\mathbf{j}_s)}$, $\sqrt{N(\mathbf{i}_n)} < \sqrt{D'}$, we have $\eta < \log(2D')$. On the other hand, by Theorem 5.2.3, we have $N(\mathbf{h}_m) < \rho''_m$, and it follows that

$$\log\left(\frac{u\sqrt{N(h_m)}}{\sqrt{N(j_s)N(i_n)}}\right) < \eta.$$

Hence, we have $\log(D^{-1}) < \eta$, and we have proved the above theorem. ■

With the above idea we can develop algorithms of complexity $O(R^{1/2}D'^{\varepsilon})$ to find the regulator of $Q(\sqrt{D'})$ and to find the value of $\delta(\mathbf{i}_r, (1))$ for a given reduced principal ideal $\mathbf{i}_r$. Also, we can develop a fast algorithm, of complexity $O((D\delta)^{\varepsilon})$, to find $\mathbf{j}_k$ for given values of δ and $\mathbf{j}_1$ such that $\mathbf{j}_k$ has a distance closest to δ from $\mathbf{j}_1$. In solving the first problem, we refer the reader to [BW88B]. As for the last two algorithms, since they are not, to the best of our knowledge, documented in the literature, we include them here.

In finding the distance $\delta(\mathbf{i}_r, (1))$ for a given reduced principal ideal $\mathbf{i}_r$, we assume that the regulator R of $Q(\sqrt{D'})$ is known. We first generate a list of reduced principal ideals $\mathbf{i}_1 = (1), \mathbf{i}_2, \ldots, \mathbf{i}_s, \mathbf{i}_{s+1}, \ldots, \mathbf{i}_t$. Here s and t are determined by $\delta(\mathbf{i}_s, (1)) \approx R^{1/2}$ and

$$\delta(\mathbf{i}_t, (1)) > \delta(\mathbf{i}_s, (1)) + \log(2D').$$

If $\mathbf{i}_r = \mathbf{i}_j$ $(1 \le j \le t)$, then $\delta(\mathbf{i}_r, (1)) = \delta(\mathbf{i}_j, (1))$. If $\mathbf{i}_r = \bar{\mathbf{i}}_j$ $(1 \le j \le t)$, then

$$\delta(\mathbf{i}_r, (1)) = R - \delta(\mathbf{i}_j, (1)).$$

Otherwise, put $\mathbf{i}_m$ equal to the reduced ideal equivalent to $\mathbf{i}_s\mathbf{i}_s$, where $\delta(\mathbf{i}_m, (1)) \approx 2\delta(\mathbf{i}_s, (1))$ and $\delta(\mathbf{i}_m, (1)) < 2\delta(\mathbf{i}_s, (1)) + \log(2D')$. We let $\mathbf{i}_{n_k}$ be a reduced ideal equivalent to $\mathbf{i}_r(\mathbf{i}_m)^k$ $(k \in \mathbf{Z})$. We note that

$$\delta(\mathbf{i}_{n_k}, \mathbf{i}_r) \approx k\delta(\mathbf{i}_m, (1))$$

and

$$\delta(\mathbf{i}_{n_{i+1}}, \mathbf{i}_{n_i}) - \delta(\mathbf{i}_{n_i}, \mathbf{i}_{n_{i-1}}) < 2\delta(\mathbf{i}_s, (1)) + 2\log(2D').$$

Starting k at one, we increase k until a reduced ideal $\mathbf{i}_{n_k}$ for which $\mathbf{i}_{n_k}$ or $\bar{\mathbf{i}}_{n_k} \in \{\mathbf{i}_1, \mathbf{i}_2, \ldots, \mathbf{i}_t\}$. If $\mathbf{i}_{n_k} = \mathbf{i}_j$ $(1 \le j \le t)$, then

$$\delta(\mathbf{i}_r, (1)) = R + \delta(\mathbf{i}_j, (1)) - \delta(\mathbf{i}_{n_k}, \mathbf{i}_r).$$

If $\mathbf{i}_{n_k} = \bar{\mathbf{i}}_j$ $(1 \le j \le t)$, then

$$\delta(\mathbf{i}_r, (1)) = R - \delta(\mathbf{i}_j, (1)) - \delta(\mathbf{i}_{n_i}, \mathbf{i}_r).$$

We now present this algorithm in full.

Algorithm 5.2.1.

Given: s, t and R.

1) Initialize dist+ $\leftarrow 0$.

2) Use the Forward Single-Step Continued Fraction Algorithm to generate a list of reduced principal ideals and their distances (ideals $\mathbf{i}_k$, and $\delta(\mathbf{i}_k,(1))$ where k = 1,2,...,s,...,t).

3) Compute u and **b** where $(u)\mathbf{b} = \mathbf{i}_s\,\mathbf{i}_s$.

4) Use the Forward Single-Step Continued Fraction Algorithm to reduce **b**, and produce a reduced principal ideal $\mathbf{i}_m$ where $(N(\mathbf{b}))\mathbf{i}_m = (\rho_m)\mathbf{b}$.

5) Compute $\delta(\mathbf{i}_m,(1))$ where

$$\delta(\mathbf{i}_m,(1)) = 2\delta(\mathbf{i}_s,(1)) + \log|(\rho_m)u| - \log(N(\mathbf{i}_s)) - 0.5\log(N(\mathbf{i}_m)).$$

6) If $\mathbf{i}_r = \mathbf{i}_j$ $(1 < j < t)$, then goto **step** 12.

7) If $\mathbf{i}_r = \overline{\mathbf{i}}_j$ $(1 < j < t)$, then goto **step** 14.

8) Compute u and **b** where $(u)\mathbf{b} = \mathbf{i}_r\mathbf{i}_m$.

9) Use the Forward Single-Step Continued Fraction Algorithm to reduce **b**, and produce a reduced principal ideal $\mathbf{i}_c$ where $(N(\mathbf{b}))\mathbf{i}_c = (\rho_c)\mathbf{b}$.

10) dist $\leftarrow$ dist + $\delta(\mathbf{i}_m,(1))$+ $\log|(\rho_c)u|$ - $0.5\log(N(\mathbf{i}_r)N(\mathbf{i}_m)N(\mathbf{i}_c))$.

11) Set $\mathbf{i}_r \leftarrow \mathbf{i}_c$, and goto **step** 6.

12) DISTANCE $\leftarrow$ R + $\delta(\mathbf{i}_j,(1))$ - dist.

13) Goto **step** 15.

14) DISTANCE $\leftarrow$ R - $\delta(\mathbf{i}_j,(1))$ - dist.

15) Stop.

+We use 'dist' to denote the distance $\delta(\mathbf{i}_{n_k}, \mathbf{i}_r)$.

The next algorithm is to find a reduced ideal $\mathbf{j}_k$ for given values of δ and $\mathbf{j}_1$ such that $\delta(\mathbf{j}_k, \mathbf{j}_1) \approx \delta$. If we have a reduced principal ideal $\mathbf{i}_n$ with $\delta(\mathbf{i}_n,(1)) \approx \delta$, then, by using Theorem 5.2.5, we can find a reduced ideal $\mathbf{j}_i$ equivalent to $\mathbf{i}_n\mathbf{j}_1$ with a distance close to δ. We then use either the Forward Single-Step Continued Fraction Algorithm or Backward Single-Step Continued Fraction Algorithm, depending on whether $\delta(\mathbf{j}_k, \mathbf{j}_1) > \delta$, to find a reduced ideal which has a distance closest to δ from $\mathbf{j}_1$. As for the problem of finding $\mathbf{i}_n$, we first find m and u such that

$$\delta = 2^m u,$$

where $u\ (\in \mathbf{Q}) < 10$ and $m \in \mathbf{Z}$. We use the Forward Single-Step Continued Fraction Algorithm to find a reduced principal ideal $\mathbf{i}_u$ with a distance close to u and then use m "doubling" steps (find $\mathbf{i}_u^{m+1}$; see [Sha72]) to find $\mathbf{i}_n$. The following is a detailed description of the algorithm.

Algorithm 5.2.2.

1) Initialize i ← 0 and DIST ← δ.

2) If DIST < 10 goto **step** 6.

3) DIST ← DIST / 2.

4) i ← i + 1.

5) Goto **step** 2.

6) Use the Forward Single-Step Continued Fraction Algorithm on (1) to find $\mathbf{i}_u$ (~(1)) which has a distance less than but closest to DIST.

7) Set m ← i.

8) For i =1 to m do

9) Compute u and **b** where $(u)\mathbf{b} = \mathbf{i}_u\mathbf{i}_u$.

10) DOUBLE ← $2\delta(\mathbf{i}_u, (1))$.

11) Use the Forward Single-Step Continued Fraction Algorithm to reduce **b** and produce a reduced principal ideal $\mathbf{i}_m$.(i.e. $(N(\mathbf{b}))\mathbf{i}_m = (\rho_m)\mathbf{b}$)

12) Compute $\delta(\mathbf{i}_m, (1))$ ← DOUBLE + $\log|(\rho_m)u|$ - $\log(N(\mathbf{i}_u))$ - $0.5\log(N(\mathbf{i}_m))$.

13) If $\delta(\mathbf{i}_m, (1)) <$ DOUBLE, apply the Forward Single-Step Continued Fraction algorithm on $\mathbf{i}_m$, as given in (5.2.1), to find ideal $\mathbf{i}_n$ such that $\delta(\mathbf{i}_n, (1)) \approx$ DOUBLE.

14) If $\delta(\mathbf{i}_m, (1)) >$ DOUBLE, apply the Backward Single-Step continued Fraction Algorithm on $\mathbf{i}_m$, as given in (5.2.3), to find ideal $\mathbf{i}_n$ such that $\delta(\mathbf{i}_n, (1)) \approx$ DOUBLE.

15) Set $\mathbf{i}_u \leftarrow \mathbf{i}_n$.

16) End For.

17) Compute u and **b** where $(u)\mathbf{b} = \mathbf{i}_n\mathbf{j}_1$.

18) Use the Forward Single-Step Continued Fraction Algorithm to reduce **b** and produce a reduced primitive ideal $\mathbf{j}_m$ such that $(N(\mathbf{b}))\mathbf{j}_m = (\rho'_m)\mathbf{b}$.

19) Compute $\delta(\mathbf{j}_m, \mathbf{j}_1) \leftarrow \delta(\mathbf{i}_n, (\mathbf{1})) + \log|(\rho'_m)u| - 0.5\log(N(\mathbf{j}_m)N(\mathbf{j}_1)N(\mathbf{i}_n))$.

20) If $\delta(\mathbf{j}_m, \mathbf{j}_1) < \delta$, apply the Forward Single-Step Continued Fraction Algorithm on $\mathbf{j}_m$, as given in (5.2.1), to find ideal $\mathbf{j}_k$ such that $\delta(\mathbf{j}_k, \mathbf{j}_1) \approx \delta$.

19) If $\delta(\mathbf{j}_m, \mathbf{j}_1) > \delta$, apply the Backward Single-Step Continued Fraction Algorithm on $\mathbf{j}_m$, as given in (5.2.1), to find ideal $\mathbf{j}_k$ such that $\delta(\mathbf{j}_k, \mathbf{j}_1) \approx \delta$.

20) Stop.

§5.3. Determination of an ideal a such that $\mathbf{a}^3 = (\lambda)$ and λ is small.

In Shanks' CUFFQI algorithm, the approach to constructing λ is to find a fixed reduced ideal $\mathbf{a}$ such that $\mathbf{a}^3 = (\lambda)$ and λ is small. Certainly, we know that $\mathbf{a}$ is either a principal ideal or an ideal of order 3. Thus, we must first produce the group $\mathbf{G}_3$ of all the ideal classes of $\mathbf{K}$ whose cubes are principal and then eliminate from $\mathbf{G}_3$ the conjugate classes. Let $\mathbf{G'}_3$ denote this set of ideal classes. The problem of finding the generators for $\mathbf{G}_3$ can be solved by using the Baby Step - Giant Step method of Shanks [Sha71] in $O(D'^{1/4+\varepsilon})$ operations under suitable Riemann Hypotheses, as given in Lenstra[Len82]. We then divide the task of constructing a generating polynomial for each distinct complex cubic field with discriminant D into two subproblems.The first problem is to compute, for a given ideal $\mathbf{a}_1$, where $\mathbf{a}_1$ is an ideal class of $\mathbf{G'}_3$ and $\mathbf{a}_1$ is reduced, an ideal $\mathbf{a}_r \sim \mathbf{a}_1$ such that $\mathbf{a}_r^3 = (\lambda)$ where λ is small. The second problem is to find λ for a given ideal $\mathbf{a}$ such that $\mathbf{a}^3 = (\lambda)$. In this section, we describe a solution to the first problem. Since we want a small λ, it is important for us to select an ideal which can provide such a λ. By Theorem 4.4.1, we need only find three distinct ideals $\mathbf{a}_r$ in each of the non-principal ideal classes in $\mathbf{G'}_3$, and only one ideal $\mathbf{a}_r$ in the principal ideal class.

We first consider the case where $\mathbf{a}$ ($\mathbf{a}_1 = (1)$) is a principal ideal. Here we have

$$\mathbf{a}_r = (\rho_r) \quad \text{and} \quad \mathbf{a}_r^3 = (\rho_r^3) = (\rho_r^3 / \varepsilon_0).$$

If we put $\lambda = \rho_r^3 / \varepsilon_0$, since

$$|N(\lambda)| = |N(\rho_r)|^3 = N(\mathbf{a}_r)^3,$$

we have

$$|\bar{\lambda}| = N(\mathbf{a}_r)^3 \varepsilon_0 / \rho_r^3.$$

In order for $|\bar{\lambda}|$ and $|\lambda|$ to be small, we want

$$|\bar{\lambda}| \approx |\lambda| \approx N(\mathbf{a}_r)^{3/2},$$

as $|\lambda\bar{\lambda}| = N(\mathbf{a}_r)^3$. Thus, we want

$$\varepsilon_0 N(\mathbf{a}_r)^{3/2} / \rho_r^3$$

to be close to 1. However,

$$3\delta(\mathbf{a}_r , \mathbf{a}_1) = \log(\rho_r^3 / N(\mathbf{a}_r)^{3/2}),$$

and we have

$$\log |\bar{\lambda}| = (R + \log(N(\mathbf{a}_r)^{3/2})) - 3\delta(\mathbf{a}_r , \mathbf{a}_1).$$

Hence, we want $R \approx 3\delta(\mathbf{a}_r , \mathbf{a}_1)$ in order to have $|\bar{\lambda}| \approx N(\mathbf{a}_r)^{3/2}$. Consequently, we want an ideal $\mathbf{a}_s$ such that

$$\delta(\mathbf{a}_s , \mathbf{a}_1) < R / 3,$$

and $$\delta(\mathbf{a}_{s+1} , \mathbf{a}_1) > R / 3.$$

We then select either $\mathbf{a}_s$ or $\mathbf{a}_{s+1}$ to be $\mathbf{a}_r$ depending on which ideal has a distance closer to 1/3 of the regulator. We can now give the algorithm for the determination of ideal $\mathbf{a}_r$ ($\mathbf{a}_r \sim (1)$).

Algorithm 5.3.1.

1) Use the Large Step Algorithm, as given in [SW88] for example, to compute the regulator R of $Q(\sqrt{D'})$.

2) Use Algorithm 5.2.2 to find the ideal $\mathbf{a}_s$ ($\sim (1)$) such that

$$\delta(\mathbf{a}_s , \mathbf{a}_1) < R/3 < \delta(\mathbf{a}_{s+1} , \mathbf{a}_1).$$

3) If $|\delta(\mathbf{a}_s,\mathbf{a}_1) - R/3| < |\delta(\mathbf{a}_{s+1},\mathbf{a}_1) - R/3|$, set $\mathbf{a}_r \leftarrow \mathbf{a}_s$; otherwise set $\mathbf{a}_r \leftarrow \mathbf{a}_{s+1}$.

4) Stop.

We now consider the case where $\mathbf{a}_1$ is not a principal ideal. We let $\mathbf{a}_1$ be a reduced ideal in a class of G'_3. If we put

(5.3.1) $$\mathbf{a}_1^2 = (u_1)\mathbf{b}_1, \qquad \text{where } u_1 \in \mathbf{Z} \text{ and } \mathbf{b}_1 \text{ is a primitive ideal,}$$

then

(5.3.2) $$(N(\mathbf{b}_1))\mathbf{b}_m = (\rho''_m)\mathbf{b}_1,$$

where $\mathbf{b}_m$ is a reduced ideal equivalent to $\mathbf{b}_1$. Multiplying $\mathbf{b}_m$ by $\mathbf{a}_1$, we get

(5.3.3) $$\mathbf{b}_m\mathbf{a}_1 = (u_2)\mathbf{c}_1, \qquad \text{where } \mathbf{c}_1 \sim (1) \text{ and } u_2 \in \mathbf{Z}.$$

Let $\mathbf{c}_t$ be a reduced ideal equivalent to $\mathbf{c}_1$. Then

(5.3.4) $$(N(\mathbf{c}_1))\mathbf{c}_t = (\rho_t)\mathbf{c}_1.$$

Let $\mathbf{c}_s$ be the conjugate ideal of $\mathbf{c}_t$. Then

$$\mathbf{c}_s = \bar{\mathbf{c}}_t \sim \bar{\mathbf{a}}_1^3 \sim (1),$$

and

(5.3.5) $$\mathbf{c}_t = \bar{\mathbf{c}}_s = (\theta_s).$$

Now, if we put

$$(N(\mathbf{a}_1))\mathbf{a}_r = (\rho'_r)\mathbf{a}_1,$$

then we have

(5.3.6) $$(N(\mathbf{a}_1)^3)\mathbf{a}_r^3 = (\rho'^3_r)\mathbf{a}_1^3.$$

The product of (5.3.1) and (5.3.3) is

$$\mathbf{b}_m\mathbf{a}_1^3 = (u_1u_2)\mathbf{b}_1\mathbf{c}_1,$$

and, from (5.3.2) , (5.3.4) we get

$$(\rho''_m\rho_t)\mathbf{b}_m\mathbf{a}_1^3 = (u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1))\mathbf{b}_m\mathbf{c}_t,$$

or $$(\rho''_m\rho_t)\mathbf{a}_1^3 = (u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1))\mathbf{c}_t.$$

By using (5.3.5), we get

$$(\rho''_m\rho_t)\mathbf{a}_1^3 = (u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1)\theta_s).$$

From (5.3.6) it follows that

$$(\rho''_m\rho_tN(\mathbf{a}_1)^3)\mathbf{a}_r^3 = (u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1)\theta_s\rho'^3_r).$$

We have $\mathbf{a}_r^3 = (\lambda)$, where

$$\lambda = \frac{u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1)\theta_s\rho'^3_r}{\rho''_m\rho_tN(\mathbf{a}_1)^3}.$$

But, since $N(\mathbf{a}_r)^3 = |N(\lambda)| = |\lambda\,\bar{\lambda}|$, we get

$$|\overline{\lambda}| = \frac{N(\mathbf{a}_r)^3 N(\mathbf{a}_1)^3 \rho''_m \rho_t}{u_1 u_2 N(\mathbf{b}_1) N(\mathbf{c}_1) \theta_s \rho'^3_r}.$$

Also, $N(\mathbf{c}_s) = N(\mathbf{c}_t) = |N(\theta_s)|$ and we now have

$$|\overline{\lambda}| = \frac{N(\mathbf{a}_r)^3 N(\mathbf{a}_1)^3 \rho''_m \rho_t |\overline{\theta}_s|}{\rho'^3_r u_1 u_2 N(\mathbf{b}_1) N(\mathbf{c}_1) N(\mathbf{c}_s)}.$$

Letting

$$\gamma = \frac{N(\mathbf{a}_1)^{3/2} \rho''_m \rho_t |\overline{\theta}_s|}{u_1 u_2 N(\mathbf{b}_1) N(\mathbf{c}_1) N(\mathbf{c}_s)}, \tag{5.3.7}$$

we have

$$|\overline{\lambda}| = \frac{N(\mathbf{a}_r)^3 N(\mathbf{a}_1)^{3/2} \gamma}{\rho'^3_r}.$$

As in the previous case, in order to have $|\overline{\lambda}| \approx |\lambda| \approx N(\mathbf{a}_r)^{3/2}$, we want $\gamma N(\mathbf{a}_r)^{3/2} N(\mathbf{a}_1)^{3/2} / |\rho'_r|^3$ to be close to 1. Since

$$\delta(\mathbf{a}_r, \mathbf{a}_1) = \log(\rho'_r / \sqrt{N(\mathbf{a}_r) N(\mathbf{a}_1)}),$$

and $\delta(\mathbf{a}_r, \mathbf{a}_1)$ is monotonically increasing with r, we select that ideal $\mathbf{a}_s$ such that

$$\delta(\mathbf{a}_s, \mathbf{a}_1) < (\log \gamma) / 3,$$

and

$$\delta(\mathbf{a}_{s+1}, \mathbf{a}_1) > (\log \gamma) / 3.$$

Once we find $\mathbf{a}_s$, we chose $\mathbf{a}_r = \mathbf{a}_s$ or $\mathbf{a}_{s+1}$ such that $\delta(\mathbf{a}_r, \mathbf{a}_1)$ is closest to $(\log\gamma) / 3$.

As mentioned earlier, we must find 3 distinct λ's in each of the non-principal ideal classes in $\mathbf{G'}_3$. By Theorem 4.4.1, we know that

$$|\overline{\lambda}_i| = (N(\mathbf{a}_r)^3 N(\mathbf{a}_1)^{3/2} \gamma \, \varepsilon_0^{\,i}) / \rho'^3_r, \text{ where } i = 0,1,2,$$

produce all the (3) distinct complex cubic fields of which the ideal class containing $\mathbf{a}_r$ is capable. Thus, we must find 3 ideals whose generators produce 3 other distinct complex cubic fields. These 3 ideals can be found by obtaining $\mathbf{a}_{r_i}$ such that

$$\delta(\mathbf{a}_{r_i}, \mathbf{a}_1) \approx (\log \gamma + i (\log \varepsilon_0)) / 3, \text{ where } i = 0, 1, 2.$$

Thus, for a given non-principal reduced ideal $\mathbf{a}_1$ in a class of $\mathbf{G'}_3$, the algorithm to find the 3 distinct ideals $\mathbf{a}_r$ is as follows:

Algorithm 5.3.2.

1) Compute u_1 and $\mathbf{b}_1$ where $(u_1)\,\mathbf{b}_1 = \mathbf{a}_1^2$.

2) Find a reduced ideal $\mathbf{b}_m$ ($\sim\mathbf{b}_1$) such that $(N(\mathbf{b}_1))\mathbf{b}_m = (\rho''_m)\mathbf{b}_1$.

3) Compute u_2 and $\mathbf{c}_1$ where $(u_2)\,\mathbf{c}_1 = \mathbf{b}_m\mathbf{a}_1$.

4) Find a reduced ideal $\mathbf{c}_t$ ($\sim\mathbf{c}_1$) such that $(N(\mathbf{c}_1))\mathbf{c}_t = (\rho_t)\mathbf{c}_1$.

5) Use Algorithm 5.2.1 to find the distance δ_s between $\bar{\mathbf{c}}_t$ ($= \mathbf{c}_s$) and (1).

6) Compute $\log\gamma \leftarrow \log(N(\mathbf{a}_1)^{3/2}\rho''_m\rho_t) + \delta_s - \log(u_1u_2N(\mathbf{b}_1)N(\mathbf{c}_1)N(\mathbf{c}_s)^{1/2})$.

7) Initialize $i \leftarrow 1$.

8) Use Algorithm 5.2.2 to find ideal $\mathbf{a}_s$ such that $\delta(\mathbf{a}_s\,,\,\mathbf{a}_1) < (\log\gamma)\,/\,3$ and $(\log\gamma)\,/\,3 < \delta(\mathbf{a}_{s+1}\,,\,\mathbf{a}_1)$.

9) Set $\mathbf{a}_r \leftarrow \mathbf{a}_s$ if $|\delta(\mathbf{a}_{s+1}\,,\,\mathbf{a}_1) - (\log\gamma)\,/\,3| < |\delta(\mathbf{a}_s\,,\,\mathbf{a}_1) - (\log\gamma)\,/\,3|$; otherwise put $\mathbf{a}_r \leftarrow \mathbf{a}_{s+1}$.

10) Save $\mathbf{a}_r$.

11) $\gamma \leftarrow \gamma + \log\varepsilon_0\,/\,3$.

12) $i \leftarrow i + 1$.

13) If $i \le 3$ goto **step** 8.

14) Stop.

§5.4. Bounds on A and B where $\lambda = (A+B\sqrt{D'})/\sigma$.

In the previous section, we presented a method for finding a reduced ideal $\mathbf{a}_r$ such that $\mathbf{a}_r^3 = (\lambda)$, where λ (> 0) is small. In this section, we determine bounds on A and B, where $\lambda = (A+B\sqrt{D'})/\sigma$. In order to do so, we must first determine bounds on λ and $|\bar{\lambda}|$. As stated earlier, $\mathbf{a}_r$ can be either $\mathbf{a}_s$ or $\mathbf{a}_{s+1}$, where $\mathbf{a}_s$ and $\mathbf{a}_{s+1}$ are defined in §5.3. We first discuss the bounds in the case where $(\lambda) = \mathbf{a}_r^3 = \mathbf{a}_s^3$.

Case 1. $|\bar{\lambda}| = \dfrac{N(a_s)^3 N(a_1)^{3/2}\nu}{|\rho_s|^3}$ where $\nu = \gamma$, (as defined in (5.3.7)), or $\nu = \varepsilon_0$. In this case we know that

$$\frac{\nu N(a_s)^{3/2} N(a_1)^{3/2}}{|\rho_s|^3} > 1,$$

so we have $|\bar{\lambda}| > N(a_s)^{3/2}$. Since $|\lambda\bar{\lambda}| = N(a_s)^3$ and $\sqrt{D'} > N(a_s)$, by Corollary 5.2.1, we have

$$D'^{3/4} > N(a_s)^{3/2} > |\lambda| = N(a_s)^3 \ / |\bar{\lambda}|. \tag{5.4.1}$$

Also, since a_s is selected such that

$$\log(\nu) - 3\log\rho_s + 3/2\ \log(N(a_s)) + 3/2\ \log(N(a_1))$$
$$< 3\log\rho_{s+1} - 3/2\ \log(N(a_{s+1})) - 3/2\ \log(N(a_1)) - \log(\nu),$$

we have

$$\frac{\rho_{s+1}{}^3}{\nu N(a_{s+1})^{3/2} N(a_1)^{3/2}} > \frac{\nu N(a_s)^{3/2} N(a_1)^{3/2}}{\rho_s{}^3},$$

or

$$\frac{\rho_s{}^6\, \psi_s{}^3}{N(a_{s+1})^{3/2} N(a_s)^{3/2} N(a_1)^3} = \frac{\rho_s{}^3\, \rho_{s+1}{}^3}{N(a_{s+1})^{3/2} N(a_s)^{3/2} N(a_1)^3} > \nu^2,$$

where $\psi_s = (P_s + \sqrt{D'}) / Q_{s-1}$. It follows that

$$\frac{\rho_s{}^3\, \psi_s{}^{3/2}}{N(a_{s+1})^{3/4} N(a_s)^{3/4} N(a_1)^{3/2}} > \nu$$

and this gives

$$\frac{N(a_s)^3 \psi_s{}^{3/2}}{N(a_{s+1})^{3/4} N(a_s)^{3/4}} > |\bar{\lambda}|.$$

Also, $N(a_s) = Q_{s-1} / \sigma$, so we have

$$\frac{N(a_s)^{3/4}\, (P_s + \sqrt{D'})^{3/2}}{\sigma^{3/2}\, N(a_{s+1})^{3/4}} > |\bar{\lambda}|. \tag{5.4.2}$$

But, as $\sqrt{D'} > N(a_s)$, we now have

$$2^3\, D'^{9/8} = 2^{3/2}(2\sqrt{D'})^{3/2}\, (\sqrt{D'})^{3/4} > |\bar{\lambda}|. \tag{5.4.3}$$

Since $|\lambda\bar{\lambda}| = N(a_s)^3$, we can easily deduce that

$$|\lambda| > D'^{3/8} / 8.$$

Although the upper bound for $|\bar{\lambda}|$ derived here is $8D'^{9/8}$, in most cases the actual size of $|\bar{\lambda}|$ tends to be much smaller. Indeed, according to the Gauss-Kuzmin Law, if $\phi_i = (P_i + \sqrt{D'}) / Q_i$, then we would expect the probability of ϕ_i occurring between n and n + 1 to be approximately

$$\log[1 + 1/(n^2 + 2n)] / \log 2,$$

For n = 1,2 and 3, this gives the values 0.415037, 0.169925 and 0.93109, respectively. Thus, about 0.678 of the time we might expect

$$(5.4.4) \qquad 4 > \frac{P_i + \sqrt{D'}}{Q_i}.$$

Based on this information and (5.4.2), we can say that, for approximately two thirds of the values of $|\bar{\lambda}|$, we would probably get

$$(5.4.5) \qquad 8D'^{3/4} > N(a_s)^{3/4} N(a_{s+1})^{3/4} \left(\frac{P_s + \sqrt{D'}}{Q_s}\right)^{3/2} > |\bar{\lambda}|.$$

We now consider the bounds in the case where $(\lambda) = a_r^3 = a_{s+1}^3$.

Case 2. $|\bar{\lambda}| = \dfrac{N(a_{s+1})^3 N(a_1)^{3/2} \nu}{|\rho_{s+1}|^3}$, where ν has the same definition as in Case 1. In this case we have

$$\frac{N(a_{s+1})^{3/2} N(a_1)^{3/2} \nu}{|\rho_{s+1}|^3} < 1,$$

so $N(a_{s+1})^{3/2} > |\bar{\lambda}|$ follows. Therefore we have

$$(5.4.6) \qquad D'^{3/4} > |\bar{\lambda}|.$$

Since $|\lambda\bar{\lambda}| = N(a_s)^3$, we have

$$|\lambda| > D'^{3/4}.$$

Furthermore,

$$\log(\nu) - 3\log|\rho_s| + 3/2 \log(N(a_s)) + 3/2 \log(N(a_1))$$
$$> 3\log|\rho_{s+1}| - 3/2 \log(N(a_{s+1})) - 3/2 \log(N(a_1)) - \log(\nu).$$

Hence, we obtain

$$|\bar{\lambda}| > \frac{N(a_{s+1})^3}{N(a_s)^{3/4} N(a_{s+1})^{3/4} \psi_s^{3/2}},$$

where $\psi_s = (P_s + \sqrt{D'}) / Q_{s-1}$. Since $|\lambda\bar{\lambda}| = N(a_{s+1})^3$, we now have

$$N(a_{s+1})^{3/4}N(a_s)^{3/4}\,\psi_s^{3/2} > |\lambda| = N(a_{s+1})^3 \,/\, |\bar{\lambda}|. \tag{5.4.7}$$

Also, $\psi_s = \sigma(P_s + \sqrt{D'}) / N(a_s)$ and we get

$$8D'^{9/8} > \frac{\sigma^{3/2}(P_s + \sqrt{D'})^{3/2}N(a_{s+1})^{3/4}}{N(a_s)^{3/4}} > |\lambda|. \tag{5.4.8}$$

Again, by using the Gauss-Kuzmin Law we can expect to have a smaller upper bound for $|\lambda|$ in most instances. By Corollary 5.2.2 and Lemma 5.2.1, we know that $[\psi_s] = q_s$. Hence, by (5.4.4), we would expect that $4 > q_s$ about 67.8% of the time. Based on this information and (5.4.7), the following inequality

$$8D'^{3/4} > N(a_{s+1})^{3/4}N(a_s)^{3/4}\,\psi_s^{3/2} > |\lambda| \tag{5.4.9}$$

probably holds for about two thirds of λ values.

We have now determined the bounds on λ and $|\bar{\lambda}|$ for both cases. Since

$$|2A / \sigma| < |\lambda| + |\bar{\lambda}|, \text{ and } |2B / \sigma| < \frac{|\lambda| + |\bar{\lambda}|}{\sqrt{D'}},$$

in either case we can say that 67.8% of the time we would expect to have

$$4.5\sigma D'^{3/4} > (8D'^{3/4} + D'^{3/4})(\sigma / 2) > |A|,$$

$$4.5\sigma D'^{1/4} > (8D'^{1/4} + D'^{1/4})(\sigma / 2) > |B|. \tag{5.4.10}$$

Also, the following bounds

$$4.5\sigma D'^{9/8} > (8D'^{9/8} + D'^{3/4})(\sigma / 2) > |A|,$$

$$4.5\sigma D'^{5/8} > (8D'^{5/8} + D'^{1/4})(\sigma / 2) > |B|$$

are unconditional.

It is well known that any cubic field **F** having discriminant D has a reduced binary cubic form $F(x,y) = a_1x^3+a_2x^2y+a_3xy^2+a_4y^3$ with discriminant D associated with it. In [ET85], Ennola and Turunen present a method for constructing a generating polynomial $f(x) = x^3-ax+b$ from this binary cubic form F(x,y) such that F(x,y) and f(x) correspond to the same cubic field **F**. Although Ennola and Turunen deal with totally real cubic fields only, this method can also be applied to complex cubic fields because the change from

positive discriminants to negative discriminants does not affect the proof of the method. Also, in [ET85] it was pointed out that the discriminant of f(x) is DE^2 where E is the index of the polynomial f(x). Furthermore,

$$E < 2D^{1/4} / \sqrt{27}$$

is given in [MB12]. As a result, we can conclude that there exists a generating polynomial with discriminant D and index I for the cubic field **F** such that

(5.4.11) $$I < 2D^{1/4} / \sqrt{27}.$$

However, we have no idea of how to find the F(x,y) here; nevertheless, by comparing (5.4.10) and (5.4.11), we can say that most of the generating polynomials constructed by the CUFFQI algorithm have indices which are not much larger than those bounded by (5.4.11). Furthermore, we can conclude that the generating polynomials constructed by the CUFFQI algorithm have relatively small values for their coefficients and index.

§5.5. Construction of λ.

In the previous section we presented a method for obtaining a reduced ideal **a** such that $\mathbf{a}^3 = (\lambda)$ where λ (> 0) and $|\overline{\lambda}|$ are small. In this section, we describe an algorithm which can determine what this λ value is, given **a**.

Let

(5.5.1) $$\mathbf{a}^2 = (u)\mathbf{b}$$

where $u \in \mathbf{Z}$ and **b** is prmitive. Put $\mathbf{b}_1 = \mathbf{b}$. We then have

(5.5.2) $$(N(\mathbf{b}_1))\mathbf{b}_m = (\rho_m))\mathbf{b}_1,$$

where $\mathbf{b}_m = \overline{\mathbf{a}}$, for some m. Since $(u)\mathbf{b}_1 = \mathbf{a}^2$, we get

(5.5.3) $$(uN(\mathbf{b}_1))\overline{\mathbf{a}} = (\rho_m)\mathbf{a}^2.$$

On multiplying (5.5.3) by **a**, we see that

$$(\rho_m)\mathbf{a}^3 = (uN(\mathbf{b}_1)N(\mathbf{a})),$$

but $N(\mathbf{a}) = N(\overline{\mathbf{a}}) = N(\mathbf{b}_m)$ and $|N(\rho_m)| = N(\mathbf{b}_1)N(\mathbf{b}_m)$; hence

$$a^3 = (\lambda) = (uN(\mathbf{b}_1)N(\mathbf{b}_m)\rho_m^{-1}) = (u\bar{\rho}_m).$$

It follows that

$$\lambda\varepsilon_0^k = u\bar{\rho}_m$$

or

$$\lambda = u\bar{\rho}_m\varepsilon_0^{-k},$$

where $k \in \mathbf{Z}$. Although k could be any integer, the following theorem allows us to restrict the possible values of k, in the case where the regulator is not exceptionally small.

Theorem 5.5.1. Suppose that $(N(\mathbf{b}_1))\mathbf{b}_m = (\rho_m))\mathbf{b}_1$ and $\lambda = u\bar{\rho}_m\varepsilon_0^{-k}$ hold. If $C_1 < \lambda < C_2$, where $C_1, C_2 \in \mathbf{Q}$, and $\log \varepsilon_0 > \max\{\log(D'/C_1), \log(2C_2)\}$, then

(5.5.4) $$\lambda = u\bar{\rho}_m$$

or

(5.5.5) $$\lambda = u\bar{\rho}_m\varepsilon_0.$$

Proof. Let s be the least value ($1 \le s \le m$) such that $\mathbf{b}_s$ is a reduced ideal. Hence, by Theorem 5.2.3, we have

$$\bar{\rho}_m = N(\mathbf{b}_1)\theta_m = N(\mathbf{b}_1)\theta_s\chi_s$$

where

$$\theta_m = \theta_s\chi_s,$$

(5.5.6) $$1/\varepsilon_0 < \chi_s < 1,$$

and

(5.5.7) $$N(\mathbf{b}_s)/(2N(\mathbf{b}_1)) < \theta_s < 1.$$

On multiplying (5.5.6) by (5.5.7), we get

$$N(\mathbf{b}_s)/(2N(\mathbf{b}_1)\varepsilon_0) < \theta_s\chi_s < 1;$$

thus,

$$N(\mathbf{b}_s)/(2\varepsilon_0) < N(\mathbf{b}_1)\theta_s\chi_s < N(\mathbf{b}_1),$$

or

$$uN(\mathbf{b}_s)/(2\varepsilon_0) < u\bar{\rho}_m < uN(\mathbf{b}_1).$$

Since $\lambda = u\bar{\rho}_m\varepsilon_0^{-k}$, we have

$$uN(b_s) / (2\varepsilon_0^{k+1}) < \lambda < uN(b_1) / \varepsilon_0^k.$$

But since $C_1 < \lambda$ and $D' > N(a)^2 = u^2N(b_1)$, we obtain the following inequality

$$D' / \varepsilon_0^k > (uN(b_1)) / \varepsilon_0^k > C_1.$$

Hence,

$$D' / C_1 > \varepsilon_0^k.$$

On the other hand, we know that $D' / C_1 < \varepsilon_0$, and therefore we have $k \leq 0$. As for the upper bound for λ, we have $C_2 > \lambda$ and it follows that

$$C_2 > uN(b_s) / (2\varepsilon_0^{k+1})$$

and

$$\varepsilon_0^{k+1} > uN(b_s) / (2C_2) > 1 / (2C_2).$$

Thus, we get

$$2C_2 > \varepsilon_0^{-k-1}.$$

Once again, we know that $2C_2 < \varepsilon_0$, and, as a consequence, we have $k \geq -1$. Our result follows. ■

In §5.4, we have shown that $8D'^{9/8} > \lambda > D'^{3/8} / 8$. Hence, we can now apply Theorem 5.5.1 to find λ if the regulator is bigger than $\log 16D'^{9/8}$. In the case where $R < \log 16D'^{9/8}$, the determination of a small λ can be done by using a direct search because there is a limited number of reduced ideals in each of the ideal classes. Thus, this theorem can be used here, as we are not interested in the discriminants which have small regulators.

In (5.5.5), since ε_0 is usually very large, it is convenient to modify (5.5.5) so that λ can be easily constructed. From (5.5.2), we have

(5.5.8) $$(N(b_1))b_m = (\rho_m)b_1.$$

Putting $a_1 = \bar{b}_1$ and $a_t = \bar{b}_m$, we then get

(5.5.9) $$(N(a_1))a_t = (\rho'_t)a_1.$$

The product of (5.5.8) and (5.5.9) is

$$(N(b_1)N(b_m)) = (\rho'_t\rho_m).$$

But, since $(N(b_1)N(b_m)) = (\rho_m\bar{\rho}_m)$, we get

$$\eta\bar{\rho}_m = \rho'_t,$$

where η is a unit (i.e. $\eta = \varepsilon_0^i$ and $i \in \mathbf{Z}$). Since $N(a_t) < \rho'_t < \varepsilon_0$ and $1/\varepsilon_0 < \bar{\rho}_m < N(b_1)$, we have

$$\eta = \rho'_t / \bar{\rho}_m > N(a_t) / N(b_1).$$

By 5.5.1, we have $N(a_t)^2 = u^2N(b_1)$ and we get

$$\eta > u^2 / N(a_t) > 1 / \sqrt{D'}.$$

Since we are only interested in D' where $\varepsilon_0 > 8D'^{9/8}$, we get

$$\eta = \rho'_t / \bar{\rho}_m \geq 1 \text{ and } i \geq 0.$$

If $\rho'_t = \bar{\rho}_m$, we get

$$\lambda = u\rho'_t\varepsilon_0.$$

It follows that

$$\varepsilon_0 = \lambda / (u\rho'_t).$$

Since u, $\rho'_t > 1$ and $8D'^{9/8} > \lambda$, we get

$$\varepsilon_0 < 8D'^{9/8},$$

which is a contradiction. Hence, we have

$$\eta = \rho'_t / \bar{\rho}_m > 1 \text{ and } i > 0.$$

If $i \geq 2$, we have

$$\varepsilon_0^2 < \varepsilon_0 / \bar{\rho}_m < \varepsilon_0^2,$$

and we get a contradiction. So i must be 1 and $\rho'_t = \varepsilon_0\bar{\rho}_m$. From this result we can find λ by using

(5.5.10) $$\lambda = u\bar{\rho}_m\varepsilon_0 = u\rho'_t.$$

Unfortunately, in attempting to determine λ, there is no *a priori* way of knowing which of $u\bar{\rho}_m$ or $u\rho'_t$ is λ. Therefore the approach that we utilized is that of attempting to

compute both $\bar{\rho}_m$ and ρ'_t. The process is terminated as soon as the lesser of $u\bar{\rho}_m$ or $u\rho'_t$ is found, which we put as our λ value. We illustrate this idea by

Algorithm 5.5.1.(Given an ideal **a**, find λ).

1) Compute u and $\mathbf{b}_1$ where $(u)\mathbf{b}_1 = \mathbf{a}^2$.

2) Initialize $\mathbf{a}_1 \leftarrow \bar{\mathbf{b}}_1$.

3) Set $j \leftarrow 2$.

4) Perform a single step of the Forward Single-Step Continued Fraction Algorithm on $\mathbf{a}_{j-1}$ and $\mathbf{b}_{j-1}$ to get $\mathbf{a}_j$ and $\mathbf{b}_j$.

5) Compute $\bar{\rho}_j$ where $(N(\mathbf{b}_1))\mathbf{b}_j = (\rho_j)\mathbf{b}_1$.

6) If $\mathbf{b}_j = \bar{\mathbf{a}}$ then goto **step** 11.

7) Compute ρ'_j where $(N(\mathbf{a}_1))\mathbf{a}_j = (\rho'_j)\mathbf{a}_1$.

8) If $\mathbf{a}_j = \mathbf{a}$ then goto **step** 13.

9) $j \leftarrow j + 1$.

10) Goto **step** 4.

11) $\lambda \leftarrow u\bar{\rho}_j$.

12) Goto **step** 14.

13) $\lambda \leftarrow u\rho'_j$.

14) Stop.

Before we leave this section, it is important to describe a technique that was used in the computation of A and B where

$$\lambda = (A + B\sqrt{D'}) / \sigma = u\bar{\rho}_m \text{ or } u\rho'_t.$$

In the first case, we know that

$$\bar{\rho}_m = N(\mathbf{b}_1)\theta_m$$

and

$$\theta_m = (-1)^{m-1}\left(A_{m-2} - B_{m-2}\left(\frac{P + \sqrt{D'}}{Q}\right)\right),$$

where the A_i's and B_i's are defined in (5.2.8) and $\mathbf{b}_1 = [Q / r , (P + \sqrt{D'}) / r]$.

Thus, we have

$$\lambda = uN(b_1)\theta_m = u(Q/\sigma)(-1)^{m-1}\left(A_{m-2} - B_{m-2}\left(\frac{P + \sqrt{D'}}{Q}\right)\right).$$
$$= u(-1)^{m-1}\left(\frac{QA_{m-2} - PB_{m-2} - \sqrt{D'}B_{m-2}}{\sigma}\right).$$

Since $N(\lambda) = \frac{|A^2 - D'B^2|}{\sigma^2}$, we get

$$A = u(QA_{m-2} - PB_{m-2}) = uG_{m-2}, \quad B = uB_{m-2}.$$

In order to minimize the precision required for the computation of A, we use the following recursive formula. Letting $G_{-2} = -P$, $G_{-1} = Q$, we then find from (5.2.7) that

(5.5.11) $$G_{i+1} = q_{i+1}G_i - G_{i-1}.$$

We now consider the second case, where $\lambda = (A + B\sqrt{D'}) / \sigma = u\rho'_t$. From §5.2 we know that

$$\theta'_t = (-1)^{t-1}\left(A_{t-2} - B_{t-2}\left(\frac{-P + \sqrt{D'}}{Q}\right)\right),$$

where the A_i's and B_i's have the same definition as in (5.2.8). Also,

$$(N(a_1)\theta_t)a_t = (N(a_t))a_1 \text{ and } \bar{b}_1 = a_1 = [Q / \sigma , (-P + \sqrt{D'}) / \sigma].$$

Now,

$$Q\theta'_t = (-1)^{t-1}(QA_{t-2} + PB_{t-2} - B_{t-2}\sqrt{D'}),$$

and

$$Q|\bar{\theta}'_t| = QA_{t-2} + PB_{t-2} + B_{t-2}\sqrt{D'}.$$

Thus, since $Q|\bar{\theta}'_t| = \sigma\rho'_t$, we have

$$\lambda = u\rho'_t = \frac{u(QA_{t-2} + PB_{t-2}) + uB_{t-2}\sqrt{D'}}{\sigma}.$$

As in the previous case, we get

$$A = u(QA_{t-2} + PB_{t-2}) = uG_{t-2},$$
$$B = uB_{t-2},$$

where $G_{-2} = P$, $G_{-1} = Q$ and the G_t's ($t \geq 0$) has the same definition as in (5.5.11).

§5.6. The CUFFQI algorithm.

Since we have now discussed all of the components of our version of the CUFFQI algorithm, we are able to present the overall algorithm. For a given fundamental discriminant D and its dual discriminant D', the following algorithm constructs all the complex cubic fields having fundamental discriminant D. We assume that the 3-ranks of the class group of $Q(\sqrt{D'})$ and $Q(\sqrt{D})$ are known.

Algorithm 5.6.1.

Given: D(<0), 3-ranks of the class group of $Q(\sqrt{D'})$ (= r') and $Q(\sqrt{D})$ (= r").

1) Compute the regulator of $Q(\sqrt{D'})$ (see, for example [BW88B]).

2) Use the Baby Step - Giant Step method as described in [Sha71] and [Len82] to produce the generators of G_3. Use the generators to construct G'_3.

3) Use Algorithm 5.3.1 to find an ideal **a** in the principal ideal class.

4) Store **a** in LIST.

5) For each ideal class in G'_3, do the following:

6) Apply Algorithm 5.3.2 to find ideals $\mathbf{a}_{r_i}$, i=1,2,3.

7) Store $\mathbf{a}_{r_i}$ (i=1,2,3) in LIST.

8) End For.

9) For each ideal **a** in LIST, do the following

10) Apply Algorithm 5.5.1 to construct $\lambda = (A + B\sqrt{D'}) / \sigma$.

11) Store the generating polynomial $x^3 - 3N(a)x + A$ in a data base.

12) End For.

13) If $r' \neq r''$ then goto **step** 15.

14) Use the criterion as given in §4.4 to eliminate all the generating polynomials that do not have a field discriminant D.

15) Stop.

§5.7. The complexity of the CUFFQI algorithm.

In this section we discuss the complexity of the Algorithm 5.6.1. It is known that the complexity of finding the regulator is $O(R^{1/2}D'^{\varepsilon})$. The Baby Step - Giant Step method of Step 2 has a complexity of $O(D'^{1/4+\varepsilon})$ under the assumption of the Generalized Riemann Hypothesis (GRH) as noted in [Len82]. Having found the generators, we can construct $\mathbf{G}'_3$ in $O\left(\frac{3^r-1}{2}D'^{\varepsilon}\right)$ operations. Thus, the complexity of Step 2 is $O(D'^{1/4+\varepsilon})$ + $O\left(\frac{3^r-1}{2}D'^{\varepsilon}\right)$ if the Generalized Riemann Hypothesis holds. On the other hand, we must note that the construction of $\mathbf{G}'_3$ can be done unconditionally in $O(D'^{0.508+\varepsilon})$ operations as mentioned in [MW87]. In Step 3, if the regulator is known, then the complexity of Algorithm 5.3.1 is $O((\delta D')^{\varepsilon})$. Since the regulator is computed in Step 1, we can see that Step 3 has a complexity of $O((\delta D')^{\varepsilon})$. In Step 6, the complexity of Algorithm 5.3.2 depends on the complexity of Algorithm 5.2.1. Since Algorithm 5.2.1 has a complexity of $O(R^{1/2}D'^{\varepsilon})$, we can conclude that Step 6 can be done in $O(R^{1/2}D'^{\varepsilon})$ operations. However, there are $\frac{3^r-1}{2}$ ideal classes in $\mathbf{G}'_3$. Thus, the overall complexity for Steps 5-8 is $O\left(\frac{3^r-1}{2}R^{1/2}D'^{\varepsilon}\right)$. In Step 10, we must consider the number of steps in the continued fraction expansion which are required in the determination of λ. In §5.4., we showed that $|\lambda|$ is less than $8D'^{9/8}$, therefore we have

$$\log|\lambda| < \log(8D'^{9/8}).$$

Also, as noted in Stephens and Williams[SW88], if it takes m steps to go from one reduced ideal to another equivalent reduced ideal, then the distance between these two ideals must be at least $(m-2)\log((1+\sqrt{5}) / 2)$. From this result, we can see that the maximum number of steps to construct λ for a given ideal $\mathbf{a}$ is approximately

$$\frac{m\log(8D'^{9/8})}{(m-2)\log((1+\sqrt{5})/2)} = O(D'^{\varepsilon}).$$

Since the multiplication of 2 ideals has a complexity of $O(D'^{\varepsilon})$, we can conclude that this step has a complexity of $O(D'^{\varepsilon})$. However, there are precisely $\frac{3^{r+1}-1}{2}$ ideals stored in LIST. Therefore, the overall complexity for Steps 9-12 is $O\left(\frac{3^{r+1}-1}{2} D'^{\varepsilon}\right)$. Finally, the criterion for eliminating cubic fields with discriminant -27D' has a complexity of $O(1)$. By combining all these results, we conclude that the CUFFQI Algorithm has an unconditional complexity of $O(D'^{0.508+\varepsilon})$. However, if the Generalized Riemann Hypothesis holds, the CUFFQI algorithm has a complexity of $O\left(\frac{3^{r}-1}{2} R^{1/2} D'^{\varepsilon}\right)$. Furthermore, the above complexity can be improved in most cases due to a heruistic of Cohen and Lenstra[CL84]. According to [CL84], the probability that the 3-rank of **K** equals to r is less than 3^{-r^2}. Thus, we would expect r to be small in general. In that case, $\frac{3^{r}-1}{2}$ also tends to be small. Hence, we would expect the CUFFQI Algorithm to have a complexity of $O(R^{1/2} D'^{\varepsilon})$ in most cases, if the Generalized Riemann Hypothesis holds.

§5.8. The Tschirnhausen Algorithm of Shanks.

For a generating polynomial which is constructed by the CUFFQI algorithm, there is no guarantee that the index we obtain has the least possible value. Although there is no known fast algorithm for obtaining a generating polynomial with a minimal index, Shanks[Sha87] pointed out that there exists a method which may reduce the size of the index for a given generating polynomial. Shanks calls this method "Tschirnhausen". Its basic idea is to transform one generating polynomial to another that corresponds to the same field; the only difference is that the new polynomial should have a smaller index. Although this method is basically sound, there is no concrete approach to implement this algorithm such that the smallest index of a generating polynomial for a given cubic field is found.

This method is based on the following theorems:

Theorem 5.8.1. ([Sha87]) For a given generating polynomial $x^3 - 3Qx + A$ with polynomial discriminant $-27B^2D'$, let $Q \equiv 1 \pmod 3$, $A \equiv 2 \pmod 9$, and $W \equiv V \pmod 3$, where $W = (Q - 1) / 3$, $V = (A - 2) / 9$. Then, by making the substitution $x = 3y + 1$ and dividing by 27 in the expression $x^3 - 3Qx + A$, we get

$$y^3 + y^2 - Wy + (V - W) / 3 = 0,$$

with polynomial discriminant $-B^2D'$. ■

Theorem 5.8.2. ([Sha87]) If

$$f(y) = y^3 + ay^2 + by + c = 0$$

has index I and if a translation $y = z + s$ gives us

$$z^3 + A'z^2 + B'Iz + HI^2 = 0$$

where $f(s) \equiv 0 \pmod{I^2}$, $f'(s) \equiv 0 \pmod I$, $A' = f''(s)$, $B = f'(s) / I$, $H = f(s) / I^2$, then the transformation $u = HI / z$ gives us

$$u^3 + Bu^2 + AHu + IH^2 = 0$$

with index H. ■

With these two theorems, we are now able to present a version of the Tschirnhausen algorithm.

Algorithm 5.8.1.

Given: a generating polynomial f(x) with discriminant D and index I.

1) Employ Theorem 5.8.1, if applicable.

2) Find the smallest positive[$] s that satisfies $f(s) \equiv 0 \pmod{I^2}$ and $f'(s) \equiv 0 \pmod I$.

3) For each s', where $f(s') \equiv 0 \pmod{I^2}$ and $f'(s') \equiv 0 \pmod I$, which lies between $s + 50I + 1$ and $s - 50I - 1$, find the corresponding H.

4) If the smallest H in **step** 3 is less than I, then apply Theorem 5.8.2 and goto **step** 2.

5) Stop.

[$]We first solve for x such that x satisfies the congruences $f(x) \equiv 0 \pmod I$ and $f'(x) \equiv 0 \pmod I$. Then we use the standard lifting technique to find s.

This algorithm can easily be modified if necessary. In Step 3, the bounds are selected by a series of trials and they can be changed if needed. Further, if there are two or more H's which are smaller than the current index at a given round, it is possible to apply Theorem 5.8.2 to each value of H . It is, however, very time consuming.

§5.9. Computational results and tables.

The entire algorithm of CUFFQI was programmed in FORTRAN with 16 bytes precision and run on an Amdahl 5870 computer. The program is capable of handling any fundamental discriminant which is less than 30 (decimal) digits. First, we ran the program for 3 of the discriminants D which are given in Quer[Que87]. They are

$$D = -408368221541174183,$$

$$D = -3082320147153282331,$$

$$D = -3161659186633662283.$$

For each of these discrminants, it is known that $Q(\sqrt{D})$ has a 3-rank of 6. The result of this computation is included in Appendix 1. We found that the running time ranged between 35 CPU seconds to 3 CPU minutes depending on the size of the regulator of $Q(\sqrt{D'})$.

We also ran this program for many other D values. They include all the D values which were published in Llorente and Quer[LQ88B] and Diaz y Diaz, Llorente and Quer[DLQ88]. We present a few examples to demonstrate the results of our computation. In Table 5.9.1, we provide a generating polynomial, $x^3 + ax^2 + bx + c$ for each of the non-isomorphic cubic fields with discriminant -35102371403731. Here the 3-rank of $Q(\sqrt{1053071142111193})$ is 4 and the 3-rank of $Q(\sqrt{-35102371403731})$ is 5. In Table 5.9.2, we present a generating polynomial, $x^3 + ax^2 + bx + c$, for each of the non-isomorphic cubic fields with discriminant -250930267537731. In this case the 3-rank of $Q(\sqrt{83643422512577})$ is 4 and the 3-rank of $Q(\sqrt{-250930267537731})$ is 4 (n is used to identify the corresponding cubic field). In Table 5.9.3, we show how some of the prime ideals split in each of the complex cubic fields which are listed in Table 5.9.2. This table

shows that all the cubic fields in Table 5.9.2 are indeed non-isomorphic. 'X' is used to denote the cubic field in which the prime completely splits and ' ' is used to denote the cubic field in which the prime is inert. Only primes p such that (D/p) = 1 are used here.

The Tschirnhausen algorithm was programmed in ALGEB, a multi-precision package written by David Ford, and was run on a MicroVAX II computer. The reason for using ALGEB instead of FORTRAN was that large integers (exceeding the precision that can be conveniently handled by other languages) might arise during the computations. We performed the Tschirnhausen algorithm on each of the generating polynomials listed in Appendix 1, and the results are also included in Appendix 1. Further, we performed the Tschirnhausen Transformation on each of the generating polynomials listed in Table 5.9.2. These newly transformed polynomials, some of which have smaller indices, are presented in Table 5.9.4. By inspecting these newly transformed polynomials, as given in Appendix 1 and Table 5.9.4, we found that every index is less than $2D^{1/4}/\sqrt{27}$.

a	b	c	Index
1	-578736	321679764	240
1	738275	-165877164	259
0	-1291312	12261401687	10765
1	-77031	-31892292	27
1	561334	-3198044.	142
1	-690579	-1281628656	1107
1	-2231671	-1291832346	125
1	15665	859992	1
1	812686	-325680036	378
0	-7018	1117533	1
1	-1598101	-857071276	315
0	188012	31398797	1
0	190922	146098889	125
0	-442384	350443673	323
0	1197704	504514291	1
1	57941	23354306	21
1	-1069851	-446685102	117
0	-1137574	60538903	413
1	2205633	-31362882656	27529
0	937124	415185025	197
0	325574	337190269	289
1	-284947	-66241510	27
1	-618857	-314229506	221
1	1093046	112034484	398
1	457395	-114555122	145
1	-3647	1142146	1
0	1175114	1616577429	1351
1	1355679	-14432864	533
1	-2050329	-3819257804	3199
1	92001	-28820682	27
1	1633331	-563591374	861
0	2818847	25218994514	22060
1	-3049137	3592613016	2589
1	3734	-2277492	2
1	-2548840	-1721132464	624
1	714773	-90608686	219
1	774690	-300379292	350
1	-8704	9124164	8
1	238883	-36825646	51
1	-389472	-118778624	64
1.	386819	-263429556	245
0	-1097182	161496361	413
1	831173	69969510	263
0	1244	1140339	1
0	928082	344135933	1
1	78136	3566404	8
1	-216864	249262596	216
1	208116	-192612752	172

a	b	c	index
0	-71767	70304884	62
1	-1121471	561805666	287
1	54779	2873154	5
1	503793	-168608174	191
0	16346	1395395	1
0	207173	100295184	82
1	-262977	277322956	239
0	-1584874	551095895	829
1	-1886776	-1065968064	328
0	314567	366651062	316
0	174023	607237034	532
1	-148089	-51688334	41
0	51932	4695667	1
1	-1628427	-2349505580	1937
1	702911	318829188	343
0	-20626	9699	1
0	-1596838	4071256409	3635
1	421829	-528770874	473
1	16263	819604	1
0	-2150812	5888489541	5273
1	829881	367617726	411
1	1453654	-218404172	622
0	-339574	189354585	179
1	410769	-100091906	125
1	156883	-1090374	21
1	-3152161	2188239588	343
1	2502255	-282051198	1359
0	-172381	67574366	64
1	1426638	-100538100	582
0	36971	9523242	8
1	-527129	-150665466	27
1	3035958	-690974804	1886
1	-95882	-89699820	78
1	-68757	7009606	1
1	-2128454	1289431716	426
1	-783859	-270017716	33
0	462659	141410114	64
0	1513586	835756907	377
1	-361511	-165387836	125
0	-1517848	171863563	649
1	3339498	499841964	2106
1	-7344	-9127376	8
1	-15629	1360696	1
1	79006	134299804	118
1	2205881	999838326	1411
0	-57709	7398178	8
1	-1373105	-668208384	219
1	18803	-30763510	27

a	b	c	index
1	1018853	-1629536844	1471
1	721221	340436754	363
1	-666337	293755614	181
1	449975	-82410000	125
1	-137021	-36499524	27
1	-2585007	5268208540	4403
1	-1995974	-6610135476	5718
1	-155526	-887452364	778
1	288175	103961748	105
1	718791	1224221128	1093
1	-216555	38732932	1
0	284897	163615892	134
1	366705	2873268	75
1	67104	6222448	8
0	-19654	418755	1
0	2478848	1508929703	125
0	304112	64560397	1
1	919948	-120026516	316
1	-618009	447749064	357
0	2466218	1535537399	323
1	-169281	144969544	125
1	-246629	-784826496	687
1	596038	-1225341276	1086
0	146843	23500966	8
1	756848	526163520	512

Table 5.9.1

n	a	b	c	Index
1	0	1801704	943731441	51
2	0	1539618	3597043217	1155
3	0	20337711	47506527742	10428
4	1	-205142	-133008540	42
5	0	-1133960	-470878908	24
6	0	19687368	385851387789	126087
7	0	-8784303	26228064564	9210
8	0	-5562264	2171939783	1803
9	0	-77622	3789009	3
10	1	-64761	11108646	3
11	0	-17096691	66793401040	23658
12	0	-434874	917094677	303
13	0	9882096	13159847993	1803
14	1	-884512	323586356	16
15	0	-5731716	23550437615	7917
16	0	-3484218	1766513119	1005
17	0	9362487	11583358362	1164
18	0	16175226	102066140493	32457
19	0	-4509426	5968374449	2301
20	0	3968958	5531149143	1515
21	0	11011737	14675231772	1374
22	0	-438888	15245434147	5001
23	0	-17152809	20182838598	11148
24	0	9944994	12427521651	969
25	0	12519408	17088260643	375
26	0	3915498	7824786489	2373
27	0	10221762	12630572109	375
28	0	1844772	1714532539	465
29	0	4129143	8978380474	2748
30	0	22442889	43783344036	5106
31	1	-1389537	-656072616	59
32	1	-17459	-9194502	3
33	0	-12068088	430902459	5295
34	0	2993046	10785586153	3477
35	1	1452971	7215486128	2377
36	1	1547976	-148057536	248
37	0	21799644	48471791215	9363
38	0	670677	4303664104	1410
39	0	113376	17307423	3
40	0	5159883	4549176954	192

Table 5.9.2

n\p	5	7	47	67	71	79	89	103	107	109	127	179	181	191	197
1			X			X	X			X	X		X		
2	X	X		X	X						X	X		X	
3			X			X									
4	X	X	X	X	X	X			X						
5												X			X
6		X			X									X	
7	X			X				X	X						
8			X				X			X		X	X		
9		X	X		X				X			X			
10		X			X		X	X			X				
11	X			X					X	X			X	X	
12							X				X			X	
13								X		X			X		
14							X					X		X	
15	X	X		X	X					X			X		
16	X	X		X	X		X	X							X
17			X			X		X				X		X	X
18									X	X		X	X	X	
19								X		X			X		X
20	X			X		X		X		X	X	X	X		
21						X	X		X						
22			X					X			X			X	
23						X			X	X	X		X	X	X
24			X												X
25	X			X			X		X		X	X			X
26		X			X					X		X	X	X	X
27	X		X	X							X	X			
28	X			X		X	X							X	X
29		X	X		X				X		X				X
30								X	X		X				X
31											X				
32							X		X						
33	X		X	X			X			X			X		X
34		X			X	X								X	X
35						X		X	X			X			
36		X	X		X		X	X	X	X			X	X	
37	X			X		X									
38	X		X	X				X						X	
39		X			X	X				X	X		X		
40		X			X	X	X	X				X			

Table 5.9.3

n	a	b	c	Index
1	0	-1801704	943731441	51
2	0	-1539618	3597043217	1155
3	5239	-3344331	518574012	223
4	1	-205142	-133008540	42
5	1	-1133960	-470878908	24
6	-155	15768	72626112	24
7	4757	5279265	2442722250	515
8	3089	110544	1019603712	752
9	0	77622	3789009	3
10	1	-64761	11108646	3
11	727	69375	369656250	125
12	0	434874	917094677	303
13	-4048	4100832	3912021387	1473
14	1	-884512	323586356	16
15	724	-9000	1113328125	375
16	3649	-653562	781813620	882
17	24419	-862407	7637004	81
18	-382	272646	212950377	81
19	3274	-243972	15096861	81
20	0	-3968958	5531149143	1515
21	3187	4872015	706358286	717
22	1795	-1963668	752870544	388
23	1627	417717	658278252	243
24	2926	4575888	529191249	739
25	0	-12519408	17088260643	375
26	-851	2208510	2034790548	926
27	0	-10221762	12630572109	375
28	0	-1844772	1714532539	465
29	5045	-4283301	934014972	583
30	-2071	1605123	369475266	269
31	1	-1389537	-656072616	59
32	1	-17459	-9194502	3
33	4952	8373060	8743236375	1285
34	9676	-6523860	1119194937	1029
35	627	-418080	3702187008	1248
36	1	1547976	-148057536	248
37	-1588	980400	432804675	215
38	0	-670677	4303664104	1410
39	0	-113376	17307423	3
40	0	-5159883	4549176954	192

Table 5.9.4

Chapter 6.
Pure Cubic Fields with Large Regulators

§6.1 Introduction.

Let δ be the real zero of $x^3 - ax^2 + bx - c$, an irreducible cubic polynomial with rational integer coefficients a, b, c, and negative discriminant D(a,b,c). Let $\mathbf{Q}(\delta)$ be the cubic field formed by adjoining δ to the rationals $\mathbf{Q}$. If a = b = 0, we say that $\mathbf{Q}(\delta)$ ($\delta = c^{1/3}$) is a pure cubic field. Let D = D(0,0,c) be the discriminant of the pure cubic field $\mathbf{F} = \mathbf{Q}(\delta)$. We may assume that $c=mn^2$ ($m,n \in \mathbf{Z}$) with m, n square-free and gcd(m,n) = 1. In this case, we have

$$D = \begin{cases} -3m^2n^2 & \text{when } m^2 \equiv n^2 \pmod 9 \\ -27m^2n^2 & \text{otherwise.} \end{cases}$$

The regulator of $\mathbf{Q}(\delta)$ is $R = \log\varepsilon_0$, where ε_0 (>1) is the fundamental unit of $\mathbf{F}$.

In Patterson and Williams [PW85] a search was made to find pure cubic fields with large regulators. The search was terminated when $c > 2^{31}-1$ because, in spite of using the rapid method of Williams, Dueck and Schmid [WDS83] (the WDS method), it was still very time-consuming to compute R. The purpose of this chapter is to provide a modified WDS method which executes more rapidly. We do this in order to extend the search begun in [PW85] to find values of c which lie between $2^{31}-1$ and 10^{12}. A brief description of the WDS method is given in §6.3, and a description of our modifications are presented in §6.4 and §6.5. Further, we are especially interested in those values of c which provide a large C(c) value, where

$$C(c) = R / (mn \operatorname{loglog} (3D^2))$$

as defined in [PW85]. Basically, C(c) is a measure which can be used to test the truth of the Generalized Riemann Hypothesis for $\zeta_{\mathbf{F}}$. We would expect C(c) to be less than ≈ 1.18738 if the GRH holds (for details, see [PW85]). We should also point out that the

largest previously determined C(c) value for $28 < c < 2^{31} - 1$ is 0.677194 for c=60435383. In §6.2, we describe a method which is similar to that used in [PW85] for selecting certain values of c for which R and C(c) are likely to be large. Finally, the results of this search are provided at the end of this chapter.

§6.2 Strategy for finding values of c.

From (3.1.1) we have

$$hR = \frac{\sqrt{|D|}\Phi(1)}{2\pi} \tag{6.2.1}$$

where $\Phi(1) = \lim_{s \to 1} \frac{\zeta_F(s)}{\zeta(s)}$ is given by the Euler product

$$\Phi(1) = \prod_p f(p). \tag{6.2.2}$$

Here, the product is taken over all the rational primes, and for each prime p the value of f(p) depends upon how the principal ideal (p) splits or factorizes in **F**. Thus, in order to maximize R we must minimize h and get $\Phi(1)$ as large as possible. By Honda [Hon71], the values of c for which 3 is not a divisor of the class number have the following form:

$$\begin{aligned}
&\text{(i)} && c = 3, \\
&\text{(ii)} && c = p && \text{where } p \equiv -1 \pmod 3, \\
&\text{(iii)} && c = 3p && \text{where } p \equiv 2, 5 \pmod 9, \\
&\text{(iv)} && c = 9p && \text{where } p \equiv 2, 5 \pmod 9, \\
&\text{(v)} && c = pq && \text{where } p \equiv 2 \pmod 9,\ q \equiv 5 \pmod 9, \\
&\text{(vi)} && c = pq^2 && \text{where } p \equiv q \equiv 2,5 \pmod 9,
\end{aligned} \tag{6.2.3}$$

and p, q are primes. In [PW85] it is suggested that the values of c of types (v) and (vi) are likely to have smaller C(c) values. Also, values of c such that $c \not\equiv \pm 1 \pmod 9$ are likely to have larger R values. Thus, we elected to search for values of c of three different types:

$$\begin{aligned}
&\text{(i)} && c = p && \text{where } p \equiv 2,5 \pmod 9, \\
&\text{(ii)} && c = 3p && \text{where } p \equiv 2,5 \pmod 9, \\
&\text{(ii)} && c = 9p && \text{where } p \equiv 2,5 \pmod 9,
\end{aligned} \tag{6.2.4}$$

where p is a prime.

We now discuss the problem of maximizing $\Phi(1)$. Since

$$\kappa_1 = \prod_{p \equiv -1 (\mathrm{mod}\ 3)} f(p)$$

converges (approximate value 1.414064387), we are only interested in the primes $p \equiv 1 \pmod 3$ in maximizing $\Phi(1)$. Hence, we see that, if r_i is the i^{th} prime of the form $1+3t$ ($t \in \mathbf{Z}^+$), then c values which should give large $\Phi(1)$ values are those for which $\left(\frac{c}{r_i}\right)_3 = 1$ ($i = 1, 2, \ldots, n$), for as large a value of n as possible. In fact, this is the strategy utilized in [PW85] for finding values of c which are likely to have a large R value. However, this strategy has a major drawback due to the possibility that a value of c ($= c_1$) which has m ($m < n$) consecutive cubic residues might have a larger $\Phi(1)$ value than a value of c ($= c_2$) which has n consecutive cubic residues. The reason for this is that c_1 might have a large number of cubic residues for the r_i's $> r_m$, whereas c_2 might have a large number of cubic non-residues for the r_i's $> r_n$. Hence, we used a different approach for finding values of c. Our strategy was first to select all the probable c values which satisfy (6.2.4) and are cubic residues of the first 15 primes $r_1, r_2, \ldots, r_{15}$ (i.e. $\left(\frac{c}{r_i}\right)_3 = 1$ for $i = 1, 2, \ldots, 15$). For each such value, we determined the number of values of r_i such that $\left(\frac{c}{r_i}\right)_3 \neq 1$ for the next nine r_i's (i.e. $i = 16, 17, \ldots, 24$). If this value had 6 or fewer, we used the Euler product method to find a reasonable estimate E (for details, see §6.4) of hR. For each pair of E and c values, we computed $\tilde{C}(c) = E / (mn \log\log(3D^2))$ of C(c). If $\tilde{C}(c)$ was 0.67 or above, then the regulator of $Q(c^{1/3})$ was computed.

Finding values of c which have 15 consecutive cubic residues requires that we find solutions of simultaneous linear congruences, a problem best solved by using a number sieve (see Lehmer [Leh80]). In our case, we were able to use the latest development in automated sieving called the "Open Architecture Sieve System" (OASiS) of Stephens and

Williams [SW90]. This system features a specially-designed computer - the Open Architecture Sieve - that is capable of testing possible solutions to a system of linear congruences at a rate of over 200 million numbers per second. We found that it took about 84 minutes for OASiS to inspect all the probable c values between $2^{31} - 1$ and 10^{12}, and 1251 numbers were generated. For the remaining work, we used a FORTRAN program with some assembly language subroutines on an Amdahl 5870 computer to find values of c and $\tilde{C}(c)$. After 85 CPU hours, in which over 99% of the time was spent in the approximation of hR, 72 numbers were found. Execution was slow because all the primes of the form $1+ 3t$ ($t \in Z$) up to 10^8 were used to compute a good approximation to hR for each given value of c.

Our results are provided in the following tables. In Tables 6.2.1, 6.2.2, 6.2.3 and 6.2.4 below, we give the number of c values that we found such that c is a cubic non-residue for i (i = 1, 2,..., 9) values of the r_j's where j = 16, 17, ..., 24. In Tables 6.2.5, 6.2.6, 6.2.7 and 6.2.8 we give those values of c for which $\tilde{C}(c)$ exceeds 0.670. In the course of our search, we found that there is only one c (c = 144646415187) value for which there is a single cubic non-residue for the first 24 r_i's. In §6.6. we show that this c value gives the best C(c) value in our search.

i	# of c values
1	0
2	0
3	19
4	48
5	82
6	98
7	86
8	58
9	11

Table 6.2.1

$(c = p \equiv 2 \pmod 9)$

i	# of c values
1	0
2	3
3	11
4	62
5	78
6	124
7	105
8	39
9	15

Table 6.2.2

$(c = p \equiv 5 \pmod 9)$

i	# of c values
1	1
2	0
3	11
4	32
5	47
6	97
7	76
8	35
9	12

Table 6.2.3

($c = 3p$, $p \equiv 2,5 \pmod 9$)

i	# of c values
1	0
2	1
3	5
4	12
5	15
6	28
7	24
8	12
9	4

Table 6.2.4

($c = 9p$, $p \equiv 2,5 \pmod 9$)

c	$\tilde{C}(c)$	c	$\tilde{C}(c)$
7823785241	0.68098	289191889433	0.67094
10389989063	0.68213	292277713727	0.67949
23002424327	0.67234	506642469059	0.67443
43595987609	0.67183	576605603657	0.68446
79600195163	0.69223	578450121761	0.70008
90307528193	0.67639	748224663941	0.69798
119087387453	0.67762	800855660207	0.68013
195511299437	0.68791	844409282933	0.67081
21355190977	0.67387	988024756357	0.67365
234187560641	0.69329		

Table 6.2.5

$(c = p \equiv 2 \pmod 9)$

c	$\tilde{C}(c)$	c	$\tilde{C}(c)$
23904870683	0.67078	399933625181	0.68002
41843313959	0.67906	404698499087	0.67827
57913659383	0.67417	416520048911	0.68003
58182013553	0.67641	464191218707	0.69844
79834584857	0.67784	466353166469	0.67562
113913197789	0.67652	471882449219	0.67301
122089073261	0.67120	493979588159	0.67711
130962864677	0.67287	530161973249	0.67061
136544134973	0.67739	533183662103	0.67011
210018369371	0.67179	760106056289	0.67246
226956644069	0.67751	778769068631	0.67084
272330743901	0.67609	792802846373	0.67644
327552647297	0.67185	902875793639`	0.67580
336949891277	0.69213		

Table 6.2.6

$(c = p \equiv 5 \pmod 9)$

c	$\tilde{C}(c)$	c	$\tilde{C}(c)$
74354863227	0.67939	293203999941	0.67695
99052148229	0.67581	362264296659	0.67926
102879790287	0.67027	413557332189	0.69612
117807496071	0.67043	455271781749	0.67854
144646415187	0.71023	748671032481	0.67041
229362553239	0.68346	912685074153	0.68285
291987409839	0.68079		

Table 6.2.7

($c = 3p$, $p \equiv 2,5 \pmod 9$)

c	$\tilde{C}(c)$	c	$\tilde{C}(c)$
11382801093	0.67118	505919205819	0.68434
109324288107	0.67974	648369068283	0.67996
149832113787	0.67959	654007847319	0.67139
298968550119	0.68056	683030699469	0.67983
368636786253	0.67510	747241701597	0.67167
373775618061	0.67943	937165977747	0.67508
433769568597	0.67296		

Table 6.2.8

($c = 9p$, $p \equiv 2,5 \pmod 9$)

§6.3 Calculation of R by using the WDS method.

In order to describe the WDS method, we must first discuss some of the results concerning the continued fraction algorithm of Voronoi [Vor96] and reduced ideals in cubic fields. The brief discussion here is analogous to that in §5.2. For a detailed description, we refer the reader to [WCS80] and [WDS83].

We define an ideal $\mathbf{a}$ to be primitive if $\mathbf{a}$ has no rational prime divisors. We say that $\mathbf{a}$ is a reduced ideal in $\mathbf{O_F}$ if $\mathbf{a}$ is primitive and there does not exist $\alpha \in \mathbf{a}$ such that $\alpha \neq 0$ and both $|\alpha| < N(\mathbf{a}), |\alpha''| = |\alpha'| < N(\mathbf{a})$ hold. With this definition, we are now able to present some of the properties of reduced ideals.

Theorem 6.3.1. If $\mathbf{a}$ is a reduced ideal of $\mathbf{O_F}$, then $N(\mathbf{a}) < \sqrt{|D|/3}$.

Theorem 6.3.2. There exist only a finite number of reduced ideals of $\mathbf{O_F}$.

Let $\mathbf{i}_1$ (= (1)) be the unit ideal. We can use Voronoi's algorithm to generate a list of reduced principal ideals equivalent to $\mathbf{i}_1$, together with a sequence of elements $\theta_g^{(1)}$, $\theta_g^{(2)}$, $\theta_g^{(3)}$, ... of $\mathbf{F}$, each of which exceeds 1. These reduced ideals can be arranged in a sequence

(6.3.1) $$\mathbf{i}_1, \mathbf{i}_2, \mathbf{i}_3, \ldots, \mathbf{i}_{k-1}, \mathbf{i}_k, \ldots$$

where

$$(N(\mathbf{i}_{k-1})\theta_g^{(k-1)})\mathbf{i}_k = (N(\mathbf{i}_k))\mathbf{i}_{k-1}.$$

If we define $\theta_1 = 1$ and

$$\theta_k = \prod_{i=1}^{k-1} \theta_g^{(i)} \quad (k > 1),$$

we get

$$(\theta_n)\mathbf{i}_n = (N(\mathbf{i}_n))\mathbf{i}_1.$$

We say that $\log\theta_n$ is the distance from $\mathbf{i}_1$ to $\mathbf{i}_n$, written as

$$\delta_n = \delta(\mathbf{i}_n, \mathbf{i}_1) = \log\theta_n .$$

Also, we note that this notion of distance in cubic fields is the extension of Shanks' infrastructure idea (see §5.2) given in Williams, Dueck and Schmid [WDS83]. Since

$\theta_g^{(i)} > 1$, we have $\delta(\mathbf{i}_{n+1}, \mathbf{i}_1) > \delta(\mathbf{i}_n, \mathbf{i}_1) > 0$ for $n > 1$, and $\delta(\mathbf{i}_n, \mathbf{i}_1) = 0$ if and only if $n = 1$. The number of reduced principal ideals is finite; at some point in (6.3.1) we get $\mathbf{i}_{p+1} = \mathbf{i}_1$ and $\theta_{p+1} = \varepsilon_0 > 1$, where ε_0 is the fundamental unit of $\mathbf{F}$. Thus, $\delta_{p+1} = R$. Furthermore, $\mathbf{i}_n = \mathbf{i}_s$ if and only if $\delta_n = mR + \delta_s$ ($m \in \mathbf{Z}$). Therefore, if $\mathbf{i}_n = \mathbf{i}_s$, then $n = qp+s$ where $q \in \mathbf{Z}$.

Suppose that $\mathbf{i}_n$ and $\mathbf{i}_m$ are two reduced principal ideals with distances δ_n and δ_m. If

$$(u)\mathbf{a}_1 = \mathbf{i}_n\mathbf{i}_m ,$$

where $u \in \mathbf{Z}$ and $\mathbf{a}_1$ is a primitive ideal in $\mathbf{O}_F$, then we can use the reduction algorithm on p.277 in [WDS83] (also, see [Vor96]) to find a reduced ideal $\mathbf{a}_k$ ($\sim \mathbf{a}_1$) such that

$$(L(\mathbf{a}_1)\rho_k)\mathbf{a}_k = (L(\mathbf{a}_k))\mathbf{a}_1$$

where $\rho_k < 1$. Since $\mathbf{a}_k$ is a reduced principal ideal, we have $\mathbf{a}_k = \mathbf{i}_t$ for some integer t and $\delta_t = \delta_n + \delta_m + \eta$. Here, η can be explicitly evaluated and $-2\log|D/3| < \eta < 0$. We note that, since $\delta_t < \delta_n + \delta_m$, we can apply Voronoi's algorithm to $\mathbf{i}_t$ to find a reduced principal ideal $\mathbf{i}_j$ such that

$$\delta_j < \delta_n + \delta_m < \delta_{j+1}.$$

We now sketch the WDS method given in [WDS83].

The first step is to use Voronoi's algorithm (see [WDS83] and [WCS80]) to generate a sequence of reduced principal ideals

$$\mathbf{i}_1(\sim (1)), \mathbf{i}_2, \mathbf{i}_3, \ldots, \mathbf{i}_t$$

such that $\delta_t < T < \delta_{t+1}$ and T is some input parameter. At the same time we also compute the distance δ_j for each of the above ideals $\mathbf{i}_j$ ($1 \le j \le t$). Since storing all t reduced ideals may require more storage than the computer is capable of handling, we choose to store only 1/x of them where x is also an input parameter. Thus, we only store the reduced ideals $\mathbf{i}_{jx}$ ($j = 1, 2, 3, \ldots, t/x$). Here, we assume that $x \mid t$. In the case where $x \nmid t$, we increase the value of T in order for x to be a factor of t. We also store the corresponding values of δ_{jx}. If, during the process of generating these ideals, we find that $N(\mathbf{i}_j) = 1$ for some j, then

$$R = \delta_j.$$

If R is not found, in this step we continue the process by using the Euler product method to find an estimate E of hR. We first note that L is an input parameter. We then find n and U such that

$$E - L = 2^n U$$

where $n \in \mathbf{Z}$ and $2U > \delta_t \geq U$. We search through the list of ideals $\{\mathbf{i}_{1x}, \mathbf{i}_{2x}, \mathbf{i}_{3x},..., \mathbf{i}_t\}$ to find $\mathbf{i}_u$ such that $\delta_{u+1} > U > \delta_u$. The Doubling algorithm on pp. 277-278 in [WDS83] can then be used n times to find a reduced ideal $\mathbf{i}_m$ with $\delta_m \approx E - L$ and $\delta_m < E - L$. Starting at $\mathbf{i}_m$, we use the Search algorithm on p.280 in [WDS83] to attempt to find an ideal, $\mathbf{i}_v$, such that

$$E - L < \delta_v < E + L \text{ and } \mathbf{i}_v = \mathbf{i}_a,$$

where $\mathbf{i}_a \in \{\mathbf{i}_1(\sim (1)), \mathbf{i}_2, \mathbf{i}_3,..., \mathbf{i}_t\}$. If $\mathbf{i}_v$ is not found, then we must increase the size of L. On the other hand, if $\mathbf{i}_v$ is found, then we probably have $hR = \delta_v - \delta_a$. However, we certainly have $h^*R = \delta_v - \delta_a$, where $h^* \in \mathbf{Z}$. Although h^*R is known, the values of h^* and R remain to be determined. The next step, therefore, is to find h^*. For an input parameter b, we find B such that $(B+1)\delta_t > h^*R/b > B\delta_t$. Assuming that $R \geq h^*R/b$, we use the following technique to find h^* and R. Since $R \geq h^*R/b$, we have $h^* < b$. We now attempt to find all the primes less than b which divide h^*. If p is such a prime, then $\delta_s = h^*R / p$ for some s. If we let

$$\frac{h^*R}{p} = 2^m U_p$$

where $2U_p > \delta_t \geq U_p$, we can repeat the above procedure to find a reduced ideal $\mathbf{i}_w$ and δ_w such that $\delta_w < h^*R / p$ and h^*R / p is close in value to δ_w. We can then apply Voronoi's algorithm to $\mathbf{i}_w$ to find $\mathbf{i}_{w+1}, \mathbf{i}_{w+2},...$ until we either find $\mathbf{i}_y$ such that $N(\mathbf{i}_y) = 1$, in which case $p \mid h^*$, or we can find $\mathbf{i}_y$ such that $\delta_y > h^*R / p$, in which case $p \nmid h^*$. If we find a prime p which does divide h^*, we must replace $\mathbf{i}_v$ by $\mathbf{i}_y$, δ_v by δ_y, and repeat the above procedure to determine the precise power of p that divides h^*. When this process has been completed for all primes less than b, we probably have the values of h^*

and R. However, we cannot be certain that $R \geq h^*R/b$. Thus, we must use the Search algorithm on p.280 in [WDS83] to determine whether or not $R < h^*R/b$. If $R < h^*R/b$, then R and h^* are calculated in this step. At the end of this process, we certainly have h^* and R. Notice that while there may be some doubt about $h = h^*$, the value R is correctly computed.

The algorithm described above was implemented in FORTRAN-H (extended) for an Amdahl 5870 computer. The purpose of this implementation was to determine the speed of the WDS method on a faster machine. The extended precision allowed us to operate on numbers of up to 33 decimal digits. For values of $c < 10^{12}$, this amount of precision is sufficient except for two of the subroutines required in the reduction algorithm on p.277 in [WDS83]. (This problem also occurred in [WDS83].) These two subroutines were modified by using special purpose multi-precision FORTRAN language subroutines, and are capable of handling up to 60 decimal digits. Also, we found that Voronoi's algorithm, except for the inversion process, for finding an adjacent reduced ideal i_k to a given reduced ideal i_{k+1} (we call this process a "baby step") required double precision. As a result, the speed of performing a baby step could be increased. This program was run with $Q = 10^8$, $T = 50000$, $b = 5000$, $x = 15$. On running the program, we found that the amount of time taken to perform a baby step was about 0.75 of a millisecond. The average time required to perform an ideal operation (Here and in the sequel, we use the term "ideal operation" to mean the multiplication of two reduced ideals followed by the reduction operation.) was about 37.5 milliseconds. The speed of the program was tested on a few c values which were selected from those mentioned in §6.2. We found that the WDS method was somewhat slow in computing regulators for $c > 2^{31}-1$. For example, it took 21 CPU minutes to compute R (= 3208632480642.32164235) for $Q(998024756357^{1/3})$. Hence, possible modifications to the WDS method were investigated. By studying the running time of the program carefully, we found that most of the computing time was spent on calculating E and executing the search step. Indeed, it took about 5 CPU minutes to

compute an approximation of hR and 11 minutes to execute the search step. As a result, modifications were focused in these two sections. In the following section, we discuss the number of primes of the form 3t+1 that are needed to obtain a reasonable estimate of hR here. In §6.5, we present a new technique for determining h^*.

§6.4 Estimation of hR by using the Euler product method.

From (6.2.1) we see that, in order to estimate a value E of hR, we must obtain a reasonable approximation of $\Phi(1)$. Since

$$\kappa_1 = \prod_{p \equiv -1 (\mathrm{mod}\ 3)} f(p)$$

converges (approximate value 1.414064387), we can approximate $\Phi(1)$ by evaluating the product over the primes $p \equiv 1 \pmod 3$ only. If we set

$$F(Q) = \prod_{p \equiv 1 (\mathrm{mod}\ 3)}^{Q} f(p),$$

$$T(Q) = \prod_{\substack{p \equiv 1 (\mathrm{mod}\ 3) \\ p > Q}} f(p)$$

and

$$\kappa_2 = f(3)\,\kappa_1 \prod_{\substack{p \equiv -1 (\mathrm{mod}\ 3) \\ p \mid c}}^{Q} f(p)$$

then

$$\Phi(1) = \kappa_2 F(Q) T(Q).$$

Hence, we can estimate hR by calculating

$$E(Q) = \frac{3\sqrt{3}cF(Q)\kappa_2}{2\pi}. \qquad (c \not\equiv \pm 1 \pmod 9)$$

Thus, the real difficulty lies in knowing the value of Q to use such that E(Q) gives a reasonable approximation to hR.

In [WDS83], the authors used $Q = 10^6$ for $c \le 2\text{x}10^7$, $Q = 10^7$ for $2\text{x}10^7 < c < 2\text{x}10^8$, and $Q = 10^8$ for $2\text{x}10^8 < c < 2^{31}-1$. Now

$$|E(Q) - hR| = L(Q)$$

where $L(Q) = (\sqrt{3}c\ 3\kappa_2 F(Q)\,|\,1 - T(Q)\,|\,) / 2\pi$. In order to estimate $|\,\log T(Q)\,|$, the authors of [WDS83] used the technique of Cornell and Washington [CW85] of applying the effective form of the Chebotarev Density Theorem as given by Oesterlé [Oes79] (this is conditional on the GRH on ζ_L where **L** is the Galois closure of **F**). We get

$$|\,\log T(Q)\,| \le B^*(Q) + 3/Q$$

where

$$B^*(Q) = \left(\frac{4+3\log Q}{\sqrt{Q}}\right)\frac{2}{3\log Q}\left[\left(\frac{1}{\pi}+\frac{5.3}{\log Q}\right)\log 3^7 c^4 + 6\left(\frac{\log Q}{2\pi}+2\right)\right].$$

It follows that

$$|\,1 - T(Q)\,| < L^*(Q)$$

where

$$L^*(Q) = \mathrm{MAX}(e^{-B^*(Q)-3/Q},\ e^{B^*(Q)+3/Q}).$$

Indeed, we have

$$|E(Q) - hR| = O\left(\frac{mn\log(3D^2)\,Q}{\sqrt{Q}}\right).$$

Consequently, we would expect that E(Q) should give a reasonable approximation to hR when Q is fairly large. In our early computations, we elected to use $Q = 10^8$. However, tests showed that using $Q = 10^8$ was very time-consuming. In fact, it took roughly 5 CPU minutes to compute $E(10^8)$ for a given c value. As a result, possible reduction of the Q value was investigated. In order to determine a good value of Q to be used, we conducted some preliminary numerical experiments. In these experiments, ten c values were selected. For each of these c values, we give $(E(j \times 10^7) - h^*R) / h^*R$ for j = 1,2,...,10 and h^*R in Table 6.4.1. Also, we calculated $|E(Q) - h^*R|$, $L^*(Q)$ and $|\,E(Q) - h^*R\,| / L^*(Q)$, where $Q = 2\times10^7$ and 10^8, for each of the selected c values. The results of these calculations are presented in Tables 6.4.2 and 6.4.3.

Q \ c	7823785241	23002424327	57913659383	99052148229
$1x10^7$	-0.0000325	-0.0000774	-0.0001353	-0.0000927
$2x10^7$	0.0000217	-0.0000421	-0.0000873	-0.0000357
$3x10^7$	0.0000062	-0.0000330	-0.0000555	-0.0000117
$4x10^7$	0.0000053	-0.0000339	-0.0000611	-0.0000117
$5x10^7$	0.0000166	-0.0000324	-0.0000453	-0.0000024
$6x10^7$	0.0000194	-0.0000165	-0.0000298	-0.0000057
$7x10^7$	0.0000165	-0.0000076	-0.0000119	-0.0000096
$8x10^7$	0.0000252	-0.0000092	0.0000039	-0.0000139
$9x10^7$	0.0000151	-0.0000190	-0.0000031	0.0000072
$1x10^8$	-0.0000058	-0.0000204	-0.0000036	-0.0000065
h^*R	24471813751.0	71695952039.6	182377744503.5	314016080815.0

Q \ c	144646415187	336949891277	792802846373
$1x10^7$	0.0000035	-0.0001671	-0.0001565
$2x10^7$	0.0000260	-0.0000424	-0.0001204
$3x10^7$	0.0000047	-0.0000547	-0.0000899
$4x10^7$	-0.0000062	-0.0000304	-0.0000536
$5x10^7$	-0.0000084	-0.0000156	-0.0000510
$6x10^7$	-0.0000015	-0.0000204	-0.0000572
$7x10^7$	-0.0000084	-0.0000213	-0.0000677
$8x10^7$	-0.0000112	-0.0000138	-0.0000454
$9x10^7$	-0.0000138	-0.0000075	-0.0000383
$1x10^8$	-0.0000080	-0.0000085	-0.0000341
h^*R	483332596164.3	1104246425511.4	2555110143668.6

Q \ c	998024756357	34619128889	508595764309
$1x10^7$	-0.0001723	0.0000625	-0.0000197
$2x10^7$	0.0000160	-0.0000016	-0.0000580
$3x10^7$	0.0000122	-0.0000007	-0.0000238
$4x10^7$	0.0000212	-0.0000174	0.0000174
$5x10^7$	-0.0000147	-0.0000450	0.0000039
$6x10^7$	-0.0000120	-0.0000219	-0.0000037
$7x10^7$	-0.0000064	-0.0000203	-0.0000042
$8x10^7$	0.0000015	-0.0000300	0.0000100
$9x10^7$	-0.0000021	-0.0000191	0.0000032
$1x10^8$	0.0000045	-0.0000157	-0.0000000
h^*R	3208632480642.3	21894297483.9	319479555147.7

Table 6.4.1

c	$L^*(Q)$	$\lvert E(Q)-h^*R \rvert$	$L^*(Q)/\lvert E(Q)-h^*R \rvert$
7823785241	1547869338.38	531969.60	2909.70
23002424327	4674962978.72	3015558.71	1550.28
57913659383	12197474324.31	15928861.77	765.75
99052148229	21305815300.59	11207057.58	1901.11
144646415187	33123650563.56	12550500.37	2639.23
336949891277	77375654059.76	46817702.02	1652.70
792802846373	183024759155.98	307557294.28	595.09
998024756357	231148357011.06	51268820.34	4508.56
34619128889	1352716920.57	1495270.82	904.66
508595764309	22624202014.28	518929.04	43597.87

$Q = 2 \times 10^7$

Table 6.4.2

c	$L^*(Q)$	$\lvert E(Q)-h^*R \rvert$	$L^*(Q)/\lvert E(Q)-h^*R \rvert$
7823785241	670480832.74	141019.05	4754.54
23002424327	2022324049.19	1462240.14	1383.03
57913659383	5270539966.63	655956.97	8034.89
99052148229	9201240060.24	2044119.68	4501.32
144646415187	14299894299.77	3875529.37	3689.79
336949891277	33371333212.28	9333186.71	3575.56
792802846373	78861835122.28	87132527.82	905.08
998024756357	99583491545.35	14294790.29	6966.42
34619128889	586488640.28	225436.99	2601.56
508595764309	9753816491.95	5008009.65	1947.64

$Q = 1 \times 10^8$

Table 6.4.3

By looking at the entries in Table 6.4.1, we notice that $E(2x10^7)$ is a fairly good estimate of hR for each of the ten c values. Indeed, the value of $(E(2x10^7) - h^*R) / h^*R$ is very small in all ten cases. From Table 6.4.1 we can see that the approximation to hR improves only slightly as the value of Q grows larger. Hence, this empirical evidence suggests that $Q = 2x10^7$ would be sufficient here, and there is only a minimal gain by using $Q = 10^8$. Furthermore, the time required to compute $E(2x10^7)$ was 1 CPU minute in comparison to the 5 CPU minutes needed to compute $E(10^8)$. Although $E(10^8)$ is a better estimate than $E(2x10^7)$, the difference can easily be made up by having a few extra ideal operations. Here, the time required for those extra ideal operations was between 2 CPU seconds and 20 CPU seconds. Thus, we would expect the running time to be reduced by a significant amount with $Q = 2x10^7$ in our computations. In Tables 6.4.2 and 6.4.3, we notice that there is a big difference between the actual value of $|E(Q) - h^*R|$ and $L^*(Q)$. Indeed, the value of $|E(Q) - h^*R|$ is much smaller than the theoretical bound $L^*(Q)$ of $|E(Q) - h^*R|$ in all ten cases. We also point out that the above phenomenon was noticed in Nield and Shanks[NS74] and [BWB76]. Thus, this empirical evidence suggests that $|E(2x10^7) - h^*R|$ is much smaller than expected.

§6.5 A new technique for determining h^*.

In our technique for finding h^*, we first produce all the primes less than b in descending order. For each prime p_s where $p_s < b$, instead of finding a reduced ideal $\mathbf{i}_y$ such that $\delta_y \approx h^*R / p_s$, we find a reduced ideal $\mathbf{i}_e$ such that

$$h^*R / p_s \le \delta_e \le h^*R / p_s + \delta_t.$$

If $p_s \mid h^*$, then $\mathbf{i}_e$ must be an ideal $\mathbf{i}_j$ in the list $\{\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_t\}$ and $\delta_e = h^*R / p_s + \delta_j$. Thus, in order to determine whether $p_s \mid h^*$, we first have to check if $\mathbf{i}_e \in \{\mathbf{i}_1, \mathbf{i}_2, ..., \mathbf{i}_t\}$. If this is the case, say $\mathbf{i}_e = \mathbf{i}_j$ where $1 \le j \le t$, then we have to check whether or not $\delta_e = h^*R / p_s + \delta_j$. Hence, we have $p_s \mid h^*$ if and only if both conditions hold. Further, if $p_s \mid h^*$, then we must repeat the above procedure to determine the precise power of p_s that

divides h^*. However, since we only store 1/x of the reduced ideals $\{i_1, i_2,..., i_t\}$, we have to employ a technique used in [WDS83] in order to determine whether $i_e \in \{i_1, i_2,..., i_t\}$. We first apply Voronoi's algorithm on i_e to find

(6.5.1) $$i_e, i_{e+1}, i_{e+2}, \cdots, i_{e+x-1}.$$

We then compare each of the reduced ideals of (6.5.1) with $\{i_{1x}, i_{2x},..., i_t\}$. If one of the reduced ideals of (6.5.1) is in $\{i_{1x}, i_{2x},..., i_t\}$, then $i_e \in \{i_1, i_2,..., i_t\}$; otherwise, $i_e \notin \{i_1, i_2,..., i_t\}$. As for the problem of finding an ideal i_e, we employ the following technique.

Initially, we create a list of reduced ideals

$$i_{t_0}, i_{t_1}, i_{t_2}, i_{t_3},..., i_{t_n}$$

where $i_{t_0} = i_t$, and i_{t_j} $(j > 1)$ is a reduced ideal equivalent to $(i_{t_{j-1}})^2$ with $\delta_{t_j} \approx 2\delta_{t_{j-1}}$ $(j = 0, 1, 2,..., n)$ and $\delta_{t_n} > h^*R / 2 > \delta_{t_{n-1}}$. For a prime p_s, we must find a reduced ideal i_e with distance δ_e where

$$h^*R / p_s < \delta_e < h^*R / p_s + \delta_t.$$

From the preceding prime p_{s+1}, we have obtained an ideal i_m such that

$$h^*R / p_{s+1} < \delta_m < h^*R / p_{s+1} + \delta_t.$$

Hence, we first must find an ideal i_s with distance δ_s such that

$$\delta_s \approx h^*R / p_s - \delta_m$$

and

$$h^*R / p_s < \delta_s + \delta_m \leq h^*R / p_s + \delta_t.$$

If i_s is obtained, then i_e can be found by obtaining a reduced ideal equivalent to $i_s i_m$ with distance $\delta_e \approx \delta_s + \delta_m$. Now, we put $h^*R / p_s - \delta_m$ as $r\delta_t$ where r is real. Put $q = [r] + 1$, and we have

$$h^*R / p_s < q\delta_t + \delta_m \leq h^*R / p_s + \delta_t.$$

Suppose we represent q in binary as

$$q = a_k 2^k + a_{k-1} 2^{k-1} + ... + a_o$$

where $a_k = 1$, $a_j = 0$ or 1 $(j < k)$. Note that $k = [\log_2 q]$. Consequently, we have

$$q\delta_t = a_k\, 2^k\, \delta_t + a_{k-1}\, 2^{k-1}\, \delta_t + \ldots + a_o\, \delta_t.$$

Since $\delta_{t_k} \approx 2^k \delta_t$, we can now find an ideal $\mathbf{i}_s$ with distance close to $q\delta_t$ by finding a reduced ideal equivalent to

$$\prod_{\substack{j=0 \\ a_j=1}}^{k} \mathbf{i}_{t_j} \quad .$$

We are now able to present the algorithm for finding h^* when h^*R is known and $R > h^*R/x$.

Algorithm 6.5.1

1) By using the Doubling algorithm on pp.277-278 in [WDS83], we use $\mathbf{i}_t$ to create a list of reduced ideals $\mathbf{i}_{t_0}, \mathbf{i}_{t_1}, \mathbf{i}_{t_2}, \ldots, \mathbf{i}_{t_n}$ where $\mathbf{i}_{t_0} = \mathbf{i}_t$, $\mathbf{i}_{t_j}$ $(j > 1)$ is a reduced ideal equivalent to $(\mathbf{i}_{t_{j-1}})^2$, $\delta_{t_j} \approx 2^j \delta_t$ and $\delta_{t_n} \geq hR / 2 \geq \delta_{t_n - 1}$.

2) Let $p_1, p_2, \ldots, p_m$ be the sequence of primes where $p_{m+1} > x > p_m$.

3) Put $E \leftarrow h^*R$, $h^* \leftarrow 1$.

4) Put $s \leftarrow m$, $\mathbf{a} \leftarrow (1)$ and $\delta' \leftarrow 0$ (δ' is the distance between $\mathbf{a}$ and (1)).

5) Put $z \leftarrow [E / p_s - \delta'] + 1$ and $j \leftarrow 0$.

6) Put rem $\leftarrow z \bmod 2$ and $z \leftarrow (z - \text{rem})/2$.

7) If rem = 1 then find a reduced ideal equivalent to $\mathbf{a}\mathbf{i}_{t_j}$ with distance close to $\delta' + \delta_{t_j}$ and replace $\mathbf{a}$ by this reduced ideal. Also, replace δ' by the new distance between $\mathbf{a}$ and (1).

8) Put $j \leftarrow j + 1$. If $z > 0$, then goto step 6.

9) If $\mathbf{a} = \mathbf{i}_k$ for some ideal $\mathbf{i}_k \in \{\mathbf{i}_1, \mathbf{i}_2, \ldots, \mathbf{i}_t\}$ and $\delta' = E / p_s + \delta_k$ (the case where $p_s \mid h^*$), then replace $E \leftarrow E / p_s$, $h^* \leftarrow h^* p_s$ and goto step 5 (to determine the precise power of p_s that divides h^*).

10) Put $s \leftarrow s - 1$. If $s > 0$, goto step 5.

11) We now have $R = E$ and h^*. We terminate the algorithm.

In using the WDS method, we must find a reduced ideal with distance close to h^*R/p_s for a prime p_s. Since $h^*R / p_s = 2^nU$ where $2U > \delta_t > U$, there are precisely n ideal operations required. In fact, we can determine n by calculating $\left\lceil \log_2\left(\frac{h^*R}{p_s\delta_t}\right) \right\rceil$.

Thus, the total number of ideal operations required for computing h^* is

$$\text{NUM1} = \sum_{p_i<b} \left\lceil \log_2\left(\frac{h^*R}{p_i\delta_t}\right) \right\rceil .$$

On the other hand, the number of ideal operations required by Algorithm 6.5.1 is determined by the number of ones in the binary representation of q (see (6.3.1)); hence, the range is from 1 to k + 1 where

$$k = \left[\log_2 \left(\left[\frac{h^*R}{p_s\delta_t} \left(\frac{p_{s+1} - p_s}{p_{s+1}} \right) \right] + 1 \right) \right].$$

Although the upper bound is k+1, in most cases the actual number of ideal operations tends to be much smaller. Indeed, the probability of needing only k/2 or less ideal operations is 1/2. Thus, we would expect the average number of ideal operations to be k/2. As a result, we would expect the total number of ideal operations required by Algorithm 6.5.1 for computing h^* to be

$$\begin{aligned} \text{NUM2} &= \frac{1}{2} \sum_{p_i<b} \left[\log_2 \left(\left[\frac{h^*R}{p_i\delta_t} \left(\frac{p_{i+1} - p_i}{p_{i+1}} \right) \right] + 1 \right) \right] + 1 \\ &\approx \frac{1}{2} \sum_{p_i<b} \left[\log_2 \left(\frac{h^*R}{p_i\delta_t} \right) \right] + \left[\log_2 \left(\frac{p_{i+1} - p_i}{p_{i+1}} \right) \right] + 1 \\ &\approx \frac{1}{2} \sum_{p_i<b} \left[\log_2 \left(\frac{h^*R}{p_i\delta_t} \right) \right] + \frac{1}{2} \sum_{p_i<b} \left[\log_2 \left(\frac{p_{i+1} - p_i}{p_{i+1}} \right) \right] + \frac{b}{2}. \end{aligned}$$

Here, the b values range between 2000 and 26000 (For details, see §6.6). In order to determine a bound on

$$g(b) = b / 2 + p(b) / 2,$$

where

$$p(b) = \sum_{p_i<b} \left[\log_2 \left(\frac{p_{i+1} - p_i}{p_{i+1}} \right) \right],$$

we computed g(b) for b = j x 2000 (j = 1,2, ... , 13). The results are summarized in Table 6.5.1.

b	b/2	p(b)/2	g(b)
2000	1000	-954	46
4000	2000	-1985	15
6000	3000	-3039	-39
8000	4000	-4097	-97
10000	5000	-5195	-195
12000	6000	-6241	-241
14000	7000	-7345	-345
16000	8000	-8437	-437
18000	9000	-9521	-521
20000	10000	-10588	-588
22000	11000	-11697	-697
24000	12000	-12818	-818
26000	13000	-13884	-884

Table 6.5.1

From Table 6.5.1 we see that the value of g(b) is either very small or negative for b lying between 2000 and 26000. Hence, we would expect

$$\text{NUM2} \approx \frac{1}{2} \sum_{p_i<b} \left[\log_2 \left(\frac{h^* R}{p_i \delta_t} \right) \right]$$

or less. As a result, by comparing NUM1 and NUM2, we would expect that Algorithm 6.5.1 is usually faster than the WDS method by at least a factor of 2. Indeed, on average,

we found that our computations were improved by a factor of two. In the following section, we present some of our results.

§6.6 Implementation and computational results.

The new technique for computing h^* was implemented in FORTRAN-H (extended) and added to our program. In this section we first discuss some of the computational techniques which were used to get the best possible performance out of this modified WDS algorithm.

As mentioned in [WDS83], the selection of input parameters b, x and T can affect the running time of the program. However, after a series of experiments, we learned that the running time of this modified WDS algorithm, on this particular computer, did not heavily depend on the values of the input parameters for the c values in which we were interested. In other words, we found that the modified WDS algorithm can achieve optimal performance by using values of the input parameters which are merely close to the optimal values. In finding these values, we analyzed our program carefully. Given our estimate E, there are four major steps involved in our program. These are: generating a sequence of reduced ideals at the beginning, finding h^*R, finding h^* by using the technique given in §6.5, and executing the Search algorithm. We further point out that there are other cost factors involved in our computation of R; however, these are insignificant in comparison to the four major factors listed above. Thus, we only consider the above four factors in determining the values for b, x and T. We put t_1 to be the time required for a baby step and t_2 to be the time required for an ideal operation. Empirically, there seem to be roughly T reduced ideals with distance less than T (see [WDS83]); hence, the time required for finding all the reduced ideals with distance less than T is approximately Tt_1. Here, for an input parameter L, we attempt to find h^*R in the range of E - L and E + L. In our computations, we used $L = 10^7$. Consequently, the maximum number of ideal operations is $2L / T$. In this step, x baby steps are required after each ideal operation. Thus, after

generating all the reduced ideals with distance less than T, the total amount of time required for finding h*R is at most

$$2Lt_1 / T + 2Lxt_2 / T.$$

The next step is to find h^*. From §6.5 we would expect

$$\frac{1}{2}\sum_{p<b}\log(E/(pT)) \quad \left(=\frac{1}{2}\sum_{p<b}\left(\log(E/T) - \log p\right)\right)$$

ideal operations to be required for finding h^*. Also, it is well known that there are about $b / \log b$ primes less than b, and that $\sum_{p<b}\log p \approx b$. Furthermore, there are about $bx / \log b$ baby steps involved in this step. Hence, the time required for this step is approximately

$$\frac{bt_2}{2}\left(\frac{\log(E/T)}{\log b} - 1\right) + \frac{bxt_1}{\log b}.$$

As for the last step, there are E/(Tb) ideal operations and Ex/(Tb) baby steps. By combining the above information, we deduced the following approximate cost formula:

(6.6.1)
$$\text{Cost} = Tt_1 + 2Lt_1 / T + 2Lxt_2 / T + \frac{bt_2}{2}\left(\frac{\log(E/T)}{\log b} - 1\right) + \frac{bxt_1}{\log b} + Et_2/(Tb) + Ext_1/(Tb).$$

Put $m = E / (Tb)$, $f = t_2 / t_1$, and $s = T / x$ where s is the number of reduced ideals that can be stored in memory. In our case, we used s = 15000. If we divide (6.6.1) by t_1, then we have

(6.6.2)
$$\text{cost} / t_1 = E/mb + 2Lmb/E + 2Lf/s + fm + E/(sb) + bf(\log(bm)/(2\log b) - 0.5) + E /(sm \log b).$$

By applying a simple optimization program to minimize (6.6.2), we found the values of the input parameters T, x, b, as given in Table 6.6.1 for our computations.

range of E	T	x	b
$2.5x10^{12} < E < 3.5\ x10^{12}$	109000	7	5200
$1.5x10^{12} < E < 2.5\ x10^{12}$	97000	6	4500
$0.5x10^{12} < E < 1.5\ x10^{12}$	80000	5	3500
$1x10^{11} < E < 0.5\ x10^{12}$	62000	4	2800
$1x10^{10} < E < 1\ x10^{11}$	32000	2	1200

Table 6.6.1

In order to calculate $\log\theta_n$ efficiently, we did not compute $\sum_{i=1}^{n}\log\theta_g^{(i)}$, i.e., a sum of logarithms. Since we only stored 1/x of the reduced ideals $\{i_1, i_2, \ldots, i_t\}$, there was no need to calculate the distance for each of the reduced ideals in $\{i_1, i_2, \ldots, i_t\}$. Thus, since the logarithm routine is fairly expensive, we only computed $\log\theta_n$, the distance $\delta(i_n,i_1)$, when n is a multiple of x. Our technique was to accumulate the partial product $\chi = \prod_{i=jx}^{(j+1)x-1} \theta_g^{(i)}$ $(j \in \mathbf{Z})$, and then we found $\log\theta_{(j+1)x}$ by computing $\log\chi + \log\theta_{jx}$. By doing that, we made t/x log calls instead of t log calls.

The reduced ideals $\{i_{1x}, i_{2x}, \ldots, i_t\}$ were sorted according to their norms by a fast, general sorting routine. A binary search was then used in determining whether or not a reduced ideal is in $\{i_{1x}, i_{2x}, \ldots, i_t\}$. Also, the reason for not using the hashing technique as in [SW88] was that a binary search is sufficient here as there is a smaller number of reduced ideals in the cubic case. Furthermore, the amount of time required for this sorting routine is not sufficiently significant to put into the cost formula (6.6.1).

With this program we computed the regulator for each of the c values listed in Tables 6.2.5, 6.2.6, 6.2.7 and 6.2.8. The results are given in Tables 6.6.2, 6.6.3, 6.6.4 and 6.6.5. On running the program, the amount of time required to calculate R for the 72 values of c ranged from 3 CPU minutes to 6 CPU minutes, depending on the size of R.

For example, we found that it took approximately 6 CPU minutes to compute a value of R when $R \approx 3 \times 10^{12}$. Indeed, the empirical evidence suggests that the modified version of the WDS method is at least twice as fast as the WDS method. Further, we noticed that the number of ideal operations was reduced by at least a half for all 72 values of c .

In Tables 6.6.6, 6.6.7, 6.6.8 and 6.6.9 we give those values of c for which C(c) exceeds 0.67. Since the largest value of C(c) which we found is 0.71022, we have nothing here that comes near to violating the truth of the GRH. Finally, we note the extremely slow growth rate of C(c).

c	Reg	C(c)
23904870683	74360135722.99645259	0.67077275
41843313959	33094292192.03615571	0.16976353
57913659383	13026981750.24716053	0.04815486
58182013553	18384322720.18053770	0.06764258
79834584857	253424953087.77135657	0.67783839
113913197789	361903194404.34921469	0.67651288
122089073261	96256524295.71490745	0.16779435
130962864677	103565808272.07382961	0.16821174
136544134973	434963928415.16482834	0.67737366
210018369371	332851167470.67811113	0.33590143
226956644069	725904714515.34610324	0.67748729
272330743901	870425045478.12549857	0.67608950
327552647297	520882901191.45680660	0.33591585
336949891277	110424642551.13602578	0.06921194
399933625181	322331191581.21099557	0.16999830
404698499087	1301526122837.74667670	0.67828714
416520048911	671621878653.61094955	0.34000806
464191218707	769385074481.28168411	0.34922223
466353166469	373864433808.38242721	0.16890383
471882449219	1507455651942.82695608	0.67299765
493979588159	1588163346721.72358785	0.67708588
530161973249	1689042680572.24642275	0.67060357
533183662103	106093622991.44474078	0.04188209
760106056289	2434590810678.76723680	0.67244265
778769068631	2488810685892.40970593	0.67082793
792802846373	2555110143668.59048090	0.67642064
902875793639	727483484062.22751900	0.16895244

Table 6.6.2.
(c = p ≡ 2 (mod 9))

c	Reg	C(c)
7823785241	3058976718.87499310	0.08512205
10389989063	16316808775.70248071	0.34105523
23002424327	71695952039.63348539	0.67232981
43595987609	68250877078.51356758	0.33591874
79600195163	258037319824.43576461	0.69222350
90307528193	71584383791.57154194	0.16909875
119087387453	379081653253.00307911	0.67760221
195511299437	634232638209.06787717	0.68790980
213555190997	679070755886.13331129	0.67385903
234187560641	383340113167.02583430	0.34664279
289191889433	229419759805.75951183	0.16773323
292277713727	939375172155.04811478	0.67949046
506642469059	405699943450.78211886	0.16860900
576605603657	938078184059.62577770	0.34223861
578450121761	962547107755.33815249	0.35003772
748224663941	2487275521768.01072796	0.69798231
800855660207	2595400816922.10179405	0.68012886
844409282933	337501024293.08100605	0.08384916
998024756357	3208632480642.32164235	0.67365702

Table 6.6.3.

$(c = p \equiv 5 \pmod 9)$

c	Reg	C(c)
74354863227	118219208940.00823437	0.33969638
99052148229	157008040407.51241785	0.33790086
102879790287	161784724853.09948311	0.33512745
117807496071	185498213308.43441708	0.33520544
144646415187	483332596164.31738229	0.71022119
229362553239	370061626156.76861086	0.34172868
291987409839	940224821906.25218496	0.68078629
293203999941	469426903290.87622223	0.33847595
362264296659	582900527602.53955311	0.33963793
413557332189	1365180219088.64133022	0.69610916
455271781749	732974717472.36287067	0.33926184
748671032481	149399876779.40296544	0.04189960
912685074153	743106728645.80169956	0.17071284

Table 6.6.4.

$(c = 3p\ ,\ p \equiv 2,5 \pmod 9)$

c	Reg	C(c)
11382801093	5810544987.74325251	0.33557701
109324288107	7204486886.90727397	0.04248299
149832113787	15835396468.88462638	0.06795788
298968550119	159084722456.55309343	0.34027878
368636786253	389797878393.40392194	0.67509407
373775618061	198906240697.19946591	0.33971471
433769568597	29165074213.28352701	0.04287279
505919205819	54359845814.67733653	0.06843249
648369068283	173378898677.59148687	0.16998872
654007847319	172692640909.58856560	0.16784507
683030699469	730740526365.54282163	0.67982679
747241701597	158071066939.24904727	0.13432992
937165977747	498996299308.56052858	0.33754109

Table 6.6.5.

(c = 9p , p ≡ 2,5 (mod 9))

c	C(c)
23904870683	0.67077275
79834584857	0.67783839
113913197789	0.67651288
136544134973	0.67737366
226956644069	0.67748729
272330743901	0.67608950
404698499087	0.67828714
471882449219	0.67299765
493979588159	0.67708588
530161973249	0.67060357
760106056289	0.67244265
778769068631	0.67082793
792802846373	0.67642064

Table 6.6.6.

(c = p ≡ 2 (mod 9))

c	C(c)
23002424327	0.67232981
79600195163	0.69222350
119087387453	0.67760221
195511299437	0.68790980
213555190997	0.67385903
292277713727	0.67949046
748224663941	0.69798231
800855660207	0.68012886
998024756357	0.67365702

Table 6.6.7.

$(c = p \equiv 5 \pmod 9)$

c	C(c)
144646415187	0.71022119
291987409839	0.68078629
413557332189	0.69610916

Table 6.6.8.

$(c = 3p\ ,\ p \equiv 2,5 \pmod 9)$

c	C(c)
368636786253	0.67509407
683030699469	0.67982679

Table 6.6.9.

$(c = 9p\ ,\ p \equiv 2,5 \pmod 9)$

Chapter 7.
Cubic Polynomials Which Have a High Density of Prime Values.

§7.1 Introduction.

Let $f_c(x) = x^3 + c$ ($c \in \mathbf{Z}^+$ and c is cube-free) and let $P_c(n)$ represent the number of prime values assumed by $f_c(x)$ for x = 0, 1, 2, 3, ..., n. In [FW90], Fung and Williams describe a method of finding quadratic polynomials of the form $x^2 + x + A$ ($A \in \mathbf{Z}^+$) which have a high asymptotic density of prime values. The basis of their strategy is Hardy and Littlewood's [HL23] conjecture F. In [HL23], an analogous conjecture, Conjecture K, is given for the cubic polynomials of the form $x^3 + c$. Thus, this conjecture allows us to extend Fung and Williams' idea to the cubic case.

For the case of polynomials of the form $x^3 + c$, Conjecture K of Hardy and Littlewood (also, see Bateman and Horn [BH65]) can be given as

$$P_c(n) \approx \frac{\kappa(c)}{3} L_c(n) \tag{7.1.1}$$

where

$$L_c(n) = 3 \int_2^n \frac{dx}{\log f_c(x)}$$

and

$$\kappa(c) = \prod_{p>3} \frac{p - \alpha_c(p)}{p - 1}. \tag{7.1.2}$$

The product of (7.1.2) is taken over all the odd primes $p \equiv 1 \pmod 3$ with $p \nmid c$, and $\alpha_c(p)$ denotes the number of solutions of the congruence

$$x^3 \equiv -c \pmod p.$$

By using

(7.1.3) $$\kappa(c) = \frac{3\sqrt{D}}{\pi h R} \prod_{\alpha_c(p)=3} \frac{p^2(p-3)}{(p-1)^3} \prod_{\alpha_c(p)=0} \frac{p^2}{p^2-1} \prod_{p\equiv -1 \pmod 3} \frac{p^3}{p^3-1}$$

where

D = the discriminant of $Q(\sqrt[3]{c})$,

R = the regulator of $Q(\sqrt[3]{c})$,

h = the class number of $Q(\sqrt[3]{c})$,

Davenport and Schinzel [DS66] computed $\kappa(2) = 1.29$ and $\kappa(3) = 1.38$. The main difficulty of (7.1.3) is that the three infinite products shown above converge very slowly. As a result, $\kappa(2)$ and $\kappa(3)$ were only computed to three significant figures. Further, in Shanks and Lal [SL72], the authors give a modified version of (7.1.3) as follows:

(7.1.4) $$\kappa(c) = \frac{2\sqrt{D}\gamma U_0}{3\pi h R} \prod_{\substack{\alpha_c(p)=3 \\ p\equiv 1 \pmod 3}} 1 - \frac{3(p+1)}{p(p-1)^2} \prod_{\substack{p \mid c \\ p\equiv 1 \pmod 3}} 1 - \frac{1}{p^3} \prod_{\substack{p \mid c \\ p\equiv -1 \pmod 3}} 1 - \frac{1}{p^2}$$

where

$$\gamma = \begin{cases} 1 & \text{when} \quad c \not\equiv \pm 1 \pmod 9 \\ 3/4 & \text{when} \quad c \equiv \pm 1 \pmod 9 \end{cases}'$$

$U_0 = 1.064378253083636.$

By using (7.1.4), they easily computed $\kappa(2)$ and $\kappa(3)$ to sixteen significant figures where

$\kappa(2) = 1.298539557557843$

$\kappa(3) = 1.390543938783812.$

Although the infinite product of (7.1.4) converges fairly quickly, the evaluation of $\kappa(c)$ remains a difficult problem due to the requirement for h and R. Indeed, as mentioned earlier, the computations of h and R are very difficult when c becomes large. In fact, to the best of our knowledge, no $\kappa(c)$ values other than $\kappa(2)$ and $\kappa(3)$ have ever been computed. Also, little work seems to have been done on finding polynomials of the form $x^3 + c$ which have a high density of prime values.

The purpose of this chapter is to find cubic polynomials $f_c(x)$ which have a high asymptotic density of prime values. As in [FW90], we do this by determining those values

of c for which the Hardy-Littlewood constant $\kappa(c)$ should be large and then evaluating $\kappa(c)$ to nine significant figures.

§7.2 Strategy for finding values of c.

In order to find large asymptotic values of $P_c(n)$, we attempt to find values of c such that $\kappa(c)$ is large. According to (7.1.4) this means that we would want $(\frac{c}{p})_3 = -1$ for as many of the small primes p of the form $3t + 1$ ($t \in \mathbf{Z}^+$) as possible. Also, we can look at this from the point of view of restricting the number of possible small prime divisors of $f_c(x)$. Clearly, if $(\frac{c}{p})_3 = -1$, then p cannot divide $f_c(x)$ for any value of x. Thus, if $(\frac{c}{p})_3 = -1$ for many small primes p, then the composite values that $f_c(x)$ can assume are considerably restricted. It follows that $f_c(x)$ should have a relatively high density of prime values. Furthermore, we can maximize $\kappa(c)$ by finding values of c which have small hR values. Since we are interested in finding values of c that have cubic non-residues for as many small primes as possible, we have also accomplished the task of minimizing hR. As in §6.2, we can minimize h by searching the values of c for which 3 is not a divisor of h. In our investigation, we elected to inspect the values of c that satisfy

$$c \equiv 2, 4, 5 \text{ or } 7 \pmod 9.$$

Here, c may be either a prime or a composite. However, c must be cube-free.

If we let N_i denote the least positive integer such that $N_i \equiv 2, 4, 5$ or 7 (mod 9) and $(\frac{N_i}{p})_3 = -1$ for all odd primes p of the form $3t + 1$ ($t \in \mathbf{Z}^+$) and $p \le r_j$, where r_j is the j^{th} prime of the form $3t + 1$ ($t \in \mathbf{Z}^+$), then N_i should be a good candidate for the kind of c values that we are seeking. In Table 7.2.1 we give all the values of N_i for i = 48, 49, ... , 63.

i	r_i	N_i	i	r_i	N_i
48	547	2438812372	56	643	104543075198
49	571	2438812372	57	661	104543075198
50	577	10996650403	58	673	538487125013
51	601	10996650403	59	691	538487125013
52	607	10996650403	60	709	538487125013
53	613	10996650403	61	727	976698454244
54	619	10996650403	62	733	976698454244
55	631	104543075198	63	739	976698454244

Table 7.2.1

If we put $N_{i,1} = N_i$ above and define $N_{i,j}$ ($j > 1$) as the least integer greater than $N_{i,j-1}$ such that $N_{i,j} \equiv 2, 4, 5$ or $7 \pmod 9$ and $(N_{i,j}/p)_3 = -1$ for all odd primes $p < r_i$, then $N_{i,j}$ are good candidates as well. Thus, instead of attempting simply to tabulate more N_i values than those given in Table 7.2.1, our strategy was to find $N_{48,j}$ for $j = 1, 2, \ldots, m$, where $N_{48,m} < 10^{12} < N_{48,m+1}$. By doing that, we were able to find all the $N_{i,j}$ values, which are less than 10^{12}, for $i \geq 48$ and $j = 1, 2, 3, \cdots$. To find these values of $N_{i,j}$, we made use of OASiS (see §6.2) again. After 25 days of continuous use, 335 numbers were found. Having these candidates for c, the next problem is to determine those that yield the largest $\kappa(c)$ values by using (7.1.4).

§7.3 Computation of $\kappa(c)$.

Put

$$F_1(Q) = \prod_{\substack{\alpha_c(p)=3 \\ p < Q \\ p\equiv 1 \pmod 3}} 1 - \frac{3(p+1)}{p(p-1)^2},$$

$$T_1(Q) = \prod_{\substack{\alpha_c(p)=3 \\ p > Q \\ p\equiv 1 \pmod 3}} 1 - \frac{3(p+1)}{p(p-1)^2}.$$

We now have

$$\kappa(c) = \frac{2\sqrt{D}\gamma U_0}{3\pi hR} F_1(Q)\, T_1(Q) \prod_{\substack{p \mid c \\ p\equiv 1 \pmod 3}} 1 - \frac{1}{p^3} \prod_{\substack{p \mid c \\ p\equiv -1 \pmod 3}} 1 - \frac{1}{p^2}. \tag{7.3.1}$$

By examining (7.3.1) we see that two problems arise in computing $\kappa(c)$: (1) determine hR, (2) find Q such that

$$\kappa(c) \approx \frac{2\sqrt{D}\gamma U_0}{3\pi hR} F_1(Q) \prod_{\substack{p \mid c \\ p\equiv 1 \pmod 3}} 1 - \frac{1}{p^3} \prod_{\substack{p \mid c \\ p\equiv -1 \pmod 3}} 1 - \frac{1}{p^2}. \tag{7.3.2}$$

approximates $\kappa(c)$ to 9 significant figures.

Clearly,

$$\log T_1(Q) = \log \prod_{\substack{\alpha_c(p)=3 \\ p > Q \\ p\equiv 1 \pmod 3}} 1 - \frac{3(p+1)}{p(p-1)^2} = \sum_{\substack{\alpha_c(p)=3 \\ p > Q \\ p\equiv 1 \pmod 3}} \log\left(1 - \frac{3(p+1)}{p(p-1)^2}\right).$$

Since

$$\log\left(1 - \frac{3(p+1)}{p(p-1)^2}\right) = \frac{-3(p+1)}{p(p-1)^2} - \frac{1}{2}\left(\frac{3(p+1)}{p(p-1)^2}\right)^2 - \frac{1}{3}\left(\frac{3(p+1)}{p(p-1)^2}\right)^3 - \cdots,$$

we have

$$\log T_1(Q) = -H_1(p) - H_2(p),$$

where

$$H_1(p) = \sum_{\substack{\alpha_c(p)=3 \\ p > Q \\ p\equiv 1 (\mathrm{mod}\ 3)}} \frac{3(p+1)}{p(p-1)^2},$$

$$H_2(p) = \sum_{\substack{\alpha_c(p)=3 \\ p > Q \\ p\equiv 1 (\mathrm{mod}\ 3)}} \left(\frac{1}{2}\left(\frac{3(p+1)}{p(p-1)^2}\right)^2 + \frac{1}{3}\left(\frac{3(p+1)}{p(p-1)^2}\right)^3 + \cdots \right).$$

We first point out that it is a simple matter to show that

$$H_1(p) < \frac{Q + 1}{12Q(B+1)},$$

where $B = [Q / 6]$. Also, we can easily deduce that

$$H_2(p) < \frac{1}{3^5(B+1)^3}.$$

Thus, we get

(7.3.3) $$| \log T_1(Q) | < \frac{Q + 1}{12Q(B+1)} + \frac{1}{3^5(B+1)^3}.$$

Now if

$$| \log T_1(Q) | < b,$$

then (7.3.2) will approximate $\kappa(c)$ to n significant figures if $b < \log((1 + \sqrt{1 + 4k}) / 2)$, where $k = 10^{1-n} / 2$. Hence, by (7.3.3), if $Q = 10^8$ is used, then (7.3.2) will yield $\kappa(c)$ to 9 significant figures. To test this we evaluated (7.3.2) for a few c values found in §7.2 with $Q = 10^8$ and $Q = 2 \times 10^8$. In every case both computations agreed to 9 (or 10) significant figures.

There remains the problem of determining hR. For this problem we used the algorithm given in the previous chapter to calculate h^* and R. However, as mentioned earlier, we cannot be certain that $h^* = h$. Thus, we used the technique as described in §3.3, with a slight modification, to determine h. However, we have to assume the truth of the Riemann Hypothesis by using this method. The slight modification occurred in the process of finding a factor of the class number. In §3.3 we determined a factor of h by finding the least possible value of m (>0) such that $\mathbf{a}^m$, where $\mathbf{a}$ is a reduced non-principal ideal in $Q(\sqrt[3]{c})$, is a principal ideal. To do this we simply started m at 1 and increased it until we

found a value for which $a^m \sim (1)$. Here, since a factor of h^* is very likely to be a factor of h, we check whether or not $a^m \sim (1)$ if $m \mid h^*$. By doing that we can significantly reduce the amount of time required in determining whether or not a reduced ideal is a principal ideal. We also mention that the method of Buchmann and Williams [BW88A] was used in principal ideal testing.

§7.4 Computational results.

The method described above was programmed in FORTRAN with some assembly language routines (most of the routines were used in previous chapters) and run on an Amdahl 5870 computer. Furthermore, we note that $F_1(10^8)$ and an approximation of hR (an estimate of $\Phi(1)$) were evaluated simultaneously. For each of the c values found in §7.2, a value of $\kappa(c)$ accurate to 9 significant figures was computed. These $\kappa(c)$ values were computed in a total of about 42 CPU hours. The average time required to compute a $\kappa(c)$ was about 7.5 CPU minutes, in which approximately 5 CPU minutes were spent on computing an estimate of $\Phi(1)$ and $F_1(10^8)$. Here, we denote by q(c) the least prime of the form $3t + 1$ ($t \in \mathbf{Z}$) such that $\left(\frac{c}{q(c)}\right)_3 = 1$. In Table 7.4.1, we give all the numbers c found by OASiS with $q(c) \geq 619$. We also provide the corresponding values of $\kappa(c)$ and q(c).

c	κ(c)	q(c)
10996650403	1.81356011	619
104543075198	1.82475834	661
122883799502	1.81250056	619
237182386703	1.78034645	631
340870581083	1.83002720	631
381969885083	1.79428621	619
389033752831	1.83409736	643
402240958123	1.81205265	619
429028811221	1.81274409	643
430691378353	1.82393826	643
435910653383	1.80811828	619
440461112263	1.84706577	619
532836531769	1.81689408	619
538487125013	1.83171092	709
630118608667	1.81203407	619
669006592193	1.76803531	631
673223095339	1.81247198	619
674479164343	1.81437510	619
681623186513	1.84979174	673
742110523157	1.81429693	661
787504388899	1.77876018	619
843080148857	1.78063201	619
855128785102	1.81289427	631
942297660302	1.83917524	619
954038967746	1.82940050	691
976698454244	1.80071119	739

Table 7.4.1

In Table 7.4.2, we give those values of c from among the 335 numbers such that $\kappa(c) > \kappa(c')$ for all the c' which are less than c. We also give the corresponding value of $P_c(10^5)$ and $3P_c(10^5) / L_c(10^5)$. In Table 7.4.3 we give the values of $P_c(10^6)$ and $3P_c(10^6) / L_c(10^6)$ for each of the last three c values listed in Table 7.4.2. By looking at Tables 7.4.2 and 7.4.3, we notice that $3P_c(n) / L_c(n)$ (where $n = 10^5, 10^6$) and $\kappa(c)$ are quite close in each case, and these results provide a confirmation of Conjecture K. Furthermore, in Table 7.4.4 we give all those c values which have $\kappa(c) > 1.84$.

c	$\kappa(c)$	$P_c(10^5)$	$3P_c(10^5)/L_c(10^5)$
2438812372	1.77585201	24618	1.7769806
7553108903	1.78730681	24719	1.7848207
10996650403	1.81356011	25113	1.8134923
13039426573	1.82833223	25149	1.8162004
34274419666	1.83146052	25334	1.8302770
34619128889	1.85557534	25770	1.8617847
159758632562	1.8732072	25986	1.8789978

Table 7.4.2

c	$\kappa(c)$	$P_c(10^6)$	$3P_c(10^6)/L_c(10^6)$
34274419666	1.83146052	47897	1.8293839
34619128889	1.85557534	48558	1.8546347
159758632562	1.8732072	49101	1.8762230

Table 7.4.3

c	κ(c)
34619128889	1.85557534
159758632562	1.87320715
205832276347	1.85622111
312945553748	1.85221205
320632593626	1.84120352
356454347681	1.86130129
440461112263	1.84706577
446441115179	1.86326589
446947523507	1.84948261
482302370219	1.85817382
502621065553	1.85094250
508595764309	1.86818077
513572881378	1.86202993
573548961598	1.84042512
647287308887	1.84695743
681623186513	1.84979174
694044605252	1.84127308
704813954582	1.84766015
716323539649	1.84112544
765362309177	1.84071454
857474554759	1.84648899
985522446218	1.84022139
987450298774	1.84562855
994791922204	1.84761623

Table 7.4.4

Chapter 8.
Computation of Principal Factors in Pure Cubic Fields.

§8.1 Introduction.

Let c be a positive cube-free integer and, $F = Q(\sqrt[3]{c})$ be the pure cubic field formed by adjoining $\sqrt[3]{c}$ to the rationals **Q**. We say that any algebraic integer of **F** is primitive if it is not divisible by a rational integer greater than 1. Also, we let S be the product of the primes which completely ramify in **F**. Further, we let $\delta^3 = c = mn^2$ and $\bar{\delta}^3 = \bar{c} = m^2n$, where $m > n$, m, n are coprime square-free integers. Note that $\delta^2 = n\bar{\delta}$, $\bar{\delta}^2 = m\delta$. We have

$$S = \begin{cases} 3mn & c \not\equiv \pm 1 \pmod 9 \text{ and } 3 \nmid c \\ mn & \text{otherwise.} \end{cases}$$

Denote by α' and α'' the conjugates of any $\alpha \in \mathbf{F}$, and write

$$\varepsilon_0 = (g_1 + g_2\delta + g_3\bar{\delta}) / 3 \qquad (g_1, g_2, g_3 \in \mathbf{Z}).$$

Note that since $N(\varepsilon_0) = 1$, we have $g_1^3 \equiv 27 \pmod{mn}$.

If there exists a primitive β ($\in \mathbf{O_F}$) such that

$$\varepsilon_0^k = \beta^3 / N(\beta),$$

where $k \in \mathbf{Z}$ and $3 \nmid k$, then each rational prime which divides $N(\beta)$ must completely ramify in **F**. Indeed, we know that $N(\beta) \mid S^2$. After Barrucand and Cohn [BC70], [BC71] we call such a value of $N(\beta)$ a principal factor of S^2. In [BC70] it is further pointed out that there are exactly six distinct principal factors of S^2 if principal factors exist for **F**. If principal factors exist for **F**, then there exist the unique primitive algebraic integers $\pm\alpha_1$, $\pm\alpha_2$, $\pm\alpha_3$, $\pm\beta_1$, $\pm\beta_2$, $\pm\beta_3$ of **F** such that

$$\varepsilon_0^k = \alpha_i^3 / N(\alpha_i) \qquad (k \equiv 1 \text{ or } 2 \pmod 3 \text{ and } i = 1, 2, 3),$$

$$\varepsilon_0^{k+j} = \beta_i^3 / N(\beta_i) \qquad (j = 1 \text{ if } k \equiv 1 \pmod 3,\ j = -1 \text{ if } k \equiv 2 \pmod 3).$$

Here $N(\alpha_i)$, $N(\beta_i)$ are divisors of S^2 and are the principal factors of **F**. These numbers are discussed in some detail in [BC70] and [BC71].

In fact, if $\alpha \in \mathbf{O}_F$, $N(\alpha) \mid S^2$, and $N(\alpha) = 3^{\tau}d_1d_2^2d_4d_5^2$, where $\tau \in Z$, $0 \le \tau \le 2$, $m = d_1d_2d_3$, $n = d_4d_5d_6$, then the six numbers

$$\alpha,\ \delta\alpha / (d_2d_4d_5),\ \bar{\delta}\alpha / (d_1d_2d_5),\ \alpha^2 / (d_2d_5),\ \delta\alpha^2 / (d_1d_2d_4d_5^2),\ \bar{\delta}\alpha^2 / (d_1d_2^2d_4d_5)$$

are all in $\mathbf{O}_F$, and each of their norms divides S^2. Thus, each of the elements of the set

$$\{3^{\tau}d_1d_2^2d_4d_5^2,\ 3^{\tau}d_1^2d_3d_5d_6^2,\ 3^{\tau}d_2d_3^2d_4^2d_6,$$
$$3^{\nu}d_1^2d_2d_4^2d_5,\ 3^{\nu}d_1d_3^2d_5^2d_6,\ 3^{\nu}d_2^2d_3d_4d_6^2\},$$

where $(\tau,\nu) = (0,0)$, $(1,2)$ or $(2,1)$, is a principal factor whenever $N(\alpha) \mid S^2$. Furthermore, if one of the principal factors is calculated, then the other five principal factors can be easily found.

Let ρ be a primitive cube root of unity and G be a cubic field of negative discriminant. We put $\Omega = Q(\rho)$ and $\mathbf{L} = G(\rho)$. Then the Galois group of the normal field $\mathbf{L}$ is generated by β and ψ, where $\beta^3 = \psi^2 = 1$ and $\beta\psi = \psi\beta^2$. If $x \in \mathbf{L}$, then we put $x' = x^{\beta}$ and $x'' = x^{\beta^2}$. Also, we define $\mathbf{F}' = \mathbf{F}^{\beta}$ and $\mathbf{F}'' = \mathbf{F}^{\beta^2}$. If we let $\mathbf{E}_J$ denote the unit group for the algebraic number field J, we see that

$$\mathbf{E}_0 = \mathbf{E}_F \times \mathbf{E}_{F'} \times \mathbf{E}_{F''} \times \mathbf{E}_{\Omega}$$

is a subgroup of $\mathbf{E}_L$. We put

$$r^* = [\ \mathbf{E}_L : \mathbf{E}_0\ ].$$

By Berwick [Ber32], we know that r^* is either 1 or 3. Furthermore, Berwick mentioned that $r^* = 3$ if and only if there exist $q \in \mathbf{Z}^+$, $\gamma \in \mathbf{F}^x$ such that

$$q\varepsilon_0 = \gamma^3.$$

Indeed, Barrucand and Cohn [BC71] showed that if $r^* = 3$, then there exist $q \in \mathbf{Z}^+$ and $\gamma \in \mathbf{F}^x$ such that $q\varepsilon_0 = \gamma^3$. However, they also proved that in a pure cubic field, F, there might not exist $q \in \mathbf{Z}^+$ and $\gamma \in \mathbf{F}^x$ such that $q\varepsilon_0 = \gamma^3$ if $r^* = 3$. Thus, Berwick's criterion in this case is false.

In [BC71], the authors proved that if H is the class number of $\mathbf{L}$ and h is the class number of $\mathbf{F}$, then

$$H = r^*h^2 / 3,$$

a result that was later generalized by Moser [Mos78]. Also, using the results of [BC71], together with a later result of Halter-Koch [Hal76] (also, see [Set78]), we have the following

Theorem 8.1.1. Consider the equation

(8.1.1) $$\varepsilon_0' / \varepsilon_0 = \rho^i \delta^3, \qquad (\delta \in \mathbf{L} = \mathbf{F}(\rho)),\ 0 \le i < 2,$$

(i) (8.1.1) has no solution if and only if $r^* = 1$,

(ii) (8.1.1) has a solution with $i = 0$ if and only if principal factors exist for **F**,

(iii) (8.1.1) has a solution with $i \neq 0$ if and only there exists a unit $\eta \in \mathbf{L}$ such that the relative norm ,

(8.1.2) $$N_{L/\Omega}(\eta) = \rho. \quad \blacksquare$$

In other words, principal factors exist for **F** if and only if

$$\varepsilon_0' / \varepsilon_0 = \rho^i \delta^3,$$

where $\rho^2 + \rho + 1 = 0$, $\delta \in \mathbf{L}$ (if $\Omega \in \mathbf{Q}(\rho)$, $i = 0$). We further point out that case(iii) of Theorem 8.1.1 can occur only for pure cubic fields. Thus, if **G** is not a pure cubic field, then principal factors exist for **G** if and only if $r^* = 3$. Also, the equation (8.1.2) is the cubic analog of the so-called non-pellian equation

$$x^2 - Dy^2 = -1.$$

Brunotte, Klingen, and Steurich [BKS77] have shown that r^* is 3 if and only if

$$g_1 \equiv 3 \pmod{mn},$$

where

$$\varepsilon_0 = (g_1 + g_2\delta + g_3\bar{\delta}) / 3 \qquad (g_1, g_2, g_3 \in \mathbf{Z}).$$

This allows us to find a method of distinguishing between (i) and the other two cases (ii) and (iii) of Theorem 8.1.1. Indeed, this idea was implemented by Williams [Wil82], but the technique is $\mathbf{O}(c)$ in complexity. However, we cannot distinguish between (ii) and (iii) of Theorem 8.1.1 by using this method. Consequently, a different technique is required for the determination of the existence of principal factors for **F**.

We define e by putting e = 1 when principal factors exist for **F** and e = 0 otherwise. For a pure cubic field, we have three possible principal factorization types:

(1) PF Type I: (Case (ii) of Theorem 8.1.1) e = 1, r* = 3,

(2) PF Type II: (Case (i) of Theorem 8.1.1) e = 0, r* = 1,

(3) PF Type III: (Case (iii) of Theorem 8.1.1) e = 0, r* = 3.

In [Wil82], Williams discovered and implemented an $\mathbf{O}(c)$ algorithm to find the principal factors of S^2. This algorithm was used to search for principal factors for all $Q(\sqrt[3]{c})$ with $2 \le c \le 15000$. Recently, this algorithm was improved by Mayer [May88], but this improved algorithm is still of time complexity $\mathbf{O}(c)$. For all such $c \le 10^5$, Mayer has found all fields with principal factors. His results can be summarized in Table 8.1.1.

Type	# of fields	% of total
PF I	62068	75.45%
PF II	16935	20.59%
PF III	3261	3.96%

Table 8.1.1

In his computations, the average running time (on an IBM PS/2 with Turbo Pascal) for a c value at 10^5 is approximately 1.56 minutes. Hence, we would expect the running time required for $c \approx 10^{12}$ to be about 30 years per number. As a result, a faster technique would be needed in order to determine the existence of principal factors for $Q(\sqrt[3]{c})$ when c is large (here, $c \approx 10^{12}$).

In this chapter, we show how the infrastructure idea can be used to produce a fast algorithm for finding principal factors in pure cubic fields. Also, we present a fast technique for determining whether r* = 1 or 3. This algorithm was implemented on a computer and was used to test a conjecture of Mayer [May88] by determining the existence of principle factors for certain pure cubic fields with large discriminant.

§8.2 Ideals of O_F.

In order to describe our algorithm for determining principal factors for **F**, it is necessary to discuss a method for finding a basis of an ideal, **a'**, where **aa'** = (L(**a**)).

We first note that we can factor **a** into a product of two ideals, say $\mathbf{a} = \mathbf{a}_1\mathbf{a}_2$, by using the following lemma of [WDS83].

Lemma 8.2.1. If

$$\mathbf{a} = \left\{ P\ ,\ P'\ (-u + \delta)\ ,\ P''\left(\frac{v + v'\delta + \delta^2}{\sigma}\right) \right\}$$

is a primitive ideal of O_F ($P, P', P'', u, v, v', \sigma \in \mathbf{Z}$), then $\mathbf{a} = \mathbf{a}_1\mathbf{a}_2$ where

$$\mathbf{a}_1 = \left\{ P_1\ ,\ P_1'\ (-c + \delta)\ ,\ P_1''\left(\frac{c^2 + c\delta + \delta^2}{\sigma}\right) \right\},$$

$$\mathbf{a}_2 = \left\{ P_2\ ,\ P_2'\ (-u + \delta)\ ,\ P_2''\left(\frac{v + v'\delta + \delta^2}{\sigma}\right) \right\},$$

$P_1 = \gcd(P,S)$, $\quad P_2 = P / P_1$,

$P_1' = \gcd(P',S)$, $\quad P_2' = P' / P_1'$,

$P_1'' = \gcd(P'',S)$, $\quad P_2'' = P'' / P_1''$. ■

Our next step is to find $\mathbf{a}_1'$ and $\mathbf{a}_2'$ separately. If $\mathbf{a}_1'$ and $\mathbf{a}_2'$ are known, then we find **a'** by multiplying $\mathbf{a}_1'$ and $\mathbf{a}_2'$. To find $\mathbf{a}_1'$ we use the following lemma. Let $\xi \in \mathbf{Z}$ be defined as being a solution of the system of congruences

$$\xi^3 \equiv c \pmod{\sigma^2}$$

$$3\xi^2 \equiv 0 \pmod{\sigma}.$$

Lemma 8.2.2. Put $T = \gcd(\sigma, P_1)$. If $\mathbf{a}_1$ is as defined by Lemma 8.2.1, then $\mathbf{a}_1' = \mathbf{b}$ where

$$\mathbf{b} = \left\{ P_1\ ,\ P_1/(P_1'T)\ (-c + \delta)\ ,\ \left(\frac{T}{P_1''}\right)\left(\frac{c^2 + c\delta + \delta^2}{\sigma}\right) \right\}.$$

Proof. We know that $N(\mathbf{a}_1) = P_1P_1'P_1''$ and $\mathbf{a}_1^3 = (f)$ where $f \in \mathbf{Z}$. Since $N(\mathbf{a}_1)^3 = |f|^3$, we have

$$\mathbf{a}_1^3 = (P_1P_1'P_1'').$$

If we multiply both sides by $\mathbf{a}_1'$, we get

$$\mathbf{a}_1^3\mathbf{a}_1' = (P_1P_1'P_1'')\mathbf{a}_1'.$$

But $\mathbf{a}_1\mathbf{a}_1' = (P_1)$. It follows that

$$\mathbf{a}_1^2 = (P_1'P_1'')\mathbf{a}_1'.$$

On the other hand, by §6 of [WDS83], we know that

$$\mathbf{a}_1^2 = (P_1'P_1'')\mathbf{b},$$

where

$$\mathbf{b} = \left\{ P_1 , P_1/(P_1'T)\,(-c+\delta) , \left(\frac{T}{P_1''}\right)\left(\frac{c^2 + c\delta + \delta^2}{\sigma}\right) \right\}.$$

Thus, we have $\mathbf{a}_1' = \mathbf{b}$. ■

In the case where $\gcd(L(\mathbf{a}_2),\sigma) = \gcd(P_2,\sigma) = 1$, we can find $\mathbf{a}_2'$ by using

Lemma 8.2.3. If

$$\mathbf{a}_2 = \left\{ P_2 , P_2'\,(-u+\delta) , P_2''\left(\frac{v + v'\delta + \delta^2}{\sigma}\right) \right\},$$

where $\gcd(P_2,\sigma) = 1$, then

$$\mathbf{a}_2' = \left\{ Q , Q'\,(-U+\delta) , Q''\left(\frac{V + V'\delta + \delta^2}{\sigma}\right) \right\},$$

where

$$Q'' = 1,\ Q' = P_2 / P_2',\ Q = P_2,$$

$$U = v',\ V = -v - v'V',$$

$$V' = u + \mu P / P',\ \mu \equiv (\xi - u)(P_2 / P_2')^{-1} \pmod{\sigma}.$$

Proof. We first note that $L(\mathbf{a}_2) = L(\mathbf{a}_2') = P_2 = Q$. Since $\mathbf{a}_2\mathbf{a}_2' = (L(\mathbf{a}_2))$, we have $N(\mathbf{a}_2\mathbf{a}_2') = L(\mathbf{a}_2)^3$ (i.e. $PP'P''QQ'Q'' = P^3$). We can easily deduce that $Q'Q'' = (P_2 / P_2'P_2'')$. Since $\gcd(P_2,\sigma) = 1$, then $P_2'' = Q'' = 1$. As a result, we get $Q' = P_2 / P_2'$. The remaining unknowns are U, V and V'. We can find those values by determining

$$U \pmod{Q/ Q'},$$

$$V' \pmod{\sigma Q' / Q''},$$

$$V \pmod{\sigma Q / Q''}.$$

We can see that

$$Q'P_2''(-U+\delta)\left(\frac{v + v'\delta + \delta^2}{\sigma}\right) \in (P_2).$$

It follows that

$$Q'P_2''\left(\frac{-Uv+\delta(v-Uv')+\delta^2(-U+v')}{\sigma}\right) = P_2x+P_2y(-\xi+\delta)+P_2z\left(\frac{\delta^2+\xi\delta+\xi^2}{\sigma}\right)$$

where $x, y, z \in \mathbf{Z}$. We get

$$Q'P_2''\left(\frac{\delta^2(-U+v')}{\sigma}\right) = P_2z\left(\frac{\delta^2}{\sigma}\right)$$

or

$$Q'P_2''(-U+v') = P_2z.$$

Thus, we have

$$U \equiv v' \pmod{P_2 / Q'P_2''}.$$

Since $P_2'' = 1$, we can put $U = v'$.

Also, we have

$$P_2'Q''(-u+\delta)\left(\frac{V + V'\delta + \delta^2}{\sigma}\right) \in (P_2).$$

By using the above technique, we get

$$P_2'Q''(V'-u) = P_2z$$

where $z \in \mathbf{Z}$. It follows that

$$V' - u \equiv 0 \pmod{P_2 / P_2'Q''}.$$

Since $Q' = P_2 / P_2'$, we have

$$V' - u \equiv 0 \pmod{Q' / Q''}$$

or

$$V' = u + \mu Q'$$

where $\mu \in \mathbf{Z}$ (here, $Q'' = 1$). Since $\left(\frac{V + V'\delta + \delta^2}{\sigma}\right) \in \mathbf{O}_F$, we must have

$$V' \equiv \xi \pmod{\sigma}.$$

Therefore,

$$u + \mu Q' \equiv \xi \pmod{\sigma}.$$

Thus, if we find μ such that

$$\mu \equiv (\xi - u)Q'^{-1} \pmod{\sigma},$$

then

$$V' = u + \mu Q'.$$

Similarly, we have

$$P_2"Q"\left(\frac{v + v'\delta + \delta^2}{\sigma}\right)\left(\frac{V + V'\delta + \delta^2}{\sigma}\right) \in (P_2).$$

We then get

$$P_2"Q"(v+v'V'+V) = P_2\sigma z,$$

where $z \in \mathbf{Z}$. Hence, we get

$$V \equiv -V'v' - v \left(\mod \frac{P_2\sigma}{P_2"Q"}\right).$$

Since $P_2' = 1$, we can put

$$V = -V'v' - v. \quad \blacksquare$$

We now can find a basis of $\mathbf{a}'$ by computing $\mathbf{a}_1'\mathbf{a}_2'$.

In the case where $\gcd(L(\mathbf{a}_2),\sigma) \neq 1$, we know that $3^q \mid L(\mathbf{a}_2)$, where $3 \mid \sigma$, $q \in \mathbf{Z}^+$; also, this can only occur when $c \equiv \pm 1 \pmod 9$. We first factor $\mathbf{a}_2$ into a product of two ideals, say $\mathbf{a}_2 = \mathbf{b}_1\mathbf{b}_2$, such that $3 \nmid L(\mathbf{b}_2)$ and $\gcd(L(\mathbf{b}_1),L(\mathbf{b}_2)) = 1$. In other words, we have to find $\mathbf{b}_1$ and $\mathbf{b}_2$, where $L(\mathbf{b}_1) = 3^q$ and $L(\mathbf{b}_2) = L(\mathbf{a}_2) / 3^q$. By §5 of [WDS83], we know that $\mathbf{b}_1$ must be one of $\mathbf{r}$, $\mathbf{r}^{2i}$, $\mathbf{r}^{2i+1}$, $\mathbf{s}^i$, $\mathbf{rs}$, $\mathbf{rs}^i$, where $i \in \mathbf{Z}$ and $(3) = \mathbf{rs}^2$. In order to determine the basis for $\mathbf{b}_1$, we can use the results described in p.253 of [WDS83]. As for the problem of finding a basis for $\mathbf{b}_2$, we can use

Lemma 8.2.4. Given that

$$\mathbf{b}_3 = \left\{ P_3 , P_3' (-u_3 + \delta) , P_3"\left(\frac{v_3 + v_3'\delta + \delta^2}{\sigma}\right) \right\}$$

is a primitive ideal of $\mathbf{O}_\mathbf{F}$ (P_3, P_3', $P_3"$, u_3, v_3, v_3', $\sigma \in \mathbf{Z}$), we can then find $\mathbf{Z}$ bases for $\mathbf{b}_1$, $\mathbf{b}_2$ such that $\mathbf{b}_3 = \mathbf{b}_1\mathbf{b}_2$ when

$$b_i = \left\{ P_i , P_i' (-u_i + \delta) , P_1'' \left(\frac{v_i + v_i'\delta + \delta^2}{\sigma} \right) \right\} (i = 1,2),$$

and

$$P_3 = P_1 P_2, \ \gcd(P_1,P_2) = 1,$$

$$P_3' = P_1' P_2', \ P_1' \mid P_1, \ P_2' \mid P_2, \ \gcd(P_1',P_2') = 1,$$

$$P_3'' = P_1'' P_2'', \ P_1'' \mid P_1, \ P_2'' \mid P_2, \ \gcd(P_1'',P_2'') = 1.$$

Proof. Clearly, P_1, P_1', P_1'',P_2, P_2', P_2'' are easy to find. By using the Corollary of Lemma 5.1 of [WDS83], we see that is is sufficient to find the values of

$$u_i \pmod{P_i / P_i'},$$

$$v_i' \pmod{\sigma P_i' / P_i''},$$

$$v_i \pmod{\sigma P_i / P_i''}.$$

By Theorem 5.3 of [WDS83], we have

$$u_1 \equiv u_3 \pmod{P_1 / P_1'},$$

$$u_2 \equiv u_3 \pmod{P_2 / P_2'}.$$

Thus, we have $u_1 = u_2 = u_3$.

Also, we know that

$$v_1' \equiv v_3' \pmod{\sigma P_1' / P_3''},$$

$$v_2' \equiv v_3' \pmod{\sigma P_2' / P_3''},$$

$$v_1 \equiv v_3 + u_1(v_3' - v_1') \pmod{\sigma P_1 / P_3''},$$

$$v_2 \equiv v_3 + u_2(v_3' - v_2') \pmod{\sigma P_2 / P_3''}.$$

We show here how to get v_i, v_i', (i = 1, 2).

Since

$$P_1'' \left(\frac{v_i + v_i'\delta + \delta^2}{\sigma} \right) \in \mathbf{O}_F,$$

we have

$$P_1'' \left(\frac{v_i + v_i'\delta + \delta^2}{\sigma} \right) = x + y(-\xi + \delta) + z \left(\frac{\xi^2 + \xi\delta + \delta^2}{\sigma} \right).$$

From this result we get

$$P_i'' = z,$$

$$P_i''v_i' = \sigma y + z\xi,$$

$$P_i''v_i = \sigma x - y\sigma\xi + z\xi^2.$$

Consequently, we get

$$P_i''v_i' = \sigma y + P_i''\xi,$$

$$P_i''v_i = \sigma x - (P_i''v_i' - P_i''\xi)\xi + P_i''\xi^2.$$

Thus,

$$v_i' \equiv \xi \pmod{\sigma / P_i''}$$

and

$$v_i \equiv -v_i'\xi + 2\xi^2 \pmod{\sigma / P_i''}.$$

Since

$$v_i' = v_3' + r_i'\sigma P_i' / P_3'' = v_3' + r_i'\sigma P_i' / (P_{3-i}''P_i''),$$

where $r_i' \in \mathbf{Z}$, we have

$$v_3' + r_i'\sigma P_i' / (P_{3-i}''P_i'') \equiv \xi \pmod{\sigma / P_i''}.$$

Put

$$r_i' = k_i P_{3-i}'' + s_i',$$

where $0 \le s_i' < P_{3-i}''$. Then, we can deduce that

$$s_i'\sigma P_i' / (P_{3-i}''P_i'') \equiv \xi - v_3' \pmod{\sigma / P_i''}.$$

It follows that

$$s_i'P_i' \equiv P_{3-i}''P_i''(\xi - v_3') / \sigma \pmod{P_{3-i}''}.$$

Since $\gcd(P_i', P_{3-i}'') = 1$, we get

$$s_i' \equiv (P_i')^{-1}P_3''(\xi - v_3') / \sigma \pmod{P_{3-i}''}.$$

Hence,

$$v_i' \equiv v_3' + s_i'\sigma P_i' / P_3'' \pmod{\sigma P_i' / P_i''}.$$

We note that

$$v_i = v_3 + u_i(v_3' - v_i') + r_i\sigma P_i / P_3''$$

where $r_i \in \mathbf{Z}$. Again, we put

$$r_i = k_i P_{3-i}'' + s_i,$$

where $0 \le s_i < P_{3-i}''$. We now have

$$s_i \sigma P_i / (P_{3-i}'' P_i'') \equiv -v_i'\xi - \xi^2 - v_3 - u_i(v_3' - v_i') \pmod{\sigma / P_i''}.$$

By using the above technique, we can easily deduce that

$$s_i P_i \equiv P_{3-i}'' P_i''(-v_i'\xi - \xi^2 - v_3 - u_i(v_3' - v_i')) / \sigma \pmod{P_{3-i}''}.$$

Since $\gcd(P_i', P_{3-i}'') = 1$, we get

$$s_i \equiv -(P_i)^{-1} P_3''(v_i'\xi + \xi^2 + v_3 + u_i(v_3' - v_i')) / \sigma \pmod{P_{3-i}''}.$$

As a result, we have

$$v_i \equiv v_3 + s_i \sigma P_i / P_3'' \pmod{\sigma P_i / P_i'}. \quad \blacksquare$$

Once we have $\mathbf{b}_1$ and $\mathbf{b}_2$, we can obtain $\mathbf{a}_2'$ by finding $\mathbf{b}_1'\mathbf{b}_2'$. To find $\mathbf{b}_2'$, we can use Lemma 8.2.3. As mentioned earlier, $\mathbf{b}_1$ is one of $\mathbf{r}$, $\mathbf{r}^{2i}$, $\mathbf{r}^{2i+1}$, $\mathbf{s}^i$, $\mathbf{rs}$, $\mathbf{rs}^{i+1}$. Thus, by using the fact that (3) = $\mathbf{rs}^2$, we can easily determine $\mathbf{b}_1'$ by using the following table.

$\mathbf{b}_1$	$\mathbf{b}_1'$
$\mathbf{r}$	$\mathbf{rs}$
$\mathbf{r}^{2i}$	$\mathbf{s}^i$
$\mathbf{r}^{2i+1}$	$\mathbf{rs}^{i+1}$
$\mathbf{s}^i$	$\mathbf{r}^{2i}$
$\mathbf{rs}$	$\mathbf{r}$
$\mathbf{rs}^{i+1}$	$\mathbf{r}^{2i+1}$

Table 8.2.1

We point out here that if $\mathbf{a}$ is reduced, it is not necessarily the case that $\mathbf{a}'$ is reduced. This is the reason why the Voronoi algorithm, starting with (1), does not possess the nice symmetry properites that the regular continued fraction expansion does in the quadratic case.

If $\mathbf{i}_1 = (1)$, let $1 \le n \le p$ $(\theta_{p+1} = \varepsilon_0)$, $(\theta_n L(\mathbf{i}_1))\mathbf{i}_n = (L(\mathbf{i}_n))\mathbf{i}_1$ and $(\rho_j L(\mathbf{b}_1))\mathbf{b}_j = (L(\mathbf{b}_j))\mathbf{b}_1$, where $\mathbf{b}_1 = \mathbf{i}_n'$, $\mathbf{b}_j$ is reduced and $\mathbf{b}_{j-1}$ is not reduced. Since

$$\mathbf{b}_j \sim \mathbf{b}_1 = \mathbf{i}_n' \sim \mathbf{i}_1' = (1),$$

we must have $\mathbf{b}_j = \mathbf{i}_q$ for some q. Furthermore, we can calculate the distance between $\mathbf{i}_q$ and $\mathbf{i}_1$ by using

Theorem 8.2.1. ([Wil85]) If $\delta_n = \delta(\mathbf{i}_n,\mathbf{i}_1)$, $\delta_q = \delta(\mathbf{i}_q,\mathbf{i}_1)$ and $\eta = \log(L(\mathbf{i}_n)\rho_j)$, then

$$\delta_q = R - \delta_n + \eta.$$

Also

$$-2\log(\sqrt{3}|D|) < \eta < \log(\sqrt{3}|D|). \quad \blacksquare$$

We require the following results in our algorithm for determining the existence of principal factors for **F**.

Lemma 8.2.5. Let $\mathbf{j}$ be a primitive ideal. If $\mathbf{i}^2 = (u)\,\mathbf{j}$ where $u \in \mathbf{Z}$, then $L(\mathbf{i})^2 \ge uL(\mathbf{j})$.

Proof. By §6 of [WDS83] we have

$$\mathbf{i} = \mathbf{i}_1\mathbf{i}_2$$

where $L(\mathbf{i}) = P = P_1P_2$ with $P_1 = L(\mathbf{i}_1)$, $P_2 = L(\mathbf{i}_2)$, $\gcd(P_1,P_2) = 1$ and $P_1 = \gcd(P,S)$. Now

$$\mathbf{i}_1^2 = (P_1'P_1'')\mathbf{j}_1,$$

$$\mathbf{i}_2^2 = (P_2'')\mathbf{j}_2,$$

where

$$L(\mathbf{j}_1) = P_1,$$

$$L(\mathbf{j}_2) \le P_2^2 / P_2'',$$

$$P_1' = \gcd(P',S),\ P_1'' = \gcd(P'',S).$$

Since $P_1'P_1'' \mid P_1$ and $u = P_1'P_1''P_2''$, we have

$$L(\mathbf{i})^2 = P_1^2P_2^2 \text{ and } uL(\mathbf{j}) \le P_1'P_1''P_1P_2^2.$$

It follows that $L(\mathbf{i})^2 \ge uL(\mathbf{j})$. $\blacksquare$

Lemma 8.2.6. If $\theta_g^{(r)}$ is as defined in §6.3, then $\theta_g^{(r)} < 6mn$.

Proof. We can easily deduce this by using the results derived in the proof of Lemma 6.2 of [WCS80]. ■

§8.3 Determination of Principal Factors in F.

In order to describe our algorithm for finding principal factors for **F**, we must use several results from [Wil81]. One of these is

Lemma 8.3.1.(Williams) Let $k \in \mathbf{Z}$ and $3 \nmid k$. If $e = 1$, then there exists $\gamma \in \mathbf{O}_F$ such that

$$N(\gamma) = 3^{\tau}st^2,\ s = s_1s_2,\ t = t_1t_2,$$

$$s_1t_1 \mid m,\ s_2t_2 \mid n,\ \tau \in \{0, 1, 2\}$$

$$\delta_1 = \delta / (s_2t) > 1,\ \delta_2 = \bar{\delta} / (s_1t) > 1 \quad N(\gamma) < 3^{\tau}mn$$

and

$$\varepsilon_0^{\,k} = \gamma^3 / N(\gamma). \ ■$$

Theorem 8.3.1 (Williams) If $e = 1$ and γ is defined as above, then if $i_1 = (1)$, either

$\gamma = \theta_r$

where

$$\theta_r = \theta_g\varepsilon_0^{\,q}$$

$(1 < g \leq p,\ q \in \mathbf{Z},\ R = \theta_{p+1})$ or

$$\chi\gamma / 3 = \theta_r,$$

where χ is a value of

$$X_1 + X_2\delta_1 + X_3\delta_2 \qquad (X_1, X_2, X_3 \in \mathbf{Z})$$

such that

$$\begin{cases} X_1 + ms_2t\,X_2 + ns_1t\,X_3 \equiv 0 \pmod 3 & \text{when } \tau = 2 \\ X_1 \equiv ms_2t\,X_2 \equiv ns_1t\,X_3 \pmod 3 & \text{when } \tau = 0 \text{ or } 1, \end{cases}$$

$$0 < \chi < 3,$$

and

$$F(\chi) < 9$$

for

$$F(\chi) = X_1^2+\delta_1^2X_2^2+\delta_2^2X_3^2-\delta_1X_1X_2-\delta_2X_1X_3-\delta_1\delta_2X_2X_3. \quad \blacksquare$$

In the case where $\gamma = \theta_r$, we have

$$\varepsilon_0^k = \theta_r^3 / N(\theta_r)$$

Thus, we get

(8.3.1) $$kR / 3 < \log \theta_r < kR / 3 + \log(9mn) / 3.$$

If we know kR, we can find all the possible θ_r's which satisfy (8.3.1) by using the method described in §6.3. For each of these θ_r's, we check whether or not $N(\theta_r) \mid S^2$. From §6.3 it is known that $(\theta_r)\mathbf{i}_r = (N(\mathbf{i}_r))\mathbf{i}_1$. Thus, if $\mathbf{i}_r$ has a basis of the form

$$\left\{ P , P' (-u + \delta) , P''\left(\frac{v + v'\delta + \delta^2}{\sigma}\right) \right\},$$

then we can easily deduce that $N(\theta_r) = P^2 / (P'P'')$ by using the formula for finding $N(\theta_r)$ as given in [Wil82] (also, see [WCS80]). If $N(\theta_r) \mid S^2$, then $\gamma = \theta_r$. Now $\theta_r = \theta_g\varepsilon_0^q$, where $1 \le g \le p$ and $q \in \mathbf{Z}$. Hence, by using Theorem 5.3 of [Wil81], we know that there can be at most 2 distinct values of g ($1 \le g \le p$), g_1, g_2 such that $N(\theta_{g_i}) \mid S^2$. If e = 1 and there are exactly j such values of g (j = 0, 1, 2), we use the notation of Mayer [May88] and say that **F** is an M_j field. If $j < 2$, **F** is called an exotic field. We note, by Theorem 5.14 of [May88], that if $3 \mid c$, then F can never be an exotic field. In [May88], Mayer gives a table of counts of M_j fields for the c values upto 100000, and they are as follows:

Type	# of fields	% of M_j fields
M_0	59164	95.32%
M_1	2818	4.54%
M_2	86	0.14%
Total	62068	100%

Table 8.3.1.

We now consider the case where **F** is an exotic field (i.e. $\gamma \neq \theta_r$) and let θ_r be as defined above. Also, we note that

$$\varepsilon_0^k = \theta_r^3 / \lambda = \gamma^3 / N(\gamma)$$

where $\lambda \in \mathbf{O_F}$. If $\theta_r = \chi\gamma / 3$, we get

(8.3.2) $$27\lambda = N(\gamma)\chi^3.$$

Hence, since $0 < \chi < 3$, we get

$$\lambda < N(\gamma) < 3^\tau mn \leq 9mn.$$

Also, since $F(\chi) < 9$, we can easily deduce that

$$|\lambda'| = |\lambda''| < N(\gamma) < 3^\tau mn \leq 9mn.$$

Put

$$\lambda = (x + y\delta + z\bar{\delta}) / 3$$

where $x,y,z \in \mathbf{Z}$. By using a technique employed in [Wil81], we get

$$|x|, \delta|y|, \bar{\delta}|z| < |\lambda| + 2|\lambda'|.$$

Consequently, we have

$$|x|, \delta|y|, \bar{\delta}|z| < 3N(\gamma) < 3(3^\tau mn) \leq 27mn.$$

Thus the values of the coefficients in λ never get very large.

If we know, for a certain θ_r, the value of λ, our task is to determine whether or not (8.3.2) holds. If (8.3.2) holds, then we can attempt to find the principal factors for **F**. On the other hand, if (8.3.2) fails, then it is not possible to find a principal factor using this particular θ_r. In this section, we present an algorithm for determining the principal factors of S^2 under the assumption that $\theta_r = \chi\gamma / 3$ and λ is known. In the following section, we present a method for finding λ.

By multiplying both sides of (8.3.2) by $N(\gamma)^2$, we get

$$(3^\tau st^2\chi)^3 = 27N(\gamma)^2\lambda = 27(3^{2\tau}s^2t^4\lambda).$$

Since

$$\chi = X_1 + X_2\delta_1 + X_3\delta_2$$

and

$$\lambda = (x + y\delta + z\bar{\delta}) / 3,$$

we get

(8.3.3) $$3^{\tau-3}(stX_1 + s_1X_2\delta + s_2X_3\bar{\delta})^3 = s^2t(x + y\delta + z\bar{\delta}) / 3.$$

From (8.3.3), we can easily deduce that

(8.3.4) $$3^{\tau-2}(s^3t^3X_1^3+s_1^3mn^2X_2^3+s_2^3m^2nX_3^3+6s^2tmnX_1X_2X_3) = s^2t\ x,$$

(8.3.5) $$3^{\tau-1}(s_1s^2t^2X_1^2X_2+sts_2^2mX_1X_3^2+s_1^2s_2mnX_2^2X_3) = s^2t\ y,$$

(8.3.6) $$3^{\tau-1}(s_2s^2t^2X_1^2X_3+sts_1^2nX_1X_2^2+s_1s_2^2mnX_2X_3^2) = s^2t\ z.$$

On the other hand, we have

(8.3.7) $$N(st\chi) = 3^{3-\tau}s^2tN(\theta_r)$$
$$= s^3t^3X_1^3+s_1^3mn^2X_2^3+s_2^3m^2nX_3^3-3s^2tmnX_1X_2X_3.$$

If we compare (8.3.7) and (8.3.4), then we find that

(8.3.8) $$3^{\tau}(mnX_1X_2X_3) = x - 3N(\theta_r).$$

Thus, if principal factors exist for **F**, then we have (8.3.8). Since $\tau \in \{0, 1, 2\}$, we can divide (8.3.8) into two cases: $\tau = 2$ and $\tau < 2$.

We first consider the case where $\tau = 2$. For this case, we shall require a lemma of [Wil82] to limit the possible values of X_1, X_2, X_3. Here, we let $\delta_m = \min(\delta_1,\delta_2)$ and $\delta_M = \max(\delta_1,\delta_2)$.

Lemma 8.3.2.(Williams) Let $\mu \in \mathbf{Q}[\delta]$ and $\mu = st^2\chi$ where χ is the least positive value of $X_1 + X_2\delta_1 + X_3\delta_2$ such that $X_1, X_2, X_3 \in \mathbf{Z}$, $F(\chi) < 9$,

$$X_1 + ms_2t\ X_2 + ns_1t\ X_3 \equiv 0 \pmod 3.$$

If it is not the case that

$$X_1 \equiv ms_2t\ X_2 \equiv ns_1t\ X_3 \pmod 3,$$

then $\chi < 3$ if and only if one of the following is true.

(i) $ms_2t \equiv ns_1t \equiv 1 \pmod 3$, $\delta_m < (\sqrt{33} - 1) / 2$. In this case χ is one of δ_m-1, δ_M-δ_m.

(ii) $ms_2t \equiv ns_1t \equiv -1 \pmod 3$, $\delta_m < 2$. In this case χ is one of δ_m+1, δ_M-δ_m, 2-δ_m.

(iii) $ms_2t \equiv 1 \pmod 3$, $ns_1t \equiv -1 \pmod 3$, $\delta_m < (\sqrt{33} - 1) / 2$. In this case χ is δ_m-1.

(iv) $ms_2t \equiv -1 \pmod 3$, $ns_1t \equiv 1 \pmod 3$, $\delta_M < (\sqrt{33} - 1)/2$ or $\delta_m < 2$. In this case χ is one of δ_m+1, δ_M-1, $2-\delta_m$. ■

We can limit the minmum value of χ yet further. We do this in

Theorem 8.3.2. Suppose that γ is defined as in Theorem 8.3.1. If χ is the least positive value of $X_1 + X_2\delta_1 + X_3\delta_2$ such that $X_1, X_2, X_3 \in \mathbf{Z}$, $0 < \chi < 3$, $F(\chi) < 9$,

$$X_1 + ms_2t\, X_2 + ns_1t\, X_3 \equiv 0 \pmod 3,$$

and it is not the case that

$$X_1 \equiv ms_2t\, X_2 \equiv ns_1t\, X_3 \pmod 3,$$

then

$$\theta = \omega\gamma / 3$$

is a minimum of $\mathbf{O}_F$ where $\omega = \delta_m-1$ when $ms_2t \equiv 1 \pmod 3$ and $\omega = \delta_m+1$ when $ms_2t \equiv -1 \pmod 3$.

Proof. We know that $\phi = \chi\gamma / 3$ is a minimum of $\mathbf{O}_F$, where χ is given by the previous lemma. We note that if $\omega \neq \chi$, then by Lemma 8.3.2

$$\chi \in \{\delta_M-\delta_m, \delta_m-1, 2-\delta_m\}.$$

Also, $\theta = \omega\gamma / 3 \in \mathbf{O}_F$ by the reasoning of Theorem 8.3.1. But

$$F(\chi) \in \{\delta_M^2+\delta_m\delta_M+\delta_m^2, 4+2\delta_m+\delta_m^2, 1+\delta_M+\delta_M^2\}$$

and

$$F(\omega) = 1+\delta_m+\delta_m^2 \text{ or } 1-\delta_m+\delta_m^2.$$

In any case, since $1 < \delta_m < \delta_M$ we have $F(\omega) < F(\chi)$. We also note that $\omega < 3$. If $\omega \neq \chi$, then $\omega > \chi$ and $\theta > \phi$. Also, $|\theta'| < |\phi'|$. If θ is not a minimum of $\mathbf{O}_F$, then there must exist a minimum ψ of $\mathbf{O}_F$ such that

$$|\psi'| < |\theta'|, \quad 0 < \psi < \theta.$$

It follows that

$$\psi < \gamma, \quad |\psi'| < |\gamma'|.$$

By Theorem 8.3.1 and Lemma 8.3.2, we get

$$\nu = 3\psi / \gamma \in \{\delta_M-\delta_m, \delta_M-1, \delta_m-1, \delta_m+1, 2-\delta_m\}.$$

Also, since $|\psi'| < |\theta'|$, we have $F(\nu) < F(\omega)$ which is not possible by the selection of ω. Thus, our result follows. ■

It follows that, if $\tau = 2$, we must have $X_1X_2X_3 = 0$ and $x = 3N(\theta_r)$ for some θ_r, where $\lambda_r = \lambda = (x + y\delta + z\tilde{\delta}) / 3$. Also, $(X_1, X_2, X_3) = (1,1,0), (1,0,1), (-1,1,0), (-1,0,1)$. From (8.3.5) and (8.3.6) we can derive that

(8.3.9) $$3ms_2^3X_1X_3^3-s_1s_2^2X_3y+s_1^2s_2X_2z-3ns_1^3X_1X_2^3 = 0.$$

Here, we have two subcases.

Subcase 1. $X_2 = 0$. In this subcase we have $X_1 = -1$ or 1, $X_3 = 1$, and $\delta_1 > \delta_2$. By (8.3.9) we get

(8.3.10) $$3ms_2 / s_1 = X_1y.$$

Also, by (8.3.6) we obtain

(8.3.11) $$3s_2t = z.$$

Since $X_2 = 0$, we must have

$$\delta_2^3 = \tilde{\delta}^3 / (s_1t)^3 = m^2n / (s_1^3t^3).$$

If we divide (8.3.10) by (8.3.11), then we get

$$X_1y / z = m / (s_1t).$$

If we raise the above equation to the 3rd power, we have

$$X_1y^3 / z^3 = m^3 / (s_1^3t^3).$$

It follows that

$$nX_1y^3 / mz^3 = m^2n / (s_1^3t^3) = \delta_2^3.$$

Since $\delta_2 > 1$, we can conclude that

(8.3.12) $$\left|\frac{y}{z}\right| \sqrt[3]{\frac{n}{m}} = \delta_2 > 1.$$

Furthermore, we can easily deduce that

$$s_1 = m / \gcd(m, y / 3),$$

$$s_2 = \gcd(n, y / 3),$$

$$t = z / 3s_2,$$

$$X_1 = \mathrm{sgn}(z).$$

Subcase 2. $X_3 = 0$. In this subcase we have $X_1 = -1$ or 1, $X_2 = 1$, and $\delta_2 > \delta_1$. By using the same technique as in Subcase 1, we get

$$3ns_1 / s_2 = X_1 z$$

and

$$3ts_1 = y.$$

Since $X_3 = 0$, we must have

$$\delta_1^3 = \delta^3 / (s_2 t)^3 = mn^2 / (s_2^3 t^3).$$

Again, by using the same method as in the previous case, we get

$$mX_1 z^3 / (ny^3) = mn^2 / (s_2^3 t^3).$$

This means that

$$\delta / (s_2 t) = \delta_1 = \left| \frac{z}{y} \right| \sqrt[3]{\frac{m}{n}}.$$

Thus, since $\delta_1 > 1$, we must have

(8.3.13) $$\left| \frac{z}{y} \right| \sqrt[3]{\frac{m}{n}} > 1.$$

Also, we can deduce that

$$s_1 = \gcd(m , z / 3),$$

$$s_2 = n / \gcd(n , z / 3),$$

$$t = y / 3,$$

$$X_1 = \mathrm{sgn}(y).$$

Since the product of δ_1 and δ_2 is one, we see that only one of (8.3.12) and (8.3.13) can occur. Thus, we can distinguish between Subcase 1 and Subcase 2 by determining which of

$$\left| \frac{y}{z} \right| \sqrt[3]{\frac{n}{m}} \quad \text{or} \quad \left| \frac{z}{y} \right| \sqrt[3]{\frac{m}{n}} > 1.$$

Once we know which case, we can determine s_1, s_2 t and X_1 by using the above formulae. We now have the values for $N(\gamma) = 9s_1 s_2 t^2$, X_2, and X_3, and can determine whether or

not (8.3.2) holds. If (8.3.2) holds, then $9s_1s_2t^2$ is a principal factor for **F**. Otherwise, we cannot find principal factors for this given λ. We now summarize our algorithm as follows:

Algorithm 8.3.1. Given: θ_r, $\lambda_r = (x + y\delta + z\bar{\delta}) / 3$ and $x = 3N(\theta_r)$.

1) Compute temp $\leftarrow |z / y| \sqrt[3]{m/n}$.

2) If temp > 1, then goto **step** 5.

3) Compute $s_1 = m / \gcd(m, y / 3)$, $s_2 = \gcd(n, y / 3)$, $t = z / 3s_2$, $X_1 = \mathrm{sgn}(z)$.

4) Goto **step** 6.

5) Compute $s_1 = \gcd(m, z / 3)$, $s_2 = n / \gcd(n, z / 3)$, $t = y / 3$, $X_1 = \mathrm{sgn}(y)$.

6) If (8.3.2) holds, then $9s_1s_2t^2$ is a principal factor; otherwise, (8.3.2) cannot hold.

7) Stop.

We now consider the case where $\tau < 2$. In this case we have $X_1X_2X_3 = -1$ and $x = 3N(\theta_r) - 3^{\tau}mn$. The equations (8.3.4), (8.3.5), (8.3.6), together with (8.3.7), become

$$st^2X_1^3 + s_1mn^2X_2/(s_2^2t) + s_2m^2nX_3/(s_1^2t) = 3^{3-\tau}N(\theta_r)-3mn,$$

$$s_1tX_2 + s_2mX_1/s_1 + mnX_3/(s_2t) = 3^{1-\tau}y,$$

$$s_2tX_3 + s_1nX_1/s_2 + mnX_2/(s_1t) = 3^{1-\tau}z.$$

Put $\rho_1 = s_2tX_3$, $\rho_2 = s_1nX_1/s_2$, $\rho_3 = mnX_2/(s_1t)$. Here, by using the last two equations above, we have

$$\rho_1 + \rho_2 + \rho_3 = 3^{1-\tau}z,$$

$$\rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3 = -n3^{1-\tau}y,$$

(8.3.14) $$\rho_1\rho_2\rho_3 = -mn^2.$$

It follows that ρ_1, ρ_2, ρ_3 are the three distinct roots of

(8.3.15) $$\rho^3 - 3^{1-\tau}z\rho^2 - n3^{1-\tau}y\rho + mn^2 = 0.$$

Also,

$$-\rho_1 / \rho_3 = st^2X_1 / (mn),$$

$$-\rho_2 / \rho_1 = s_1nX_2 / (s_2^2t),$$

(8.3.16) $$-\rho_3 / \rho_2 = s_2 m X_3 / (s_1^2 t).$$

Thus, we see that

$$3^{\tau} | mn\rho_1 / \rho_3 |, 3^{\tau} | mn\rho_2 / \rho_1 |, 3^{\tau} | mn\rho_3 / \rho_2 |$$

are principal factors for **F**.

By using the above equations, we obtain

$$-mn(\rho_1 / \rho_3 + \rho_2 / \rho_1 + \rho_3 / \rho_2) = 3^{3-\tau} N(\theta_r) - 3mn$$

and

$$\rho_1^2\rho_2 + \rho_1\rho_3^2 + \rho_2^2\rho_3 = n(3^{3-\tau} N(\theta_r) - 3mn).$$

Furthermore, since

$$(\rho_1 + \rho_2 + \rho_3)(\rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3) - 3\rho_1\rho_2\rho_3$$
$$= (\rho_1^2\rho_2 + \rho_1\rho_3^2 + \rho_2^2\rho_3) + (\rho_1\rho_2^2 + \rho_1^2\rho_3 + \rho_2\rho_3^2),$$

it follows that

$$(\rho_1\rho_2^2+\rho_1^2\rho_3+\rho_2\rho_3^2) = -3^{2-2\tau} nyz + 3mn^2 - (\rho_1^2\rho_2+\rho_1\rho_3^2+\rho_2^2\rho_3)$$
$$= -3^{2-2\tau} nyz - n3^{3-\tau} N(\theta_r) + 6mn^2.$$

If we define

$$E(x,y,z) = x^2y + zy^2 + z^2x,$$

then we have

$$E(\rho_1,\rho_2,\rho_3) = E(\rho_3,\rho_1,\rho_2) = E(\rho_2,\rho_3,\rho_1) = n(3^{3-\tau} N(\theta_r) - 3mn).$$

On the other hand, we have

$$E(\rho_1,\rho_3,\rho_2) = -3^{2-2\tau} nyz - n3^{3-\tau} N(\theta_r) + 6mn^2 \neq E(\rho_1,\rho_2,\rho_3)$$

and

$$E(\rho_1,\rho_3,\rho_2) = E(\rho_2,\rho_1,\rho_3) = E(\rho_3,\rho_2,\rho_1).$$

Let ρ,ρ',ρ'' be the roots of (8.3.15). If $E(\rho,\rho',\rho'') = n(3^{3-\tau} N(\theta_r) - 3mn)$, then

$$3^{\tau} | mn\rho / \rho'' |, 3^{\tau} | mn\rho' / \rho |, 3^{\tau} | mn\rho'' / \rho' |$$

are principal factors of S^2. Further, by the conditions of Lemma 8.3.1, the least of these must be $| (mn\rho_1) / \rho_3 | = st^2$. If $E(\rho,\rho',\rho'') \neq n(3^{3-\tau} N(\theta_r) - 3mn)$, then we replace ρ' by ρ'' and ρ'' by ρ'. This is because if $E(\rho,\rho',\rho'') \neq n(3^{3-\tau} N(\theta_r) - 3mn)$, then

$$E(\rho,\rho'',\rho') = n(3^{3-\tau}N(\theta_r)-3mn).$$

Also, in the case where $E(\rho,\rho'',\rho') = n(3^{3-\tau}N(\theta_r)-3mn)$ we have

$$|\, mn\rho / \rho'' \,| = |\, mn\rho_1 / \rho_3 \,| \text{ or } |\, mn\rho_2 / \rho_1 \,| \text{ or } |\, mn\rho_3 / \rho_2 \,|.$$

Again, the least of these is $|\, mn\rho_1 / \rho_3 \,|$.

If ρ, ρ', ρ'' are the roots of (8.3.15) and ρ, ρ', $\rho'' \in \mathbf{Z}$, it is a simple matter to use Newon's method to find one of them, say ρ. When ρ is determined, we then have to find the other two zeros ρ' and ρ'' subject to

$$E(\rho,\rho',\rho'') = n(3^{3-\tau}N(\theta_r)-3mn)).$$

If this does hold, since $E(\rho,\rho',\rho'') \neq E(\rho,\rho'',\rho')$, we get

$$\begin{aligned} g &= (\rho - \rho')(\rho' - \rho'')(\rho'' - \rho) = E(\rho,\rho'',\rho') - E(\rho,\rho',\rho'') \\ &= 9(mn^2 - 3^{-2\tau}nyz - 2(3^{-\tau})N(\theta_r)). \end{aligned}$$

Now,

$$\rho' - \rho'' = (\rho'^2 - \rho'(\rho + \rho'') + \rho\rho'')(\rho''^2 - \rho''(\rho + \rho') + \rho\rho') / g.$$

By (8.3.14), we can deduce that

$$\rho'^2 - \rho'(\rho + \rho'') + \rho\rho'' = 3\rho'^2 - 2(3^{1-\tau})\rho'z - 3^{1-\tau}yn$$

and

$$\rho''^2 - \rho''(\rho + \rho') + \rho\rho' = 3\rho''^2 - 2(3^{1-\tau})\rho''z - 3^{1-\tau}yn.$$

This means that

$$\begin{aligned} \rho'-\rho'' = {} & (9(\rho'^2\rho''^2 - 2(3^{-\tau})z(\rho'^2\rho''+\rho'\rho''^2) - 3^{-\tau}yn(\rho'^2+\rho''^2) \\ & + 4(3^{-2\tau})\rho'\rho''z^2 + 2(3^{-2\tau})nyz(\rho'+\rho'') + 3^{-2\tau}y^2n^2)) / g. \end{aligned}$$

By using the fact that

$$\rho' + \rho'' = 3^{1-\tau}z - \rho$$

and

$$\rho'\rho'' = -n3^{1-\tau}y - \rho(3^{1-\tau}z - \rho),$$

we find that

$$\begin{aligned} \rho'-\rho'' = w = {} & (3^{-\tau})mn^2z + 3(3^{-3\tau})nyz^2 + 4(3^{-2\tau})n^2y^2 \\ & +(6(3^{-3\tau})z^3+7(3^{-2\tau})nyz-mn^2)\rho-(2(3^{-2\tau})z^2+2(3^{-\tau})ny)\rho'. \end{aligned}$$

Since

$$\rho' = (\rho' + \rho'' + \rho' - \rho'') / 2,$$

we get

(8.3.17) $$\rho' = ((3^{1-\tau}z - \rho) + w) / 2.$$

Also, we have

(8.3.18) $$\rho'' = 3^{1-\tau}z - \rho - \rho'.$$

Once ρ, ρ', ρ'' are known, the least of $|\rho / \rho''|$, $|\rho' / \rho|$, $|\rho'' / \rho'|$ gives us $|\rho_1 / \rho_3|$ as noted above. We proceed to find ρ_2. With the values of ρ_1, ρ_2 and ρ_3, we use (8.3.16) to find the values for X_1, X_2, and X_3. We verify our solution with (8.3.2). Here is a detailed description of the algorithm for $\tau < 2$.

Algorithm 8.3.2. Given: θ_r, $\lambda_r = (x + y\delta + z\bar{\delta}) / 3$ and $x = 3N(\theta_r) - 3^{\tau}mn$.

1) Use Newton's method to find a root, ρ, of (8.3.15).
2) Use (8.3.17) and (8.3.18) to find ρ' and ρ''.
3) $|\rho_1 / \rho_3| \leftarrow \min\{|\rho / \rho''|, |\rho' / \rho|, |\rho'' / \rho'|\}$. The remaining root is ρ_2.
4) Use (8.3.16) to find X_1, X_2, and X_3.
5) If (8.3.2) holds, then $3^{\tau}| mn\rho_1 / \rho_3|$ is a principal factor for **F**; otherwise, (8.3.2) does not hold.
6) Stop.

§8.4 Construction of λ's.

Note that if $e = 1$, $\theta_r = \chi\gamma / 3$ and

$$\varepsilon_0^{\,k} = \gamma^3 / N(\gamma) = \theta_r^{\,3} / \lambda \qquad \text{for } \lambda \in \mathbf{O}_F,$$

it is important that we determine the upper and lower bounds for θ_r in order for us to find λ. Since $\theta_r^{\,3} = \gamma^3\chi^3 / 27$ and $0 < \chi < 3$, we get

$$\theta_r^{\,3} < \gamma^3.$$

But, as $\varepsilon_0^{\,k} = \gamma^3 / N(\gamma)$, it follows that

$$\theta_r^3 < N(\gamma)\varepsilon_0^k.$$

By Lemma 8.3.1 we have

$$\theta_r^3 < N(\gamma)\varepsilon_0^k < 9mn\varepsilon_0^k$$

and

$$3\delta_r < kR + \log(9mn).$$

Also, since

$$\theta'_r = \gamma'\chi' / 3,$$

we have

$$|\theta'_r|^2 = |\gamma'|^2|\chi'|^2 / 9.$$

But $|\theta'_r|^2 = N(\theta_r) / \theta_r$ (because $|\theta'_r|^2 = \theta'_r\theta''_r$) and $|\gamma'|^2 = N(\gamma) / \gamma$; hence, we have

$$N(\theta_r) / \theta_r < N(\gamma) / \gamma$$

or

$$\theta_r > N(\theta_r)\gamma / N(\gamma).$$

It follows that

$$\theta_r^3 > N(\theta_r)^3\varepsilon_0^k / N(\gamma)^2$$

and

$$3\delta_r > kR + 3\log N(\theta_r) - 2\log(9mn) > kR - 2\log(9mn).$$

Thus,

(8.4.1) $$(kR - 2\log(9mn))/ 3 < \delta_r < (kR + \log(9mn)) / 3.$$

Since

$$\delta_r > ((r-1) / 4)\log 2$$

(see [Wil86]) (empirical evidence suggests that $\delta_r \approx 1.12r$), there are only $\mathbf{O}(\log(mn))$ values of δ_r to check if kR is known.

Hence, for each θ_r which satisfies (8.4.1), we need to find the corresponding λ_r such that

$$\varepsilon_0^k = \theta_r^3 / \lambda_r.$$

We first note that

$$\lambda_{r+1} = (\theta_g^{(r)})^3\lambda_r.$$

If λ_r is known, then all the subsequent $\lambda_{r+1}, \lambda_{r+2}, \lambda_{r+3}, \cdots$can be found by using $\theta_g^{(r)}$, $\theta_g^{(r+1)}$, $\theta_g^{(r+2)}$, ···. Thus, our main objective is to find an initial λ_r .

By §6.3 we know that, for any r, there exists a reduced ideal $\mathbf{i}_u$ such that $\mathbf{i}_u = \mathbf{i}_r$, $1 \le u \le p$, $\delta_u = \delta_r - jR$, and $0 < \delta_u < R$. In fact, if

$$N(\theta_r)^3\varepsilon_0^k / N(\gamma)^2 < \theta_r^3 < N(\gamma)\varepsilon_0^k < 9mn\varepsilon_0^k,$$

we have

$$N(\theta_u)^3\varepsilon_0^i / N(\gamma)^2 < \theta_u^3 < N(\gamma)\varepsilon_0^i < 9mn\varepsilon_0^i,$$

where i = k mod 3 and can only be 1 or 2. If $k \equiv 2 \pmod 3$, we can replace k by 2k and therefore we may assume without loss of generality that $k \equiv 1 \pmod 3$. Hence, we may assume that

(8.4.2) $$N(\theta_u)^3\varepsilon_0 / (9mn)^2 < \theta_u^3 < N(\gamma)\varepsilon_0 < 9mn\varepsilon_0.$$

Suppose we have any u and $\mathbf{i}_u$.We can use the technique given in §8.2 to compute $\mathbf{i}_u'$, and then use our reduction algorithm to find ϕ_s (< 1) such that

(8.4.3) $$(\phi_s L(\mathbf{i}_u'))\mathbf{i}_s = (L(\mathbf{i}_s))\mathbf{i}_u'$$

and $\mathbf{i}_s$ is reduced. Here, we know that $\delta_s \approx R - \delta_u$ by Theorem 8.2.1. We next compute

(8.4.4) $$\mathbf{i}_s^2 = (v)\mathbf{a}_1 \qquad (v \in \mathbf{Z}).$$

We now use our reduction algorithm again to find $\mathbf{a}_v$ and γ_v such that

(8.4.5) $$(\gamma_v L(\mathbf{a}_1))\mathbf{a}_v = (L(\mathbf{a}_v))\mathbf{a}_1$$

and $\mathbf{a}_v$ is reduced. By using (8.4.4) and (8.4.5) we get

(8.4.6) $$(v\gamma_v L(\mathbf{a}_1))\mathbf{a}_v = (L(\mathbf{a}_v))\mathbf{i}_s^2.$$

On the other hand, by squaring both sides of (8.4.3) we get

$$(\phi_s^2 L(\mathbf{i}_u')^2)\mathbf{i}_s^2 = (L(\mathbf{i}_s)^2)\mathbf{i}_u'^2.$$

By using (8.4.6) to replace $\mathbf{i}_s^2$, we have

$$(v\gamma_v L(\mathbf{a}_1)\phi_s^2 L(\mathbf{i}_u')^2)\mathbf{a}_v = (L(\mathbf{a}_v)L(\mathbf{i}_s)^2)\mathbf{i}_u'^2.$$

It follows that

$$\left(\frac{v\gamma_v L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}\right)a_v = (L(a_v))i_u'^2.$$

Initially, since $L(i_s)^2 > vL(a_1)$ by Lemma 8.8.1, we know that

$$\left(\frac{v\gamma_v L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}\right) \leq L(i_u)^2.$$

We now continue to increase the value of v and γ_v until we have

$$\left(\frac{v\gamma_v L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}\right) \leq L(i_u)^2$$

and

$$\left(\frac{v\gamma_{v+1} L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}\right) > L(i_u)^2.$$

In that case, we have

$$\left(\frac{v\gamma_{v+1} L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}\right) > \frac{L(i_u)^2}{\theta_g(j)} > \frac{L(i_u)^2}{6mn}$$

by Lemma 8.2.2. Hence we now have

$$\frac{L(i_u)^2}{6mn} < \frac{v\gamma_v L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2} \leq L(i_u)^2. \tag{8.4.7}$$

Since $i_s \sim (1)$ and a_v is reduced and principal, we have $a_v = i_t$. Put

$$\omega = \frac{v\gamma_v L(a_1)\phi_s{}^2 L(i_u)^2}{L(i_s)^2}. \tag{8.4.8}$$

Since $(\omega)\, i_t = (L(i_t))\, i_u{}^2 = (L(i_t)\theta_u{}^2)$, we get

$$(\omega L(i_t)) = (L(i_t)\theta_t\theta_u{}^2).$$

It follows that

$$\theta_t\theta_u{}^2 = \varepsilon_0{}^j\omega, \tag{8.4.9}$$

where $j \in \mathbf{Z}$. Although j could be any integer, the following theorem allows us to restrict the possible values of j in the case when the fundamental unit is not exceptionally small.

Theorem 8.4.1. Suppose that $\theta_t\theta_u{}^2 = \varepsilon_0{}^j\omega$ and $\theta_u < (9mn\varepsilon_0)^{1/3}$. If $\varepsilon_0 > (9mn)^5$, then $j = 1$.

Proof. Since

$$\theta_u{}^2 > N(\theta_u)^2 = N(i_u')^2 \geq L(i_u')^2 = L(i_u)^2 \geq \omega,$$

we have $\theta_u{}^2 / \omega > 1$. Thus, $j > 0$.

Suppose that $j \geq 2$. We first note that

$$\varepsilon_0^j < \frac{\theta_u^2 \varepsilon_0}{\omega}.$$

Hence, we get

$$\varepsilon_0 \leq \varepsilon_0^{j-1} < \frac{\theta_u^2}{\omega} < \frac{(6mn)\theta_u^2}{L(i_u)^2} < 6mn(9mn\varepsilon_0)^{2/3}.$$

It follows that

$$\varepsilon_0 < (6mn)^3(9mn)^2.$$

Consequently, if $\varepsilon_0 > (9mn)^5$, then $j = 1$. ■

We can use the method we are about to describe here to find λ_r, if $\varepsilon_0 > (9mn)^5$. In the case where $\varepsilon_0 < (9mn)^5$, the determination of λ_r can be done by a direct search method because there is a limited number of reduced ideals in the principal ideal class. Here, we are especially interested in those pure cubic fields which do not have small regulators. We have

$$\theta_t \theta_u^2 = \varepsilon_0 \omega.$$

If $\rho = \theta_t / \theta_u$, then

$$\rho \theta_u^3 = \varepsilon_0 \omega.$$

Put

$$\lambda_r = \omega / \rho,$$

and we have

$$\theta_u^3 / \lambda_r = \varepsilon_0.$$

Since (see [WDS83] p.242) we know that $L(i_v) \leq 3mn$ and that $L(i_v) \mid N(\theta_v)$ for any reduced i_v and in our case $\varepsilon_0 > (9mn)^2$, we know that we can find θ_u and i_u such that

$$\theta_u^3 < L(i_u)^2 \varepsilon_0 / (9mn)^2 < N(\theta_u)^3 \varepsilon_0 / (9mn)^2,$$

$$\theta_{u+1}^3 > L(i_{u+1})^2 \varepsilon_0 / (9mn)^2.$$

For this i_u we have the following

Theorem 8.4.2. For the selection of i_u above, we have

$$1 < \rho < (9mn)^7.$$

Proof. Since $\rho = \omega \varepsilon_0 / \theta_u^3$, we get

$$\rho > (9mn)^2\omega\varepsilon_0 / (L(i_u)^2\varepsilon_0) > ((9mn)^2 / L(i_u)^2)(L(i_u)^2 / 6mn) > 1.$$

Also,

$$\begin{aligned}\rho = \omega\varepsilon_0 / \theta_u{}^3 &< \omega(9mn)^2\theta_g{}^{(u)3} / L(\mathbf{i}_{u+1})^2 \\ &< L(i_u)^2(9mn)^2(6mn)^3 \quad \text{(by Lemma 8.2.2 \& (8.4.7))} \\ &< (3mn)^2(9mn)^2(6mn)^3 < (9mn)^7. \ \blacksquare\end{aligned}$$

Before we leave this section, it is important to describe the technique that was used in the computation of λ_r , where $\lambda_r = (x + y\delta + z\bar{\delta}) / 3$. In the process of finding λ_r, the coefficients can get fairly large. Thus, in order to eliminate the precision problem, we elected to compute λ_r modulo p where p is a large prime. The main difficulty in computing λ_r is to calculate γ_v, ϕ_s and ρ. To solve this problem, we applied a method of Williams as given in §5 of [Wil82].

We note that

$$(\gamma_v L(\mathbf{a}_1))\mathbf{a}_v = (L(\mathbf{a}_v))\mathbf{a}_1,$$

where $\mathbf{a}_1$ is not reduced and $\mathbf{a}_v$ is reduced. In using the reduction algorithm of Voronoi to reduce $\mathbf{a}_1$, a sequence of ideals $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, , \cdots, \mathbf{a}_v$ is found. For each ideal $\mathbf{a}_i$, Voronoi's algorithm generates the integers σ_i, $M_1{}^{(i)}$, $M_2{}^{(i)}$, $M_3{}^{(i)}$, $N_1{}^{(i)}$, $N_2{}^{(i)}$, $N_3{}^{(i)}$. If we put

$$\gamma_g{}^{(i)} = (M_1{}^{(i)} + M_2{}^{(i)}\delta + M_3{}^{(i)}\delta^2) / \sigma_i,$$

$$\gamma_h{}^{(i)} = (N_1{}^{(i)} + N_2{}^{(i)}\delta + N_3{}^{(i)}\delta^2) / \sigma_i \ ,$$

then the module $\mathbf{Z} + \gamma_g{}^{(i)}\mathbf{Z} + \gamma_h{}^{(i)}\mathbf{Z}$ is the fractional ideal $(1 / L(\mathbf{a}_i))\mathbf{a}_i$. Thus, if we define

$$\gamma_1 = 1, \quad \gamma_j = \prod_{i=1}^{j-1} \gamma_g{}^{(i)},$$

$$\gamma_{j+1} = \gamma_g{}^{(j)}\gamma_j, \ \ \zeta_{j+1} = \gamma_h{}^{(j)}\gamma_j,$$

then $\{\gamma_{k-1}, \gamma_k, \zeta_k\}$ is a basis of $(1 / L(\mathbf{a}_1))\mathbf{a}_1$. It follows that there exist rational integers $x_1{}^{(k)}$, $y_1{}^{(k)}$, $z_1{}^{(k)}$, $x_2{}^{(k)}$, $y_2{}^{(k)}$, $z_2{}^{(k)}$ such that

$$\gamma_{k+1} = x_1{}^{(k)}\gamma_k + y_1{}^{(k)}\gamma_{k-1} + z_1{}^{(k)}\zeta_k,$$

$$\zeta_{k+1} = x_2{}^{(k)}\gamma_k + y_2{}^{(k)}\gamma_{k-1} + z_2{}^{(k)}\zeta_k.$$

Thus, if we put

$$\gamma_k = (G_1^{(k)} + G_2^{(k)}\delta + G_3^{(k)}\delta^2) / \sigma_1,$$

$$\zeta_k = (H_1^{(k)} + H_2^{(k)}\delta + H_3^{(k)}\delta^2) / \sigma_1,$$

we get

$$G_i^{(k+1)} = x_1^{(k)}G_i^{(k)} + y_1^{(k)}G_i^{(k-1)} + z_1^{(k)}H_i^{(k)},$$

(8.4.10) $$H_i^{(k+1)} = x_2^{(k)}G_i^{(k)} + y_2^{(k)}G_i^{(k-1)} + z_2^{(k)}H_i^{(k)} \quad (i = 1,2,3)$$

Also, $G_1^{(1)} = \sigma_1$, $G_2^{(1)} = 0$, $G_3^{(1)} = 0$, $G_1^{(2)} = M_1^{(1)}$, $G_2^{(2)} = M_2^{(1)}$, $G_3^{(2)} = M_3^{(1)}$, $H_1^{(2)} = N_1^{(1)}$, $H_2^{(2)} = N_2^{(1)}$, $H_3^{(2)} = N_3^{(1)}$.

If we start with k = 1 in (8.4.10), we can use (8.4.10) as a pair of congruences modulo p to find γ_v (mod p). However, we do need to show how to find $x_i^{(k)}$, $y_i^{(k)}$, $z_i^{(k)}$, k = 1,2. Let $M_1^{*(k)}$, $M_2^{*(k)}$, $M_3^{*(k)}$, $N_1^{*(k)}$, $N_2^{*(k)}$, $N_3^{*(k)}$ be defined by

$$1 / \gamma_g^{(k-1)} = (M_1^{*(k)} + M_2^{*(k)}\delta + M_3^{*(k)}\delta^2) / \sigma_k,$$

$$\gamma_h^{(k-1)} / \gamma_g^{(k-1)} = (N_1^{*(k)} + N_2^{*(k)}\delta + N_3^{*(k)}\delta^2) / \sigma_k.$$

Again, by using the method of [Wil83], we have

$$E_k^* x_1^{(k)} = M_2^{(k)}N_3^{*(k)} - M_3^{(k)}N_2^{*(k)}, \qquad E_k^* x_2^{(k)} = N_2^{(k)}N_3^{*(k)} - N_3^{(k)}N_2^{*(k)},$$

$$E_k^* z_1^{(k)} = M_3^{(k)}M_2^{*(k)} - M_2^{(k)}M_3^{*(k)}, \qquad E_k^* z_2^{(k)} = N_3^{(k)}M_2^{*(k)} - N_2^{(k)}M_3^{*(k)},$$

$$\sigma_k x_1^{(k)} = M_1^{(k)} - y_1^{(k)}M_1^{*(k)} - z_1^{(k)}N_1^{*(k)}, \qquad \sigma_k x_2^{(k)} = N_1^{(k)} - y_2^{(k)}N_1^{*(k)} - z_2^{(k)}N_1^{*(k)},$$

where $E_k^* = M_2^{*(k)}N_3^{*(k)} - M_3^{*(k)}N_2^{*(k)}$.

Similiarly, we can apply the above technique to find ϕ_s and ρ. If γ_v, ϕ_s and ρ (mod p) are known, we can easily compute λ_r modulo p. Hence, we can determine X_r, Y_r, Z_r, $W_r \in \mathbf{Z}/p\mathbf{Z}$ such that

$$\lambda_r \text{ modulo } p = (X_r + Y_r\delta + Z_r\delta^2) / W_r.$$

Once we find the initial λ_r modulo p, we can use

$$\lambda_{r+1} = (\theta_g^{(r)})^3\lambda_r \text{ modulo } p$$

to compute the subsequent λ_{r+1}, λ_{r+2}, λ_{r+3}, $\cdots$ modulo p. If principal factors exist for **F** and **F** is an exotic field, then one of the above λ's satisfies (8.3.2). In that case we convert $(X_r + Y_r\delta + Z_r\delta^2) / W_r$ to $(x + y\delta + z\bar{\delta}) / 3$ by finding W_r^{-1} (mod p). From §8.3 it is known

that $|x|, |y|, |z| < 27mn$. Thus, if $p > 54mn$, then the coefficients x, y and z can be computed exactly. We further illustrate the above idea for constructing λ_r by

Algorithm 8.4.1. (Given that kR, p is a prime and $p > 54mn$.)

1) Use the method discussed in §6.3 to find h^*R where $h^* \in \mathbf{Z}$. If $3 \mid h^*$, we will have a reduced principal ideal $\mathbf{i}_q$ such that $\delta(\mathbf{i}_q,\mathbf{i}_1) = h^*R / 3$ and $\mathbf{i}_q = \mathbf{i}_1$. In this case, replace h^* by $h^* / 3$ and repeat until we find that $3 \nmid h^*$. Put $k = h^*$ and we have kR.

2) Find a reduced ideal $\mathbf{i}_r$ such that $3\delta_r < 3\log(L(\mathbf{i}_r)) + kR - 2\log(9mn)$ and $3\delta_{r+1} > 3\log(L(\mathbf{i}_r)) + kR - 2\log(9mn)$. Now, we have $\mathbf{i}_u = \mathbf{i}_r$.

3) Use the method presented in §8.2 to Compute $\mathbf{i}_u'$.

4) Use the reduction algorithm to find $\mathbf{i}_s$ such that $(\phi_s L(\mathbf{i}_u'))\mathbf{i}_s = (L(\mathbf{i}_s))\mathbf{i}_u'$. In the process of finding $\mathbf{i}_s$, we also calculate $\log\phi_s$ and ϕ_s modulo p by using the method discussed above.

5) Compute f and $\mathbf{a}_1$ where $\mathbf{i}_s^2 = (f)\mathbf{a}_1$.

6) Use the reduction algorithm to find $\mathbf{a}_v$ such that $(\gamma_v L(\mathbf{a}_1))\mathbf{a}_v = (L(\mathbf{a}_v))\mathbf{a}_1$. In the process of finding $\mathbf{a}_v$, we also calculate $\log\gamma_v$ and γ_v modulo p by using the method discussed above.

7) Increase the value of v until

$$2\log L(\mathbf{i}_u) - \log(6mn) < \log(v\gamma_v L(\mathbf{a}_1)\phi_s^2 L(\mathbf{i}_u)^2) - 2\log L(\mathbf{i}_s) \le 2\log L(\mathbf{i}_u) \text{ holds.}$$

8) Use (8.4.8) to find ω modulo p.

9) Set $j \leftarrow 1$ and $\mathbf{b}_j \leftarrow \mathbf{i}_u$.

10) Use Voronoi's algorithm on $\mathbf{b}_j$ to find $\mathbf{b}_{j+1}$.

11) Use the technique above to compute θ_{j+1} modulo p where $\mathbf{b}_1 = (\theta_{j+1})\mathbf{b}_{j+1}$.

12) If $\mathbf{b}_{j+1} = \mathbf{a}_v$ then goto **step** 15.

13) $j \leftarrow j + 1$.

14) Goto **step** 10.

15) Find λ_r modulo p $(= (X_r + Y_r\delta + Z_r\delta^2)/W_r)$ where $\lambda_r = \omega / \theta_{j+1}$ modulo p.

16) Stop.

§8.5 The overall algorithm.

Since we have discussed all of the components of the algorithm for determining principal factors for **F**, we are now able to present the overall algorithm. For a given pure cubic field **F**, the following algorithm determines whether or not principal factors exist for **F**; in the former case, then this algorithm will also find the principal factors.

Algorithm 8.5.1.

Given: $Q(\sqrt[3]{c})$, p is a prime and $p > 54mn$.

1) Apply Algorithm 8.4.1 to find kR, λ_r modulo p (= $(X_r+Y_r\delta+Z_r\delta^2) / W_r$), $\theta_g^{(r)}$, i_r and δ_r.
2) Set count = 1.
3) Set i = r and dist = δ_r.
4) Use the formula presented in §8.3 to find $N(\theta_i)$
5) If $N(\theta_i) \mid S^2$, then $N(\theta_i)$ is a principal factor for **F**. Print the principal factor and goto **step** 20..
6) If $X_i \equiv W_iN(\theta_i) \pmod p$, then convert $(X_r + Y_r\delta + Z_r\delta^2) / W_r$ to $(x + y\delta + z\bar{\delta})/3$ by finding $W_r^{-1} \pmod p$, apply Algorithm 8.3.1 and goto **step** 9.
7) If $X_i \equiv W_i(N(\theta_i)-3^{\tau-1}mn) \pmod p$, then convert $(X_r + Y_r\delta + Z_r\delta^2) / W_r$ to $(x + y\delta + z\bar{\delta}) / 3$ by finding $W_r^{-1} \pmod p$, apply Algorithm 8.3.1 and goto **step** 9.
8) Goto **step** 10.
9) If a principal factor is found, then print that principal factor and goto **step** 20.
10) Compute $\lambda_{i+1}=(\theta_g^{(i)})^3\lambda_i \pmod p$ where $\lambda_{i+1} \bmod p=(X_{i+1}+Y_{i+1}\delta+Z_{i+1}\delta^2)/W_{i+1}$.
11) Apply the Voronoi algorithm on $\theta_g^{(i)}$ to find $\theta_g^{(i+1)}$.
12) Compute dist $\leftarrow$ dist + $\log\theta_g^{(i)}$.
13) Set i $\leftarrow$ i + 1.

14) If dist < (kR + log(9mn)) / 3, then goto **step** 4.

15) If count = 2, then goto **step** 19.

16) Set count ← count + 1, kR ← 2kR.

17) Apply Algorithm 8.4.1 (except **step** 1) to find λ_r modulo p
(= $(X_r+Y_r\delta+Z_r\delta^2) / W_r$), $\theta_g^{(r)}$, i_r and δ_r.

18) Goto **step** 3.

19) Print 'Principal factors don't exist for $Q(\sqrt[3]{c})$'.

20) Stop.

Before we leave this section, it is important to discuss the complexity of the above algorithm. In step 1 of Algorithm 8.4.1, it is known that the computation of kR is $\mathbf{O}(c^{2/5+\varepsilon})$ if the GRH for ζ_L holds. If we do not assume the GRH, there is an algorithm for finding R of $\mathbf{O}(R^{1/2}c^{\varepsilon})$ (see [BW88]). As for the remainder of Algorithm 8.4.1, it is known that all those operations involving ideals have a complexity of $\mathbf{O}(c^{\varepsilon})$. Thus, the complexity of Algorithm 8.4.1 is $\mathbf{O}(c^{2/5+\varepsilon})$ under the truth of GRH. We further point out that Algorithm 8.3.1 and Algorithm 8.3.2 have a complexity of $\mathbf{O}(c^{\varepsilon})$. Since there are only $\mathbf{O}(\log c)$ values of λ to check, we can conclude that Algorithm 8.5.1 has a complexity of $\mathbf{O}(c^{2/5+\varepsilon})$ if GRH holds. Also, Algorithm 8.5.1 has a complexity of $\mathbf{O}(c^{1/2})$ unconditionally.

§8.6 Determination of r*.

If e = 0, then r* can be either 1 or 3. In [Wil82], we have seen that the value of r* can be calculated by using the Voronoi algorithm. However, this method is very time consuming if ε_0 is large. In this section we describe a new theorem for determining r*. In order to develop our criterion for finding r*, we have to present the following results.

Denote by A/3 (mod mn), where $A \in \mathbf{Z}$, the value of A/3 (mod mn) when $3 \mid A$ or the value of $3^{-1}A$ (mod mn) when $3 \nmid mn$.

Lemma 8.6.1. If $\alpha = (a_1 + a_2\delta + a_3\bar{\delta}) / 3 \in \mathbf{O}_F$, $\beta = (b_1 + b_2\delta + b_3\bar{\delta}) / 3 \in \mathbf{O}_F$, $\gamma = \alpha\beta = (c_1 + c_2\delta + c_3\bar{\delta}) / 3 \in \mathbf{O}_F$, then

$$c_1/3 \equiv (a_1/3)\,(b_1/3) \pmod{mn}.$$

Proof. We know that

$$3c_1 = a_1b_1 + a_3b_2\delta\bar{\delta} + a_2b_3\delta\bar{\delta}.$$

If $3 \nmid mn$, then since $3c_1 \equiv a_1b_1 \pmod{mn}$, we get

$$c_1/3 \equiv (a_1/3)\,(b_1/3) \pmod{mn}.$$

If $3 \mid mn$, then $3 \mid \gcd(a_1, a_2, a_3)$ and $3 \mid \gcd(b_1, b_2, b_3)$. It follows that

$$3c_1 \equiv a_1b_1 \pmod{9mn}.$$

Thus, we have

$$c_1/3 \equiv (a_1/3)\,(b_1/3) \pmod{mn}. \quad \blacksquare$$

With this lemma we have the following

Theorem 8.6.1. Let $\varepsilon_0 = (g_1 + g_2\delta + g_3\bar{\delta}) / 3$ be the fundamental unit of **F**. If $3 \nmid k$ $(k \in \mathbf{Z})$ and

$$\eta = \varepsilon_0^{\,k} = (G_1 + G_2\delta + G_3\bar{\delta}) / 3,$$

then $g_1 \equiv 3 \pmod{mn}$ if and only if $G_1 \equiv 3 \pmod{mn}$.

Proof. By the previous lemma, we have

$$G_1/3 \equiv (g_1/3)^k \pmod{mn}.$$

Also, since $N(\varepsilon_0) = 1$, we have

$$g_1^{\,3} + g_2^{\,3}\delta^3 + g_3^{\,3}\bar{\delta}^3 - 3\delta\bar{\delta}g_1g_2g_3 = 27.$$

Hence, we have

$$(g_1/3)^3 \equiv 1 \pmod{mn}.$$

Consequently, we have

$$G_1/3 \equiv (g_1/3) \pmod{mn} \text{ or } G_1/3 \equiv (g_1/3)^2 \pmod{mn}.$$

If $G_1/3 \equiv (g_1/3) \pmod{mn}$, then

$$G_1 \equiv g_1 \pmod{mn}.$$

If $G_1/3 \equiv (g_1/3)^2 \pmod{mn}$, then

$$(G_1/3)(g_1/3) \equiv 1 \pmod{mn}.$$

Hence, we have

$$G_1 g_1 \equiv 9 \pmod{mn}.$$

It follows that $g_1 \equiv 3 \pmod{mn}$ if and only if $G_1 \equiv 3 \pmod{mn}$. ■

We know that $r^* = 3$ if and only if $g_1 \equiv 3 \pmod{mn}$. Consequently, it is important to have a criterion for determining whether or not $g_1 \equiv 3 \pmod{mn}$. We can determine that by using

Theorem 8.6.2. Let $\varepsilon_0^k = \theta^3 / \lambda$, where $\theta, \lambda \in \mathbf{O}_F$, $\lambda = (x + y\delta + z\bar{\delta}) / 3$, $k \in \mathbf{Z}$, $3 \nmid k$. If $\gcd(N(\theta),mn) = 1$, then we have $g_1 \equiv 3 \pmod{mn}$ if and only if $x \equiv 3N(\theta) \pmod{mn}$.

Proof. Let $\varepsilon_0^k = (G_1 + G_2\delta + G_3\bar{\delta}) / 3$, $\theta = (t_1 + t_2\delta + t_3\bar{\delta}) / 3$. We get

$$27N(\theta) = t_1^3 + t_2^3\delta^3 + t_3^3\bar{\delta}^3 - 3\delta\bar{\delta}t_1t_2t_3.$$

Thus, we have

$$(t_1/3)^3 \equiv N(\theta) \pmod{mn}.$$

Also, $\lambda\varepsilon_0^k = \theta^3$, and we obtain

$$(t_1/3)^3 \equiv (G_1/3)(x/3) \pmod{mn}.$$

Hence,

$$N(\theta) \equiv (G_1/3)(x/3) \pmod{mn}. \tag{8.6.1}$$

Here we divide our proof into two cases; when $3 \nmid mn$ and when $3 \mid mn$.We first consider the case of $3 \nmid mn$. In this case, if $x \equiv 3N(\theta) \pmod{mn}$, then $x/3 \equiv N(\theta) \pmod{mn}$. By (8.6.1) we get $G_1 \equiv 3 \pmod{mn}$. Thus, we have

$$g_1 \equiv 3 \pmod{mn},$$

by Theorem 8.6.1. On the other hand, if $g_1 \equiv 3 \pmod{mn}$, then $G_1/3 \equiv 1 \pmod{mn}$. Thus, we can easily deduce that

$$x \equiv 3N(\theta) \pmod{mn}.$$

In the case where $3 \mid mn$, if we have $x \equiv 3N(\theta) \pmod{mn}$, then

$$x/3 \equiv N(\theta) \pmod{(mn/3)}.$$

By (8.6.1) we get

$$N(\theta) \equiv N(\theta)(G_1/3) \pmod{(mn/3)}.$$

This means that

$$G_1/3 \equiv 1 \pmod{(mn/3)}.$$

It follows that

$$g_1 \equiv 3 \pmod{mn}.$$

On the other hand, if $g_1 \equiv 3 \pmod{mn}$, then $G_1 \equiv 3 \pmod{mn}$. Hence, we get $G_1/3 \equiv 1 \pmod{(mn/3)}$ which implies that

$$x/3 \equiv N(\theta) \pmod{(mn/3)}.$$

Thus, we have $x \equiv 3N(\theta) \pmod{mn}$. ■

Lemma 8.6.2. Let $\theta \in \mathbf{O}_F$. If $p \mid mn$ and $p^\alpha \parallel N(\theta)$, then $\mathfrak{p}^\alpha \mid (\theta)$, where $(p) = \mathfrak{p}^3$.

Proof. Let $\gamma = \theta'\theta'' \in \mathbf{O}_F$; we have

$$\mathfrak{p}^{3\alpha} \mid (\theta)(\gamma).$$

If $\mathfrak{p}^\beta \parallel (\theta)$, where $\beta < \alpha$, then $\mathfrak{p}^{3\alpha-\beta} \mid (\gamma)$. It follows that $N(\mathfrak{p})^{3\alpha-\beta} \mid N(\gamma)$. Since $N(\mathfrak{p}) = p$, we get $p^{3\alpha-\beta} \mid N(\theta)^2$. Since $\beta < \alpha$, we have $3\alpha-\beta > 2\alpha$ and $3\alpha - \beta \geq 2\alpha + 1$. Thus, we have $p^{2\alpha+1} \mid N(\theta)^2$ and $p^{\alpha+1} \mid N(\theta)$, a contradiction. ■

Corollary 8.6.2. If θ is a minimum of $\mathbf{O}_F$, then $p^3 \nmid N(\theta)$ if $p \mid mn$.

Proof. In this case we have $\mathfrak{p}^3 \mid (\theta)$. Hence, we have $\theta = p\gamma$, where $\gamma \in \mathbf{O}_F$.It follows that θ cannot be a minimum. ■

By using the above results, we have the following theorem for determining whether or not $g_1 \equiv 3 \pmod{mn}$.

Theorem 8.6.3. Let $\varepsilon_0^k = \theta^3 / \lambda$, where $\theta, \lambda \in \mathbf{O}_F$, $3 \nmid k$, $\lambda = (x + y\delta + z\tilde{\delta}) / 3$. We have

$$g_1 \equiv 3 \pmod{mn}$$

if and only if

$$x/f \equiv 3N(\theta)/f \pmod{(mn / 3^i)}$$

where $3^i \parallel mn$, $f = \gcd(N(\theta), m^2n^2)$.

Proof. Since

$$\lambda\varepsilon_0^{\,k} = \theta^3,$$

we get

$$t_1^{\,3} + t_2^{\,3}\delta^3 + t_3^{\,3}\bar{\delta}^3 + 6\delta\bar{\delta}t_1t_2t_3 = 3(xG_1 + G_2z\delta\bar{\delta} + G_3y\delta\bar{\delta}) \tag{8.6.1}$$

where $\theta = (t_1 + t_2\delta + t_3\bar{\delta}) / 3$. Also,

$$27N(\theta) = t_1^{\,3} + t_2^{\,3}\delta^3 + t_3^{\,3}\bar{\delta}^3 - 3\delta\bar{\delta}t_1t_2t_3.$$

Further, if $p \mid mn$ and $p \mid N(\theta)$, we have $p^j \parallel N(\theta)$ for $j = 1$ or 2 by Corollary 8.6.2. Now $p^j \parallel f$ and $\gcd(N(\theta)/f\,,\, mn) = 1$. Since $p^j \mid (\theta)$ and $p^{3j} \mid (\lambda)$, we have $\lambda = p^j\mu$; hence, $\lambda = f\nu$. Putting $\nu = (r_1 + r_2\delta + r_3\bar{\delta}) / 3$, we get $x = fr_1$, $y = fr_2$, $z = fr_3$. Now if $p^j \mid N(\theta)$, then $p \mid t_1$. Further, if $j = 2$, then $p \mid t_2t_3$. Thus, $f \mid t_1t_2t_3$ and

$$t_1^{\,3} + t_2^{\,3}\delta^3 + t_3^{\,3}\bar{\delta}^3 \equiv 27N(\theta) \pmod{3fmn}.$$

By (8.6.1) we have

$$27N(\theta) \equiv 3xG_1 \pmod{3fmn}.$$

It follows that

$$9(N(\theta)/f) \equiv (x/f)G_1 \pmod{mn}.$$

Since m and n are square-free numbers, we have either $3 \nmid mn$ or $3 \parallel mn$. We first consider the case where $3 \nmid mn$. If $g_1 \equiv 3 \pmod{mn}$, then we have $G_1 \equiv 3 \pmod{mn}$ by Theorem 8.6.1. Consequently, we get

$$x/f \equiv 3(N(\theta)/f) \pmod{mn}.$$

On the other hand, if $x/f \equiv 3(N(\theta)/f) \pmod{mn}$, we get

$$9(N(\theta)/f) \equiv 3(N(\theta)/f)G_1 \pmod{mn}.$$

Thus, $3 \equiv G_1 \pmod{mn}$ and $g_1 \equiv 3 \pmod{mn}$.

We now consider the case where $3 \mid mn$. In this case we have

$$3(N(\theta)/f) \equiv (x/f)(G_1/3) \pmod{(mn/3)}$$

Here, $g_1 \equiv 3 \pmod{mn}$ implies that $G_1/3 \equiv 1 \pmod{(mn/3)}$. Hence,

$$x/f \equiv 3(N(\theta)/f) \pmod{(mn/3)}.$$

On the other hand, if $(x/f) \equiv 3(N(\theta)/f) \pmod{(mn/3)}$, we get

$$3(N(\theta)/f) \equiv 3(N(\theta)/f)(G_1/3) \pmod{(mn/3)}.$$

This means that $G_1/3 \equiv 1 \pmod{(mn/3)}$. Hence, we have $g_1 \equiv 3 \pmod{mn}$. ■

Hence, we can use the above theorem to determine r*. However, the amount of precision required to compute x can get quite large. In order to reduce the amount of precision we can use the following technique to find r*.

We note that

$$\theta_u^3 / \lambda = \varepsilon_0^k$$

where $\theta_u, \lambda \in \mathbf{O}_F$, $\lambda = (x + y\delta + z\bar{\delta}) / 3$, $k \in \mathbf{Z}$, $3 \nmid k$. If $\theta_u^3 \approx \varepsilon_0^k$, then λ should be small. Thus, we select θ_u such that

$$\theta_u^3 > \varepsilon_0^k$$

and

$$\theta_{u-1}^3 < \varepsilon_0^k.$$

Consequently, $\lambda > 1$. Since $\theta_u = \theta_g^{(u-1)}\theta_{u-1}$, we have

$$\lambda < (\theta_g^{(u-1)})^3.$$

It follows that

$$\lambda < (6mn)^3.$$

Since

$$N(\lambda) = \lambda|\lambda'|^2 = N(\theta_u)^3,$$

we get

$$|\lambda'| < N(\theta_u)^{3/2}.$$

From §8.3 we have deduced that $|x| \le \lambda + 2|\lambda'|$. Since $N(\theta_u) < 3mn$, we have

$$|x| < (7mn)^3.$$

We now select three distinct primes p_1, p_2, p_3 such that

$$p_1p_2p_3 > 8(7mn)^3$$

and $p_1, p_2, p_3 \approx 14mn$.By using these three primes, we find

$$x/f \equiv r_1 \pmod{p_1},$$

$$x/f \equiv r_2 \pmod{p_2},$$

$$x/f \equiv r_3 \pmod{p_3}.$$

Put $P = p_1p_2p_3$ and $P_i = P / p_i$ $(i = 1, 2, 3)$. By the Chinese Remainder Theorem, we know that if

$$\xi_i P_i \equiv 1 \pmod{p_i} \quad (i = 1, 2, 3),$$

then

$$x/f \equiv \sum_{i=1}^{3}(\xi_i P_i r_i) \pmod{P}.$$

Here, our objective is to find $x/f \pmod{mn}$. We note that $|x/f| < P/8$ and

$$x/f = \sum_{i=1}^{3}(\xi_i P_i r_i) - jP$$

where $j \in \mathbf{Z}$. Thus,

$$-P / 2 < 4x/f = \sum_{i=1}^{3}(4\xi_i r_i P_i) - 4jP < P / 2.$$

We define $4\xi_i r_i = k_i + p_i s_i$, where $0 \le k_i < p_i$. Note that $0 < s_i < 4p_i$. Hence, we can easily deduce that

$$\sum_{i=1}^{3}(4\xi_i r_i P_i) = \sum_{i=1}^{3}(P_i k_i) + P\sum_{i=1}^{3}s_i.$$

Thus, we get

$$-1 / 2 < \sum_{i=1}^{3}(P_i k_i)/P + \sum_{i=1}^{3}s_i - 4j < 1 / 2.$$

Since

$$0 < \sum_{i=1}^{3}(P_i k_i)/P < 3,$$

we have

$$-7/2 < -1/2 - \sum_{i=1}^{3}(P_i k_i)/P < \sum_{i=1}^{3}s_i - 4j < 1/2 - \sum_{i=1}^{3}(P_i k_i)/P < 1/2.$$

Hence, we obtain

$$0 < \left(\sum_{i=1}^{3}s_i + 7/2\right) / 4 - j < 1.$$

Thus,

$$j = \left[\left(2\sum_{i=1}^{3} s_i + 7\right)/8\right].$$

We can now compute j by using numbers which do not exceed 56mn. Once j is known, we can find x/f (mod mn) by computing

$$\sum_{i=1}^{3}(\xi_i P_i r_i) - jP \pmod{mn}.$$

§8.7. Computational Results.

Algorithm 8.5.1 was implemented in FORTRAN-H (extended) for an Amdahl 5870 computer. The extended feature is sufficient for c values which are less than $1.1\text{x}10^{12}$. We further note that this program is a modification of the program used in Chapter 6, along with some additional subroutines. A glance at Table 8.3.1 of §8.3 reveals that there seem to be very few M_0 fields; nevertheless, Mayer [May88] has conjectured that there exists an infinitude of such fields. In order to test this conjecture and our program we decided to search for M_0 fields for large values of c. To find such c values, we used a theorem of [May88].

Theorem 8.7.1. If $c = mn^2 \equiv \pm 2, \pm 4 \pmod 9$, $m > n$, $m \equiv -n \pmod 3$, and $\mathbf{Q}(\sqrt[3]{c})$ has a principal factor with norm $3n^2$, then $\mathbf{Q}(\sqrt[3]{c})$ is of type

$$M_2 \Leftrightarrow m > 8n,$$

$$M_1 \Leftrightarrow 8n > m > \alpha n,$$

$$M_0 \Leftrightarrow \alpha n > m$$

where $\alpha \approx 1.40080587$[3] and 1.40080587 is an approximation of a positive zero of the polynomial $x^4 + x^3 + x - 8^3 \in \mathbf{Z}[x]$ ■

To simplify matters, we elected to examine values of c ($\equiv \pm 2, \pm 4 \pmod 9$) for which m and n are the distinct primes p, q respectively. In this case the only possible principal factor sets are

$$S_1 = \{ 3q^2, 3pq, 3p^2, 9q, 9p^2q^2, 9p\}$$

$$S_2 = \{ 9q^2, 9pq, 9p^2, 3q, 3p^2q^2, 3p\}$$

$$S_3 = \{ q^2, pq, p^2, q, p^2q^2, p\}$$

$$S_4 = \{ 3, 3pq^2, 3p^2q, 9, 9p^2q, 9pq^2\}.$$

If $N(\alpha)$ is a principal factor for $\alpha \in \mathbf{O}_F$ then

$$\alpha = x + y\delta + z\bar{\delta}$$

and

$$x^3 + pq^2y^3 + p^2qz^3 - 3pqxyz = N(\alpha).$$

Thus, if $q \equiv 1 \pmod 3$ we must have $(N(\alpha)/q)_3 = 1$. We further restrict our c values by insisting that $p \equiv -1 \pmod 3$, $q \equiv 1 \pmod 3$, $(9p/q)_3 = 1$and $(3/q)_3 \neq 1$. It follows that since $(9p/q)_3 = 1$and $(3/q)_3 \neq 1$, we must have $(3p/q)_3 \neq 1$ and $(p/q)_3 \neq 1$; hence S_2, S_3, S_4 cannot be principal factor sets for these c values. It follows, then, that if we select a c value where $c = pq^2 \equiv \pm 2, \pm 4 \pmod 9$, p > q, p, q are primes, $p \equiv -1 \pmod 3$, $q \equiv 1 \pmod 3$, $(9p/q)_3 = 1$, $(3/q)_3 \neq 1$ and e = 1, then $3q^2$ is a principal factor for $\mathbf{Q}(\sqrt[3]{c})$. Furthermore, if $\alpha q > p$ and the above criteria hold, then by Theorem 8.7.1 $\mathbf{Q}(\sqrt[3]{c})$ is of type M_0.

We tested our program by finding all the c values where

$$c = pq^2 \equiv \pm 2, \pm 4 \pmod 9,\ 1\text{x}10^{12} < c < 1.01\text{x}10^{12},$$

$$\alpha q > p > q,\ p, q \text{ are primes},\ p \equiv -1 \pmod 3,$$

$$q \equiv 1 \pmod 3,\ (9p/q)_3 = 1,\ (3/q)_3 \neq 1.$$

There were 185 c values found. For each of these c values, we determined whether or not principal factors exist for $\mathbf{Q}(\sqrt[3]{c})$. Curiously, it turned out that e = 1 for every one of these c values. All 185 pure cubic fields were computed in about 3.5 CPU hours, in which over 3 CPU hours were spent on computing kR. In fact, if kR is known, then the average running time required for a c value, where $c \approx 1\text{x}10^{12}$, is approximately 6 CPU seconds. In Table 8.7.2 below, we give the first 18 c values (all the c values which lie between $1\text{x}10^{12}$ and $1.001\text{x}10^{12}$) and the corresponding principal factor found by our program.

c	m	n	principal factor
1000176144971	16691	7741	3^2x7741
1000178086007	14543	8293	3x8293^2
1000203058121	12329	9007	3^2x9007
1000267680551	10559	9733	3x9733^2
1000312204757	13397	8641	3x8641^2
1000331866217	14033	8443	3^2x8443
1000344830099	11171	9463	3^2x9463
1000399868177	10457	9781	3^2x9781
1000429179257	10193	9907	3x9907^2
1000564085237	14957	8179	3^2x8179
1000675948847	13127	8731	3x8731^2
1000733088683	16883	7699	3^2x7699
1000738466033	14657	8263	3x8263^2
1000740540089	12809	8839	3x8839^2
1000770294071	17231	7621	3^2x7621
1000794654569	14489	8311	3x8311^2
1000862291183	10247	9883	3^2x9883
1000882120313	11177	9463	3x9463^2

Table 8.7.2

As we were easily able to find 185 M_0 fields for large values of c, our results provide some numerical confirmation of Mayer's conjecture. It is remarkable that every field tested did have principal factors. If it could be proved that the Diophantine equation

$$x^3 + pq^2y^3 + p^2qz^3 - 3pqxyz = 9p$$

is always soluble when the primes p, q satisfy the conditions that $pq^2 \equiv \pm 2, \pm 4 \pmod 9$, $p \equiv -1 \pmod 3$, $q \equiv 1 \pmod 3$, $(9p/q)_3 = 1$, $(3/q)_3 \neq 1$, $\alpha q > p$, then Mayer's conjecture would gain even more confidence.

Chapter 9.
Conclusion

§9.1 Open Problems.

In the previous chapters, we discussed a number of computational algorithms for solving various problems in complex cubic fields. These problems include: the construction of all non-isomorphic complex cubic fields for a given bound on the absolute discriminant, the computation of the class number and class group structure of a complex cubic field, the determination of all non-isomorphic complex cubic fields for a given fundamental discriminant, the calculation of the regulator of a pure cubic field, the search for cubic polynomials of the form $x^3 - c$ which have a high density of prime values, and the computation of principal factors in a pure cubic field. In this chapter, we conclude our thesis by discussing a few unsolved problems that are related to it.

In Chapter 2, we discussed an algorithm for finding all non-isomorphic complex cubic fields for a given bound. As we mentioned earlier in Chapter 4, this algorithm is inefficient when the absolute value of the given bound is large. Furthermore, it is of some interest to continue the investigation of the Davenport and Heilbronn densities by extending the upper bound on the absolute discriminant. In order to do this, we need an efficient algorithm for counting the number of non-isomorphic complex cubic fields for a given bound on the absolute discriminant without actually finding the generating polynomial for each field. Although we do not have such a fast computational algorithm for solving this problem, it may be that the paper by Davenport and Heilbronn [DH71] could be used to shed some light on this problem.

In Chapters 4 and 5, we presented a computational version of the CUFFQI algorithm of Shanks. Unfortunately, this algorithm is restricted to discriminants which are fundamental. Hence, the next logical step would be to generalize the CUFFQI algorithm such that it can produce all the non-isomorphic complex cubic fields for any given discriminant. Although we do not know how to implement such an algorithm at this point,

it is possible that some of the ideas in [Ber31] could provide some techniques for solving this problem.

In Chapter 6, we gave a fast algorithm for computing the regulator of a pure cubic field. Since parallel processors are widely used at the moment, it would be of some interest to see if it is possible to implement a parallel algorithm for finding the regulator of a pure cubic field or indeed any complex cubic field. If such an algorithm exists and we have access to a parallel machine, then we should be able to find some pure cubic fields with large regulators.

Let c be a positive cube-free integer. In Chapter 7, we investigated cubic polynomials of the form $x^3 - c$ which have a high density of prime values. It would be of some interest to investigate more general polynomials like $x^3 + bx - c$.

The problems mentioned above represent only a sample of the many open problems related to this thesis. There is much more work yet to be done in the development of algorithms for solving problems arising in cubic number fields.

REFERENCES

[Ang73] I.O.Angell, "A table of complex cubic fields", Bull. London Math. Soc. **51**(1973),37-38.

[Ara81A] M.Arai, "On Voronoi's theory of cubic fields. I", Proc. Japan Acad. Ser. A Math. Sci. **57**(1981), 226-229.

[Ara81B] M.Arai, "On Voronoi's theory of cubic fields. II", Proc. Japan Acad. Ser. A Math. Sci. **57**(1981), 281-283.

[Arw29] A.Arwin, "On cubic fields", Ann. Math. **30**(1929), 1-11.

[Atk81] A.O.L.Atkin, "The computation of pure cubic units", Abstracts A.M.S. **2**(1981), 33.

[BC70] P.Barrucand and H.Cohn, "A rational genus, class divisibility, and unit theory for pure cubic fields", J. Number Theory **2**(1970), 7-21.

[BC71] P.Barrucand and H.Cohn, "Remarks on principal factors in a relative cubic field", J. Number Theory **3**(1971), 226-239.

[Ber13] W.E.H.Berwick, "The classification of ideal numbers that depend on a cubic irrationality",Proc. London Math. Soc. **12**(1913), 393-429.

[Ber25] W.E.H.Berwick, "On cubic fields with a given discriminant",Proc. London Math. Soc. **23**(1925), 359-378.

[Ber32] W.E.H.Berwick, "Algebraic number-fields with two independent units",Proc. London Math. Soc. **34**(1932), 360-378.

[Ber74] L.Bernstein, "Fundamental units from the preperiod of a generalized Jacobi-Perron algorithm", J. Reine Angew. Math. **268/269**(1974), 391-409.

[BH65] P.T.Bateman and R.A.Horn, "Primes represented by irreducible polynomials in one variable", Proc. Sympos. Pure Math. **8**(1965), 119-132.

[BKS77] H.Brunotte, J.Klingen and M.Steurich, "Einige Bemerkungen zu Einheiten in reinen kubischen Körpern", Arch. Math. **29**(1977), 154-157.

[Bil56] K.K.Billevich, "On the units of algebraic number fields of the third and fourth degrees", Mat. Sbornik **40**(1956), 123-136.

[BLW87] P.Barrucand, J.Loxton and H.C.Williams, "Some explicit upper bounds on the class number and regulator of a cubic field with negative discriminant", Pacific J. Math. **128**(1987), 209-222.

[BP89] J.Buchmann and A.Pethö, "On the computation of independent units by Dirichlet's method", Math. Comp. **52**(1989), 149-159.

[Bre81] A.Brentjes, "A two-dimensional continued fraction algorithm for best approximations with an application in cubic number fields", J. Reine Angew. Math. **326**(1981), 18-44.

[Buc82] J.Buchmann, Zahlengeometrische kettenbruchalgorithmen zur einheitenberchnung, Doctoral Dissertation, Köln, 1982.

[Buc85A] J.Buchmann, "A generalization of Voronoi's unit algorithm I", J. Number Theory **20**(1985), 177-191.

[Buc85B] J.Buchmann, "A generalization of Voronoi's unit algorithm II", J. Number Theory **20**(1985), 192-209.

[Buc86] J.Buchmann, "Generalized continued fractions and number theoretic computations", Bericht Nr. 269 der math.-stat. Sektion in der Forschungsgesellschaft Joanneum, Graz, 1986.

[Buc87] J.Buchmann, "On the computation of units and class numbers by a generalization of Lagrange's algorithm", J. Number Theory **26**(1987), 8-30.

[BWB76] P.Barracund, H.C.Williams and L.Baniuk, "A computational technique for determining the class number of a pure cubic field", Math. Comp. **30**(1976), 312-323.

[BW88A] J.Buchmann and H.C.Williams, "On the infrastructure of the principal ideal class of an algebraic number field of unit rank one", Math. Comp. **50**(1988), 569-574.

[BW88B] J.Buchmann and H.C.Williams, "Computation of real quadratic fields with class number one", Math. Comp. **51**(1988), 809-824.

[BW89] J.Buchmann and H.C.Williams, "On the computation of the class number of an algebraic number field", Math. Comp. **53**(1989), 679-688.

[BWZ71] B.D.Beach, H.C.Williams and C.R.Zarnke, "Some computer results on units in quadratic and cubic fields", Proc. of the 25th Summer meeting of the Can. Math. Cong. (1971), 609-648.

[Cas50] J.W.S.Cassels, "The rational solutions of the diophantine equation $Y^2 = X^3-D$", Acta Math. 82(1950), 243-273.

[Cha80] L.Charve, "De la réduction des formes quadratiques ternaires positives et de son application aux irrationelles du troisième degré, Ann. Sci. École. Norm. Sup. **9**(1880), 3-156.

[CL84] H.Cohen and H.W.Lenstra, Jr., "Heuristics on class groups of number fields", Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. Vol. 1068, 33-62, Springer-Verlag, Berlin and New York, 1984.

[CM87] H.Cohen and J.Martinet, "Class groups of number fields: numerical heuristics", Math. Comp. **48**(1987), 123-138.

[Coh57] H.Cohn, "A numerical study of Dedekind's cubic class number formula", J. Nat. Bur. Standards **59**(1957), 265-271.

[CW85] G.Cornell and L.C.Washington, "Class numbers of cyclotomic fields", J. Number Theory **21**(1985), 260-274.

[Ded00] R.Dedekind, "Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern", J. Reine Angew. Math. **121**(1900), 40-123.

[DF64] B.N.Delone and D.K.Faddeev, The Theory of Irrationalities of the Third Degree, Translation of the A.M.S., Vol 10, 1964.

[DH71] H.Davenport and H.Heilbronn, "On the density of discriminants of cubic fields II", Proc. Royal Soc. London Ser. A **322**(1971), 405-420.

[DLQ88] F.Diaz y Diaz, P.Llorente and J.Quer, "Cubic fields, a congruential criterion for Scholz's theorem and new real quadratic fields with 3-rank equal to 4", Arch. Math. **50**(1988), 356-359.

[DS66] H.Davenport and A.Schinzel, "A note on certain arithmetical constants", Illinois J. Math. **10**(1966), 181-185.

[DW85] G.Dueck and H.C.Williams, "Computation of the class number and class group of a complex cubic field", Math. Comp. **45**(1985), 223-231. "Corrigendum", Math. Comp. **50**(1988), 655-657.

[EFO78] H.Eisenbeis, G.Frey and B.Ommerborn, "Computation of the 2-rank of pure cubic fields", Math. Comp. **32**(1978), 559-569.

[ET85] V.Ennola and R.Turunen, "On totally real cubic fields", Math. Comp. **44**(1985), 495-518.

[FW90] G.W.Fung and H.C.Williams, "Quadratic polynomials which have a high density of primes values", Math. Comp. **55**(1990), 345-353.

[Hal76] F.Halter-Koch, "Eine Bemerkung über kubische Einheiten", Arch. Math. **27**(1976), 593-595.

[Has30] H.Hasse, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage", Math. Zeit. **31**(1930), 565-582.

[Has80] H.Hasse, Vorlesungen über Klassenk örpertheorie, Springer-Verlag, 1980.

[Her50] Ch.Hermite, "Sur différents objets de la théorie des nombres, J. Reine Angew. Math. **40**(1850), 261-278, 279-315.

[HL23] G.H.Hardy and J.E.Littlewood, "Partitio numerorum III: On the expression of a number as a sum of primes", Acta Math. **44**(1923), 1-70.

[Hon71] T.Honda, "Pure cubic fields whose class numbers are multiples of three", J. Number Theory **3**(1971), 7-12.

[Hua82] L.K.Hua, Introduction to Number Theory, Springer-Verlag, 1982.

[Jae30] C.G.Jaeger "A character symbol for primes relative to a cubic field", Amer. J. of Math. **52**(1930), 85-96.

[JH78] N.S.Jeans and M.D.Hendy, "Some inequalities related to the determination of the fundamental unit of a pure cubic field", Math. Comp. **32**(1978), 925-935.

[Leh80] D.H.Lehmer, "A history of the sieve process", A History of Computing in the Twentieth Century, Academic Press, New York, 1908, 445-456.

[Len82] H.W.Lenstra, Jr., "On the calculation of regulators and class numbers of quadratic fields",London Math. Soc. Lect. Note Ser. **56**(1982), 123-150.

[LN83] P.Llorente and E.Nart, "Effective determination of the decomposition of the rational primes in a cubic field", Proc. of A.M.S **87**(1983), 579-585.

[LO82] P.Llorente and A.V.Onetto, "On the real cubic fields", Math. Comp. **39**(1982), 689-692.

[LQ88A] P.Llorente and J.Quer, "On totally real cubic fields with discriminant $D < 10^7$", Math. Comp. **50**(1988), 581-594.

[LQ88B] P.Llorente and J.Quer, "On the 3-Sylow subgroup of the class group of quadratic fields", Math. Comp. **50**(1988), 321-333.

[Mar92] A.Markoff, "Sur les nombres entiers dépendants d'une racine cubique d'un nombre entier ordinaire", Mem. Acad. Imp. Sci. St. Petersburg, v.7 38(1892), 1-37.

[Mat90] G.B.Mathews, "On the arithmetical theory of the form $x^3+ny^3+n^2z^3-3nxyz=1$", Proc. London Math. Soc., **21**(1890), 280-287.

[May88] D.Mayer, Differental principal factors and units in pure cubic number fields, unpublished MS, 1988.

[MB12] G.B.Mathews and W.E.H.Berwick, "On the reduction of arithmetical binary cubics which have a negative discriminant", Proc. London Math. Soc., **10**(1912), 48-58.

[Mei91] E.Meissel, Beitrag zur Pell'schen Gleichung höherer Grade, Progr., Kiel, 1891.

[MP67] J.Martinet and J.J.Payan, "Sur les extensions cubiques non-galoisiennes des rationnels et leur clôture galoisienne", J. Reine Angew. Math. **228**(1967), 15-37.

[Mos79] N.Moser, "Unités et nombre de classes d'une extension galoisienne dihédrale de **Q**", Abh. Math. Sem. Univ. Hamburg **48**(1979), 54-75.

[MW87] R.A.Mollin and H.C.Williams, "Computation of the class number of a real quadratic field", Advances in the Theory of Computation and Computational Math. (1987), to appear.

[Nag23] T.Nagell, "Über die Einheiten in reinen kubischen Zahlkörpern", Skrifter Vid. selsk. Christiania, Mat naturv. Kl., No. 11 (1923).

[Nak81] K.Nakamula, "Class number calculation and elliptic unit. I, cubic case", Proc. Japan Acad. **57A**(1981), 77-81.

[Nak82] K.Nakamula, "Class number calculation of a cubic field from the elliptic unit", J. Reine Angew Math. **331**(1982), 114-123.

[Nak88] K.Nakamula, "A table for pure cubic fields", Adv. Studies in Pure Math. **13**(1988), 461-477.

[NS74] C.Nield and D.Shanks, "On t he 3-rank of quadratic fields and the Euler product", Math.Comp. **28**(1974), 279-291.

[Ost79] J.Oesterlé "Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée", Astérisque, **61**(1979), 165-167.

[Pie26] T.A.Pierce, "An approximation to the least root of a cubic equation with application to the determination of units in pure cubic fields", Bull. Amer. Math. Soc. **32**(1926), 263-268.

[Poc28] H.C.Pocklington, "The practical calculation of unit algebraical numbers", Cam. Phil. Soc. **24**(1928), 471-476.

[Poh87] M.Pohst, "On computing isomorphisms of equation orders", Math. Comp. **48**(1987), 309-314.

[PW85] C.D.Patterson and H.C.Williams, "Some periodic continued fractions with long periods", Math. Comp. **44**(1985), 523-532.

[PWZ82] M.Pohst, P.Weiler and H. Zassenhaus, "An effective computation of fundamental units II", Math. Comp. **38**(1982), 293-328.

[PZ76] M.Pohst and H. Zassenhaus, "On unit computation in real quadratic fields", Symbolic and algebraic computation , Lecture Notes in Computer Science 72, Springer, 1976, 140-152.

[PZ77] M.Pohst and H. Zassenhaus, "An effective number geometric method of computing the fundamental units of an algebraic number field", Math. Comp. **31**(1977), 754-778.

[PZ82] M.Pohst and H. Zassenhaus, "An effective computation of fundamental units I", Math. Comp. **38**(1982), 275-292.

[PZ89] M.Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory , Cambridge University Press, 1989.

[Que87] J.Quer, Sobre el 3-rang dels cossos quadratics i la corba el-liptica $y^2 = x^3 + M$, (Catalan) Doctoral Dissertation, Bellaterra, 1987.

[Rei99] L.W.Reid, "Tafel der Klassenzahlen für kubische Zahlkörper", Diss. Göttingen 1899. Abstract in Amer. J. Math. **23**(1901), 68-84.

[RS78] R.J.Rudman and R.P.Steiner, "A generalization of Berwick's unit algorithm", J. Number Theory, **10**(1978), 16-34.

[Rud73] R.J.Rudman, "On the fundamental unit of a purely cubic field, Pac. J. of Math., **46**(1973), 253-256.

[Sch32] A.Scholz, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander", J. Reine Angew. Math. **166**(1932), 201-203.

[Sch83] R.Schoof, "Quadratic fields and factorization", Computation Methods in Number Theory (H.W. Lenstra and R. Tijdeman, eds.)Math. Centrum Tracts., Number 155, Part II, Amsterdam, 1983, 235-286.

[Sel55] E.Selmer, "Tables for the purely cubic field $K(\sqrt[3]{m})$", Avh. Norske Vid. Akad. Oslo I **5**(1955), 1-38.

[Sel] E.Selmer, Supplement to tables for the purely cubic field $K(\sqrt[3]{m})$, unpublished MS.

[Set78] B.Setzer, "Units in totally complex S_3 fields", J. Number Theory **10**(1978), 244-249.

[Sha71] D.Shanks, "Class number, a theory of factorization and genera", Proc. Symp. Pure Math. AMS **20**(1971), 415-440.

[Sha72] D.Shanks, "The infrastructure of real quadratic fields and its application", Proc. 1972 Number Theory Conf. Boulder, Colorado, 1972, 217-224.

[Sha74] D.Shanks, "The simplest cubic fields", Math. Comp. **28**(1974), 1137-1152.

[Sha75] D.Shanks, Review of I.O.Angell, "A table of complex cubic fields", Math. Comp. **29**(1975), 661-665.

[Sha76A] D.Shanks, "A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)", Congressus Numerantium **17**(1976), 15-40.

[Sha76B] D.Shanks, "Recent applications of the infrastructure of real quadratic fields $\mathbf{Q}(\sqrt{N})$", Abstract 731-12-12, Notices AMS **23**(1976), 59.

[Sha87] D.Shanks, Determining all cubic fields having a given fundamental discriminant, unpublished MS, 1987.

[Sha88] D.Shanks, "Determining all cubic fields having a given fundamental discriminant", a talk presented at the AMS Summer Research Conference on Computational Number Theory, Brunswick, Maine, 1988.

[Sha89] D.Shanks, "On Gauss and composition II", NATO ASI Ser. C. 265, 1989, 179-204.

[SL72] D.Shanks and M.Lal, "Bateman's constants reconsidered and the distribution of cubic residues", Math. Comp. **26**(1972), 265-285.

[SR76] R.Steiner and R.Rudman, "On an algorithm of Billevich for finding units in algebraic number fields", Math. Comp. **30**(1976), 413-435.

[ST79] I.N.Stewart and D.O.Tall, Algebraic Number Theory, Chapman and Hall, 1979.

[Ste69] H.J.Stender, "Über die Grundeinheit für spezielle unendliche Klassen reiner kubischer Zahlkörper", Abh. Math. Sem. Univ. Hamburg, **33**(1969), 203-215.

[Ste76] R.Steiner, "On the units in algebraic number fields", Congressus Numerantium **18**(1976), 413-435.

[Sve70] M.Sved, "Units in pure cubic number fields", Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math. **13**(1970), 141-149.

[SW88] A.J.Stephens and H.C.Williams, "Computation of a real quadratic fields with class number one", Math. Comp. **51**(1988), 809-824.

[SW89] A.J.Stephens and H.C.Williams, "Some computational results on a problem from Eisenstein", Proc. of the Inter. Number Theory Conf.,Laval Univ., Quebec, 1989, 869-886.

[SW90] A.J.Stephens and H.C.Williams, "An open architecture number sieve", Lecture notes of the London Math. Soc., 154(1990), 38-75.

[Sze70] G.Szekeres, "Multidimensional continued fractions", Ann. Univ. Sci. Budap. Rolando Eötvos, Sect. Math. **13**(1970), 113-140.

[Tor55] L.Tornheim, "Minimal basis and inessential discriminant divisors for a cubic field", Pac. J. Math. **5**(1955), 623-631.

[TW86] M.Tennenhouse and H.C.Williams, "A note on class-number one in certain real quadratic and pure cubic fields", Math. Comp. **46**(1986), 333-336.

[Usp31] J.V.Uspensky, "A method for finding units in cubic orders of a negative discriminant", Trans. Amer. Math. **33**(1931), 1-31.

[Vor52] G.F.Voronoi, Collected works in 3 volumes, (in Russian) Izdatelstvo Akademii Nauk Ukrainskoissr, Kiev, 1952-1953.

[Vor94] G.F.Voronoi, Concerning algebraic integers derivable from a root of an equation of the third degree, (Russian) Master's Thesis, St. Petersburg, 1894.

[Vor96] G.F.Voronoi, On a generalization of the algorithm of continued fractions, (Russian) Doctoral Dissertation, Warsaw, 1896.

[Wad70] H.Wada, "A table of fundamental units of purely cubic fields", Proc. Japan Acad. **46**(1970), 1135-1140.

[Wah22] G.E.Wahlin, "The factorization of the rational primes in a cubic domain", Amer. J. Math. **44**(1922), 191-203.

[WCS80] H.C.Williams, G.Cormack and E.Seah, "Calculation of the regulator of a pure cubic field", Math. Comp. **34**(1980), 567-611.

[WDS83] H.C.Williams, G.Dueck and B.Schmid, "A rapid method of evaluating the regulator and class number of a pure cubic field", Math. Comp. **41**(1983), 235-286.

[WD84] H.C.Williams and G.Dueck, "An analogue of the nearest integer continued fraction for certain cubic irrationalities", Math. Comp. **42**(1984), 683-705.

[Wil76] H.C.Williams, "Some results on fundamental units in cubic fields", J. Reine Angew. Math. **286/287**(1976), 75-85. "Corrigendum", Math. Comp. **33**(1979), 847-848.

[Wil77] H.C.Williams, "Certain pure cubic fields with class-number one", Math. Comp. **31**(1977), 578-580.

[Wil80] H.C.Williams, "Improving the speed of calculating the regulator of certain pure cubic fields", Math. Comp. **35**(1980), 1423-1434.

[Wil81] H.C.Williams, "Some results concerning Voronoi's continued fraction over $Q(\sqrt[3]{D})$", Math. Comp. **36**(1981), 631-652.

[Wil82] H.C.Williams, "Determination of principal factors in $Q(\sqrt{D})$ and $Q(\sqrt[3]{D})$", Math. Comp. **38**(1982), 261-274.

[Wil85] H.C.Williams, "Continued fractions and number-theoretic computations", Rocky Mountain J. of Math. **15**(1985), 621-655.

[Wil86] H.C.Williams, "The spacing of the minima in certain cubic lattices", Pac. J. Math. **124**(1986), 483-496.

[Wil87] H.C.Williams, "Effective primality tests for some integers of the forms $A^{5n} - 1$ and $A^{7n} - 1$", Math. Comp. **48**(1987), 385-403.

[Wol23] C.Wolfe, "On the indeterminate cubic equation $x^3+Dy^3+D2z^3-3Dxyz = 1$", Univ. of Calf. Publ. in Math. Vol. 1 **16**(1923), 359-369.

[WS79] H.C.Williams and D.Shanks, "A note on class number one in pure cubic fields", Math. Comp. **33**(1979), 1317-1320.

[WW87] H.C.Williams and M.C.Wunderlich, "On the parallel generation of the residues for the continued fraction factoring algorithm", Math. Comp. **48**(1987), 405-423.

[WZ72] H.C.Williams and C.R.Zarnke, "Computer calculation of units in cubic fields", Proc. of the 25th summer meething of the Can. Math. Cong. 1971, 609-648.

[WZ74] H.C.Williams and C.R.Zarnke, "Some algorithms for solving a cubic congruence modulo p", Utilitas Math. 6(1974), 285-306.

[Zol69] E. Zolotarev, On an indeterminate equation of the third degree, (Russian) Doctoral Dissertation, St. Petersburg, 1869.

Appendix 1

Coefficients of the generating polynomials $X^3 + AX^2 + BX + C$ for all the distinct cubic fields with negative fundamental discriminant D.

Note: 1) A, B and C are the coefficients of a generating polynomial of a complex cubic field before Tschirnhausen transformation is applied.
2) A', B' and C' are the coefficients of a generating polynomial of a complex cubic field after Tschirnhausen transformation is applied.

D = -408368221541174183

(1) A=	0 B=	11707457 C=	1306969383870 INDEX=		10628
a'=		29233 b'=	-51751872		
c'=		31735037952 ind'=	1728		
(2) A=	1 B=	-7001856 C=	7864126137 INDEX=		27
a'=		1 b'=	-7001856		
c'=		7864126137 ind'=	27		
(3) A=	0 B=	-125345551 C=	3703380687301 INDEX=		29791
a'=		-4036 b'=	15624765		
c'=		474513461071 ind'=	3991		
(4) A=	0 B=	-101992423 C=	688798773478 INDEX=		4580
a'=		0 b'=	-101992423		
c'=		688798773478 ind'=	4580		
(5) A=	1 B=	167353236 C=	225353720735 INDEX=		7019
a'=		1 b'=	167353236		
c'=		225353720735 ind'=	7019		
(6) A=	1 B=	214407526 C=	2194379325035 INDEX=		20369
a'=		34545 b'=	-142987228		
c'=		187882451635 ind'=	5543		
(7) A=	0 B=	-3940945 C=	3013773223 INDEX=		1
a'=		0 b'=	-3940945		
c'=		3013773223 ind'=	1		
(8) A=	1 B=	-173020478 C=	-938527957576 INDEX=		2738
a'=		1 b'=	-173020478		
c'=		-938527957576 ind'=	2738		
(9) A=	0 B=	172307369 C=	1135757549546 INDEX=		11636
a'=		15079 b'=	-21758700		
c'=		582611913536 ind'=	7076		
(10) A=	0 B=	-1857697 C=	982293255 INDEX=		1
a'=		0 b'=	-1857697		
c'=		982293255 ind'=	1		
(11) A=	1 B=	190136 C=	-118707083 INDEX=		1
a'=		1 b'=	190136		
c'=		-118707083 ind'=	1		
(12) A=	0 B=	-275591551 C=	1769844699099 INDEX=		1441
a'=		0 b'=	-275591551		
c'=		1769844699099 ind'=	1441		
(13) A=	1 B=	-167001776 C=	857370011712 INDEX=		1728
a'=		1 b'=	-167001776		
c'=		857370011712 ind'=	1728		

(14) A=	1 B=	-216541724 C=		-3240567017683 INDEX=		24389
a'=			33404 b'=		-82485943	
c'=			53638459421 ind'=		1483	
(15) A=	1 B=	6086696 C=		5344659472 INDEX=		64
a'=			1 b'=		6086696	
c'=			5344659472 ind'=		64	
(16) A=	0 B=	-66052051 C=		868475669951 INDEX=		6859
a'=			0 b'=		-66052051	
c'=			868475669951 ind'=		6859	
(17) A=	1 B=	63180986 C=		99854034487 INDEX=		1769
a'=			1 b'=		63180986	
c'=			99854034487 ind'=		1769	
(18) A=	0 B=	42289181 C=		147617058447 INDEX=		1477
a'=			0 b'=		42289181	
c'=			147617058447 ind'=		1477	
(19) A=	1 B=	144528380 C=		1518991425793 INDEX=		13495
a'=			10807 b'=		17592128	
c'=			1061026683055 ind'=		8867	
(20) A=	1 B=	25640806 C=		-72193382160 INDEX=		714
a'=			1 b'=		25640806	
c'=			-72193382160 ind'=		714	
(21) A=	1 B=	-88794942 C=		-731694846832 INDEX=		5342
a'=			66887 b'=		-1463320	
c'=			8547200 ind'=		40	
(22) A=	1 B=	330896814 C=		-7466091131065 INDEX=		63565
a'=			5227 b'=		3840254	
c'=			230194863085 ind'=		1903	
(23) A=	1 B=	92698426 C=		-618214568295 INDEX=		5751
a'=			1 b'=		92698426	
c'=			-618214568295 ind'=		5751	
(24) A=	1 B=	19180538 C=		-9040257343 INDEX=		273
a'=			1 b'=		19180538	
c'=			-9040257343 ind'=		273	
(25) A=	1 B=	26694286 C=		108074219297 INDEX=		979
a'=			1 b'=		26694286	
c'=			108074219297 ind'=		979	
(26) A=	1 B=	-31415038 C=		260935679801 INDEX=		2049
a'=			1 b'=		-31415038	
c'=			260935679801 ind'=		2049	
(27) A=	0 B=	-227697139 C=		2782567576247 INDEX=		19907
a'=			-9101 b'=		58042182	
c'=			480506586083 ind'=		4913	
(28) A=	1 B=	15495624 C=		120726045440 INDEX=		1000
a'=			1 b'=		15495624	
c'=			120726045440 ind'=		1000	
(29) A=	1 B=	-218601304 C=		1244230362020 INDEX=		216
a'=			1 b'=		-218601304	
c'=			1244230362020 ind'=		216	
(30) A=	1 B=	317587336 C=		4407489012992 INDEX=		39976
a'=			8221 b'=		-13660348	

```
c'=                                224920326784 ind'=                    2372

(31) A=   1 B=          10170938 C=                -189224534608 INDEX=          1542
a'=                                           1 b'=                   10170938
c'=                               -189224534608 ind'=                     1542

(32) A=   1 B=           7403060 C=                  13277124775 INDEX=           125
a'=                                           1 b'=                    7403060
c'=                                13277124775 ind'=                       125

(33) A=   0 B=         220520831 C=                 433067480413 INDEX=         10837
a'=                                       20642 b'=                   17376723
c'=                               343377291517 ind'=                       5629

(34) A=   1 B=         -58352082 C=               -1227993870427 INDEX=          9887
a'=                                           1 b'=                   -58352082
c'=                               -1227993870427 ind'=                     9887

(35) A=   1 B=         -95378312 C=                -358574744367 INDEX=            27
a'=                                           1 b'=                   -95378312
c'=                                -358574744367 ind'=                       27

(36) A=   1 B=        -111171508 C=                 479907780175 INDEX=          1331
a'=                                           1 b'=                  -111171508
c'=                                479907780175 ind'=                       1331

(37) A=   0 B=         242629907 C=                1552111540705 INDEX=         17297
a'=                                       14662 b'=                   -20735007
c'=                               225791042393 ind'=                       3613

(38) A=   1 B=         -51459328 C=                -142318703180 INDEX=            64
a'=                                           1 b'=                   -51459328
c'=                               -142318703180 ind'=                        64

(39) A=   1 B=        -219508356 C=                1419962721692 INDEX=          5452
a'=                                           1 b'=                  -219508356
c'=                               1419962721692 ind'=                      5452

(40) A=   1 B=          95104666 C=                 471564746295 INDEX=          4809
a'=                                       30711 b'=                       12560
c'=                                       4809 ind'=                          1

(41) A=   1 B=         -27512820 C=                -172866756691 INDEX=          1331
a'=                                           1 b'=                   -27512820
c'=                               -172866756691 ind'=                      1331

(42) A=   0 B=        -106489597 C=                 478887409540 INDEX=          1826
a'=                                           0 b'=                  -106489597
c'=                                478887409540 ind'=                       1826

(43) A=   1 B=         276419076 C=                -347958534955 INDEX=         14659
a'=                                       30019 b'=                   216131780
c'=                               1394950806475 ind'=                      9755

(44) A=   1 B=         -45733320 C=                -909426410791 INDEX=          7331
a'=                                           1 b'=                   -45733320
c'=                               -909426410791 ind'=                      7331

(45) A=   0 B=         273163787 C=                 820276248887 INDEX=         15625
a'=                                       31495 b'=                  -162713420
c'=                                246747216251 ind'=                       5363

(46) A=   1 B=          73763608 C=                 492305901627 INDEX=          4467
a'=                                           1 b'=                    73763608
c'=                                492305901627 ind'=                       4467
```

```
(47) A=    1 B=          57660876 C=          -217277201860 INDEX=          2236
a'=                         39137 b'=             -7627178
c'=                    1452586096 ind'=              806

(48) A=    0 B=         -65016745 C=           263508596544 INDEX=          1378
a'=                             0 b'=            -65016745
c'=                  263508596544 ind'=              1378

(49) A=    1 B=         115612820 C=          -224884757971 INDEX=          4299
a'=                         31124 b'=             29850867
c'=                   70201298619 ind'=             4041

(50) A=    1 B=        -141031024 C=          -644691258323 INDEX=             1
a'=                             1 b'=           -141031024
c'=                  -644691258323 ind'=                1

(51) A=    1 B=           312470 C=             103084459 INDEX=             1
a'=                             1 b'=              312470
c'=                   103084459 ind'=                1

(52) A=    1 B=         -18344204 C=            33173266065 INDEX=           111
a'=                             1 b'=            -18344204
c'=                   33173266065 ind'=              111

(53) A=    1 B=        -260737600 C=          2513603846623 INDEX=         15625
a'=                        -12371 b'=             80635856
c'=                   502149390625 ind'=             5669

(54) A=    1 B=        -242829300 C=         -1525058481177 INDEX=          3675
a'=                             1 b'=           -242829300
c'=                 -1525058481177 ind'=             3675

(55) A=    0 B=        -163474471 C=           817830006906 INDEX=          1196
a'=                             0 b'=           -163474471
c'=                   817830006906 ind'=             1196

(56) A=    1 B=        -151995070 C=           724850816968 INDEX=           590
a'=                             1 b'=           -151995070
c'=                   724850816968 ind'=              590

(57) A=    1 B=          10567496 C=            23043307520 INDEX=           216
a'=                             1 b'=             10567496
c'=                    23043307520 ind'=              216

(58) A=    1 B=           7320434 C=           -74628663416 INDEX=           610
a'=                             1 b'=              7320434
c'=                  -74628663416 ind'=              610

(59) A=    1 B=         -98607634 C=          4656489319177 INDEX=         37739
a'=                         -2407 b'=             15261308
c'=                   377085106619 ind'=             3161

(60) A=    1 B=          35205072 C=           311653427189 INDEX=          2617
a'=                             1 b'=             35205072
c'=                   311653427189 ind'=             2617

(61) A=    0 B=        -123299935 C=           801735839349 INDEX=          4913
a'=                             0 b'=           -123299935
c'=                   801735839349 ind'=             4913

(62) A=    1 B=          80628604 C=          -580082190973 INDEX=          5233
a'=                         36193 b'=             81595088
c'=                   106770411337 ind'=             4517

(63) A=    0 B=        -184832761 C=           996814659889 INDEX=          1961
a'=                             0 b'=           -184832761
```

```
c'=                                  996814659889 ind'=                  1961

(64) A=   1 B=          62563672 C=                  752683886999 INDEX=          6313
a'=                         31856 b'=                    -6992741
c'=                     742718137 ind'=                       343

(65) A=   0 B=        -229892269 C=                14326739077508 INDEX=        115982
a'=                         -1967 b'=                     2414340
c'=                  128357743328 ind'=                      1052

(66) A=   1 B=         -86021638 C=                 -460867093160 INDEX=          2794
a'=                             1 b'=                    -86021638
c'=                  -460867093160 ind'=                     2794

(67) A=   1 B=         -34816528 C=                 -234268448441 INDEX=          1793
a'=                             1 b'=                    -34816528
c'=                  -234268448441 ind'=                     1793

(68) A=   1 B=          -4301078 C=                  255702687681 INDEX=          2079
a'=                             1 b'=                     -4301078
c'=                  255702687681 ind'=                      2079

(69) A=   1 B=           9901352 C=                  -23700146560 INDEX=           216
a'=                             1 b'=                      9901352
c'=                  -23700146560 ind'=                       216

(70) A=   1 B=         -42457138 C=                 -939018001400 INDEX=          7586
a'=                             1 b'=                    -42457138
c'=                  -939018001400 ind'=                     7586

(71) A=   1 B=         117536862 C=                 -706412473533 INDEX=          6993
a'=                             1 b'=                    117536862
c'=                  -706412473533 ind'=                     6993

(72) A=   1 B=         -89685292 C=                  516995333833 INDEX=          3257
a'=                             1 b'=                    -89685292
c'=                   516995333833 ind'=                     3257

(73) A=   0 B=         -19652737 C=                   36889557659 INDEX=           125
a'=                             0 b'=                    -19652737
c'=                   36889557659 ind'=                      125

(74) A=   1 B=           4142252 C=                   706002887 INDEX=            27
a'=                             1 b'=                      4142252
c'=                   706002887 ind'=                         27

(75) A=   1 B=         274473312 C=                 3365862517559 INDEX=         30847
a'=                         68627 b'=                    -36666388
c'=                  5419205099 ind'=                      1331

(76) A=   1 B=        -159189026 C=                 -842635486135 INDEX=          2725
a'=                             1 b'=                   -159189026
c'=                  -842635486135 ind'=                     2725

(77) A=   1 B=         -96993538 C=                  527941529291 INDEX=          3081
a'=                             1 b'=                    -96993538
c'=                   527941529291 ind'=                     3081

(78) A=   1 B=          59522318 C=                  255638249797 INDEX=          2527
a'=                             1 b'=                     59522318
c'=                   255638249797 ind'=                     2527

(79) A=   1 B=         146056298 C=                   54337056472 INDEX=          5542
a'=                             1 b'=                    146056298
c'=                    54337056472 ind'=                      5542
```

```
(80) A=    0 B=          -668755 C=                    1006127966 INDEX=                 8
a'=                            0 b'=                     -668755
c'=                   1006127966 ind'=                         8

(81) A=    1 B=        -48122576 C=                  248322633792 INDEX=              1728
a'=                            1 b'=                   -48122576
c'=                   248322633792 ind'=                    1728

(82) A=    0 B=          4156433 C=                   13888148050 INDEX=               116
a'=                            0 b'=                     4156433
c'=                   13888148050 ind'=                      116

(83) A=    0 B=        -35132599 C=                   90574444963 INDEX=               343
a'=                            0 b'=                   -35132599
c'=                   90574444963 ind'=                      343

(84) A=    1 B=        -38344170 C=                  -94496595975 INDEX=               195
a'=                            1 b'=                   -38344170
c'=                   -94496595975 ind'=                     195

(85) A=    0 B=        -87446329 C=                  492204445187 INDEX=              3077
a'=                            0 b'=                   -87446329
c'=                   492204445187 ind'=                    3077

(86) A=    1 B=         35651490 C=                  -499385334667 INDEX=              4115
a'=                            1 b'=                    35651490
c'=                   -499385334667 ind'=                   4115

(87) A=    1 B=       -120439658 C=                  -974399186623 INDEX=              6757
a'=                            1 b'=                  -120439658
c'=                   -974399186623 ind'=                   6757

(88) A=    1 B=          128772 C=                    121732721 INDEX=                 1
a'=                            1 b'=                     128772
c'=                   121732721 ind'=                          1

(89) A=    1 B=        -19798148 C=                  -34488491265 INDEX=                51
a'=                            1 b'=                   -19798148
c'=                   -34488491265 ind'=                     51

(90) A=    1 B=         58213926 C=                   770963899457 INDEX=              6421
a'=                        35647 b'=                    53379452
c'=                   35732100901 ind'=                     2359

(91) A=    0 B=        -36208315 C=                  2821363311113 INDEX=             22931
a'=                        -1577 b'=                    1992804
c'=                   658061203019 ind'=                    5357

(92) A=    1 B=        -65709342 C=                   489331486757 INDEX=              3613
a'=                            1 b'=                   -65709342
c'=                   489331486757 ind'=                    3613

(93) A=    0 B=         34357961 C=                    81911932713 INDEX=               917
a'=                        52033 b'=                     -170910
c'=                      668493 ind'=                         27

(94) A=    1 B=         49640982 C=                  2816918352431 INDEX=             22931
a'=                         2178 b'=                    -5076631
c'=                   650711358899 ind'=                    5327

(95) A=    1 B=       -323760874 C=                 10785731114440 INDEX=             85786
a'=                        -3349 b'=                    13784962
c'=                   149020919464 ind'=                    1318

(96) A=    1 B=       -218199588 C=                 -1388874230820 INDEX=              5076
a'=                            1 b'=                  -218199588
```

```
c'=                          -1388874230820 ind'=                    5076

(97) A=   0 B=        60632435 C=                    89191506692 INDEX=          1646
a'=                          0 b'=                     60632435
c'=                   89191506692 ind'=                    1646

(98) A=   0 B=      -153513163 C=                   732094148810 INDEX=             8
a'=                          0 b'=                   -153513163
c'=                  732094148810 ind'=                       8

(99) A=   0 B=       -77314171 C=                   261778011734 INDEX=            64
a'=                          0 b'=                    -77314171
c'=                  261778011734 ind'=                      64

(100) A=   1 B=        35229142 C=                   171725627904 INDEX=          1542
a'=                          1 b'=                     35229142
c'=                  171725627904 ind'=                    1542

(101) A=   1 B=      -117184168 C=                 -16042449746864 INDEX=        130384
a'=                       -883 b'=                     2329054
c'=                  114717580096 ind'=                     938

(102) A=   0 B=      -181874155 C=                   944103677978 INDEX=            64
a'=                          0 b'=                   -181874155
c'=                  944103677978 ind'=                      64

(103) A=   1 B=       105402200 C=                 -1169524646977 INDEX=         10095
a'=                          1 b'=                    105402200
c'=                 -1169524646977 ind'=                   10095

(104) A=   1 B=           344672 C=                    95291575 INDEX=             1
a'=                          1 b'=                       344672
c'=                   95291575 ind'=                         1

(105) A=   0 B=       -12411631 C=                   164552951249 INDEX=          1331
a'=                      78607 b'=                     16882938
c'=                 1080507131 ind'=                      901

(106) A=   1 B=       247835632 C=                  -4756285445343 INDEX=         40557
a'=                      67630 b'=                       668277
c'=                   1891755 ind'=                           27

(107) A=   0 B=       -92537995 C=                   3974961082427 INDEX=         32201
a'=                      -2483 b'=                     22480896
c'=                  431116036481 ind'=                    3659

(108) A=   1 B=       -92664404 C=                  -1315899985125 INDEX=         10329
a'=                          1 b'=                    -92664404
c'=                 -1315899985125 ind'=                   10329

(109) A=   0 B=       -29711455 C=                    845838535193 INDEX=          6859
a'=                          0 b'=                    -29711455
c'=                  845838535193 ind'=                      6859

(110) A=   0 B=         -442231 C=                     167145269 INDEX=             1
a'=                          0 b'=                      -442231
c'=                   167145269 ind'=                         1

(111) A=   0 B=       -73610251 C=                   243083576259 INDEX=             1
a'=                          0 b'=                    -73610251
c'=                  243083576259 ind'=                      1

(112) A=   1 B=           227206 C=                   -115627045 INDEX=             1
a'=                          1 b'=                       227206
c'=                  -115627045 ind'=                        1
```

```
(113) A=    0 B=          -85992223 C=                    307313001953 INDEX=          125
a'=                                          0 b'=           -85992223
c'=                                307313001953 ind'=             125

(114) A=    0 B=          -68839303 C=                    307219783077 INDEX=         1745
a'=                                          0 b'=           -68839303
c'=                                307219783077 ind'=            1745

(115) A=    1 B=          318694890 C=                    931601210400 INDEX=        19350
a'=                                      26749 b'=          -187439040
c'=                                405551333376 ind'=            7104

(116) A=    1 B=         -151300888 C=                   -719137975148 INDEX=          512
a'=                                          1 b'=          -151300888
c'=                               -719137975148 ind'=             512

(117) A=    1 B=         -212608064 C=                  -1193309107660 INDEX=           64
a'=                                          1 b'=          -212608064
c'=                               -1193309107660 ind'=              64

(118) A=    1 B=           53302242 C=                     1626612624 INDEX=         1218
a'=                                          1 b'=            53302242
c'=                                1626612624 ind'=              1218

(119) A=    1 B=          322624380 C=                   -2688456043225 INDEX=        28405
a'=                                      48131 b'=           -82921392
c'=                                43228144753 ind'=             3217

(120) A=    1 B=          124277150 C=                     145763421925 INDEX=         4495
a'=                                      29738 b'=            20954623
c'=                                70026746455 ind'=             3947

(121) A=    1 B=          -34237516 C=                    -714410131855 INDEX=         5775
a'=                                      53851 b'=           147425742
c'=                               121191614775 ind'=             4581

(122) A=    1 B=           97690004 C=                     -82208043245 INDEX=         3095
a'=                                          1 b'=            97690004
c'=                                -82208043245 ind'=            3095

(123) A=    1 B=          105871712 C=                    -263992545805 INDEX=         4029
a'=                                          1 b'=           105871712
c'=                               -263992545805 ind'=             4029

(124) A=    1 B=            5053548 C=                     -1257638347 INDEX=           37
a'=                                          1 b'=             5053548
c'=                                -1257638347 ind'=               37

(125) A=    0 B=           82986269 C=                    170924517874 INDEX=         2744
a'=                                          0 b'=            82986269
c'=                               170924517874 ind'=             2744

(126) A=    1 B=           -5857884 C=                     -5460405445 INDEX=            1
a'=                                          1 b'=            -5857884
c'=                                -5460405445 ind'=               1

(127) A=    0 B=          -41409247 C=                    370986204305 INDEX=         2899
a'=                                          0 b'=           -41409247
c'=                               370986204305 ind'=             2899

(128) A=    0 B=           -1162915 C=                      498112723 INDEX=            1
a'=                                          0 b'=            -1162915
c'=                                498112723 ind'=               1

(129) A=    1 B=         -211737992 C=                   1187495087888 INDEX=          512
a'=                                          1 b'=          -211737992
```

```
c'=                    1187495087888 ind'=                  512

(130) A=   1 B=        155251872 C=          216118470656 INDEX=          6304
a'=                         24645 b'=              -2695600
c'=                    138545176576 ind'=             4688

(131) A=   1 B=        -63468068 C=          -270470112261 INDEX=          1527
a'=                             1 b'=          -63468068
c'=                   -270470112261 ind'=             1527

(132) A=   1 B=       -181738938 C=          -988154387845 INDEX=          2399
a'=                             1 b'=         -181738938
c'=                   -988154387845 ind'=             2399

(133) A=   1 B=         49861578 C=            13034575197 INDEX=          1107
a'=                         45222 b'=              -96625
c'=                    17296875 ind'=              125

(134) A=   1 B=        268642136 C=          5811722151680 INDEX=         49224
a'=                          5623 b'=          -10943802
c'=                    241286006304 ind'=             2214

(135) A=   1 B=        -20866038 C=           -65688973483 INDEX=           443
a'=                             1 b'=          -20866038
c'=                    -65688973483 ind'=              443

(136) A=   1 B=         44129266 C=            47050776632 INDEX=           994
a'=                             1 b'=           44129266
c'=                    47050776632 ind'=               994

(137) A=   1 B=        -23124290 C=           167282437313 INDEX=          1315
a'=                             1 b'=          -23124290
c'=                    167282437313 ind'=              1315

(138) A=   1 B=       -349212720 C=          2761091155475 INDEX=          9325
a'=                        -21751 b'=          159705676
c'=                    541592652325 ind'=              7621

(139) A=   1 B=        111870516 C=           158514762267 INDEX=          3921
a'=                             1 b'=          111870516
c'=                    158514762267 ind'=              3921

(140) A=   1 B=        169641424 C=           129665567315 INDEX=          6995
a'=                         26295 b'=           33597788
c'=                    184158491195 ind'=              5131

(141) A=   0 B=        -77742001 C=           428552315496 INDEX=          2746
a'=                             0 b'=          -77742001
c'=                    428552315496 ind'=              2746

(142) A=   1 B=         88586960 C=          -592599998300 INDEX=          5480
a'=                         30687 b'=             123608
c'=                      350720 ind'=                  8

(143) A=   0 B=        192386375 C=          1878279799511 INDEX=         17407
a'=                         11054 b'=            1897689
c'=                    682792516783 ind'=              6263

(144) A=   1 B=        130500216 C=          1007728181667 INDEX=          9429
a'=                             1 b'=          130500216
c'=                   1007728181667 ind'=              9429

(145) A=   1 B=         40677452 C=           185513328809 INDEX=          1713
a'=                             1 b'=           40677452
c'=                    185513328809 ind'=              1713
```

(146) A=	0 B=	-256306999 C=		4567346237803 INDEX=		34847
a'=			-4292 b'=		47904915	
c'=		249725066663 ind'=			2677	
(147) A=	1 B=	69520850 C=		446575584509 INDEX=		4059
a'=			33445 b'=		-13828176	
c'=		3906223299 ind'=			981	
(148) A=	1 B=	-23743250 C=		62699864189 INDEX=		359
a'=			1 b'=		-23743250	
c'=		62699864189 ind'=			359	
(149) A=	1 B=	-140281730 C=		-907065718600 INDEX=		5230
a'=			1 b'=		-140281730	
c'=		-907065718600 ind'=			5230	
(150) A=	1 B=	-48060076 C=		-369777630676 INDEX=		2820
a'=			1 b'=		-48060076	
c'=		-369777630676 ind'=			2820	
(151) A=	0 B=	14371445 C=		59372726074 INDEX=		512
a'=			0 b'=		14371445	
c'=		59372726074 ind'=			512	
(152) A=	1 B=	-344122680 C=		39980890028628 INDEX=		324480
a'=			-1007 b'=		2685468	
c'=		44902840320 ind'=			372	
(153) A=	0 B=	199461779 C=		476729598479 INDEX=		9631
a'=			20897 b'=		15810498	
c'=		446517054511 ind'=			6809	
(154) A=	1 B=	-185399582 C=		3249375475973 INDEX=		25213
a'=			-7117 b'=		19892740	
c'=		558140811325 ind'=			4705	
(155) A=	1 B=	-38943524 C=		187452174875 INDEX=		1321
a'=			1 b'=		-38943524	
c'=		187452174875 ind'=			1321	
(156) A=	1 B=	-55889686 C=		-167946404473 INDEX=		393
a'=			1 b'=		-55889686	
c'=		-167946404473 ind'=			393	
(157) A=	1 B=	157268022 C=		1331598002747 INDEX=		12463
a'=			12874 b'=		-23238547	
c'=		705350077927 ind'=			7523	
(158) A=	1 B=	14330966 C=		17402237017 INDEX=		221
a'=			1 b'=		14330966	
c'=		17402237017 ind'=			221	
(159) A=	0 B=	-164755609 C=		932406174368 INDEX=		3698
a'=			0 b'=		-164755609	
c'=		932406174368 ind'=			3698	
(160) A=	0 B=	-183408433 C=		983084363000 INDEX=		1862
a'=			0 b'=		-183408433	
c'=		983084363000 ind'=			1862	
(161) A=	1 B=	-4160628 C=		-14037848055 INDEX=		111
a'=			1 b'=		-4160628	
c'=		-14037848055 ind'=			111	
(162) A=	1 B=	19286936 C=		-36996146945 INDEX=		401
a'=			1 b'=		19286936	

```
c'=                                  -36996146945 ind'=                  401

(163) A=   1 B=          -73318602 C=                  424889776472 INDEX=          2842
a'=                          94643 b'=                      42363490
c'=                     4966917928 ind'=                     1322

(164) A=   1 B=          -21170526 C=                  -41524440535 INDEX=           145
a'=                              1 b'=                     -21170526
c'=                   -41524440535 ind'=                      145

(165) A=   1 B=         -104401582 C=                  739052170333 INDEX=          4997
a'=                              1 b'=                     -104401582
c'=                   739052170333 ind'=                     4997

(166) A=   1 B=          194886864 C=                 4277386016327 INDEX=         35807
a'=                           5755 b'=                     -17590304
c'=                   330261173783 ind'=                     3037

(167) A=   0 B=          -18628483 C=                   34554630057 INDEX=           125
a'=                              0 b'=                     -18628483
c'=                    34554630057 ind'=                      125

(168) A=   1 B=          -39413482 C=                   95492713432 INDEX=            58
a'=                              1 b'=                     -39413482
c'=                    95492713432 ind'=                       58

(169) A=   1 B=          121909412 C=                  -705270002740 INDEX=          7116
a'=                              1 b'=                     121909412
c'=                   -705270002740 ind'=                     7116

(170) A=   1 B=          -55537772 C=                  -207194477523 INDEX=          1077
a'=                              1 b'=                     -55537772
c'=                   -207194477523 ind'=                     1077

(171) A=   1 B=              95046 C=                     122496155 INDEX=             1
a'=                              1 b'=                       95046
c'=                    122496155 ind'=                          1

(172) A=   1 B=             -91854 C=                     123418007 INDEX=             1
a'=                              1 b'=                      -91854
c'=                    123418007 ind'=                          1

(173) A=   0 B=          -81606955 C=                  302267773869 INDEX=           847
a'=                              0 b'=                     -81606955
c'=                   302267773869 ind'=                      847

(174) A=   0 B=          -40555009 C=                  261080245853 INDEX=          1963
a'=                              0 b'=                     -40555009
c'=                   261080245853 ind'=                     1963

(175) A=   1 B=         -241875102 C=                 1645395493923 INDEX=          6357
a'=                              1 b'=                     -241875102
c'=                  1645395493923 ind'=                     6357

(176) A=   1 B=           93481956 C=                  -841455989748 INDEX=          7404
a'=                          31089 b'=                      35884772
c'=                    23248441536 ind'=                     1772

(177) A=   1 B=         -213246778 C=                 1611367042432 INDEX=          8758
a'=                              1 b'=                     -213246778
c'=                  1611367042432 ind'=                     8758

(178) A=   0 B=           -7652653 C=                   12965081580 INDEX=            82
a'=                              0 b'=                      -7652653
c'=                    12965081580 ind'=                       82
```

```
(179) A=   0 B=          -60219547 C=                  217892888986 INDEX=          1000
a'=                              0 b'=                   -60219547
c'=                  217892888986 ind'=                       1000

(180) A=   1 B=          126303712 C=                  544364857661 INDEX=          6271
a'=                              1 b'=                   126303712
c'=                  544364857661 ind'=                       6271

(181) A=   0 B=          312911951 C=                 2799108627347 INDEX=         28603
a'=                          11201 b'=                   -13316742
c'=                  226334652307 ind'=                       2813

(182) A=   1 B=           96439692 C=                  578401430481 INDEX=          5559
a'=                          30267 b'=                     5034554
c'=                     654010791 ind'=                        343

(183) A=   0 B=             201503 C=                     117951865 INDEX=             1
a'=                              0 b'=                      201503
c'=                     117951865 ind'=                          1

(184) A=   1 B=          -22681488 C=                  -41584961395 INDEX=             1
a'=                              1 b'=                   -22681488
c'=                  -41584961395 ind'=                          1

(185) A=   0 B=          144574727 C=                  287957490955 INDEX=          5923
a'=                          28790 b'=                     40912251
c'=                  127354977787 ind'=                       4637

(186) A=   1 B=           32823472 C=                 -194556774928 INDEX=          1688
a'=                              1 b'=                    32823472
c'=                 -194556774928 ind'=                       1688

(187) A=   1 B=           92956782 C=                  219840451616 INDEX=          3326
a'=                              1 b'=                    92956782
c'=                  219840451616 ind'=                       3326

(188) A=   1 B=           46713740 C=                   67245066349 INDEX=          1139
a'=                              1 b'=                    46713740
c'=                   67245066349 ind'=                       1139

(189) A=   1 B=          -26133504 C=                   86039211015 INDEX=           561
a'=                              1 b'=                   -26133504
c'=                   86039211015 ind'=                        561

(190) A=   0 B=          -67115029 C=                  256467821508 INDEX=          1178
a'=                              0 b'=                   -67115029
c'=                  256467821508 ind'=                       1178

(191) A=   1 B=          175817506 C=                 -1409393884360 INDEX=         13586
a'=                          13261 b'=                     31747912
c'=                 1050187800704 ind'=                       8792

(192) A=   1 B=           19418338 C=                   -86544737463 INDEX=           753
a'=                              1 b'=                    19418338
c'=                  -86544737463 ind'=                        753

(193) A=   1 B=          141262430 C=                    7474956493 INDEX=          5255
a'=                          26970 b'=                      2063207
c'=                   16038307295 ind'=                       1747

(194) A=   1 B=         -156314844 C=                  -958610454565 INDEX=          4831
a'=                              1 b'=                  -156314844
c'=                  -958610454565 ind'=                       4831

(195) A=   1 B=           85502808 C=                  194604946407 INDEX=          2937
a'=                              1 b'=                    85502808
```

```
c'=                                194604946407 ind'=                    2937

(196) A=   1 B=          203425182 C=          -1006181441803 INDEX=          12223
a'=                           61583 b'=              -142453400
c'=                        86202030625 ind'=                 3775

(197) A=   0 B=          -96122533 C=            494850064655 INDEX=           2737
a'=                               0 b'=              -96122533
c'=                       494850064655 ind'=                 2737

(198) A=   1 B=         -229465054 C=          -4499264668663 INDEX=          34929
a'=                           -6326 b'=              17047125
c'=                       397863140625 ind'=                 3375

(199) A=   1 B=          -12941538 C=            17915652755 INDEX=              1
a'=                               1 b'=              -12941538
c'=                        17915652755 ind'=                    1

(200) A=   1 B=          143467466 C=            909826154200 INDEX=           9146
a'=                               1 b'=              143467466
c'=                       909826154200 ind'=                 9146

(201) A=   1 B=          293132202 C=          -527249690056 INDEX=          16282
a'=                           23249 b'=              135451234
c'=                      1165879839208 ind'=                 8462

(202) A=   0 B=           73525625 C=            395358873594 INDEX=           3772
a'=                               0 b'=               73525625
c'=                       395358873594 ind'=                 3772

(203) A=   0 B=          -22221211 C=             41079161014 INDEX=             64
a'=                               0 b'=              -22221211
c'=                        41079161014 ind'=                   64

(204) A=   1 B=          -88540654 C=          -417933821813 INDEX=           2179
a'=                               1 b'=              -88540654
c'=                      -417933821813 ind'=                 2179

(205) A=   1 B=           71096192 C=          -412447454623 INDEX=           3843
a'=                               1 b'=               71096192
c'=                      -412447454623 ind'=                 3843

(206) A=   0 B=            -380347 C=             152565475 INDEX=              1
a'=                               0 b'=                -380347
c'=                       152565475 ind'=                    1

(207) A=   1 B=           25526284 C=            234002524859 INDEX=           1945
a'=                               1 b'=               25526284
c'=                       234002524859 ind'=                 1945

(208) A=   1 B=           -8422826 C=          -18026402785 INDEX=            125
a'=                               1 b'=               -8422826
c'=                      -18026402785 ind'=                  125

(209) A=   1 B=          -15437860 C=          -37542026471 INDEX=            239
a'=                               1 b'=              -15437860
c'=                      -37542026471 ind'=                  239

(210) A=   1 B=          -64511940 C=            333632654163 INDEX=           2175
a'=                               1 b'=              -64511940
c'=                       333632654163 ind'=                 2175

(211) A=   0 B=           -6417253 C=             7594662227 INDEX=             35
a'=                               0 b'=               -6417253
c'=                        7594662227 ind'=                   35
```

```
(212) A=   1 B=       -162509618 C=                    969231237605 INDEX=          4481
a'=                             1 b'=                     -162509618
c'=                   969231237605 ind'=                      4481

(213) A=   0 B=        -63052261 C=                    192707758079 INDEX=             1
a'=                             0 b'=                      -63052261
c'=                   192707758079 ind'=                         1

(214) A=   1 B=         4840528 C=                     -43711446453 INDEX=           357
a'=                             1 b'=                       4840528
c'=                   -43711446453 ind'=                       357

(215) A=   1 B=       273650492 C=                    -381238283093 INDEX=         14503
a'=                         23356 b'=                   116716469
c'=                 1011912148327 ind'=                    8353

(216) A=   1 B=         -405128 C=                      -988990336 INDEX=             8
a'=                             1 b'=                       -405128
c'=                    -988990336 ind'=                         8

(217) A=   1 B=        -1037004 C=                     -25092112500 INDEX=           204
a'=                             1 b'=                      -1037004
c'=                   -25092112500 ind'=                       204

(218) A=   1 B=        61988252 C=                     -110449629248 INDEX=          1772
a'=                         39449 b'=                    -8527750
c'=                  5426750000 ind'=                       1750

(219) A=   0 B=       117299447 C=                     417855529048 INDEX=          5230
a'=                         30935 b'=                    38425278
c'=                  57855703480 ind'=                      3326

(220) A=   1 B=        -4214152 C=                      -3473480828 INDEX=             8
a'=                             1 b'=                      -4214152
c'=                   -3473480828 ind'=                        8

(221) A=   1 B=       -329389712 C=                    2410065097188 INDEX=          5832
a'=                        170927 b'=                    -75692400
c'=                   8398080000 ind'=                       1200

(222) A=   1 B=       -169730694 C=                    -912141138280 INDEX=          2666
a'=                             1 b'=                      -169730694
c'=                 -912141138280 ind'=                      2666

(223) A=   1 B=       -186514370 C=                   -1121696931832 INDEX=          4430
a'=                             1 b'=                      -186514370
c'=                 -1121696931832 ind'=                     4430

(224) A=   0 B=        -44409133 C=                     437770901325 INDEX=          3437
a'=                             0 b'=                      -44409133
c'=                   437770901325 ind'=                       3437

(225) A=   1 B=       203763764 C=                     140947971385 INDEX=          9175
a'=                             1 b'=                       203763764
c'=                   140947971385 ind'=                       9175

(226) A=   1 B=        56737232 C=                     214369012249 INDEX=          2197
a'=                             1 b'=                       56737232
c'=                   214369012249 ind'=                       2197

(227) A=   1 B=       -90299874 C=                    1185834224817 INDEX=          9261
a'=                             1 b'=                      -90299874
c'=                  1185834224817 ind'=                       9261

(228) A=   1 B=       301855142 C=                    9711455357407 INDEX=         80653
a'=                          3879 b'=                     -8058832
```

```
c'=                                158758091077 ind'=                1403

(229) A=   0 B=      -54069835 C=                285624163803 INDEX=          1961
a'=                                          0 b'=                -54069835
c'=                                285624163803 ind'=                1961

(230) A=   0 B=       83417105 C=                625462671659 INDEX=          5617
a'=                                      30884 b'=                 -2054625
c'=                                 87765625 ind'=                   125

(231) A=   0 B=     -173554621 C=               1582147595011 INDEX=         10691
a'=                                      51601 b'=                -213023148
c'=                                222987414899 ind'=                4567

(232) A=   1 B=        4045644 C=                 -1101450393 INDEX=            27
a'=                                          1 b'=                  4045644
c'=                                 -1101450393 ind'=                   27

(233) A=   1 B=      -85055610 C=                -408663110371 INDEX=          2239
a'=                                          1 b'=                 -85055610
c'=                                -408663110371 ind'=                2239

(234) A=   1 B=       -4886248 C=                 -28956604883 INDEX=           233
a'=                                          1 b'=                  -4886248
c'=                                 -28956604883 ind'=                 233

(235) A=   0 B=         248789 C=                   113328771 INDEX=             1
a'=                                          0 b'=                    248789
c'=                                    113328771 ind'=                    1

(236) A=   0 B=     -314208565 C=                7431925177476 INDEX=         57862
a'=                                      -3631 b'=                 30538944
c'=                                172775006208 ind'=                1728

(237) A=   0 B=     -267381235 C=                2730856358926 INDEX=         17488
a'=                                      -7801 b'=                 81186816
c'=                                293399953408 ind'=                4096

(238) A=   1 B=      -27304798 C=                -598508209784 INDEX=          4846
a'=                                          1 b'=                 -27304798
c'=                                -598508209784 ind'=                4846

(239) A=   0 B=      -84486937 C=                 585531673080 INDEX=          4094
a'=                                          0 b'=                 -84486937
c'=                                585531673080 ind'=                4094

(240) A=   1 B=        -500634 C=                  -183780163 INDEX=             1
a'=                                          1 b'=                    -500634
c'=                                 -183780163 ind'=                       1

(241) A=   1 B=       77864448 C=                 -55347064183 INDEX=          2197
a'=                                      36349 b'=                  4385678
c'=                                 7063023253 ind'=                1793

(242) A=   1 B=     -256305236 C=                1914857554485 INDEX=          8805
a'=                                          1 b'=                 -256305236
c'=                                1914857554485 ind'=                8805

(243) A=   1 B=       43553236 C=                 -82247585503 INDEX=          1121
a'=                                          1 b'=                  43553236
c'=                                 -82247585503 ind'=                1121

(244) A=   1 B=       50377652 C=                 -854897483935 INDEX=          7041
a'=                                      37257 b'=                 82582400
c'=                                 75519125625 ind'=                3275
```

```
(245) A=    1 B=       229601376 C=          873754494527 INDEX=          13001
a'=                        18521 b'=              45395990
c'=                798095312225 ind'=                7835

(246) A=    0 B=          277541 C=             982250842 INDEX=              8
a'=                            0 b'=                277541
c'=                    982250842 ind'=                   8

(247) A=    1 B=          447932 C=             -42395309 INDEX=              1
a'=                            1 b'=                447932
c'=                    -42395309 ind'=                   1

(248) A=    1 B=       -55161230 C=          161956508549 INDEX=            301
a'=                            1 b'=             -55161230
c'=                161956508549 ind'=                 301

(249) A=    1 B=         -431348 C=            -164505319 INDEX=              1
a'=                            1 b'=               -431348
c'=                    -164505319 ind'=                   1

(250) A=    0 B=       -39134035 C=           94233154466 INDEX=              8
a'=                            0 b'=             -39134035
c'=                 94233154466 ind'=                   8

(251) A=    1 B=       283863602 C=         -2502604151216 INDEX=          25262
a'=                        11255 b'=               4812800
c'=                423826030592 ind'=                4096

(252) A=    0 B=       167695091 C=          1900643858733 INDEX=          16883
a'=                        10402 b'=             -27772875
c'=                547951423347 ind'=                5697

(253) A=    1 B=        -6986372 C=           -11842651777 INDEX=             77
a'=                            1 b'=              -6986372
c'=                -11842651777 ind'=                  77

(254) A=    0 B=        -4680385 C=            3899299527 INDEX=              1
a'=                            0 b'=              -4680385
c'=                  3899299527 ind'=                   1

(255) A=    1 B=      -154111062 C=           787117985568 INDEX=           2262
a'=                            1 b'=            -154111062
c'=                787117985568 ind'=                2262

(256) A=    0 B=       184316675 C=            91669392091 INDEX=           7867
a'=                        25106 b'=              30907683
c'=                189890255323 ind'=                4913

(257) A=    1 B=      -224024494 C=         -1802089496528 INDEX=          10226
a'=                       -15603 b'=             114788378
c'=                696682204616 ind'=                8254

(258) A=    1 B=        56530812 C=            61471749311 INDEX=           1421
a'=                            1 b'=              56530812
c'=                 61471749311 ind'=                1421

(259) A=    1 B=          -27958 C=              122986561 INDEX=              1
a'=                            1 b'=                -27958
c'=                    122986561 ind'=                   1

(260) A=    0 B=       177036665 C=           976848244599 INDEX=          10837
a'=                        17045 b'=             -28180800
c'=                373536662517 ind'=                5871

(261) A=    1 B=        97415392 C=          -106339559749 INDEX=           3131
a'=                            1 b'=              97415392
```

```
c'=                                -106339559749 ind'=                3131

(262) A=   0 B=        -141832429 C=                858757688652 INDEX=          4562
a'=                             0 b'=                -141832429
c'=                   858757688652 ind'=                4562

(263) A=   0 B=        -341818747 C=               2435545829114 INDEX=          1000
a'=                             0 b'=                -341818747
c'=                  2435545829114 ind'=                1000

(264) A=   0 B=         215749529 C=               3781857288541 INDEX=         32311
a'=                          7139 b'=                 -21080190
c'=                   320809489111 ind'=                3151

(265) A=   1 B=         -63249254 C=               -193692018585 INDEX=            39
a'=                             1 b'=                 -63249254
c'=                  -193692018585 ind'=                  39

(266) A=   0 B=         -91510591 C=                387066210639 INDEX=          1549
a'=                             0 b'=                 -91510591
c'=                   387066210639 ind'=                1549

(267) A=   0 B=           4379153 C=                 14962716289 INDEX=           125
a'=                             0 b'=                  4379153
c'=                    14962716289 ind'=                 125

(268) A=   1 B=         104062468 C=                537078805473 INDEX=          5487
a'=                         33719 b'=                 74382432
c'=                   125002249623 ind'=                4773

(269) A=   1 B=         -28334936 C=                -71770632643 INDEX=           343
a'=                             1 b'=                 -28334936
c'=                   -71770632643 ind'=                 343

(270) A=   0 B=        -232201423 C=               1486888961330 INDEX=          4852
a'=                             0 b'=                -232201423
c'=                  1486888961330 ind'=                4852

(271) A=   1 B=         216467520 C=               -1177924893696 INDEX=         13824
a'=                         15997 b'=                 -17751300
c'=                   310592102400 ind'=                4740

(272) A=   1 B=         233918198 C=                 693918314728 INDEX=         12538
a'=                         19983 b'=                  56504000
c'=                   802432000000 ind'=                8000

(273) A=   1 B=        -156796678 C=                 904220204624 INDEX=          4038
a'=                             1 b'=                -156796678
c'=                   904220204624 ind'=                4038

(274) A=   1 B=        -194360668 C=               2433773559481 INDEX=         17881
a'=                         -5460 b'=                  80626655
c'=                   400557448609 ind'=                4733

(275) A=   0 B=        -300041485 C=               2722247114149 INDEX=         15013
a'=                        -10546 b'=                  90084411
c'=                   286570561093 ind'=                4369

(276) A=   1 B=          35173928 C=                -342052559897 INDEX=          2857
a'=                             1 b'=                  35173928
c'=                  -342052559897 ind'=                2857

(277) A=   1 B=         302479142 C=               -8774211316495 INDEX=         73221
a'=                          4443 b'=                 -12226606
c'=                   159733734909 ind'=                1477
```

```
(278) A=   0 B=       -151466809 C=                1197226309927 INDEX=          7793
a'=                            0 b'=                 -151466809
c'=                1197226309927 ind'=                   7793

(279) A=   0 B=        -68680855 C=                 223103607011 INDEX=           343
a'=                            0 b'=                  -68680855
c'=                 223103607011 ind'=                     343

(280) A=   1 B=        261171038 C=                25814991163528 INDEX=        210322
a'=                         1247 b'=                  -1053860
c'=                  70752320800 ind'=                     580

(281) A=   1 B=        113598508 C=                 828915535712 INDEX=          7732
a'=                            1 b'=                  113598508
c'=                 828915535712 ind'=                    7732

(282) A=   1 B=          1411600 C=                  -898638801 INDEX=             9
a'=                            1 b'=                    1411600
c'=                  -898638801 ind'=                        9

(283) A=   1 B=       -169531428 C=                -870287344489 INDEX=          1531
a'=                            1 b'=                 -169531428
c'=                -870287344489 ind'=                    1531

(284) A=   1 B=          7394776 C=                  1432445840 INDEX=            64
a'=                            1 b'=                    7394776
c'=                 1432445840 ind'=                       64

(285) A=   0 B=        127943561 C=                 234086055067 INDEX=          4913
a'=                            0 b'=                  127943561
c'=                 234086055067 ind'=                    4913

(286) A=   1 B=       -112788098 C=                -518988264091 INDEX=          1937
a'=                            1 b'=                 -112788098
c'=                -518988264091 ind'=                    1937

(287) A=   1 B=        -20791530 C=                  76308027275 INDEX=           545
a'=                            1 b'=                  -20791530
c'=                  76308027275 ind'=                     545

(288) A=   0 B=        -19546105 C=                  48498666249 INDEX=           287
a'=                            0 b'=                  -19546105
c'=                  48498666249 ind'=                     287

(289) A=   1 B=       -103425634 C=                -608547020768 INDEX=          3694
a'=                            1 b'=                 -103425634
c'=                -608547020768 ind'=                    3694

(290) A=   1 B=         82747442 C=                  274661704496 INDEX=          3246
a'=                            1 b'=                   82747442
c'=                 274661704496 ind'=                    3246

(291) A=   1 B=        -83171598 C=                  291942641187 INDEX=            27
a'=                            1 b'=                  -83171598
c'=                 291942641187 ind'=                      27

(292) A=   1 B=       -166537202 C=                 1046507723153 INDEX=          5213
a'=                            1 b'=                 -166537202
c'=                1046507723153 ind'=                    5213

(293) A=   1 B=       -214114338 C=                -1571372808715 INDEX=          8191
a'=                            1 b'=                 -214114338
c'=               -1571372808715 ind'=                    8191

(294) A=   1 B=         14963876 C=                   -86836911175 INDEX=           729
a'=                            1 b'=                   14963876
```

```
c'=                                  -86836911175 ind'=                  729

(295) A=   0 B=          363179 C=                  89599201 INDEX=          1
a'=                                            0 b'=                  363179
c'=                                     89599201 ind'=                       1

(296) A=   1 B=       214024806 C=                -728510162553 INDEX=      11451
a'=                                        19089 b'=                -13057300
c'=                                  142608933291 ind'=                    3529

(297) A=   0 B=          840173 C=                   7865310510 INDEX=         64
a'=                                            0 b'=                  840173
c'=                                   7865310510 ind'=                      64

(298) A=   0 B=         -4938835 C=                   8932981522 INDEX=         64
a'=                                            0 b'=                 -4938835
c'=                                   8932981522 ind'=                      64

(299) A=   1 B=         27072494 C=                 100715748344 INDEX=        930
a'=                                            1 b'=                 27072494
c'=                                 100715748344 ind'=                     930

(300) A=   0 B=        164138645 C=                1544125040998 INDEX=      14176
a'=                                        12443 b'=                -36329496
c'=                                  508976011264 ind'=                    5992

(301) A=   1 B=        -22443638 C=                -224281051633 INDEX=       1793
a'=                                            1 b'=                 -22443638
c'=                                 -224281051633 ind'=                    1793

(302) A=   1 B=        133935278 C=                -147337609607 INDEX=       4997
a'=                                        27438 b'=                 -1058155
c'=                                    587892053 ind'=                     343

(303) A=   0 B=         43428011 C=                 246718902693 INDEX=       2197
a'=                                            0 b'=                  43428011
c'=                                  246718902693 ind'=                    2197

(304) A=   1 B=         -2311594 C=                  -1359093203 INDEX=          1
a'=                                            1 b'=                 -2311594
c'=                                  -1359093203 ind'=                       1

(305) A=   0 B=       -171055261 C=                 876518579059 INDEX=       1331
a'=                                            0 b'=                 -171055261
c'=                                  876518579059 ind'=                    1331

(306) A=   1 B=       -273633234 C=               -2202166233013 INDEX=      10951
a'=                                       -12134 b'=                 111231737
c'=                                  320870531119 ind'=                    5413

(307) A=   1 B=        -37604456 C=                -151678998400 INDEX=       1000
a'=                                            1 b'=                 -37604456
c'=                                 -151678998400 ind'=                    1000

(308) A=   1 B=        -77064592 C=                -267924421868 INDEX=        512
a'=                                            1 b'=                 -77064592
c'=                                 -267924421868 ind'=                     512

(309) A=   1 B=        147879750 C=                -150060222181 INDEX=       5759
a'=                                        26405 b'=                  2803304
c'=                                   3603296879 ind'=                     791

(310) A=   1 B=       -274728474 C=               -1796928604353 INDEX=       3219
a'=                                            1 b'=                 -274728474
c'=                                 -1796928604353 ind'=                    3219
```

```
(311) A=   0 B=          -323924395 C=                    4612526088486 INDEX=          32768
a'=                             -8681 b'=                       35319726
c'=                      345260556288 ind'=                         3246

(312) A=   1 B=           -86598090 C=                     373344951488 INDEX=           1690
a'=                                1 b'=                      -86598090
c'=                      373344951488 ind'=                         1690

(313) A=   1 B=           -8220652 C=                       38349456113 INDEX=            303
a'=                                1 b'=                       -8220652
c'=                       38349456113 ind'=                          303

(314) A=   1 B=          -215294954 C=                    1421008043135 INDEX=           5981
a'=                             -4658 b'=                      141305767
c'=                      212383402061 ind'=                         5959

(315) A=   1 B=           -26633680 C=                     -52913797811 INDEX=              1
a'=                                1 b'=                      -26633680
c'=                      -52913797811 ind'=                            1

(316) A=   1 B=           96687214 C=                      -195858858861 INDEX=          3375
a'=                                1 b'=                       96687214
c'=                     -195858858861 ind'=                         3375

(317) A=   0 B=          -133256587 C=                     592280561209 INDEX=           125
a'=                                0 b'=                      -133256587
c'=                      592280561209 ind'=                          125

(318) A=   1 B=           63231854 C=                       23307887605 INDEX=           1585
a'=                                1 b'=                       63231854
c'=                       23307887605 ind'=                          1585

(319) A=   1 B=          -236900088 C=                    3494050661115 INDEX=          26019
a'=                             36963 b'=                      -21527794
c'=                      3353354739 ind'=                           359

(320) A=   0 B=           -22277527 C=                     2424450175115 INDEX=          19711
a'=                             -1084 b'=                       10263477
c'=                      759892184191 ind'=                         6209

(321) A=   1 B=          -218891712 C=                    -1246572803152 INDEX=             8
a'=                                1 b'=                      -218891712
c'=                     -1246572803152 ind'=                           8

(322) A=   1 B=           -17092358 C=                      -28124356528 INDEX=            58
a'=                                1 b'=                      -17092358
c'=                      -28124356528 ind'=                           58

(323) A=   0 B=           219418295 C=                     3753881807448 INDEX=          32174
a'=                             6823 b'=                        2056626
c'=                      432404274744 ind'=                         3666

(324) A=   1 B=           67995894 C=                      -213754089256 INDEX=          2470
a'=                                1 b'=                       67995894
c'=                     -213754089256 ind'=                         2470

(325) A=   1 B=           33271162 C=                       141940092251 INDEX=          1301
a'=                                1 b'=                       33271162
c'=                      141940092251 ind'=                         1301

(326) A=   1 B=           61778314 C=                       -34223942361 INDEX=          1545
a'=                                1 b'=                       61778314
c'=                      -34223942361 ind'=                         1545

(327) A=   1 B=          -31496498 C=                      238758880655 INDEX=           1861
a'=                                1 b'=                      -31496498
```

```
c'=                                238758880655 ind'=                    1861

(328) A=   1 B=          21970932 C=          -125858975503 INDEX=          1073
a'=                              1 b'=            21970932
c'=                   -125858975503 ind'=             1073

(329) A=   1 B=        -198219818 C=          1923901051535 INDEX=         12979
a'=                         -10478 b'=            90490049
c'=                   569312530291 ind'=             6623

(330) A=   0 B=          51497501 C=           132921790723 INDEX=          1583
a'=                              0 b'=            51497501
c'=                   132921790723 ind'=             1583

(331) A=   1 B=        -171504066 C=         -4198266209241 INDEX=         33405
a'=                         -5034 b'=            11404367
c'=                   433169349405 ind'=             3601

(332) A=   1 B=          46814476 C=          -392968383145 INDEX=          3349
a'=                              1 b'=            46814476
c'=                   -392968383145 ind'=             3349

(333) A=   1 B=        -168446152 C=          1000189517563 INDEX=          4397
a'=                              1 b'=          -168446152
c'=                  1000189517563 ind'=             4397

(334) A=   0 B=         115843265 C=           262290627931 INDEX=          4447
a'=                              0 b'=           115843265
c'=                   262290627931 ind'=             4447

(335) A=   0 B=           7358039 C=            76973716749 INDEX=           629
a'=                              0 b'=             7358039
c'=                    76973716749 ind'=              629

(336) A=   1 B=          11125038 C=            47976756827 INDEX=           407
a'=                              1 b'=            11125038
c'=                    47976756827 ind'=              407

(337) A=   1 B=         212418860 C=           384071072188 INDEX=         10180
a'=                              1 b'=           212418860
c'=                   384071072188 ind'=            10180

(338) A=   0 B=         -49855579 C=           149410093302 INDEX=           512
a'=                              0 b'=           -49855579
c'=                   149410093302 ind'=              512

(339) A=   1 B=          21052726 C=            91894019960 INDEX=           806
a'=                              1 b'=            21052726
c'=                    91894019960 ind'=              806

(340) A=   1 B=         -11945612 C=           101114500172 INDEX=           812
a'=                              1 b'=           -11945612
c'=                   101114500172 ind'=              812

(341) A=   1 B=         150231566 C=          -630577381760 INDEX=          7714
a'=                              1 b'=           150231566
c'=                  -630577381760 ind'=             7714

(342) A=   1 B=         -75735576 C=           318038623524 INDEX=          1560
a'=                              1 b'=           -75735576
c'=                   318038623524 ind'=             1560

(343) A=   1 B=          -3609768 C=             2815958852 INDEX=             8
a'=                              1 b'=            -3609768
c'=                    2815958852 ind'=                8
```

(344) A= 0 B= 162044993 C=	539214992450 INDEX=	7804
a'= 0 b'=	162044993
c'= 539214992450 ind'=	7804
(345) A= 1 B= -108109196 C=	916180554057 INDEX=	6567
a'= 1 b'=	-108109196
c'= 916180554057 ind'=	6567
(346) A= 0 B= 145704857 C=	10635298638095 INDEX=	86653
a'= 1769 b'=	-6606450
c'= 166219950925 ind'=	1385
(347) A= 0 B= 332833931 C=	5221056717713 INDEX=	46513
a'= 62024 b'=	15041807
c'= 1109844065 ind'=	671
(348) A= 1 B= 139336414 C=	5653524313827 INDEX=	46257
a'= 3046 b'=	-5618175
c'= 311495794425 ind'=	2595
(349) A= 1 B= 80108200 C=	424232714873 INDEX=	4115
a'= 1 b'=	80108200
c'= 424232714873 ind'=	4115
(350) A= 1 B= 98453470 C=	209803241559 INDEX=	3501
a'= 1 b'=	98453470
c'= 209803241559 ind'=	3501
(351) A= 1 B= -236222378 C=	3611934877457 INDEX=	27083
a'= -7711 b'=	36156296
c'= 430947973043 ind'=	3989
(352) A= 0 B= -23384815 C=	96795154981 INDEX=	703
a'= 0 b'=	-23384815
c'= 96795154981 ind'=	703
(353) A= 1 B= -215218436 C=	3210675718935 INDEX=	24165
a'= 38265 b'=	58478
c'= 24165 ind'=	1
(354) A= 1 B= -338346286 C=	-5913028572173 INDEX=	43957
a'= -6758 b'=	27121373
c'= 261059260333 ind'=	2437
(355) A= 1 B= -54640908 C=	272401855325 INDEX=	1819
a'= 1 b'=	-54640908
c'= 272401855325 ind'=	1819
(356) A= 1 B= 150934394 C=	233101019369 INDEX=	6105
a'= 25235 b'=	-6402642
c'= 26692775505 ind'=	2091
(357) A= 1 B= -80341906 C=	-731248367008 INDEX=	5502
a'= 1 b'=	-80341906
c'= -731248367008 ind'=	5502
(358) A= 1 B= -15793088 C=	25401958400 INDEX=	64
a'= 1 b'=	-15793088
c'= 25401958400 ind'=	64
(359) A= 0 B= 297761867 C=	991884239068 INDEX=	17990
a'= 37193 b'=	16422400
c'= 2372927488 ind'=	512
(360) A= 1 B= 89875926 C=	47104097472 INDEX=	2694
a'= 1 b'=	89875926

```
c'=                                  47104097472 ind'=                    2694

(361) A=    1 B=             -448792 C=                    -868771667 INDEX=                    7
a'=                                            1 b'=                    -448792
c'=                                  -868771667 ind'=                         7

(362) A=    1 B=           -117693086 C=                    575969478557 INDEX=                 2443
a'=                                            1 b'=                 -117693086
c'=                                  575969478557 ind'=                    2443

(363) A=    1 B=             66473402 C=                    508240114349 INDEX=                 4467
a'=                                            1 b'=                   66473402
c'=                                  508240114349 ind'=                    4467

(364) A=    1 B=            122044622 C=                   3343133495455 INDEX=                27509
a'=                                         4787 b'=                 -22162738
c'=                                  467175471269 ind'=                    4121
```

Coefficients of the generating polynomials $X^3 + AX^2 + BX + C$ for all the distinct cubic fields with negative fundamental discriminant D.

Note: 1) A, B and C are the coefficients of a generating polynomial of a complex cubic field before Tschirnhausen transformation is applied.
2) A', B' and C' are the coefficients of a generating polynomial of a complex cubic field after Tschirnhausen transformation is applied.

D = -3082320147153282331

(1) A=	1	B=	30583620	C=	-106120857749347728	INDEX=	314082516
a'=			365	b'=	-586369		
c'=			314082516	ind'=	1		
(2) A=	1	B=	-122253415	C=	1293463363500	INDEX=	3505
a'=			1	b'=	-122253415		
c'=			1293463363500	ind'=	3505		
(3) A=	0	B=	-181541786	C=	974031624755	INDEX=	739
a'=			0	b'=	-181541786		
c'=			974031624755	ind'=	739		
(4) A=	0	B=	199178866	C=	543071246255	INDEX=	3583
a'=			0	b'=	199178866		
c'=			543071246255	ind'=	3583		
(5) A=	1	B=	-255530812	C=	5589691406204	INDEX=	15876
a'=			1	b'=	-255530812		
c'=			5589691406204	ind'=	15876		
(6) A=	1	B=	662699071	C=	1664958106176	INDEX=	20049
a'=			49284	b'=	494873716		
c'=			5029771242129	ind'=	15839		
(7) A=	1	B=	95545603	C=	2328454366750	INDEX=	6973
a'=			1	b'=	95545603		
c'=			2328454366750	ind'=	6973		
(8) A=	1	B=	-257428924	C=	1861736178224	INDEX=	2868
a'=			1	b'=	-257428924		
c'=			1861736178224	ind'=	2868		
(9) A=	1	B=	-22251776	C=	182908537536	INDEX=	528
a'=			1	b'=	-22251776		
c'=			182908537536	ind'=	528		
(10) A=	1	B=	337848395	C=	-2005677392250	INDEX=	9235
a'=			1	b'=	337848395		
c'=			-2005677392250	ind'=	9235		
(11) A=	1	B=	-309570806	C=	2135339233108	INDEX=	1202
a'=			1	b'=	-309570806		
c'=			2135339233108	ind'=	1202		
(12) A=	1	B=	-812973035	C=	16300004640058	INDEX=	40375
a'=			-9101	b'=	183964888		
c'=			1022336344000	ind'=	5032		
(13) A=	1	B=	104998529	C=	-423429206322	INDEX=	1753
a'=			1	b'=	104998529		
c'=			-423429206322	ind'=	1753		
(14) A=	0	B=	-75553784	C=	515883825229	INDEX=	1331
a'=			0	b'=	-75553784		

```
c'=                                515883825229 ind'=                    1331

(15) A=   1 B=          -209805459 C=                -1870812214694 INDEX=          4321
a'=                              1 b'=                    -209805459
c'=                 -1870812214694 ind'=                       4321

(16) A=   1 B=          -590197229 C=                 5958323630596 INDEX=          6649
a'=                              1 b'=                    -590197229
c'=                  5958323630596 ind'=                       6649

(17) A=   1 B=          -128493505 C=                  567367621356 INDEX=           259
a'=                              1 b'=                    -128493505
c'=                   567367621356 ind'=                        259

(18) A=   1 B=          -741591399 C=                -17561600076692 INDEX=         46607
a'=                         -12689 b'=                     123795864
c'=                  1585207723968 ind'=                       5832

(19) A=   1 B=          -182291007 C=                 3133068035374 INDEX=          8839
a'=                              1 b'=                    -182291007
c'=                  3133068035374 ind'=                       8839

(20) A=   1 B=          -898465845 C=                10415182217652 INDEX=          3009
a'=                              1 b'=                    -898465845
c'=                 10415182217652 ind'=                       3009

(21) A=   1 B=            18922183 C=                 -376068777110 INDEX=          1117
a'=                              1 b'=                      18922183
c'=                  -376068777110 ind'=                       1117

(22) A=   1 B=           146724169 C=                  194712604294 INDEX=          2105
a'=                              1 b'=                     146724169
c'=                   194712604294 ind'=                       2105

(23) A=   1 B=           -16201429 C=                   26701253678 INDEX=            27
a'=                              1 b'=                     -16201429
c'=                    26701253678 ind'=                         27

(24) A=   0 B=            7580962 C=                  139311205549 INDEX=           413
a'=                              0 b'=                      7580962
c'=                   139311205549 ind'=                        413

(25) A=   0 B=            6078901 C=                   20840352506 INDEX=            64
a'=                              0 b'=                      6078901
c'=                    20840352506 ind'=                         64

(26) A=   1 B=          -868198439 C=               329432802344748 INDEX=        974577
a'=                           -834 b'=                      4421956
c'=                   114658009473 ind'=                        343

(27) A=   1 B=          -546360312 C=                 4915355597524 INDEX=            64
a'=                              1 b'=                    -546360312
c'=                  4915355597524 ind'=                         64

(28) A=   1 B=          -537940002 C=                 6476521262860 INDEX=         12862
a'=                         144817 b'=                     483125059
c'=                   416860622638 ind'=                       5693

(29) A=   1 B=          -563831857 C=                -5498036344584 INDEX=          5671
a'=                              1 b'=                    -563831857
c'=                 -5498036344584 ind'=                       5671

(30) A=   1 B=          -100492019 C=                 -729007893642 INDEX=          1827
a'=                              1 b'=                    -100492019
c'=                  -729007893642 ind'=                       1827
```

```
(31) A=   1 B=          -69672446 C=                  1286631308004 INDEX=          3750
a'=                             1 b'=                     -69672446
c'=                  1286631308004 ind'=                      3750

(32) A=   1 B=         -327635760 C=                -10807268013248 INDEX=         31264
a'=                         71115 b'=                     396901297
c'=                   643549712416 ind'=                      4537

(33) A=   0 B=         -266940662 C=                  2301763118213 INDEX=          4661
a'=                             0 b'=                    -266940662
c'=                  2301763118213 ind'=                      4661

(34) A=   1 B=         -261731665 C=                  2170054954542 INDEX=          4241
a'=                        201823 b'=                    -100059840
c'=                    12663558144 ind'=                      1728

(35) A=   1 B=          221587565 C=                   458459891358 INDEX=          3995
a'=                             1 b'=                     221587565
c'=                   458459891358 ind'=                      3995

(36) A=   1 B=          494122521 C=                 -5885198556426 INDEX=         21447
a'=                         24306 b'=                     -85793084
c'=                  1936814422023 ind'=                      9503

(37) A=   0 B=         -245367257 C=                  1882588100228 INDEX=          3446
a'=                             0 b'=                    -245367257
c'=                  1882588100228 ind'=                      3446

(38) A=   1 B=          276164784 C=                 -2045856649580 INDEX=          8000
a'=                             1 b'=                     276164784
c'=                 -2045856649580 ind'=                      8000

(39) A=   1 B=           -3046599 C=                    -9350451432 INDEX=            27
a'=                             1 b'=                      -3046599
c'=                   -9350451432 ind'=                        27

(40) A=   1 B=          -57287742 C=                   730857204756 INDEX=          2106
a'=                             1 b'=                     -57287742
c'=                   730857204756 ind'=                      2106

(41) A=   1 B=          403433183 C=                   251809882274 INDEX=          9261
a'=                         43683 b'=                       -117056
c'=                    37933056 ind'=                           64

(42) A=   1 B=           72480914 C=                  -370263640492 INDEX=          1302
a'=                             1 b'=                      72480914
c'=                  -370263640492 ind'=                      1302

(43) A=   1 B=          118953691 C=                   204472690144 INDEX=          1597
a'=                             1 b'=                     118953691
c'=                   204472690144 ind'=                      1597

(44) A=   1 B=          285163966 C=                 -1945936183724 INDEX=          7954
a'=                         54303 b'=                     129570025
c'=                   303290991250 ind'=                      6175

(45) A=   0 B=           12730189 C=                    12726586510 INDEX=            64
a'=                             0 b'=                      12730189
c'=                   12726586510 ind'=                        64

(46) A=   1 B=          770541745 C=                 -13123112610518 INDEX=         45851
a'=                         91319 b'=                     270630373
c'=                   245515365836 ind'=                      5941

(47) A=   0 B=           55710502 C=                   407226486753 INDEX=          1295
a'=                             0 b'=                      55710502
```

```
c'=                                407226486753 ind'=                    1295

(48) A=   1 B=          789041331 C=                3282406639768 INDEX=          27053
a'=                            30519 b'=                    87042916
c'=                      1867275539792 ind'=                    8308

(49) A=   1 B=          309238825 C=                -2010030782784 INDEX=          8589
a'=                            1 b'=                   309238825
c'=                     -2010030782784 ind'=                    8589

(50) A=   0 B=           -4055654 C=                   3161793041 INDEX=             1
a'=                            0 b'=                    -4055654
c'=                      3161793041 ind'=                       1

(51) A=   0 B=          -831942938 C=                11136360120063 INDEX=          18415
a'=                       -25433 b'=                   322541682
c'=                      1756326131740 ind'=                    9766

(52) A=   1 B=           10374276 C=                   -7453135844 INDEX=             44
a'=                            1 b'=                    10374276
c'=                     -7453135844 ind'=                      44

(53) A=   1 B=           18738951 C=                 -176668121484 INDEX=           531
a'=                            1 b'=                    18738951
c'=                     -176668121484 ind'=                     531

(54) A=   1 B=          -498541627 C=                -7237424360430 INDEX=          17263
a'=                       119643 b'=                   933861544
c'=                      1957277282752 ind'=                   10648

(55) A=   0 B=           742191418 C=                 4386818239527 INDEX=          26441
a'=                       93963 b'=                    -76371449
c'=                       17035330576 ind'=                    1331

(56) A=   0 B=          -866689532 C=                12199187799637 INDEX=          21419
a'=                       -25840 b'=                   294676902
c'=                      1979324842211 ind'=                    9613

(57) A=   1 B=          704848220 C=                 10987864618956 INDEX=          38884
a'=                       19155 b'=                    98569951
c'=                      3150303950884 ind'=                    9001

(58) A=   1 B=          769554341 C=                -10711716180436 INDEX=          39957
a'=                       19282 b'=                    11435720
c'=                      1942818382653 ind'=                    6973

(59) A=   1 B=          109290825 C=                  -419572462778 INDEX=           1799
a'=                            1 b'=                   109290825
c'=                     -419572462778 ind'=                     1799

(60) A=   1 B=          258309783 C=                 -2270283899490 INDEX=          8217
a'=                       56632 b'=                   165656534
c'=                       363048498153 ind'=                    6647

(61) A=   1 B=          -209138370 C=                 1415943602596 INDEX=          2386
a'=                            1 b'=                  -209138370
c'=                      1415943602596 ind'=                    2386

(62) A=   0 B=          -639087203 C=                 6531485795506 INDEX=          5912
a'=                            0 b'=                  -639087203
c'=                      6531485795506 ind'=                    5912

(63) A=   1 B=          -224764037 C=                 3076514562370 INDEX=          8257
a'=                            1 b'=                  -224764037
c'=                      3076514562370 ind'=                    8257
```

(64) A= 1 B= -196201851 C= 1698938996224 INDEX= 3935
a'= 1 b'= -196201851
c'= 1698938996224 ind'= 3935

(65) A= 1 B= -243939410 C= -1466713713468 INDEX= 66
a'= 1 b'= -243939410
c'= -1466713713468 ind'= 66

(66) A= 1 B= -36273259 C= -260280995464 INDEX= 729
a'= 1 b'= -36273259
c'= -260280995464 ind'= 729

(67) A= 1 B= 774844221 C= -2295982545932 INDEX= 25493
a'= 51334 b'= 641208414
c'= 6544984333797 ind'= 16023

(68) A= 1 B= 213211369 C= 3833475078718 INDEX= 11887
a'= 1 b'= 213211369
c'= 3833475078718 ind'= 11887

(69) A= 1 B= 272056301 C= 668214252656 INDEX= 5481
a'= 1 b'= 272056301
c'= 668214252656 ind'= 5481

(70) A= 1 B= -102797395 C= 1300353980172 INDEX= 3661
a'= 1 b'= -102797395
c'= 1300353980172 ind'= 3661

(71) A= 1 B= 361295383 C= 2086719678280 INDEX= 9967
a'= 1 b'= 361295383
c'= 2086719678280 ind'= 9967

(72) A= 1 B= -81423207 C= 344223490264 INDEX= 581
a'= 1 b'= -81423207
c'= 344223490264 ind'= 581

(73) A= 0 B= 73581703 C= 678865785508 INDEX= 2134
a'= 0 b'= 73581703
c'= 678865785508 ind'= 2134

(74) A= 1 B= 517131503 C= 813327814826 INDEX= 13611
a'= 1 b'= 517131503
c'= 813327814826 ind'= 13611

(75) A= 1 B= -863620859 C= -38903953797756 INDEX= 111453
a'= -6143 b'= 60986072
c'= 772082187072 ind'= 2632

(76) A= 0 B= -522211436 C= 10892898266673 INDEX= 29233
a'= -10688 b'= 208740606
c'= 2024064885553 ind'= 8321

(77) A= 0 B= -336691514 C= 2377915259121 INDEX= 1
a'= 0 b'= -336691514
c'= 2377915259121 ind'= 1

(78) A= 0 B= 3649141 C= 327577270 INDEX= 8
a'= 0 b'= 3649141
c'= 327577270 ind'= 8

(79) A= 1 B= -102709384 C= -708129575152 INDEX= 1728
a'= 1 b'= -102709384
c'= -708129575152 ind'= 1728

(80) A= 0 B= 24081319 C= 82181832428 INDEX= 278
a'= 0 b'= 24081319

```
c'=                                82181832428 ind'=                   278

(81) A=   1 B=        -659360576 C=          -9517320971072 INDEX=          20528
a'=                        -26647 b'=               248819527
c'=                  3770661231152 ind'=                13553

(82) A=   1 B=        -174326884 C=           1449576728336 INDEX=           3396
a'=                            1 b'=           -174326884
c'=                  1449576728336 ind'=                3396

(83) A=   1 B=         -31050600 C=             98789335812 INDEX=            216
a'=                            1 b'=            -31050600
c'=                    98789335812 ind'=                 216

(84) A=   1 B=          60072471 C=           -634347901994 INDEX=           1951
a'=                            1 b'=             60072471
c'=                  -634347901994 ind'=                1951

(85) A=   0 B=          18069808 C=              8442015013 INDEX=             91
a'=                            0 b'=             18069808
c'=                    8442015013 ind'=                  91

(86) A=   1 B=         416053313 C=           -779394469726 INDEX=           9939
a'=                        42486 b'=              -7768082
c'=                  32166589539 ind'=                1799

(87) A=   0 B=          57230401 C=            918900261906 INDEX=           2764
a'=                            0 b'=             57230401
c'=                  918900261906 ind'=                2764

(88) A=   0 B=        -833994461 C=           9305737677968 INDEX=           2402
a'=                            0 b'=            -833994461
c'=                  9305737677968 ind'=               2402

(89) A=   1 B=        -582003419 C=           8869811775024 INDEX=          20817
a'=                       -21494 b'=              244459364
c'=                  3081663101313 ind'=               12167

(90) A=   1 B=        -111389012 C=           1158333155664 INDEX=           3156
a'=                            1 b'=            -111389012
c'=                  1158333155664 ind'=               3156

(91) A=   1 B=        -500446787 C=          -6014755893236 INDEX=          12419
a'=                            1 b'=            -500446787
c'=                 -6014755893236 ind'=               12419

(92) A=   1 B=         134324291 C=           -620454223852 INDEX=           2553
a'=                        71683 b'=              -26006920
c'=                  11823208512 ind'=                2152

(93) A=   1 B=         353934265 C=           -911597086358 INDEX=           8051
a'=                        47571 b'=               31689778
c'=                  92741369036 ind'=                3394

(94) A=   1 B=         134729795 C=           1616464113450 INDEX=           5105
a'=                            1 b'=             134729795
c'=                  1616464113450 ind'=               5105

(95) A=   1 B=        -488459369 C=         -26667009141714 INDEX=          77961
a'=                        83269 b'=                3788125
c'=                  64000000 ind'=                   125

(96) A=   1 B=         324237029 C=          -1725137540446 INDEX=           8385
a'=                            1 b'=             324237029
c'=                 -1725137540446 ind'=               8385
```

```
(97) A=    1 B=        37823264 C=        148033126656 INDEX=        512
a'=                           1 b'=           37823264
c'=                148033126656 ind'=              512

(98) A=    0 B=      -101455763 C=        503016522414 INDEX=        928
a'=                           0 b'=         -101455763
c'=                503016522414 ind'=              928

(99) A=    0 B=      -191609084 C=       2532378781899 INDEX=       6859
a'=                           0 b'=         -191609084
c'=               2532378781899 ind'=             6859

(100) A=    1 B=       59278944 C=        904849475716 INDEX=       2728
a'=                           1 b'=           59278944
c'=                904849475716 ind'=             2728

(101) A=    1 B=      549787619 C=        180325508244 INDEX=      14695
a'=                       37564 b'=            7798450
c'=                134468434375 ind'=             3025

(102) A=    1 B=      250559331 C=        558589625926 INDEX=       4811
a'=                           1 b'=          250559331
c'=                558589625926 ind'=             4811

(103) A=    1 B=     -345310949 C=      -3044670134024 INDEX=       5269
a'=                           1 b'=         -345310949
c'=              -3044670134024 ind'=             5269

(104) A=    1 B=      -38867897 C=       -257712938226 INDEX=        711
a'=                           1 b'=          -38867897
c'=               -257712938226 ind'=              711

(105) A=    1 B=     -253990341 C=       1725738266926 INDEX=       2197
a'=                           1 b'=         -253990341
c'=               1725738266926 ind'=             2197

(106) A=    1 B=      328846366 C=       2872431286828 INDEX=      10882
a'=                       50211 b'=          117695029
c'=                230964454018 ind'=             4607

(107) A=    0 B=      851406232 C=      21592624462469 INDEX=      69893
a'=                       12728 b'=          -40557456
c'=               1003420322253 ind'=             3789

(108) A=    1 B=       34323694 C=      -2702562001964 INDEX=       8002
a'=                           1 b'=           34323694
c'=              -2702562001964 ind'=             8002

(109) A=    1 B=     -101996249 C=       1173487917346 INDEX=       3269
a'=                           1 b'=         -101996249
c'=               1173487917346 ind'=             3269

(110) A=    1 B=     -297133269 C=      -2072243484494 INDEX=       1889
a'=                           1 b'=         -297133269
c'=              -2072243484494 ind'=             1889

(111) A=    0 B=      -23446046 C=         43698397905 INDEX=          1
a'=                           0 b'=          -23446046
c'=                 43698397905 ind'=                1

(112) A=    1 B=     -283023922 C=      -5304973129716 INDEX=      14734
a'=                           1 b'=         -283023922
c'=              -5304973129716 ind'=            14734

(113) A=    1 B=     -138849249 C=        930345514618 INDEX=       2027
a'=                           1 b'=         -138849249
```

```
c'=                                930345514618 ind'=                    2027

(114) A=   1 B=          296510379 C=                  16124836591558 INDEX=          48077
a'=                             6172 b'=                    5706954
c'=                      2363182675317 ind'=                    7011

(115) A=   1 B=          -42009750 C=                    225203100748 INDEX=            590
a'=                                1 b'=                  -42009750
c'=                      225203100748 ind'=                     590

(116) A=   1 B=          232463475 C=                    389645902276 INDEX=           4199
a'=                                1 b'=                  232463475
c'=                      389645902276 ind'=                    4199

(117) A=   1 B=         -364079385 C=                   -5075860999928 INDEX=          12769
a'=                                1 b'=                 -364079385
c'=                     -5075860999928 ind'=                   12769

(118) A=   1 B=          -48852870 C=                    199936711132 INDEX=            446
a'=                                1 b'=                  -48852870
c'=                      199936711132 ind'=                     446

(119) A=   1 B=          391834863 C=                    102597135606 INDEX=           8841
a'=                                1 b'=                  391834863
c'=                      102597135606 ind'=                    8841

(120) A=   1 B=         -651820555 C=                    8788129877856 INDEX=          17809
a'=                           -18091 b'=                   308117706
c'=                      1709678318436 ind'=                    9798

(121) A=   1 B=         -189945376 C=                    1062684067440 INDEX=           1000
a'=                                1 b'=                 -189945376
c'=                      1062684067440 ind'=                    1000

(122) A=   1 B=           -1994936 C=                     -2913128924 INDEX=              8
a'=                                1 b'=                   -1994936
c'=                     -2913128924 ind'=                       8

(123) A=   0 B=          -245643983 C=                    1556764671934 INDEX=           1412
a'=                                0 b'=                  -245643983
c'=                      1556764671934 ind'=                    1412

(124) A=   1 B=          -256273664 C=                    1744052287168 INDEX=           2192
a'=                                1 b'=                  -256273664
c'=                      1744052287168 ind'=                    2192

(125) A=   1 B=          -906638825 C=                  643708647403816 INDEX=        1904911
a'=                             -472 b'=                     840750
c'=                       59678956719 ind'=                     177

(126) A=   1 B=          116510548 C=                    -413356016004 INDEX=           1884
a'=                                1 b'=                  116510548
c'=                     -413356016004 ind'=                    1884

(127) A=   1 B=          -17540759 C=                     29705512104 INDEX=             27
a'=                                1 b'=                  -17540759
c'=                      29705512104 ind'=                      27

(128) A=   1 B=          -12666795 C=                    -246926067318 INDEX=            729
a'=                                1 b'=                  -12666795
c'=                     -246926067318 ind'=                     729

(129) A=   0 B=          -260957867 C=                    1788125293798 INDEX=           2224
a'=                                0 b'=                  -260957867
c'=                      1788125293798 ind'=                    2224
```

```
(130) A=   1 B=          16693491 C=                  244913954436 INDEX=          729
a'=                             1 b'=                   16693491
c'=                   244913954436 ind'=                   729

(131) A=   1 B=         414638434 C=                -6245645755764 INDEX=        20838
a'=                         19935 b'=                   22553239
c'=                  4605774983382 ind'=                  14867

(132) A=   1 B=         246357779 C=                 -378199878070 INDEX=         4545
a'=                             1 b'=                  246357779
c'=                   -378199878070 ind'=                  4545

(133) A=   0 B=         -29282459 C=                   64710069686 INDEX=           64
a'=                             0 b'=                  -29282459
c'=                    64710069686 ind'=                    64

(134) A=   1 B=           8087249 C=                   -2202273142 INDEX=           27
a'=                             1 b'=                    8087249
c'=                    -2202273142 ind'=                    27

(135) A=   1 B=         -923284302 C=                -27247022665940 INDEX=        74038
a'=                         -9357 b'=                   95116249
c'=                   968616128182 ind'=                   3617

(136) A=   1 B=          -74616372 C=                 -328236836724 INDEX=          636
a'=                             1 b'=                  -74616372
c'=                   -328236836724 ind'=                   636

(137) A=   1 B=         -105196554 C=                  1759988539708 INDEX=         5062
a'=                             1 b'=                  -105196554
c'=                   1759988539708 ind'=                  5062

(138) A=   1 B=         -368307539 C=                 -2773449230862 INDEX=         1593
a'=                             1 b'=                  -368307539
c'=                  -2773449230862 ind'=                  1593

(139) A=   0 B=          501227857 C=                 26319868650142 INDEX=        78940
a'=                          6367 b'=                   -8492253
c'=                   1372021485340 ind'=                  4169

(140) A=   1 B=         -197407215 C=                 -3488417517878 INDEX=         9829
a'=                             1 b'=                  -197407215
c'=                  -3488417517878 ind'=                  9829

(141) A=   0 B=           -7587428 C=                   42993736323 INDEX=          125
a'=                             0 b'=                   -7587428
c'=                    42993736323 ind'=                    125

(142) A=   1 B=          778525005 C=                  1246285842292 INDEX=        25019
a'=                         50622 b'=                   -452960228
c'=                   1130093481377 ind'=                  7847

(143) A=   1 B=          -90052749 C=                  -807630326606 INDEX=         2183
a'=                             1 b'=                   -90052749
c'=                   -807630326606 ind'=                  2183

(144) A=   0 B=          335104402 C=                  2717642354097 INDEX=        10655
a'=                         48686 b'=                    79218000
c'=                    121367109375 ind'=                   3375

(145) A=   1 B=          -15619944 C=                    32122527796 INDEX=           64
a'=                             1 b'=                   -15619944
c'=                    32122527796 ind'=                    64

(146) A=   1 B=         -265124929 C=                 -1962997238182 INDEX=         3093
a'=                             1 b'=                  -265124929
```

```
c'=                          -1962997238182 ind'=                  3093

(147) A=   0 B=       204263677 C=                  2458379358978 INDEX=          8000
a'=                             0 b'=                  204263677
c'=                    2458379358978 ind'=                  8000

(148) A=   1 B=       194631501 C=                 -2143069914392 INDEX=          7057
a'=                         56706 b'=                   17456896
c'=                    3487632913 ind'=                     703

(149) A=   1 B=      -767558419 C=                  8208848594738 INDEX=          1863
a'=                             1 b'=                  -767558419
c'=                    8208848594738 ind'=                  1863

(150) A=   1 B=      -314696656 C=                  2149709470500 INDEX=           200
a'=                             1 b'=                  -314696656
c'=                    2149709470500 ind'=                   200

(151) A=   1 B=        -4843375 C=                    -4118208828 INDEX=             1
a'=                             1 b'=                    -4843375
c'=                   -4118208828 ind'=                        1

(152) A=   1 B=       -84490987 C=                   947449927724 INDEX=          2661
a'=                             1 b'=                   -84490987
c'=                     947449927724 ind'=                  2661

(153) A=   0 B=       250572919 C=                   1192758665500 INDEX=          5734
a'=                             0 b'=                   250572919
c'=                    1192758665500 ind'=                  5734

(154) A=   1 B=         2840671 C=                    -8933632716 INDEX=            27
a'=                             1 b'=                     2840671
c'=                   -8933632716 ind'=                       27

(155) A=   1 B=       229557026 C=                   1673247676988 INDEX=          6342
a'=                             1 b'=                   229557026
c'=                    1673247676988 ind'=                  6342

(156) A=   0 B=      -223327238 C=                   4733226861019 INDEX=         13483
a'=                         88114 b'=                   224426430
c'=                     160388388283 ind'=                  3449

(157) A=   1 B=       -22033247 C=                    -40846869510 INDEX=            27
a'=                             1 b'=                   -22033247
c'=                    -40846869510 ind'=                       27

(158) A=   1 B=       322970699 C=                    532202228736 INDEX=          6797
a'=                             1 b'=                   322970699
c'=                     532202228736 ind'=                  6797

(159) A=   1 B=       447189738 C=                   1233025704436 INDEX=         11374
a'=                             1 b'=                   447189738
c'=                    1233025704436 ind'=                  11374

(160) A=   1 B=      -320148311 C=                  -5279384086622 INDEX=         14197
a'=                         89237 b'=                  -162704358
c'=                     78937648308 ind'=                   2358

(161) A=   1 B=        -5799400 C=                    -73180794364 INDEX=           216
a'=                             1 b'=                    -5799400
c'=                    -73180794364 ind'=                   216

(162) A=   1 B=       517090345 C=                   28311147330678 INDEX=         84855
a'=                          6695 b'=                   -44857246
c'=                    1115663017980 ind'=                  3626
```

```
(163) A=   1 B=        -604052331 C=          10748026051506 INDEX=       26943
a'=                        -19237 b'=            169500152
c'=                3009064938432 ind'=               10568

(164) A=   1 B=         653474051 C=           -732675818196 INDEX=       19153
a'=                        58077 b'=           -440217479
c'=                 898952694148 ind'=               6859

(165) A=   1 B=          24832403 C=            241670719844 INDEX=         729
a'=                       133827 b'=             -945344
c'=                      2985984 ind'=                64

(166) A=   1 B=        -306583892 C=          -2536898131344 INDEX=        4356
a'=                            1 b'=          -306583892
c'=               -2536898131344 ind'=               4356

(167) A=   0 B=        -305468033 C=           2628319016732 INDEX=        4850
a'=                       201269 b'=          -295463355
c'=                110120341250 ind'=               4765

(168) A=   1 B=        -303813864 C=          85590523350324 INDEX=      253248
a'=                        -1193 b'=             2996081
c'=                 448644280128 ind'=               1331

(169) A=   1 B=           171921 C=             -336702554 INDEX=           1
a'=                            1 b'=             171921
c'=                  -336702554 ind'=                  1

(170) A=   0 B=           855898 C=             145847313 INDEX=           1
a'=                            0 b'=             855898
c'=                  145847313 ind'=                  1

(171) A=   1 B=        113373298 C=            487906893364 INDEX=        1994
a'=                            1 b'=          113373298
c'=                 487906893364 ind'=               1994

(172) A=   1 B=         18533745 C=           -134729263028 INDEX=         409
a'=                            1 b'=           18533745
c'=                -134729263028 ind'=                409

(173) A=   0 B=        101664307 C=            223448431384 INDEX=        1342
a'=                            0 b'=          101664307
c'=                 223448431384 ind'=               1342

(174) A=   0 B=        150616876 C=            9978831089321 INDEX=       29609
a'=                         5087 b'=            -1262736
c'=                3831800649984 ind'=              11376

(175) A=   0 B=        -14091443 C=              20538807234 INDEX=           8
a'=                            0 b'=          -14091443
c'=                  20538807234 ind'=                  8

(176) A=   1 B=        -387147729 C=           -3369422479346 INDEX=        4913
a'=                            1 b'=          -387147729
c'=               -3369422479346 ind'=               4913

(177) A=   1 B=        -517478160 C=           -4537909060844 INDEX=         736
a'=                            1 b'=          -517478160
c'=               -4537909060844 ind'=                736

(178) A=   1 B=          -1410392 C=             2778356800 INDEX=           8
a'=                            1 b'=            -1410392
c'=                  2778356800 ind'=                  8

(179) A=   1 B=        -150975129 C=            -866172378884 INDEX=        1451
a'=                            1 b'=          -150975129
```

```
c'=                                -866172378884 ind'=                    1451

(180) A=   1 B=          63205653 C=                    189328270896 INDEX=                 801
a'=                                           1 b'=                63205653
c'=                                189328270896 ind'=                     801

(181) A=   0 B=         -41612807 C=                    300767687318 INDEX=                 836
a'=                                           0 b'=               -41612807
c'=                                300767687318 ind'=                     836

(182) A=   0 B=         -674223917 C=                   7142503615576 INDEX=                7010
a'=                                           0 b'=              -674223917
c'=                               7142503615576 ind'=                    7010

(183) A=   1 B=          -89077992 C=                  -2523844347020 INDEX=                7408
a'=                                           1 b'=               -89077992
c'=                               -2523844347020 ind'=                   7408

(184) A=   1 B=         -232032942 C=                  -2359655738244 INDEX=                5706
a'=                                           1 b'=              -232032942
c'=                               -2359655738244 ind'=                   5706

(185) A=   0 B=          108866566 C=                    105304291971 INDEX=                1331
a'=                                           0 b'=               108866566
c'=                                105304291971 ind'=                    1331

(186) A=   1 B=         -508828037 C=                   53802052515736 INDEX=              158699
a'=                                       -3148 b'=                11063866
c'=                                700529284499 ind'=                    2101

(187) A=   1 B=         -308118810 C=                  -3636926593308 INDEX=                8826
a'=                                           1 b'=              -308118810
c'=                               -3636926593308 ind'=                   8826

(188) A=   1 B=          90704546 C=                    184920633396 INDEX=                1126
a'=                                           1 b'=                90704546
c'=                                184920633396 ind'=                    1126

(189) A=   1 B=          46732795 C=                    -660673802808 INDEX=                1989
a'=                                       96399 b'=                 1334848
c'=                                8146944 ind'=                         64

(190) A=   1 B=         -86958304 C=                    312097765764 INDEX=                   8
a'=                                           1 b'=               -86958304
c'=                                312097765764 ind'=                       8

(191) A=   1 B=          -5677249 C=                     23885857076 INDEX=                  69
a'=                                           1 b'=                -5677249
c'=                                 23885857076 ind'=                      69

(192) A=   1 B=          49467223 C=                   -1293554125074 INDEX=                3849
a'=                                           1 b'=                49467223
c'=                               -1293554125074 ind'=                   3849

(193) A=   1 B=           3663808 C=                     -140748560 INDEX=                   8
a'=                                           1 b'=                 3663808
c'=                                -140748560 ind'=                       8

(194) A=   1 B=          30024479 C=                    122078395896 INDEX=                 407
a'=                                           1 b'=                30024479
c'=                                122078395896 ind'=                     407

(195) A=   0 B=         -264723941 C=                   1754728898248 INDEX=                1702
a'=                                           0 b'=              -264723941
c'=                               1754728898248 ind'=                    1702
```

(196) A=	1 B=	588767383 C=		178298235730 INDEX=		16283
a'=			40552 b'=		175140750	
c'=		2327199333075 ind'=			11955	
(197) A=	0 B=	28296496 C=		100370573865 INDEX=		343
a'=			0 b'=		28296496	
c'=		100370573865 ind'=			343	
(198) A=	1 B=	-15813771 C=		-25872131124 INDEX=		27
a'=			1 b'=		-15813771	
c'=		-25872131124 ind'=			27	
(199) A=	1 B=	583751753 C=		753739697744 INDEX=		16221
a'=			146156 b'=		95658970	
c'=		16133606027 ind'=			1331	
(200) A=	1 B=	217929008 C=		2706228896420 INDEX=		8808
a'=			58433 b'=		171174869	
c'=		289899192552 ind'=			5737	
(201) A=	1 B=	-426303616 C=		3728355335348 INDEX=		4608
a'=			1 b'=		-426303616	
c'=		3728355335348 ind'=			4608	
(202) A=	1 B=	-871552077 C=		19137858667414 INDEX=		48469
a'=			-15676 b'=		109475490	
c'=		1732691186829 ind'=			5979	
(203) A=	0 B=	-378840752 C=		2873544043443 INDEX=		1331
a'=			0 b'=		-378840752	
c'=		2873544043443 ind'=			1331	
(204) A=	1 B=	-425218315 C=		-4746890606584 INDEX=		9879
a'=			1 b'=		-425218315	
c'=		-4746890606584 ind'=			9879	
(205) A=	1 B=	-20339659 C=		-2286684405216 INDEX=		6767
a'=			73963 b'=		-230533128	
c'=		230160719808 ind'=			5832	
(206) A=	1 B=	289598315 C=		32814586050 INDEX=		5615
a'=			51668 b'=		6049330	
c'=		132351305375 ind'=			4855	
(207) A=	1 B=	-38766815 C=		136244489500 INDEX=		295
a'=			1 b'=		-38766815	
c'=		136244489500 ind'=			295	
(208) A=	0 B=	-518289539 C=		5793908981550 INDEX=		10648
a'=			0 b'=		-518289539	
c'=		5793908981550 ind'=			10648	
(209) A=	0 B=	70797733 C=		248169361126 INDEX=		1000
a'=			0 b'=		70797733	
c'=		248169361126 ind'=			1000	
(210) A=	0 B=	546496 C=		299966591 INDEX=		1
a'=			0 b'=		546496	
c'=		299966591 ind'=			1	
(211) A=	0 B=	-490832753 C=		9901447990436 INDEX=		26558
a'=			-13885 b'=		190738479	
c'=		2638300641662 ind'=			9967	
(212) A=	1 B=	-312848894 C=		3358502389836 INDEX=		7686
a'=			1 b'=		-312848894	

```
c'=                    3358502389836 ind'=                    7686

(213) A=   1 B=        -24207426 C=          -257528096460 INDEX=          750
a'=                            1 b'=             -24207426
c'=                   -257528096460 ind'=             750

(214) A=   1 B=        517267565 C=          5645474267022 INDEX=        21419
a'=                        24159 b'=             9607696
c'=                   3396163740416 ind'=            12592

(215) A=   1 B=        255580293 C=          -767179881956 INDEX=         5179
a'=                            1 b'=           255580293
c'=                   -767179881956 ind'=            5179

(216) A=   0 B=        653650609 C=          4580982555038 INDEX=        23372
a'=                        28013 b'=            16299891
c'=                   1935860713772 ind'=            9101

(217) A=   0 B=        233262922 C=            89080875539 INDEX=         4067
a'=                            0 b'=           233262922
c'=                     89080875539 ind'=            4067

(218) A=   1 B=       -419931587 C=          3342993567880 INDEX=         1343
a'=                            1 b'=          -419931587
c'=                   3342993567880 ind'=            1343

(219) A=   1 B=        -65837635 C=           320832759746 INDEX=          729
a'=                            1 b'=           -65837635
c'=                    320832759746 ind'=             729

(220) A=   1 B=        670938223 C=          -9940876657530 INDEX=        35463
a'=                        54534 b'=            -372729890
c'=                    840556723825 ind'=            9035

(221) A=   1 B=       -197671461 C=          1974728793556 INDEX=         4913
a'=                            1 b'=          -197671461
c'=                   1974728793556 ind'=            4913

(222) A=   0 B=        427128829 C=          1904423524818 INDEX=        11528
a'=                        45839 b'=             101512359
c'=                    390883688712 ind'=            5823

(223) A=   0 B=       -477152696 C=         18538272932417 INDEX=        53567
a'=                        -8692 b'=            36122382
c'=                   2017481547023 ind'=            6137

(224) A=   0 B=        134936356 C=            74046128889 INDEX=         1799
a'=                            0 b'=           134936356
c'=                     74046128889 ind'=            1799

(225) A=   1 B=        258149366 C=          -375566143564 INDEX=         4854
a'=                            1 b'=           258149366
c'=                   -375566143564 ind'=            4854

(226) A=   0 B=          -106382 C=             338139567 INDEX=            1
a'=                            0 b'=             -106382
c'=                    338139567 ind'=               1

(227) A=   1 B=        775538921 C=         -21904723942356 INDEX=        69343
a'=                        11394 b'=            32465104
c'=                   1673771447167 ind'=            4913

(228) A=   1 B=         -1139345 C=             576915712 INDEX=            1
a'=                            1 b'=            -1139345
c'=                    576915712 ind'=               1
```

```
(229) A=   0 B=        543481846 C=                4746363992611 INDEX=          20141
a'=                       142655 b'=                 -192173523
c'=                    66577774374 ind'=                2913

(230) A=   1 B=         67557575 C=                -421587358128 INDEX=           1399
a'=                             1 b'=                 67557575
c'=                  -421587358128 ind'=                1399

(231) A=   1 B=        434986591 C=                -686881565142 INDEX=          10533
a'=                        42419 b'=                  9870074
c'=                    28954837812 ind'=                1658

(232) A=   0 B=        -29782142 C=                 454042841053 INDEX=           1331
a'=                             0 b'=                 -29782142
c'=                   454042841053 ind'=                1331

(233) A=   0 B=           669454 C=                   264029105 INDEX=              1
a'=                             0 b'=                    669454
c'=                    264029105 ind'=                   1

(234) A=   1 B=         -5362811 C=                 10297338108 INDEX=             27
a'=                             1 b'=                  -5362811
c'=                   10297338108 ind'=                  27

(235) A=   1 B=       -182675982 C=                -1302038983116 INDEX=          2634
a'=                             1 b'=                -182675982
c'=                  -1302038983116 ind'=                2634

(236) A=   1 B=        152200463 C=                -762266798844 INDEX=           3109
a'=                             1 b'=                 152200463
c'=                   -762266798844 ind'=                3109

(237) A=   1 B=       -270367474 C=                 7263898254516 INDEX=          20894
a'=                         40209 b'=                 -706538279
c'=                   3130800440414 ind'=               12241

(238) A=   1 B=         -2198879 C=                   1298971636 INDEX=              1
a'=                             1 b'=                  -2198879
c'=                    1298971636 ind'=                  1

(239) A=   1 B=        -27181862 C=                   55734011956 INDEX=            34
a'=                             1 b'=                  -27181862
c'=                    55734011956 ind'=                 34

(240) A=   1 B=        874173045 C=                 18925316417952 INDEX=          63279
a'=                       134315 b'=                   64228273
c'=                    8391375398 ind'=                 1471

(241) A=   1 B=       -584967624 C=                 5739504035524 INDEX=           5368
a'=                             1 b'=                 -584967624
c'=                   5739504035524 ind'=                5368

(242) A=   1 B=        130652003 C=                -219400997794 INDEX=           1821
a'=                             1 b'=                 130652003
c'=                  -219400997794 ind'=                1821

(243) A=   1 B=        -77249365 C=                 1169866367588 INDEX=          3375
a'=                             1 b'=                  -77249365
c'=                   1169866367588 ind'=               3375

(244) A=   1 B=       -265241915 C=                 1712207374726 INDEX=          1211
a'=                             1 b'=                 -265241915
c'=                   1712207374726 ind'=               1211

(245) A=   1 B=        -62951409 C=                 -524108676222 INDEX=          1443
a'=                             1 b'=                  -62951409
```

```
c'=                    -524108676222 ind'=                  1443

(246) A=   1 B=         108134980 C=          -2529710622864 INDEX=          7596
a'=                             1 b'=             108134980
c'=                    -2529710622864 ind'=             7596

(247) A=   0 B=        -148632278 C=            698735187277 INDEX=           125
a'=                             0 b'=            -148632278
c'=                     698735187277 ind'=           125

(248) A=   0 B=        -490888547 C=           4409054142562 INDEX=          4096
a'=                             0 b'=            -490888547
c'=                    4409054142562 ind'=          4096

(249) A=   1 B=         507971099 C=          18993473348088 INDEX=         57707
a'=                         92995 b'=            86792121
c'=                    24857531296 ind'=            2119

(250) A=   1 B=           2322770 C=             3092604828 INDEX=            10
a'=                             1 b'=             2322770
c'=                    3092604828 ind'=               10

(251) A=   1 B=        -725192699 C=         -10707213984056 INDEX=         22567
a'=                        101051 b'=           -363495396
c'=                    330687430128 ind'=           3828

(252) A=   1 B=        -160460591 C=           1487043581638 INDEX=          3743
a'=                             1 b'=            -160460591
c'=                    1487043581638 ind'=          3743

(253) A=   1 B=        -257720747 C=           2612795711614 INDEX=          6131
a'=                             1 b'=            -257720747
c'=                    2612795711614 ind'=          6131

(254) A=   0 B=          -1627544 C=            867672961 INDEX=             1
a'=                             0 b'=              -1627544
c'=                     867672961 ind'=                1

(255) A=   1 B=         366717560 C=           6748400400 INDEX=          8000
a'=                             1 b'=             366717560
c'=                    6748400400 ind'=             8000

(256) A=   1 B=        -102008471 C=            726854948706 INDEX=          1803
a'=                             1 b'=            -102008471
c'=                     726854948706 ind'=           1803

(257) A=   1 B=         244700330 C=           3087928023756 INDEX=         10126
a'=                         55363 b'=           151246705
c'=                    244417023694 ind'=           4913

(258) A=   1 B=        -351114095 C=          -5994640752908 INDEX=         16081
a'=                        100306 b'=           526510558
c'=                    756544812361 ind'=           6859

(259) A=   0 B=         243108949 C=           3526775909850 INDEX=         11296
a'=                         49867 b'=            21230205
c'=                    5300365600 ind'=             685

(260) A=   1 B=        -113746869 C=            -601701987056 INDEX=          1123
a'=                             1 b'=            -113746869
c'=                     -601701987056 ind'=          1123

(261) A=   1 B=         -65506521 C=            208370824804 INDEX=           125
a'=                             1 b'=             -65506521
c'=                     208370824804 ind'=           125
```

```
(262) A=   1 B=       -303525617 C=                2194744346464 INDEX=          2431
a'=                            1 b'=                   -303525617
c'=                2194744346464 ind'=                     2431

(263) A=   0 B=        -22781834 C=                 306620189869 INDEX=           899
a'=                            0 b'=                    -22781834
c'=                 306620189869 ind'=                      899

(264) A=   1 B=        210781180 C=                2142502297296 INDEX=          7236
a'=                            1 b'=                    210781180
c'=                2142502297296 ind'=                     7236

(265) A=   1 B=           653263 C=                   -269706464 INDEX=             1
a'=                            1 b'=                     653263
c'=                   -269706464 ind'=                        1

(266) A=   1 B=       -628907609 C=               -6115981440302 INDEX=          2197
a'=                            1 b'=                   -628907609
c'=               -6115981440302 ind'=                     2197

(267) A=   1 B=        39872184 C=                 -941062456880 INDEX=          2800
a'=                        90785 b'=                    -684639
c'=                      2041200 ind'=                        27

(268) A=   1 B=       -200106924 C=               -2843094352772 INDEX=          7772
a'=                            1 b'=                   -200106924
c'=               -2843094352772 ind'=                     7772

(269) A=   1 B=        204416505 C=               -2566946263050 INDEX=          8295
a'=                        54038 b'=                     3380750
c'=                      129609375 ind'=                      125

(270) A=   1 B=       -628682257 C=               13487143600956 INDEX=         35651
a'=                        65469 b'=                    -163853426
c'=                 107688979244 ind'=                     1738

(271) A=   1 B=       -227790352 C=                1606419374244 INDEX=          2696
a'=                            1 b'=                   -227790352
c'=                1606419374244 ind'=                     2696

(272) A=   1 B=       -265474335 C=                7615693991008 INDEX=         21995
a'=                        46310 b'=                    -545622206
c'=                1699810573595 ind'=                     8791

(273) A=   1 B=        -68000811 C=                2813649872128 INDEX=          8303
a'=                        74310 b'=                    -257077772
c'=                 267026481023 ind'=                     5671

(274) A=   0 B=       -383007584 C=                3293092543269 INDEX=          4699
a'=                            0 b'=                    -383007584
c'=                3293092543269 ind'=                     4699

(275) A=   1 B=       -535657367 C=               23041391281290 INDEX=         66717
a'=                        -7226 b'=                     59387060
c'=                1464386444325 ind'=                     4685

(276) A=   1 B=        33371473 C=                  202042722850 INDEX=           637
a'=                            1 b'=                     33371473
c'=                 202042722850 ind'=                      637

(277) A=   1 B=       -722621382 C=               -8176589319236 INDEX=          9794
a'=                            1 b'=                   -722621382
c'=               -8176589319236 ind'=                     9794

(278) A=   1 B=        188106979 C=               -6120944992694 INDEX=         18353
a'=                        10803 b'=                    -94552646
```

```
c'=                                5382932624228 ind'=                   17126

(279) A=   1 B=        -360943990 C=                -4365237263812 INDEX=          10290
a'=                         115237 b'=                   -549379735
c'=                    669305075250 ind'=                     8065

(280) A=   1 B=          12427381 C=                   -35750552772 INDEX=            117
a'=                              1 b'=                     12427381
c'=                   -35750552772 ind'=                      117

(281) A=   1 B=         390478834 C=                    -7690505916 INDEX=           8790
a'=                              1 b'=                    390478834
c'=                    -7690505916 ind'=                      8790

(282) A=   1 B=         -15416479 C=                    23295701556 INDEX=              1
a'=                              1 b'=                    -15416479
c'=                    23295701556 ind'=                         1

(283) A=   1 B=         633440194 C=                  -292072246412 INDEX=          18182
a'=                              1 b'=                    633440194
c'=                  -292072246412 ind'=                     18182

(284) A=   1 B=         -98180779 C=                  2544505297016 INDEX=           7449
a'=                              1 b'=                    -98180779
c'=                  2544505297016 ind'=                      7449

(285) A=   1 B=         353011418 C=                  1665951251820 INDEX=           9022
a'=                              1 b'=                    353011418
c'=                  1665951251820 ind'=                      9022

(286) A=   0 B=           -738992 C=                     417070977 INDEX=              1
a'=                              0 b'=                      -738992
c'=                    417070977 ind'=                         1

(287) A=   1 B=         654320205 C=                  4692922139646 INDEX=          23589
a'=                          27754 b'=                     -8438092
c'=                  1517632306749 ind'=                      8021

(288) A=   0 B=         173582974 C=                  1246751638037 INDEX=           4517
a'=                              0 b'=                    173582974
c'=                  1246751638037 ind'=                      4517

(289) A=   1 B=        -571612797 C=                  6111353008084 INDEX=           9209
a'=                              1 b'=                   -571612797
c'=                  6111353008084 ind'=                      9209

(290) A=   1 B=         304044154 C=                108372099932676 INDEX=         320802
a'=                            965 b'=                     -4272577
c'=                   353010841602 ind'=                      1049

(291) A=   0 B=         276334141 C=                  2477363196930 INDEX=           9008
a'=                          51773 b'=                     66545199
c'=                    69968459952 ind'=                      2787

(292) A=   1 B=         -59195262 C=                   -901781126540 INDEX=           2618
a'=                              1 b'=                    -59195262
c'=                   -901781126540 ind'=                      2618

(293) A=   0 B=        -531420269 C=                  4783675634816 INDEX=           2386
a'=                              0 b'=                   -531420269
c'=                  4783675634816 ind'=                      2386

(294) A=   0 B=         112885522 C=                   414882289731 INDEX=           1837
a'=                              0 b'=                    112885522
c'=                   414882289731 ind'=                      1837
```

```
(295) A=   0 B=        705329461 C=                  7345916259974 INDEX=      30464
a'=                          90960 b'=                  -259514486
c'=                   203890045343 ind'=                     4913

(296) A=   1 B=        295783445 C=                  2853024292722 INDEX=      10241
a'=                              1 b'=                  295783445
c'=                   2853024292722 ind'=                   10241

(297) A=   1 B=        167389085 C=                  -450926759500 INDEX=       2805
a'=                              1 b'=                  167389085
c'=                   -450926759500 ind'=                    2805

(298) A=   0 B=       -892854272 C=                  14472836505961 INDEX=      30185
a'=                         -17821 b'=                  216604578
c'=                   1330042983140 ind'=                    6638

(299) A=   1 B=          -278015 C=                      342461686 INDEX=          1
a'=                              1 b'=                    -278015
c'=                    342461686 ind'=                         1

(300) A=   1 B=       -382601992 C=                   3195589660944 INDEX=       4096
a'=                              1 b'=                 -382601992
c'=                   3195589660944 ind'=                    4096

(301) A=   0 B=       -119351219 C=                    556545541570 INDEX=        712
a'=                              0 b'=                 -119351219
c'=                    556545541570 ind'=                      712

(302) A=   1 B=       -126316750 C=                  -1889757757308 INDEX=       5354
a'=                              1 b'=                 -126316750
c'=                  -1889757757308 ind'=                    5354

(303) A=   1 B=       -279391519 C=                  -1833120486162 INDEX=       1063
a'=                              1 b'=                 -279391519
c'=                  -1833120486162 ind'=                    1063

(304) A=   1 B=        584610938 C=                  -1462221478396 INDEX=      16674
a'=                          37637 b'=                  152228261
c'=                   2998900952754 ind'=                   13411

(305) A=   1 B=        299471318 C=                   1603207150404 INDEX=       7574
a'=                              1 b'=                  299471318
c'=                   1603207150404 ind'=                    7574

(306) A=   1 B=         -1322425 C=                    -676294074 INDEX=          1
a'=                              1 b'=                   -1322425
c'=                    -676294074 ind'=                         1

(307) A=   0 B=       -522226736 C=                   9835147550965 INDEX=      25739
a'=                         -18832 b'=                  128622000
c'=                   3784035171875 ind'=                   12125

(308) A=   1 B=       -307971237 C=                   4389124568274 INDEX=      11439
a'=                              1 b'=                 -307971237
c'=                   4389124568274 ind'=                   11439

(309) A=   1 B=        124444179 C=                    495659596446 INDEX=       2157
a'=                          75775 b'=                     -86536
c'=                    138048 ind'=                            8

(310) A=   1 B=        188560399 C=                    525884265190 INDEX=       3335
a'=                              1 b'=                  188560399
c'=                    525884265190 ind'=                    3335

(311) A=   0 B=         15235732 C=                    113608383831 INDEX=        343
a'=                              0 b'=                   15235732
```

```
c'=                                  113608383831 ind'=                          343

(312) A=   1 B=          111237745 C=                    3873225536922 INDEX=          11541
a'=                                        54245 b'=                    -49595338
c'=                                  18380704404 ind'=                       1262

(313) A=   1 B=          272009579 C=                    5917155682838 INDEX=          18243
a'=                                        62160 b'=                    544574068
c'=                                2092156149483 ind'=                       10709

(314) A=   0 B=         -479331011 C=                    4127463752962 INDEX=           2512
a'=                                            0 b'=                   -479331011
c'=                                4127463752962 ind'=                        2512

(315) A=   1 B=         -155522399 C=                     871454604136 INDEX=           1331
a'=                                            1 b'=                   -155522399
c'=                                 871454604136 ind'=                        1331

(316) A=   0 B=         -101855216 C=                    2171388772655 INDEX=           6319
a'=                                            0 b'=                   -101855216
c'=                                2171388772655 ind'=                        6319

(317) A=   0 B=          -51862124 C=                     143755596799 INDEX=              1
a'=                                            0 b'=                    -51862124
c'=                                 143755596799 ind'=                           1

(318) A=   1 B=         -279525985 C=                   -2667395433004 INDEX=           5829
a'=                                            1 b'=                   -279525985
c'=                               -2667395433004 ind'=                        5829

(319) A=   1 B=          -24744195 C=                    -160876074800 INDEX=            455
a'=                                            1 b'=                    -24744195
c'=                                -160876074800 ind'=                         455

(320) A=   0 B=          144034144 C=                     798859236987 INDEX=           3077
a'=                                            0 b'=                    144034144
c'=                                 798859236987 ind'=                        3077

(321) A=   1 B=         -860601561 C=                   26860079032168 INDEX=          74113
a'=                                        -7160 b'=                    108764134
c'=                                 885713271937 ind'=                        3457

(322) A=   1 B=          142058251 C=                    -527193566364 INDEX=           2481
a'=                                            1 b'=                    142058251
c'=                                -527193566364 ind'=                         2481

(323) A=   1 B=         -371028300 C=                   -2762260996100 INDEX=            740
a'=                                            1 b'=                   -371028300
c'=                               -2762260996100 ind'=                         740

(324) A=   0 B=           18565012 C=                     111726756521 INDEX=            343
a'=                                            0 b'=                     18565012
c'=                                 111726756521 ind'=                         343

(325) A=   1 B=          -59796615 C=                     567520017250 INDEX=           1595
a'=                                            1 b'=                    -59796615
c'=                                 567520017250 ind'=                        1595

(326) A=   1 B=          525952545 C=                    2898805096846 INDEX=          16199
a'=                                            1 b'=                    525952545
c'=                                2898805096846 ind'=                       16199

(327) A=   1 B=          373691833 C=                    1248779376576 INDEX=           9021
a'=                                            1 b'=                    373691833
c'=                                1248779376576 ind'=                        9021
```

(328) A= 1 B= -110888165 C= 1111544859042 INDEX= 3009
a'= 1 b'= -110888165
c'= 1111544859042 ind'= 3009

(329) A= 0 B= 393671284 C= 3107520950787 INDEX= 12797
a'= 0 b'= 393671284
c'= 3107520950787 ind'= 12797

(330) A= 1 B= 211774733 C= -589881845656 INDEX= 3921
a'= 1 b'= 211774733
c'= -589881845656 ind'= 3921

(331) A= 0 B= -55691708 C= 165449708157 INDEX= 125
a'= 0 b'= -55691708
c'= 165449708157 ind'= 125

(332) A= 1 B= -27166801 C= 68941131324 INDEX= 125
a'= 1 b'= -27166801
c'= 68941131324 ind'= 125

(333) A= 1 B= -161417689 C= 3465408147428 INDEX= 9987
a'= 85368 b'= -121173338
c'= 48205341483 ind'= 2197

(334) A= 1 B= 50611756 C= -76122367152 INDEX= 468
a'= 1 b'= 50611756
c'= -76122367152 ind'= 468

(335) A= 0 B= -634223819 C= 6150123135110 INDEX= 512
a'= 0 b'= -634223819
c'= 6150123135110 ind'= 512

(336) A= 0 B= -542319284 C= 4861056690431 INDEX= 1
a'= 0 b'= -542319284
c'= 4861056690431 ind'= 1

(337) A= 1 B= 4172759 C= 8513666396 INDEX= 27
a'= 1 b'= 4172759
c'= 8513666396 ind'= 27

(338) A= 1 B= 29584386 C= 331472944324 INDEX= 998
a'= 121227 b'= -16559
c'= 998 ind'= 1

(339) A= 1 B= -48755092 C= -376309410736 INDEX= 1044
a'= 1 b'= -48755092
c'= -376309410736 ind'= 1044

(340) A= 0 B= 647846884 C= 4466065918905 INDEX= 22969
a'= 51437 b'= -666508955
c'= 2371420673600 ind'= 13315

(341) A= 1 B= 163836305 C= -688981430998 INDEX= 3141
a'= 1 b'= 163836305
c'= -688981430998 ind'= 3141

(342) A= 1 B= -775459891 C= -9094714228980 INDEX= 10925
a'= -23151 b'= 384448030
c'= 1030053792500 ind'= 9710

(343) A= 1 B= -173120661 C= -1427245901874 INDEX= 3333
a'= 1 b'= -173120661
c'= -1427245901874 ind'= 3333

(344) A= 0 B= 365513377 C= 12724342572626 INDEX= 38492
a'= 10181 b'= -69727905

```
c'=                                2365330359132 ind'=                    7839

(345) A=   1 B=          296786905 C=                -1042210560834 INDEX=          6591
a'=                                1 b'=                  296786905
c'=                     -1042210560834 ind'=                  6591

(346) A=   0 B=         -363980093 C=                 2835054424024 INDEX=          2798
a'=                                0 b'=                 -363980093
c'=                     2835054424024 ind'=                   2798

(347) A=   1 B=         -403485895 C=                -26399186552532 INDEX=         77585
a'=                            -5126 b'=                  17884638
c'=                     1429879834665 ind'=                   4293

(348) A=   1 B=          462312820 C=                 -3809464411172 INDEX=         15980
a'=                            50935 b'=                  313454829
c'=                     1488405979980 ind'=                   9651

(349) A=   0 B=          707986999 C=                  1204390139180 INDEX=         21754
a'=                            66611 b'=                   32639488
c'=                     4719902720 ind'=                       512

(350) A=   1 B=         -176251759 C=                  1534966275876 INDEX=          3679
a'=                                1 b'=                 -176251759
c'=                     1534966275876 ind'=                   3679

(351) A=   1 B=          252968503 C=                 14299501988686 INDEX=         42569
a'=                            71586 b'=                  -91223834
c'=                      38184885999 ind'=                    2197

(352) A=   1 B=          617745348 C=                 15553684872016 INDEX=         49244
a'=                           121261 b'=                  -10334952
c'=                      240231744 ind'=                       216

(353) A=   1 B=         -710079262 C=                 -7397514132316 INDEX=          3834
a'=                                1 b'=                 -710079262
c'=                     -7397514132316 ind'=                  3834

(354) A=   0 B=           58673077 C=                    1682479354 INDEX=           512
a'=                                0 b'=                   58673077
c'=                     1682479354 ind'=                       512

(355) A=   0 B=           17774608 C=                      30851285 INDEX=           125
a'=                          198599 b'=                      -36792
c'=                            8000 ind'=                         8

(356) A=   1 B=          294498460 C=                  1157981292400 INDEX=          6700
a'=                                1 b'=                  294498460
c'=                     1157981292400 ind'=                   6700

(357) A=   1 B=         -459047527 C=                  4248864139374 INDEX=          5711
a'=                                1 b'=                 -459047527
c'=                     4248864139374 ind'=                   5711

(358) A=   1 B=           34913384 C=                   106018582848 INDEX=           392
a'=                                1 b'=                   34913384
c'=                      106018582848 ind'=                    392

(359) A=   0 B=         -870505766 C=                 54233154008977 INDEX=        157823
a'=                            -5158 b'=                   26405406
c'=                      649732197143 ind'=                    2029

(360) A=   0 B=         -454167227 C=                  3740680995846 INDEX=          1000
a'=                                0 b'=                 -454167227
c'=                     3740680995846 ind'=                   1000
```

```
(361) A=    0 B=        -5661662 C=          42551571059 INDEX=          125
a'=                             0 b'=           -5661662
c'=                  42551571059 ind'=              125

(362) A=    1 B=        22900209 C=          -2135254616 INDEX=          125
a'=                             1 b'=           22900209
c'=                  -2135254616 ind'=              125

(363) A=    0 B=         -134714 C=           338411279 INDEX=            1
a'=                             0 b'=            -134714
c'=                   338411279 ind'=                1

(364) A=    1 B=       135557015 C=        -572678466288 INDEX=         2471
a'=                             1 b'=          135557015
c'=                  -572678466288 ind'=            2471
```

Coefficients of the generating polynomials $X^3 + AX^2 + BX + C$ for all the distinct cubic fields with negative fundamental discriminant D.

Note: 1) A, B and C are the coefficients of a generating polynomial of a complex cubic field before Tschirnhausen transformation is applied.
2) A', B' and C' are the coefficients of a generating polynomial of a complex cubic field after Tschirnhausen transformation is applied.

D = -3161659186633662283

(1) A=	1	B=	146967997	C=	1132558335310	INDEX=	3869
a'=			1	b'=	146967997		
c'=			1132558335310	ind'=	3869		
(2) A=	1	B=	-88889429	C=	-322599303620	INDEX=	1
a'=			1	b'=	-88889429		
c'=			-322599303620	ind'=	1		
(3) A=	0	B=	-513868778	C=	4927790697473	INDEX=	5975
a'=			0	b'=	-513868778		
c'=			4927790697473	ind'=	5975		
(4) A=	1	B=	-158249958	C=	13770055974244	INDEX=	40178
a'=			-3879	b'=	22652569		
c'=			2864058556322	ind'=	8443		
(5) A=	0	B=	-118999487	C=	766853693966	INDEX=	1700
a'=			0	b'=	-118999487		
c'=			766853693966	ind'=	1700		
(6) A=	1	B=	-450844689	C=	-6929903637720	INDEX=	17151
a'=			-22631	b'=	231454340		
c'=			4884594097776	ind'=	16876		
(7) A=	1	B=	117434120	C=	262538186304	INDEX=	1624
a'=			1	b'=	117434120		
c'=			262538186304	ind'=	1624		
(8) A=	1	B=	11919795	C=	39737621350	INDEX=	125
a'=			1	b'=	11919795		
c'=			39737621350	ind'=	125		
(9) A=	1	B=	115092107	C=	482482858176	INDEX=	1979
a'=			1	b'=	115092107		
c'=			482482858176	ind'=	1979		
(10) A=	1	B=	-61444013	C=	185591578782	INDEX=	27
a'=			1	b'=	-61444013		
c'=			185591578782	ind'=	27		
(11) A=	0	B=	-821106452	C=	10295512361855	INDEX=	14311
a'=			-27800	b'=	385951854		
c'=			1678831438471	ind'=	10831		
(12) A=	1	B=	-534772945	C=	7957277905218	INDEX=	18635
a'=			90396	b'=	-559666964		
c'=			876699992435	ind'=	6859		
(13) A=	1	B=	-970549149	C=	34528392012202	INDEX=	94999
a'=			-9896	b'=	33321772		
c'=			1155108895831	ind'=	3487		
(14) A=	1	B=	12899952	C=	12716930836	INDEX=	64
a'=			1	b'=	12899952		

```
c'=                                  12716930836 ind'=                    64

(15) A=   1 B=          -505418189 C=                 5623438653310 INDEX=          10331
a'=                                           1 b'=          -505418189
c'=                                5623438653310 ind'=               10331

(16) A=   1 B=          -368677131 C=                 2921931014044 INDEX=           3085
a'=                                           1 b'=          -368677131
c'=                                2921931014044 ind'=                3085

(17) A=   1 B=          -389460156 C=                15713910190000 INDEX=          45100
a'=                                       -7095 b'=            99023383
c'=                                2121769233100 ind'=                6859

(18) A=   0 B=          -458219030 C=                 4381341209319 INDEX=           6497
a'=                                           0 b'=          -458219030
c'=                                4381341209319 ind'=                6497

(19) A=   1 B=           -15426543 C=                  -25089869736 INDEX=             27
a'=                                           1 b'=           -15426543
c'=                                 -25089869736 ind'=                  27

(20) A=   1 B=          -192448729 C=                -1766580213018 INDEX=           4199
a'=                                           1 b'=          -192448729
c'=                               -1766580213018 ind'=                4199

(21) A=   0 B=             3492901 C=                    1086748902 INDEX=              8
a'=                                           0 b'=             3492901
c'=                                  1086748902 ind'=                   8

(22) A=   1 B=             1127392 C=                  -21895357184 INDEX=             64
a'=                                           1 b'=             1127392
c'=                                -21895357184 ind'=                  64

(23) A=   1 B=           370182527 C=                 1830658412024 INDEX=           9633
a'=                                       48159 b'=            74689126
c'=                                 191100571428 ind'=                4454

(24) A=   1 B=            14613379 C=                  -18552221168 INDEX=             83
a'=                                           1 b'=            14613379
c'=                                -18552221168 ind'=                  83

(25) A=   1 B=           207674604 C=                 1540056377680 INDEX=           5620
a'=                                       56219 b'=           -43092993
c'=                                 32128871220 ind'=                2391

(26) A=   1 B=            14115175 C=                  -601572865826 INDEX=           1759
a'=                                           1 b'=            14115175
c'=                                -601572865826 ind'=                1759

(27) A=   0 B=           -51577850 C=                  379255538379 INDEX=           1027
a'=                                           0 b'=           -51577850
c'=                                 379255538379 ind'=                1027

(28) A=   1 B=           250275770 C=                -1699063244100 INDEX=           6670
a'=                                       52707 b'=           -19121807
c'=                                  8026738030 ind'=                1097

(29) A=   0 B=          -513537551 C=                 4980595434494 INDEX=           6364
a'=                                           0 b'=          -513537551
c'=                                4980595434494 ind'=                6364

(30) A=   0 B=          -106872485 C=                  427165367464 INDEX=            118
a'=                                           0 b'=          -106872485
c'=                                 427165367464 ind'=                 118
```

```
(31) A=    1 B=          -334929168 C=                    2657628420516 INDEX=          3576
a'=                                        1 b'=                -334929168
c'=                     2657628420516 ind'=                        3576

(32) A=    0 B=           942639352 C=                    23676440027303 INDEX=         76465
a'=                                    12331 b'=                 3551232
c'=                     1282869821440 ind'=                        4096

(33) A=    0 B=           341623930 C=                     2551292835919 INDEX=         10297
a'=                                    45949 b'=                  158904
c'=                         659008 ind'=                             8

(34) A=    1 B=          -446033577 C=                     4011529526008 INDEX=          5017
a'=                                        1 b'=                -446033577
c'=                     4011529526008 ind'=                        5017

(35) A=    1 B=           173637982 C=                    -2087832304988 INDEX=          6622
a'=                                        1 b'=                 173637982
c'=                    -2087832304988 ind'=                        6622

(36) A=    1 B=            80188125 C=                      -80181216776 INDEX=           841
a'=                                        1 b'=                  80188125
c'=                      -80181216776 ind'=                          841

(37) A=    1 B=           671920887 C=                    -3241554852050 INDEX=         21761
a'=                                    55548 b'=                 689909212
c'=                     6431038797041 ind'=                       17191

(38) A=    1 B=           443982449 C=                    -5171302349826 INDEX=         18415
a'=                                    24335 b'=                  59232438
c'=                     5193737798940 ind'=                       16794

(39) A=    1 B=           476305885 C=                     8977097539234 INDEX=         28721
a'=                                    17026 b'=                  74563932
c'=                     4191846062481 ind'=                       12081

(40) A=    1 B=          -777093224 C=                     22457046757440 INDEX=         60936
a'=                                    -8729 b'=                 118111955
c'=                     1155713699400 ind'=                        4355

(41) A=    1 B=           810222183 C=                     38362174564468 INDEX=        115067
a'=                                     7044 b'=                   2811988
c'=                      979092330563 ind'=                        2917

(42) A=    1 B=           876313339 C=                    -5292937844390 INDEX=         33025
a'=                                    53337 b'=                -233201783
c'=                      336127256064 ind'=                        4931

(43) A=    1 B=           571741214 C=                     22800975619172 INDEX=         68382
a'=                                     8365 b'=                   4456091
c'=                     1650575243358 ind'=                        4913

(44) A=    1 B=           239768197 C=                      -852658922376 INDEX=          4863
a'=                                        1 b'=                 239768197
c'=                     -852658922376 ind'=                        4863

(45) A=    1 B=           -11356383 C=                      -30789983570 INDEX=            79
a'=                                        1 b'=                 -11356383
c'=                      -30789983570 ind'=                          79

(46) A=    1 B=           428452341 C=                     4954137745660 INDEX=         17581
a'=                                   110687 b'=                 -665363972
c'=                     1002251385296 ind'=                        7756

(47) A=    1 B=          -272307351 C=                     -2950456926626 INDEX=          6985
a'=                                        1 b'=                -272307351
```

```
c'=                                -2950456926626 ind'=                    6985

(48) A=   1 B=        -27413483 C=                    56003320542 INDEX=          27
a'=                                           1 b'=          -27413483
c'=                                56003320542 ind'=                 27

(49) A=   1 B=        108808987 C=                   128868858040 INDEX=        1331
a'=                                           1 b'=          108808987
c'=                               128868858040 ind'=                1331

(50) A=   1 B=        387279993 C=                 20443319519302 INDEX=       60353
a'=                                        6417 b'=            -701000
c'=                             1898081571392 ind'=                5608

(51) A=   1 B=        141041361 C=                  -561755982870 INDEX=        2499
a'=                                           1 b'=          141041361
c'=                              -561755982870 ind'=                2499

(52) A=   1 B=        574795327 C=                 -6255133004058 INDEX=       23967
a'=                                       24009 b'=           15580804
c'=                             3086400851568 ind'=               11348

(53) A=   1 B=        350500544 C=                  1284228332144 INDEX=        8280
a'=                                           1 b'=          350500544
c'=                              1284228332144 ind'=                8280

(54) A=   1 B=       -446000549 C=                 -7814327917200 INDEX=       20229
a'=                                      -16057 b'=          243981332
c'=                             3312248234064 ind'=               12796

(55) A=   1 B=        292851240 C=                 -7582374844976 INDEX=       22864
a'=                                       12945 b'=          -42642791
c'=                             4437279607504 ind'=               13931

(56) A=   1 B=        329729341 C=                   654750725512 INDEX=        7001
a'=                                           1 b'=          329729341
c'=                               654750725512 ind'=                7001

(57) A=   1 B=       -269344888 C=                  2204317729236 INDEX=        4096
a'=                                           1 b'=         -269344888
c'=                              2204317729236 ind'=                4096

(58) A=   1 B=       -337384634 C=                 -2549994472428 INDEX=        2634
a'=                                           1 b'=         -337384634
c'=                             -2549994472428 ind'=                2634

(59) A=   0 B=        511997692 C=                   476209482407 INDEX=       13105
a'=                                           0 b'=          511997692
c'=                               476209482407 ind'=               13105

(60) A=   1 B=        199115689 C=                  2959250478492 INDEX=        9207
a'=                                       54962 b'=           32073608
c'=                             10286511543 ind'=                1057

(61) A=   1 B=          -747939 C=                    -423433358 INDEX=           1
a'=                                           1 b'=            -747939
c'=                               -423433358 ind'=                   1

(62) A=   1 B=       -130113215 C=                 -2705869795076 INDEX=        7729
a'=                                           1 b'=         -130113215
c'=                             -2705869795076 ind'=                7729

(63) A=   0 B=       -305533631 C=                  2962961959154 INDEX=        6236
a'=                                           0 b'=         -305533631
c'=                              2962961959154 ind'=                6236
```

(64) A= 1 B=	-5819798 C=		43452151956 INDEX=		126
a'=		1 b'=		-5819798	
c'=		43452151956 ind'=		126	
(65) A= 1 B=	106560127 C=		469303106302 INDEX=		1847
a'=		82369 b'=		18100764	
c'=		4425973488 ind'=		1548	
(66) A= 0 B=	-637313090 C=		6280624327597 INDEX=		3061
a'=		0 b'=		-637313090	
c'=		6280624327597 ind'=		3061	
(67) A= 1 B=	-399453816 C=		4115325270484 INDEX=		8000
a'=		1 b'=		-399453816	
c'=		4115325270484 ind'=		8000	
(68) A= 1 B=	-69909273 C=		993183771754 INDEX=		2827
a'=		1 b'=		-69909273	
c'=		993183771754 ind'=		2827	
(69) A= 1 B=	-382166636 C=		3007942389660 INDEX=		2580
a'=		1 b'=		-382166636	
c'=		3007942389660 ind'=		2580	
(70) A= 1 B=	-232643031 C=		-1745726284098 INDEX=		3177
a'=		1 b'=		-232643031	
c'=		-1745726284098 ind'=		3177	
(71) A= 0 B=	881080 C=		125568727 INDEX=		1
a'=		0 b'=		881080	
c'=		125568727 ind'=		1	
(72) A= 1 B=	-267340869 C=		2301357760462 INDEX=		4589
a'=		1 b'=		-267340869	
c'=		2301357760462 ind'=		4589	
(73) A= 0 B=	18133219 C=		315477126856 INDEX=		926
a'=		0 b'=		18133219	
c'=		315477126856 ind'=		926	
(74) A= 1 B=	-96095802 C=		446574431052 INDEX=		762
a'=		1 b'=		-96095802	
c'=		446574431052 ind'=		762	
(75) A= 1 B=	-409688227 C=		-5907671921088 INDEX=		14527
a'=		103779 b'=		-38830592	
c'=		3808165888 ind'=		512	
(76) A= 1 B=	269772005 C=		-959762411406 INDEX=		5719
a'=		52259 b'=		-25562448	
c'=		42810695424 ind'=		2736	
(77) A= 1 B=	112040764 C=		500744933964 INDEX=		1980
a'=		1 b'=		112040764	
c'=		500744933964 ind'=		1980	
(78) A= 0 B=	-734831798 C=		18913856214695 INDEX=		50527
a'=		-8093 b'=		151717188	
c'=		1189501783408 ind'=		4852	
(79) A= 1 B=	-488096942 C=		-6020057564732 INDEX=		12742
a'=		1 b'=		-488096942	
c'=		-6020057564732 ind'=		12742	
(80) A= 1 B=	-52291232 C=		227753158912 INDEX=		512
a'=		1 b'=		-52291232	

c'= 227753158912 ind'= 512

(81) A= 1 B= 326875831 C= 3958295266620 INDEX= 13341
a'= 1 b'= 326875831
c'= 3958295266620 ind'= 13341

(82) A= 1 B= 405491747 C= -2947171350334 INDEX= 12591
a'= 1 b'= 405491747
c'= -2947171350334 ind'= 12591

(83) A= 1 B= -44300596 C= 302668719504 INDEX= 820
a'= 1 b'= -44300596
c'= 302668719504 ind'= 820

(84) A= 0 B= -144384551 C= 783212005846 INDEX= 1196
a'= 0 b'= -144384551
c'= 783212005846 ind'= 1196

(85) A= 0 B= 924477559 C= 14923568311604 INDEX= 53866
a'= 17749 b'= 60249915
c'= 2063268235386 ind'= 6189

(86) A= 1 B= -25765513 C= -51188661718 INDEX= 27
a'= 1 b'= -25765513
c'= -51188661718 ind'= 27

(87) A= 1 B= -244566356 C= -1806625295700 INDEX= 3060
a'= 1 b'= -244566356
c'= -1806625295700 ind'= 3060

(88) A= 1 B= -766272875 C= -14239235506226 INDEX= 34091
a'= -16414 b'= 181062442
c'= 1802303931131 ind'= 7271

(89) A= 1 B= 540676838 C= -2397750300612 INDEX= 15782
a'= 1 b'= 540676838
c'= -2397750300612 ind'= 15782

(90) A= 0 B= -35249240 C= 80552063273 INDEX= 1
a'= 0 b'= -35249240
c'= 80552063273 ind'= 1

(91) A= 1 B= 373371139 C= 3021941426332 INDEX= 11993
a'= 50723 b'= 180055318
c'= 551624319332 ind'= 6782

(92) A= 1 B= -130213084 C= -1056564399408 INDEX= 2596
a'= 185769 b'= 42865
c'= 2596 ind'= 1

(93) A= 1 B= -247663385 C= 16694445642364 INDEX= 48589
a'= -4693 b'= 52266750
c'= 2253368322900 ind'= 6810

(94) A= 1 B= 359349237 C= 443754100420 INDEX= 7771
a'= 1 b'= 359349237
c'= 443754100420 ind'= 7771

(95) A= 1 B= -215912938 C= -2401312733356 INDEX= 6042
a'= 131571 b'= -270553997
c'= 145839191898 ind'= 4913

(96) A= 0 B= 357372940 C= 11807896344909 INDEX= 35333
a'= 10451 b'= -53052186
c'= 2787417684692 ind'= 8882

```
(97) A=   0 B=        127341241 C=                    971943595498 INDEX=          3268
a'=                           0 b'=                    127341241
c'=                 971943595498 ind'=                      3268

(98) A=   1 B=       -804241403 C=                   8786640421122 INDEX=          1113
a'=                           1 b'=                   -804241403
c'=                8786640421122 ind'=                      1113

(99) A=   0 B=        -14420555 C=                     21254631434 INDEX=             8
a'=                           0 b'=                    -14420555
c'=                  21254631434 ind'=                         8

(100) A=  0 B=         583441834 C=                    8631466031271 INDEX=         29791
a'=                       65996 b'=                    -86493548
c'=                  35863492871 ind'=                      1759

(101) A=  1 B=         43925361 C=                    -1226442727970 INDEX=          3599
a'=                           1 b'=                    43925361
c'=                -1226442727970 ind'=                      3599

(102) A=  1 B=        611830037 C=                    -6061392923038 INDEX=         24567
a'=                       25510 b'=                    82290920
c'=                3728232914487 ind'=                     12319

(103) A=  1 B=           879607 C=                     127866670 INDEX=             1
a'=                           1 b'=                      879607
c'=                   127866670 ind'=                         1

(104) A=  1 B=        313151547 C=                    -4420329249438 INDEX=         14343
a'=                           1 b'=                    313151547
c'=                -4420329249438 ind'=                     14343

(105) A=  0 B=        -46560683 C=                     213659913510 INDEX=           512
a'=                           0 b'=                    -46560683
c'=                  213659913510 ind'=                       512

(106) A=  1 B=         12385072 C=                    -14073923180 INDEX=            64
a'=                           1 b'=                    12385072
c'=                -14073923180 ind'=                        64

(107) A=  0 B=         92502694 C=                     319685564751 INDEX=          1369
a'=                           0 b'=                    92502694
c'=                  319685564751 ind'=                      1369

(108) A=  1 B=       -342792310 C=                   -99775530847876 INDEX=        291486
a'=                       -1169 b'=                     2900567
c'=                  399697554126 ind'=                      1171

(109) A=  0 B=       -178440848 C=                    1333261013955 INDEX=          2827
a'=                           0 b'=                   -178440848
c'=                 1333261013955 ind'=                      2827

(110) A=  0 B=         -96675536 C=                     365866955479 INDEX=             1
a'=                           0 b'=                    -96675536
c'=                  365866955479 ind'=                         1

(111) A=  1 B=       -224592429 C=                    1295435220130 INDEX=             1
a'=                           1 b'=                   -224592429
c'=                 1295435220130 ind'=                         1

(112) A=  1 B=         11138635 C=                     161916070150 INDEX=           475
a'=                           1 b'=                    11138635
c'=                  161916070150 ind'=                       475

(113) A=  1 B=         498702907 C=                    7161041959990 INDEX=         24389
a'=                       20535 b'=                    -28613300
```

```
c'=                          3131894509136 ind'=                    11332

(114) A=   0 B=       737988628 C=                  18970777851215 INDEX=      59849
a'=                         86529 b'=                    86146567
c'=                   27773458986 ind'=                    2197

(115) A=   1 B=      -119923454 C=                   -511823390580 INDEX=        234
a'=                             1 b'=                  -119923454
c'=                  -511823390580 ind'=                    234

(116) A=   1 B=        28930141 C=                   -3870112279760 INDEX=      11311
a'=                             1 b'=                    28930141
c'=                  -3870112279760 ind'=                   11311

(117) A=   1 B=       720298042 C=                  16012513060084 INDEX=      51598
a'=                         14275 b'=                    46443265
c'=                   2281106353198 ind'=                    6649

(118) A=   0 B=      -734969366 C=                  16495808412991 INDEX=      42679
a'=                         52939 b'=                  -425747268
c'=                    861179593456 ind'=                    4492

(119) A=   1 B=       205749837 C=                  -1373591360840 INDEX=       5209
a'=                             1 b'=                    205749837
c'=                  -1373591360840 ind'=                    5209

(120) A=   0 B=       182838820 C=                   1482093202131 INDEX=       5147
a'=                             0 b'=                    182838820
c'=                   1482093202131 ind'=                    5147

(121) A=   1 B=      -206275723 C=                   -1392847475416 INDEX=       2337
a'=                             1 b'=                   -206275723
c'=                  -1392847475416 ind'=                    2337

(122) A=   1 B=       264758874 C=                   -7736483175308 INDEX=      23122
a'=                         11525 b'=                    33747231
c'=                   5096861282898 ind'=                   14847

(123) A=   1 B=       277811809 C=                   1142858222962 INDEX=       6187
a'=                             1 b'=                    277811809
c'=                   1142858222962 ind'=                    6187

(124) A=   1 B=       513599957 C=                   2787382419780 INDEX=      15419
a'=                         33335 b'=                   -11872070
c'=                   1846076225516 ind'=                   10942

(125) A=   1 B=      -642390753 C=                   7509239541916 INDEX=      12091
a'=                             1 b'=                   -642390753
c'=                   7509239541916 ind'=                   12091

(126) A=   0 B=       962420068 C=                  42132307430605 INDEX=     127621
a'=                          8275 b'=                   -37645206
c'=                    643786176436 ind'=                    2246

(127) A=   1 B=      -125071023 C=                   -2305512868940 INDEX=       6551
a'=                             1 b'=                   -125071023
c'=                  -2305512868940 ind'=                    6551

(128) A=   1 B=       -49235032 C=                    -219966765552 INDEX=        512
a'=                             1 b'=                    -49235032
c'=                   -219966765552 ind'=                     512

(129) A=   0 B=      -354438734 C=                   4197762140113 INDEX=       9703
a'=                             0 b'=                   -354438734
c'=                   4197762140113 ind'=                    9703
```

```
(130) A=   1 B=        -168968267 C=                  1535763951222 INDEX=          3747
a'=                              1 b'=                  -168968267
c'=                 1535763951222 ind'=                      3747

(131) A=   1 B=         402614347 C=                  5880606152620 INDEX=         19439
a'=                          64517 b'=                   760368892
c'=                 4399472113904 ind'=                     15044

(132) A=   0 B=           922228 C=                    29952425 INDEX=             1
a'=                              0 b'=                   922228
c'=                       29952425 ind'=                       1

(133) A=   1 B=        -355229221 C=                  5650317902754 INDEX=         14695
a'=                          87236 b'=                  -389585838
c'=                  454111958295 ind'=                      5559

(134) A=   1 B=        -216146587 C=                 -4339520461758 INDEX=         12167
a'=                          83267 b'=                  -172464680
c'=                  98134155200 ind'=                      2840

(135) A=   1 B=        -144993281 C=                   672016199772 INDEX=            27
a'=                              1 b'=                  -144993281
c'=                  672016199772 ind'=                        27

(136) A=   1 B=        -168391851 C=                 12025093454424 INDEX=         35055
a'=                         -4790 b'=                    11657738
c'=                 3319440714855 ind'=                      9731

(137) A=   1 B=         219023183 C=                  1126976122182 INDEX=          4913
a'=                          57776 b'=                    -4783478
c'=                   578009537 ind'=                       343

(138) A=   1 B=        -431597579 C=                  6965317781560 INDEX=         17681
a'=                         -20074 b'=                   238333690
c'=                 4366521419225 ind'=                     15715

(139) A=   1 B=        -659152042 C=                  7008645234588 INDEX=          7562
a'=                              1 b'=                  -659152042
c'=                 7008645234588 ind'=                      7562

(140) A=   1 B=        -817076761 C=                 15671842257764 INDEX=         37515
a'=                         -15976 b'=                   169423982
c'=                 1648545692115 ind'=                      6629

(141) A=   0 B=         560711740 C=                  2301671475533 INDEX=         16379
a'=                          51485 b'=                   439985880
c'=                 3740513898176 ind'=                     15112

(142) A=   0 B=        -128693858 C=                   563559053557 INDEX=           125
a'=                              0 b'=                  -128693858
c'=                  563559053557 ind'=                       125

(143) A=   1 B=          57369717 C=                  -240874061648 INDEX=           857
a'=                              1 b'=                    57369717
c'=                 -240874061648 ind'=                       857

(144) A=   1 B=         168621480 C=                   414071386084 INDEX=          2744
a'=                          67905 b'=                     9701659
c'=                  4861163384 ind'=                      1331

(145) A=   1 B=          -1903809 C=                   -1068047720 INDEX=             1
a'=                              1 b'=                    -1903809
c'=                  -1068047720 ind'=                         1

(146) A=   1 B=         -30201008 C=                   -418290537296 INDEX=          1208
a'=                              1 b'=                   -30201008
```

```
c'=                                -418290537296 ind'=                    1208

(147) A=   1 B=        -21229485 C=                -289568050196 INDEX=          839
a'=                              1 b'=                  -21229485
c'=                   -289568050196 ind'=                   839

(148) A=   0 B=         89362270 C=                  969768870747 INDEX=         2989
a'=                              0 b'=                   89362270
c'=                    969768870747 ind'=                  2989

(149) A=   1 B=        208593927 C=                -3963770760204 INDEX=        12069
a'=                          54307 b'=                 100466072
c'=                    90873969984 ind'=                  2744

(150) A=   1 B=         -2177474 C=                  -15790276868 INDEX=           46
a'=                              1 b'=                   -2177474
c'=                   -15790276868 ind'=                    46

(151) A=   1 B=        264170858 C=                 -471183244852 INDEX=         5022
a'=                              1 b'=                  264170858
c'=                   -471183244852 ind'=                  5022

(152) A=   1 B=       -771092568 C=                -8610861584156 INDEX=         7288
a'=                              1 b'=                  -771092568
c'=                  -8610861584156 ind'=                  7288

(153) A=   0 B=         -1171190 C=                   595902023 INDEX=            1
a'=                              0 b'=                   -1171190
c'=                    595902023 ind'=                     1

(154) A=   0 B=        302394205 C=                  899079841394 INDEX=         6472
a'=                              0 b'=                  302394205
c'=                    899079841394 ind'=                  6472

(155) A=   1 B=       -175125607 C=                 1865162103762 INDEX=         4787
a'=                              1 b'=                  -175125607
c'=                   1865162103762 ind'=                  4787

(156) A=   1 B=           596745 C=                   292801924 INDEX=            1
a'=                              1 b'=                     596745
c'=                    292801924 ind'=                     1

(157) A=   0 B=        111970087 C=                 5644962175212 INDEX=        16550
a'=                          56951 b'=                 150300087
c'=                    150044302550 ind'=                  3011

(158) A=   1 B=        -71320241 C=                 -423897174518 INDEX=         1037
a'=                              1 b'=                   -71320241
c'=                   -423897174518 ind'=                  1037

(159) A=   1 B=         -2985514 C=                  118415663172 INDEX=          346
a'=                              1 b'=                   -2985514
c'=                    118415663172 ind'=                   346

(160) A=   1 B=         40253517 C=                  117207388944 INDEX=          447
a'=                              1 b'=                   40253517
c'=                    117207388944 ind'=                   447

(161) A=   1 B=        474901130 C=                -5978430696796 INDEX=        20994
a'=                         124234 b'=                 836031672
c'=                   1493320178421 ind'=                  9267

(162) A=   1 B=        183853471 C=                  907326604420 INDEX=         3859
a'=                              1 b'=                  183853471
c'=                    907326604420 ind'=                  3859
```

```
(163) A=   1 B=          430712082 C=                    215473019220 INDEX=          10074
a'=                                    1 b'=                430712082
c'=                       215473019220 ind'=                    10074

(164) A=   1 B=          193666115 C=                   -1398683532636 INDEX=           5089
a'=                                    1 b'=                193666115
c'=                      -1398683532636 ind'=                     5089

(165) A=   1 B=            8085420 C=                     18529620300 INDEX=             60
a'=                                    1 b'=                  8085420
c'=                       18529620300 ind'=                       60

(166) A=   1 B=          397897103 C=                     553975650552 INDEX=          9073
a'=                                44207 b'=                 -5348160
c'=                       27091832832 ind'=                     1728

(167) A=   1 B=          525626110 C=                   11637695948788 INDEX=         36610
a'=                                15619 b'=                -83562329
c'=                     1844990274610 ind'=                     7099

(168) A=   1 B=         -100064376 C=                    -705787321968 INDEX=          1728
a'=                                    1 b'=               -100064376
c'=                      -705787321968 ind'=                     1728

(169) A=   0 B=          -40855382 C=                     684625572445 INDEX=          1979
a'=                                    0 b'=                -40855382
c'=                       684625572445 ind'=                     1979

(170) A=   1 B=         -634722009 C=                    13495769672212 INDEX=         35099
a'=                                52804 b'=                -553366380
c'=                     1439902253475 ind'=                     6405

(171) A=   1 B=          743582146 C=                    -9507405720588 INDEX=         35946
a'=                                21349 b'=                 -48354145
c'=                     1175684420106 ind'=                     5719

(172) A=   1 B=          468591987 C=                     683720036244 INDEX=         11583
a'=                                40584 b'=                  15999076
c'=                      662185295343 ind'=                     7561

(173) A=   1 B=          506777582 C=                    -4679912995140 INDEX=         18754
a'=                                28435 b'=                 157465645
c'=                     5850902345026 ind'=                    17663

(174) A=   0 B=          645891034 C=                    22722489882191 INDEX=         68921
a'=                                10154 b'=                 -53309520
c'=                     1210561595001 ind'=                     4191

(175) A=   1 B=         -524286720 C=                    -5293051444796 INDEX=          7544
a'=                                    1 b'=               -524286720
c'=                     -5293051444796 ind'=                    7544

(176) A=   0 B=         -859826777 C=                    10382999363604 INDEX=         10790
a'=                                    0 b'=               -859826777
c'=                     10382999363604 ind'=                    10790

(177) A=   1 B=           40305341 C=                      229209123242 INDEX=           729
a'=                                    1 b'=                 40305341
c'=                       229209123242 ind'=                     729

(178) A=   1 B=         -685237668 C=                     9307977896656 INDEX=         18244
a'=                               -14817 b'=                 304863121
c'=                     1362222576964 ind'=                     8641

(179) A=   1 B=         -107793048 C=                     434912870356 INDEX=           176
a'=                                    1 b'=               -107793048
```

```
c'=                                434912870356 ind'=                       176

(180) A=   1 B=          -519223807 C=                 -11182931654842 INDEX=          29847
a'=                           -10006 b'=                      212557412
c'=                      2037868663143 ind'=                      8263

(181) A=   1 B=          -291218654 C=                   3142385055340 INDEX=           7286
a'=                                1 b'=                     -291218654
c'=                      3142385055340 ind'=                      7286

(182) A=   1 B=           291295986 C=                  -1945108904220 INDEX=           7974
a'=                                1 b'=                      291295986
c'=                     -1945108904220 ind'=                      7974

(183) A=   1 B=           225652963 C=                    -15954611928 INDEX=           3813
a'=                                1 b'=                      225652963
c'=                       -15954611928 ind'=                      3813

(184) A=   1 B=          -155597993 C=                  -2204545569854 INDEX=           6061
a'=                                1 b'=                     -155597993
c'=                     -2204545569854 ind'=                      6061

(185) A=   1 B=           583388306 C=                  -6242398011468 INDEX=          24166
a'=                            79377 b'=                      518601928
c'=                      1065140806080 ind'=                      8632

(186) A=   1 B=            20274989 C=                   -111983298168 INDEX=            343
a'=                                1 b'=                       20274989
c'=                      -111983298168 ind'=                       343

(187) A=   1 B=           618986091 C=                   1025392169200 INDEX=          17579
a'=                           106531 b'=                      -35600896
c'=                       3138650112 ind'=                       512

(188) A=   0 B=          -217539530 C=                   4308038301653 INDEX=          12061
a'=                                0 b'=                     -217539530
c'=                      4308038301653 ind'=                      12061

(189) A=   1 B=          -440718794 C=                  -3573269210900 INDEX=            854
a'=                                1 b'=                     -440718794
c'=                     -3573269210900 ind'=                       854

(190) A=   0 B=           638514550 C=                    363163137867 INDEX=          18179
a'=                            96459 b'=                      -608614010
c'=                       985116198900 ind'=                      8990

(191) A=   1 B=           331124856 C=                   1247880057652 INDEX=           7696
a'=                                1 b'=                      331124856
c'=                      1247880057652 ind'=                      7696

(192) A=   1 B=             4082241 C=                    -10120557890 INDEX=             31
a'=                                1 b'=                       4082241
c'=                       -10120557890 ind'=                        31

(193) A=   1 B=          -412595722 C=                   3758571419892 INDEX=           5638
a'=                                1 b'=                     -412595722
c'=                      3758571419892 ind'=                      5638

(194) A=   0 B=           488091946 C=                    328810101647 INDEX=          12167
a'=                                0 b'=                      488091946
c'=                       328810101647 ind'=                      12167

(195) A=   1 B=           750361985 C=                  220103005899624 INDEX=         643621
a'=                             1166 b'=                        -290988
c'=                       181476020781 ind'=                       531
```

```
(196) A=   1 B=          -1083583 C=                    -553159764 INDEX=                1
a'=                              1 b'=                   -1083583
c'=                   -553159764 ind'=                          1

(197) A=   1 B=          -40034635 C=                -1034969960916 INDEX=             3011
a'=                              1 b'=                   -40034635
c'=                -1034969960916 ind'=                       3011

(198) A=   1 B=          215821059 C=                 -303578725266 INDEX=             3675
a'=                          60137 b'=                    -5173216
c'=                   6325939200 ind'=                        1312

(199) A=   0 B=         -348832760 C=                 15699314146897 INDEX=            45289
a'=                          -6797 b'=                    78191550
c'=                2250976522500 ind'=                        7050

(200) A=   0 B=          168693835 C=                    74286248848 INDEX=             2474
a'=                              0 b'=                   168693835
c'=                   74286248848 ind'=                        2474

(201) A=   1 B=          207782453 C=                    57088408902 INDEX=             3373
a'=                              1 b'=                   207782453
c'=                   57088408902 ind'=                        3373

(202) A=   1 B=         -401309171 C=                 -3165956962946 INDEX=             1955
a'=                              1 b'=                  -401309171
c'=                -3165956962946 ind'=                       1955

(203) A=   1 B=          181490693 C=                 -3021048117942 INDEX=             9247
a'=                          52954 b'=                   -49957058
c'=                   24961804903 ind'=                        1643

(204) A=   1 B=           54973577 C=                  6643281207296 INDEX=            19419
a'=                          62778 b'=                   326505400
c'=                  592777111875 ind'=                        5525

(205) A=   1 B=          772922408 C=                  2572641487632 INDEX=            25312
a'=                          35397 b'=                   233457163
c'=                   3737235826912 ind'=                      12151

(206) A=   1 B=          760292940 C=                -28430337946356 INDEX=            86364
a'=                           8859 b'=                    14963977
c'=                   1341360825084 ind'=                        3941

(207) A=   1 B=           13764829 C=                    34884188742 INDEX=              117
a'=                              1 b'=                    13764829
c'=                   34884188742 ind'=                         117

(208) A=   1 B=         -337712960 C=                 -2413243091600 INDEX=             1000
a'=                              1 b'=                  -337712960
c'=                -2413243091600 ind'=                       1000

(209) A=   0 B=          329297515 C=                   588695606824 INDEX=             6938
a'=                          48419 b'=                    -8872929
c'=                   27447567498 ind'=                        1989

(210) A=   1 B=          160639697 C=                  4395377798804 INDEX=            13047
a'=                          58871 b'=                   193551926
c'=                   268209214332 ind'=                       4534

(211) A=   0 B=          -27630962 C=                    56280714395 INDEX=               19
a'=                              0 b'=                   -27630962
c'=                   56280714395 ind'=                          19

(212) A=   1 B=         -659461850 C=                  7448387511244 INDEX=            10534
a'=                              1 b'=                  -659461850
```

```
c'=                                7448387511244 ind'=                    10534

(213) A=   1 B=          216578055 C=                  -411054034796 INDEX=          3781
a'=                                       1 b'=                 216578055
c'=                             -411054034796 ind'=                    3781

(214) A=   0 B=         -152934575 C=                  1634311163902 INDEX=          4276
a'=                                       0 b'=                -152934575
c'=                             1634311163902 ind'=                    4276

(215) A=   1 B=          193866422 C=                  -919201467444 INDEX=          4054
a'=                                       1 b'=                 193866422
c'=                             -919201467444 ind'=                    4054

(216) A=   1 B=          851971407 C=                 38466323339044 INDEX=        115837
a'=                                    7379 b'=                  8470704
c'=                              993091915008 ind'=                    2928

(217) A=   0 B=          155803756 C=                    69999598173 INDEX=          2197
a'=                                       0 b'=                 155803756
c'=                              69999598173 ind'=                    2197

(218) A=   1 B=          491226089 C=                  4535491788914 INDEX=         18045
a'=                                   70666 b'=                 -303210708
c'=                              358032560977 ind'=                    4913

(219) A=   1 B=           72265360 C=                    28567679844 INDEX=           696
a'=                                       1 b'=                  72265360
c'=                              28567679844 ind'=                     696

(220) A=   1 B=         -293217743 C=                 -1932682040136 INDEX=           27
a'=                                       1 b'=                -293217743
c'=                          -1932682040136 ind'=                      27

(221) A=   0 B=          248307013 C=                  2286087949034 INDEX=         8000
a'=                                       0 b'=                 248307013
c'=                              2286087949034 ind'=                    8000

(222) A=   0 B=          -43806878 C=                  2047667851873 INDEX=         5975
a'=                                       0 b'=                 -43806878
c'=                              2047667851873 ind'=                    5975

(223) A=   1 B=          -98227329 C=                   374678565382 INDEX=            1
a'=                                       1 b'=                 -98227329
c'=                               374678565382 ind'=                       1

(224) A=   1 B=           78784183 C=                  -147529417152 INDEX=          897
a'=                                       1 b'=                  78784183
c'=                             -147529417152 ind'=                     897

(225) A=   1 B=         -878055938 C=                 11219865036100 INDEX=        14786
a'=                                  171803 b'=                -1110190121
c'=                              1777090438034 ind'=                   10963

(226) A=   1 B=         -242312834 C=                 -1767584354508 INDEX=         2946
a'=                                       1 b'=                -242312834
c'=                          -1767584354508 ind'=                    2946

(227) A=   0 B=          -16880702 C=                    50421224171 INDEX=          125
a'=                                       0 b'=                 -16880702
c'=                              50421224171 ind'=                     125

(228) A=   1 B=          298175837 C=                   868523163924 INDEX=         6323
a'=                                       1 b'=                 298175837
c'=                              868523163924 ind'=                    6323
```

```
(229) A=   1 B=          743675422 C=                  -122656400924 INDEX=          22814
a'=                          41977 b'=                    341061357
c'=                  4133863058094 ind'=                      13461

(230) A=   0 B=         -115175924 C=                   490027509137 INDEX=            343
a'=                              0 b'=                   -115175924
c'=                   490027509137 ind'=                        343

(231) A=   0 B=          268527715 C=                   847113845032 INDEX=           5534
a'=                          53117 b'=                    -11623623
c'=                   9803818574 ind'=                         1331

(232) A=   0 B=          -14484563 C=                    21393959070 INDEX=              8
a'=                              0 b'=                    -14484563
c'=                    21393959070 ind'=                         8

(233) A=   1 B=          151234237 C=                   765667931352 INDEX=           3063
a'=                              1 b'=                    151234237
c'=                   765667931352 ind'=                        3063

(234) A=   1 B=         -820574222 C=                  20975414557548 INDEX=          55302
a'=                         -10957 b'=                    121470125
c'=                  1267265736438 ind'=                       4787

(235) A=   1 B=         -212304131 C=                   1575400558794 INDEX=           3015
a'=                              1 b'=                   -212304131
c'=                   1575400558794 ind'=                       3015

(236) A=   0 B=          -12310190 C=                    160668173509 INDEX=            467
a'=                              0 b'=                    -12310190
c'=                    160668173509 ind'=                        467

(237) A=   0 B=         -941762648 C=                   14378474948905 INDEX=          26623
a'=                         -26612 b'=                    252291798
c'=                  2421478165887 ind'=                       9537

(238) A=   1 B=          -49065611 C=                    648395871610 INDEX=           1855
a'=                              1 b'=                    -49065611
c'=                    648395871610 ind'=                        1855

(239) A=   0 B=           91431832 C=                    238312603133 INDEX=           1205
a'=                              0 b'=                     91431832
c'=                    238312603133 ind'=                        1205

(240) A=   0 B=           99252694 C=                    250191063301 INDEX=           1331
a'=                              0 b'=                     99252694
c'=                    250191063301 ind'=                        1331

(241) A=   0 B=          120057340 C=                   1512477523203 INDEX=           4661
a'=                              0 b'=                    120057340
c'=                   1512477523203 ind'=                       4661

(242) A=   1 B=          -55306565 C=                   -244648336262 INDEX=            545
a'=                              1 b'=                    -55306565
c'=                   -244648336262 ind'=                       545

(243) A=   1 B=           6171815 C=                     106261430454 INDEX=            311
a'=                              1 b'=                     6171815
c'=                    106261430454 ind'=                        311

(244) A=   1 B=          259696641 C=                    834226650162 INDEX=           5301
a'=                              1 b'=                    259696641
c'=                    834226650162 ind'=                        5301

(245) A=   1 B=           -6081769 C=                     11478654300 INDEX=             29
a'=                              1 b'=                     -6081769
```

```
c'=                                  11478654300 ind'=                    29

(246) A=   1 B=          852511377 C=                  14196409955406 INDEX=          50049
a'=                            17937 b'=                    81668764
c'=                      2460816439056 ind'=                 7012

(247) A=   1 B=         -115925694 C=                   1468056578452 INDEX=           4054
a'=                             1 b'=                  -115925694
c'=                      1468056578452 ind'=                 4054

(248) A=   1 B=         -704586679 C=                 -23121510631180 INDEX=          64209
a'=                         -8991 b'=                    89146042
c'=                      1336307691396 ind'=                 4562

(249) A=   1 B=           15119737 C=                    454906178290 INDEX=           1331
a'=                             1 b'=                    15119737
c'=                       454906178290 ind'=                 1331

(250) A=   1 B=          724426942 C=                   -8002988967788 INDEX=          32062
a'=                         23741 b'=                   -55413777
c'=                       892821825198 ind'=                 5277

(251) A=   1 B=              92837 C=                    -341992374 INDEX=              1
a'=                             1 b'=                       92837
c'=                      -341992374 ind'=                    1

(252) A=   1 B=          105624546 C=                   -3177625870980 INDEX=          9366
a'=                             1 b'=                   105624546
c'=                     -3177625870980 ind'=                9366

(253) A=   0 B=          528068455 C=                   1728608668492 INDEX=          14554
a'=                             0 b'=                   528068455
c'=                      1728608668492 ind'=                14554

(254) A=   1 B=          607739615 C=                   80154128456544 INDEX=         234839
a'=                          2604 b'=                    -4853288
c'=                       487638721559 ind'=                 1441

(255) A=   1 B=           44100574 C=                    -57641133860 INDEX=           370
a'=                             1 b'=                    44100574
c'=                      -57641133860 ind'=                  370

(256) A=   1 B=         -330244659 C=                   -7317772828130 INDEX=          20291
a'=                        -15686 b'=                    96984090
c'=                      5319254827971 ind'=                16191

(257) A=   0 B=         -591441923 C=                    5546822888622 INDEX=           1000
a'=                             0 b'=                  -591441923
c'=                      5546822888622 ind'=                 1000

(258) A=   1 B=          593683388 C=                   -4771269573588 INDEX=          21428
a'=                         27711 b'=                     6052453
c'=                      2424487538132 ind'=                10637

(259) A=   1 B=           -6790557 C=                    11476130472 INDEX=             27
a'=                             1 b'=                    -6790557
c'=                       11476130472 ind'=                   27

(260) A=   0 B=          -18713000 C=                    31159424727 INDEX=              1
a'=                             0 b'=                   -18713000
c'=                       31159424727 ind'=                   1

(261) A=   1 B=         -357175161 C=                   -2998768914890 INDEX=          4375
a'=                             1 b'=                  -357175161
c'=                     -2998768914890 ind'=                4375
```

```
(262) A=    0 B=
a'=
c'=

(263) A=    1 B=
a'=
c'=

(264) A=    0 B=
a'=
c'=

(265) A=    0 B=
a'=
c'=

(266) A=    1 B=
a'=
c'=

(267) A=    1 B=
a'=
c'=

(268) A=    1 B=
a'=
c'=

(269) A=    1 B=
a'=
c'=

(270) A=    0 B=
a'=
c'=

(271) A=    1 B=
a'=
c'=

(272) A=    0 B=
a'=
c'=

(273) A=    1 B=
a'=
c'=

(274) A=    1 B=
a'=
c'=

(275) A=    0 B=
a'=
c'=

(276) A=    0 B=
a'=
c'=

(277) A=    1 B=
a'=
c'=

(278) A=    1 B=
a'=
```

```
990648100 C=
                23053 b'=
         2924702004784 ind'=

  258351 C=
                    1 b'=
          338529430 ind'=

 -302672 C=
                    0 b'=
          348146985 ind'=

  502270 C=
                    0 b'=
          313570727 ind'=

383142945 C=
                44721 b'=
         144300834816 ind'=

-10639153 C=
                    1 b'=
         -177422674836 ind'=

 31338442 C=
                    1 b'=
          70852315060 ind'=

 13198896 C=
                    1 b'=
          11793586240 ind'=

  375784 C=
                    0 b'=
          330510039 ind'=

 -3189107 C=
                    1 b'=
          9494720838 ind'=

 -664940 C=
                    0 b'=
          400816727 ind'=

685629486 C=
                49673 b'=
         5998960253214 ind'=

457459737 C=
                37381 b'=
         796992000000 ind'=

-31981547 C=
                    0 b'=
          349205689514 ind'=

557304136 C=
                31723 b'=
         2912990989888 ind'=

-278099027 C=
                    1 b'=
         2470864514032 ind'=

 34981563 C=
                    1 b'=
```

```
11522488802013 INDEX=      48619
          153266316
               7756

  338529430 INDEX=          1
             258351
                  1

  348146985 INDEX=          1
            -302672
                  1

  313570727 INDEX=          1
             502270
                  1

  574630214004 INDEX=    8601
            -8695808
                4096

-177422674836 INDEX=     517
           -10639153
                 517

  70852315060 INDEX=      286
            31338442
                 286

  11793586240 INDEX=       64
            13198896
                  64

  330510039 INDEX=          1
             375784
                  1

  9494720838 INDEX=        27
            -3189107
                  27

  400816727 INDEX=          1
             -664940
                  1

1197221932612 INDEX=    20494
           540250893
               17109

1994328864234 INDEX=    12453
           -39304000
                8000

  349205689514 INDEX=     1000
            -31981547
                 1000

3331132892633 INDEX=    17713
            47666808
               12824

2470864514032 INDEX=     4993
           -278099027
                4993

  71637094372 INDEX=      313
            34981563
```

```
c'=                                  71637094372 ind'=                    313

(279) A=   0 B=      -412060175 C=                    8781729374398 INDEX=          23876
a'=                        -13807 b'=                        186616287
c'=                  3363487592036 ind'=                       11869

(280) A=   1 B=       255479629 C=                     258972618130 INDEX=           4655
a'=                            1 b'=                        255479629
c'=                   258972618130 ind'=                        4655

(281) A=   1 B=         -375589 C=                       -353604870 INDEX=              1
a'=                            1 b'=                          -375589
c'=                    -353604870 ind'=                           1

(282) A=   1 B=       658497819 C=                    -1100815802738 INDEX=          19277
a'=                        36447 b'=                        113951908
c'=                  1892393480528 ind'=                        9908

(283) A=   0 B=        94932514 C=                      284075867109 INDEX=           1331
a'=                            0 b'=                         94932514
c'=                   284075867109 ind'=                        1331

(284) A=   0 B=        -2193875 C=                       3009758434 INDEX=              8
a'=                            0 b'=                         -2193875
c'=                    3009758434 ind'=                           8

(285) A=   1 B=      -435246959 C=                    -5502997177550 INDEX=          12421
a'=                            1 b'=                        -435246959
c'=                  -5502997177550 ind'=                       12421

(286) A=   0 B=        68107990 C=                      732145236063 INDEX=           2231
a'=                        88943 b'=                         12219714
c'=                   852072444 ind'=                            618

(287) A=   1 B=      -618905508 C=                    -15930570437136 INDEX=          43212
a'=                       -13299 b'=                         83961991
c'=                  2295832861452 ind'=                        7289

(288) A=   0 B=      -255739886 C=                     2285209134369 INDEX=           4841
a'=                            0 b'=                        -255739886
c'=                  2285209134369 ind'=                        4841

(289) A=   1 B=       540468853 C=                     3055553081638 INDEX=          16717
a'=                        32633 b'=                         52395540
c'=                  3025046533968 ind'=                       13452

(290) A=   1 B=       200246197 C=                     1279482802474 INDEX=           4913
a'=                            1 b'=                        200246197
c'=                  1279482802474 ind'=                        4913

(291) A=   1 B=      -334141578 C=                     2879215306564 INDEX=           4858
a'=                            1 b'=                        -334141578
c'=                  2879215306564 ind'=                        4858

(292) A=   1 B=       -13304599 C=                      -18686448348 INDEX=              1
a'=                            1 b'=                         -13304599
c'=                   -18686448348 ind'=                           1

(293) A=   1 B=      -641471949 C=                    -7797132235430 INDEX=          13609
a'=                            1 b'=                        -641471949
c'=                  -7797132235430 ind'=                       13609

(294) A=   1 B=      -279106394 C=                    -1823074601780 INDEX=            934
a'=                            1 b'=                        -279106394
c'=                  -1823074601780 ind'=                         934
```

```
(295) A=   1 B=          490819519 C=                    2895992288752 INDEX=          14873
a'=                                    1 b'=                490819519
c'=                      2895992288752 ind'=                    14873

(296) A=   1 B=         -830770846 C=                   11096129083212 INDEX=          18058
a'=                                -24467 b'=                326115973
c'=                      1645900184122 ind'=                     9547

(297) A=   1 B=          164473513 C=                   -2159827116548 INDEX=           6743
a'=                                    1 b'=                164473513
c'=                     -2159827116548 ind'=                     6743

(298) A=   1 B=           90219927 C=                     317091511384 INDEX=           1337
a'=                                    1 b'=                 90219927
c'=                       317091511384 ind'=                     1337

(299) A=   0 B=          133863595 C=                     834930712704 INDEX=           2998
a'=                                    0 b'=                133863595
c'=                       834930712704 ind'=                     2998

(300) A=   0 B=          485130211 C=                    1423173291728 INDEX=          12718
a'=                                38221 b'=                -12071997
c'=                       640572707662 ind'=                     7097

(301) A=   1 B=          -59940599 C=                    -301849067508 INDEX=            711
a'=                                    1 b'=                -59940599
c'=                      -301849067508 ind'=                      711

(302) A=   1 B=           -9625713 C=                      14744429874 INDEX=             27
a'=                                    1 b'=                 -9625713
c'=                        14744429874 ind'=                       27

(303) A=   1 B=         -248917829 C=                    2635407856470 INDEX=           6309
a'=                                    1 b'=                -248917829
c'=                      2635407856470 ind'=                     6309

(304) A=   1 B=          114571332 C=                     508758360624 INDEX=           2028
a'=                                    1 b'=                 114571332
c'=                       508758360624 ind'=                     2028

(305) A=   1 B=         -467111343 C=                    4233730880044 INDEX=           4913
a'=                                    1 b'=                -467111343
c'=                      4233730880044 ind'=                     4913

(306) A=   1 B=          616823743 C=                    16168671160492 INDEX=          50293
a'=                                12907 b'=                 -54915410
c'=                      1564820626612 ind'=                     5578

(307) A=   0 B=         -672816554 C=                   23304734800523 INDEX=          65213
a'=                                -9427 b'=                 63398388
c'=                      1505012742608 ind'=                     4804

(308) A=   1 B=         -238803523 C=                    1904758762926 INDEX=           3709
a'=                                    1 b'=                -238803523
c'=                      1904758762926 ind'=                     3709

(309) A=   0 B=           -5586230 C=                      18834951219 INDEX=             53
a'=                                    0 b'=                 -5586230
c'=                        18834951219 ind'=                       53

(310) A=   1 B=          -36161888 C=                     111652688496 INDEX=            216
a'=                                    1 b'=                 -36161888
c'=                       111652688496 ind'=                      216

(311) A=   1 B=           8238314 C=                     -119419740636 INDEX=            350
a'=                                    1 b'=                  8238314
```

```
c'=                          -119419740636 ind'=                        350

(312) A=   1 B=          -161066153 C=                  -9580725062496 INDEX=          27903
a'=                            73961 b'=                     653576000
c'=                      1785792000000 ind'=                      8000

(313) A=   1 B=           -13151491 C=                   -358070676666 INDEX=           1045
a'=                                1 b'=                     -13151491
c'=                      -358070676666 ind'=                      1045

(314) A=   1 B=            74249904 C=                    237627437104 INDEX=           1000
a'=                                1 b'=                      74249904
c'=                       237627437104 ind'=                      1000

(315) A=   0 B=           522489700 C=                    519477646937 INDEX=          13519
a'=                            44272 b'=                     184954194
c'=                      2027701412671 ind'=                     12247

(316) A=   1 B=             6156443 C=                     7129175222 INDEX=             27
a'=                                1 b'=                       6156443
c'=                        7129175222 ind'=                        27

(317) A=   1 B=           -68329560 C=                    218478309904 INDEX=             64
a'=                                1 b'=                     -68329560
c'=                       218478309904 ind'=                        64

(318) A=   0 B=           -94482044 C=                    372463107217 INDEX=            343
a'=                                0 b'=                     -94482044
c'=                       372463107217 ind'=                       343

(319) A=   1 B=           258752060 C=                   -494885319600 INDEX=           4900
a'=                                1 b'=                     258752060
c'=                      -494885319600 ind'=                      4900

(320) A=   0 B=          -200793338 C=                   1152050115213 INDEX=           1045
a'=                                0 b'=                    -200793338
c'=                      1152050115213 ind'=                      1045

(321) A=   0 B=           750695920 C=                    8885348759871 INDEX=          34777
a'=                            52469 b'=                    -392957227
c'=                       968194544538 ind'=                       9347

(322) A=   0 B=           -35831588 C=                      92979092613 INDEX=            125
a'=                                0 b'=                     -35831588
c'=                        92979092613 ind'=                        125

(323) A=   0 B=          -965270027 C=                   19663583884746 INDEX=          46520
a'=                            77453 b'=                     113205723
c'=                       43500340280 ind'=                        967

(324) A=   0 B=          -558133325 C=                   82776356467584 INDEX=         241442
a'=                            -2281 b'=                       6621765
c'=                       476612544050 ind'=                       1405

(325) A=   0 B=            63101239 C=                     17039090844 INDEX=            566
a'=                                0 b'=                      63101239
c'=                       17039090844 ind'=                        566

(326) A=   1 B=           -512399448 C=                    5340892425444 INDEX=          8568
a'=                                1 b'=                     -512399448
c'=                      5340892425444 ind'=                      8568

(327) A=   1 B=          -266952115 C=                    1681740255288 INDEX=           295
a'=                                1 b'=                    -266952115
c'=                      1681740255288 ind'=                       295
```

```
(328) A=   1 B=          -1237799 C=                    630507430 INDEX=                1
a'=                             1 b'=                    -1237799
c'=                     630507430 ind'=                         1

(329) A=   0 B=           625313860 C=                 540857737907 INDEX=            17659
a'=                         52880 b'=                   -752324066
c'=                  2740082880899 ind'=                    12571

(330) A=   1 B=           85636832 C=                  506597825012 INDEX=             1728
a'=                             1 b'=                     85636832
c'=                   506597825012 ind'=                      1728

(331) A=   1 B=         -618018465 C=                 -9445044083576 INDEX=            21521
a'=                        -15820 b'=                   273526024
c'=                  1933692861761 ind'=                     9479

(332) A=   0 B=           428636335 C=                  3841535461244 INDEX=            15022
a'=                             0 b'=                    428636335
c'=                  3841535461244 ind'=                    15022

(333) A=   1 B=           248385235 C=                 -6726787150812 INDEX=            20145
a'=                         12504 b'=                   -51615284
c'=                  5099906608545 ind'=                    15911

(334) A=   1 B=           516946685 C=                  -213272133900 INDEX=            13235
a'=                         41543 b'=                    86975698
c'=                  1015158434540 ind'=                     8758

(335) A=   1 B=             4235449 C=                   -66642520776 INDEX=              195
a'=                             1 b'=                     4235449
c'=                   -66642520776 ind'=                      195

(336) A=   1 B=           90446821 C=                   544027483822 INDEX=             1861
a'=                             1 b'=                     90446821
c'=                   544027483822 ind'=                      1861

(337) A=   1 B=          -105786927 C=                  -434962192652 INDEX=             343
a'=                             1 b'=                    -105786927
c'=                  -434962192652 ind'=                      343

(338) A=   1 B=           587165296 C=                  1122431855872 INDEX=            16336
a'=                             1 b'=                    587165296
c'=                  1122431855872 ind'=                    16336

(339) A=   0 B=           -46246829 C=                   255642239928 INDEX=              658
a'=                             0 b'=                    -46246829
c'=                   255642239928 ind'=                      658

(340) A=   0 B=           -40717022 C=                   108766824939 INDEX=              125
a'=                             0 b'=                    -40717022
c'=                   108766824939 ind'=                      125

(341) A=   0 B=            -8122340 C=                    8916407977 INDEX=                1
a'=                             0 b'=                     -8122340
c'=                     8916407977 ind'=                        1

(342) A=   0 B=          -718313336 C=                  8010301106931 INDEX=             8891
a'=                             0 b'=                    -718313336
c'=                  8010301106931 ind'=                     8891

(343) A=   1 B=           538462117 C=                  8513220108934 INDEX=            28573
a'=                         81438 b'=                    678723928
c'=                  1868953098625 ind'=                    12167

(344) A=   0 B=          -163397408 C=                  1720445067493 INDEX=             4445
a'=                             0 b'=                    -163397408
```

```
c'=                                1720445067493 ind'=                    4445

(345) A=   1 B=          -59138429 C=                  283295735832 INDEX=          651
a'=                                1 b'=                  -59138429
c'=                    283295735832 ind'=                     651

(346) A=   0 B=          580626565 C=                 2678490108998 INDEX=        17576
a'=                            33047 b'=                    7231185
c'=                   1476335226600 ind'=                    9165

(347) A=   1 B=         -254091093 C=                 1558865664316 INDEX=            1
a'=                                1 b'=                  -254091093
c'=                   1558865664316 ind'=                       1

(348) A=   0 B=            -206930 C=                    344109273 INDEX=            1
a'=                                0 b'=                  -206930
c'=                    344109273 ind'=                        1

(349) A=   1 B=          485349491 C=                 1447546193280 INDEX=        12749
a'=                                1 b'=                   485349491
c'=                   1447546193280 ind'=                    12749

(350) A=   0 B=            8694373 C=                   19551689910 INDEX=           64
a'=                                0 b'=                    8694373
c'=                     19551689910 ind'=                      64

(351) A=   1 B=          161745397 C=                 2883080437672 INDEX=         8737
a'=                            52854 b'=                  -104256950
c'=                    105504735625 ind'=                     3475

(352) A=   0 B=         -462041282 C=                 4646898233665 INDEX=         7721
a'=                                0 b'=                  -462041282
c'=                   4646898233665 ind'=                    7721

(353) A=   1 B=          549968710 C=                 1345067087700 INDEX=        15030
a'=                            39065 b'=                   155426237
c'=                   3255349037670 ind'=                    14717

(354) A=   0 B=         -219700343 C=                 1423522051270 INDEX=         1972
a'=                                0 b'=                  -219700343
c'=                   1423522051270 ind'=                    1972

(355) A=   0 B=         -176639780 C=                 2515057066493 INDEX=         6859
a'=                           110872 b'=                  -130911318
c'=                     41812196499 ind'=                     2469

(356) A=   1 B=           23076635 C=                  277692020064 INDEX=          821
a'=                                1 b'=                   23076635
c'=                    277692020064 ind'=                      821

(357) A=   1 B=         -379088652 C=                 6026483838748 INDEX=        15532
a'=                            89549 b'=                  -273040143
c'=                    218069419788 ind'=                     3747

(358) A=   1 B=          256986543 C=                -2622927938108 INDEX=         8957
a'=                            51379 b'=                    15259038
c'=                     3420893268 ind'=                       618

(359) A=   1 B=          119424752 C=                 1000698847152 INDEX=         3272
a'=                                1 b'=                   119424752
c'=                   1000698847152 ind'=                    3272

(360) A=   1 B=          155715092 C=                 1196789957040 INDEX=         4124
a'=                                1 b'=                   155715092
c'=                   1196789957040 ind'=                    4124
```

```
(361) A=    1 B=          -308362888 C=                    2885500659392 INDEX=                5832
a'=                                1 b'=                        -308362888
c'=                  2885500659392 ind'=                           5832

(362) A=    1 B=          -115449997 C=                    1747658002308 INDEX=                4913
a'=                                1 b'=                        -115449997
c'=                  1747658002308 ind'=                           4913

(363) A=    1 B=           359311255 C=                   19799626362300 INDEX=               58365
a'=                           100369 b'=                        212221200
c'=                   134461691136 ind'=                           4944

(364) A=    1 B=          -388753803 C=                    5037572234764 INDEX=               11933
a'=                                1 b'=                        -388753803
c'=                  5037572234764 ind'=                          11933
```