Computational Techniques in Quadratic Fields

by

Michael John Jacobson, Jr.

A thesis
presented to the University of Manitoba
in partial fulfilment of the
requirements for the degree of
Master of Science
in
Computer Science

Winnipeg, Manitoba, Canada, 1995

ISBN 0-612-16170-6

Canada

Name_____

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

Computer Science

SUBJECT TERM

0984

SUBJECT CODE

U·M·I

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS

Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION

General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0680
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0279
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523

Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0288
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS

Language
- General 0679
- Ancient 0289
- Linguistics 0290
- Modern 0291

Literature
- General 0401
- Classical 0294
- Comparative 0295
- Medieval 0297
- Modern 0298
- African 0316
- American 0591
- Asian 0305
- Canadian (English) 0352
- Canadian (French) 0355
- English 0593
- Germanic 0311
- Latin American 0312
- Middle Eastern 0315
- Romance 0313
- Slavic and East European 0314

PHILOSOPHY, RELIGION AND THEOLOGY

Philosophy 0422
Religion
- General 0318
- Biblical Studies 0321
- Clergy 0319
- History of 0320
- Philosophy of 0322

Theology 0469

SOCIAL SCIENCES

American Studies 0323
Anthropology
- Archaeology 0324
- Cultural 0326
- Physical 0327

Business Administration
- General 0310
- Accounting 0272
- Banking 0770
- Management 0454
- Marketing 0338

Canadian Studies 0385
Economics
- General 0501
- Agricultural 0503
- Commerce-Business 0505
- Finance 0508
- History 0509
- Labor 0510
- Theory 0511

Folklore 0358
Geography 0366
Gerontology 0351
History
- General 0578
- Ancient 0579
- Medieval 0581
- Modern 0582
- Black 0328
- African 0331
- Asia, Australia and Oceania 0332
- Canadian 0334
- European 0335
- Latin American 0336
- Middle Eastern 0333
- United States 0337

History of Science 0585
Law 0398
Political Science
- General 0615
- International Law and Relations 0616
- Public Administration 0617

Recreation 0814
Social Work 0452
Sociology
- General 0626
- Criminology and Penology 0627
- Demography 0938
- Ethnic and Racial Studies 0631
- Individual and Family Studies 0628
- Industrial and Labor Relations 0629
- Public and Social Welfare 0630
- Social Structure and Development 0700
- Theory and Methods 0344

Transportation 0709
Urban and Regional Planning 0999
Women's Studies 0453

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES

Agriculture
- General 0473
- Agronomy 0285
- Animal Culture and Nutrition 0475
- Animal Pathology 0476
- Food Science and Technology 0359
- Forestry and Wildlife 0478
- Plant Culture 0479
- Plant Pathology 0480
- Plant Physiology 0817
- Range Management 0777
- Wood Technology 0746

Biology
- General 0306
- Anatomy 0287
- Biostatistics 0308
- Botany 0309
- Cell 0379
- Ecology 0329
- Entomology 0353
- Genetics 0369
- Limnology 0793
- Microbiology 0410
- Molecular 0307
- Neuroscience 0317
- Oceanography 0416
- Physiology 0433
- Radiation 0821
- Veterinary Science 0778
- Zoology 0472

Biophysics
- General 0786
- Medical 0760

EARTH SCIENCES

Biogeochemistry 0425
Geochemistry 0996
Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleoecology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES

Environmental Sciences 0768
Health Sciences
- General 0566
- Audiology 0300
- Chemotherapy 0992
- Dentistry 0567
- Education 0350
- Hospital Management 0769
- Human Development 0758
- Immunology 0982
- Medicine and Surgery 0564
- Mental Health 0347
- Nursing 0569
- Nutrition 0570
- Obstetrics and Gynecology 0380
- Occupational Health and Therapy 0354
- Ophthalmology 0381
- Pathology 0571
- Pharmacology 0419
- Pharmacy 0572
- Physical Therapy 0382
- Public Health 0573
- Radiology 0574
- Recreation 0575
- Speech Pathology 0460
- Toxicology 0383

Home Economics 0386

PHYSICAL SCIENCES

Pure Sciences

Chemistry
- General 0485
- Agricultural 0749
- Analytical 0486
- Biochemistry 0487
- Inorganic 0488
- Nuclear 0738
- Organic 0490
- Pharmaceutical 0491
- Physical 0494
- Polymer 0495
- Radiation 0754

Mathematics 0405
Physics
- General 0605
- Acoustics 0986
- Astronomy and Astrophysics 0606
- Atmospheric Science 0608
- Atomic 0748
- Electronics and Electricity 0607
- Elementary Particles and High Energy 0798
- Fluid and Plasma 0759
- Molecular 0609
- Nuclear 0610
- Optics 0752
- Radiation 0756
- Solid State 0611

Statistics 0463

Applied Sciences

Applied Mechanics 0346
Computer Science 0984
Engineering
- General 0537
- Aerospace 0538
- Agricultural 0539
- Automotive 0540
- Biomedical 0541
- Chemical 0542
- Civil 0543
- Electronics and Electrical 0544
- Heat and Thermodynamics 0348
- Hydraulic 0545
- Industrial 0546
- Marine 0547
- Materials Science 0794
- Mechanical 0548
- Metallurgy 0743
- Mining 0551
- Nuclear 0552
- Packaging 0549
- Petroleum 0765
- Sanitary and Municipal 0554
- System Science 0790

Geotechnology 0428
Operations Research 0796
Plastics Technology 0795
Textile Technology 0994

PSYCHOLOGY

General 0621
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0989
Psychobiology 0349
Psychometrics 0632
Social 0451

COMPUTATIONAL TECHNIQUES IN QUADRATIC FIELDS

BY

MICHAEL JOHN JACOBSON

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

MASTER OF SCIENCE

I hereby declare that I am the sole author of this thesis.

I authorize the University of Manitoba to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the University of Manitoba to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Abstract

Since Kummer's work on Fermat's Last Theorem, algebraic number theory has been a subject of interest for many mathematicians. In particular, a great amount of effort has been expended on the simplest algebraic extensions of the rationals, quadratic fields. These are intimately linked to binary quadratic forms and have proven to be a good testing ground for algebraic number theorists because, although computing with ideals and field elements is relatively easy, there are still many unsolved and difficult problems remaining. For example, it is not known whether there exist infinitely many real quadratic fields with class number one, and the best unconditional algorithm known for computing the class number has complexity $O\left(D^{1/2+\epsilon}\right)$. In fact, the apparent difficulty of computing class numbers has given rise to cryptographic algorithms based on arithmetic in quadratic fields. Factoring methods using quadratic fields have also been proposed which are dependent on being able to compute class numbers and regulators.

The main goal of this thesis is to provide extensive numerical evidence in support of some unresolved conjectures related to quadratic fields. We first give an algorithm for computing class numbers and regulators of real quadratic fields, based on an algorithm due to Buchmann and Williams, that has complexity $O\left(D^{1/5+\epsilon}\right)$ and is conditional on the truth of the Extended Riemann Hypothesis. Our algorithm makes use of some improvements, including a new method for estimating $L(1,\chi)$ due to Bach, and it performs about 1.5 times as quickly as similar algorithms which use truncated Euler products to estimate $L(1,\chi)$. We then use this algorithm to compute class numbers of $\mathbb{Q}(\sqrt{D})$ for all square-free $D < 10^8$ and $\mathbb{Q}(\sqrt{p})$ for all prime $p < 10^9$ in order to test some heuristics due to Cohen and Lenstra on the distribution of real quadratic fields with certain class numbers, as well as a conjecture due to Hooley. Using a new sieving device, the MSSU, we examine the size of the regulator of $\mathbb{Q}(\sqrt{D})$ by employing a strategy of Shanks to find fields with large $L(1,\chi)$ values. Our results lend support to a result of Littlewood that gives bounds on $L(1,\chi)$ assuming the truth of the Extended Riemann Hypothesis. Finally, we use MSSU to search for values of A such that the quadratic polynomial $x^2 + x + A$ has a high asymptotic density of prime values in order to test a conjecture of Hardy and Littlewood.

Acknowledgements

I would like to take this opportunity to thank, first of all, my supervisor Dr. H.C. Williams. I first came into contact with him as a second year undergraduate student when he hired me as a summer research assistant, and I have been working with him ever since. It was he who introduced me to the fascinating subject of computational number theory. His generous financial support and constant encouragement have been immensely helpful to me throughout my studies, and are greatly appreciated.

I also wish to thank the other members of my examining committee, Dr. M.W. Giesbrecht and Dr. J. Fabrykowski, for their careful reading of this thesis and their helpful suggestions for improving it.

Special thanks go out to Richard Lukes for supplying me with all the numbers generated by his sieve, the MSSU, which were used in Chapters 5 and 6.

Finally, I wish to thank my family and friends, especially Barbara, for all the support and encouragement I received from them during my studies, and for their patience with my reclusiveness during the last few months while I finished this work.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The origins of algebraic number theory can be traced back to Kummer's attempt to prove Fermat's Last Theorem (FLT), which states that there do not exist integers x, y, and z such that $x^n + y^n = z^n$ for $n > 2$ and $xyz \neq 0$ and until recently had been unproved, despite the efforts of many of the most talented mathematicians. At one time Kummer thought he had proved it, but his proof hinged upon the false assumption that cyclotomic integers always factor uniquely. The ring of cyclotomic integers $\mathbb{Z}[\zeta_m]$, as defined by Kummer, is the set of all complex numbers of the form $a_0 + a_1\zeta_m + \cdots + a_n\zeta_m^n$ where the $a_i \in \mathbb{Z}$ and ζ_m is a primitive m^{th} root of unity for some positive $m \in \mathbb{Z}$. It is a subset of the cyclotomic field $\mathcal{K} = \mathbb{Q}(\zeta_m)$, the set of all complex numbers of the form $b_0 + b_1\zeta_m + \cdots + b_n\zeta_m^n$ where the $b_i \in \mathbb{Q}$. Kummer found that unique factorization holds in $\mathbb{Z}[\zeta_m]$ if and only if a quantity called the *class number* h of $\mathcal{K}$ is equal to 1. In order to circumvent this problem, Kummer developed the idea of ideal complex numbers and was eventually able to prove that FLT holds for all regular prime exponents, the primes p with the property that $p \nmid h$ where $\mathcal{K} = \mathbb{Q}(\zeta_p)$.

Algebraic number fields are a natural generalization of Kummer's cyclotomic fields. Rather than a primitive m^{th} root of unity, we use a zero ϱ of a polynomial which is irreducible over $\mathbb{Q}$ to form a finite extension of the rationals $\mathbb{Q}(\varrho)$. Each such field $\mathcal{K}$

also contains a ring of algebraic integers $\mathcal{O}_\mathcal{K}$. Dedekind introduced his theory of ideals based on Kummer's ideal complex numbers in an effort to solve problems that he saw in Kummer's methods, and eventually a complete theory for algebraic numbers appeared in the late 1800's as a result of his and Kronecker's work.

As in cyclotomic fields, unique factorization holds in an algebraic number field if and only if the class number of the corresponding field is equal to 1. For example, consider the field $\mathbb{Q}(\sqrt{-5})$. The irreducible polynomial x^2+5 has $\sqrt{-5}$ as a zero, so $\mathbb{Q}(\sqrt{-5})$ is an algebraic number field. The ring of algebraic integers in this field contains elements of the form $a_0 + a_1\sqrt{-5}$ with $a_0, a_1 \in \mathbb{Z}$, so 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all integers in $\mathbb{Q}(\sqrt{-5})$. It can be shown that each of these integers is prime in $\mathbb{Q}(\sqrt{-5})$, i.e., none of them has any non-trivial divisors. However, we can write the algebraic integer 6 as either $6 = 2 \cdot 3$ or $6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$. Thus, 6 factors as a product of primes in two different ways in $\mathbb{Q}(\sqrt{-5})$. In fact, the class number of this field is two, so we know that unique factorization does not hold. Class numbers larger than one provide some indication of how far away their corresponding fields are from unique factorization, but it is not clear exactly what kind of measure is provided.

If ϱ is a zero of a polynomial in $\mathbb{Z}[x]$ of degree n but not of any of lower degree, then we say that the field $\mathbb{Q}(\varrho)$ has degree n. *Quadratic fields* are fields of degree 2, i.e., they are fields where the rationals are finitely extended by a root of an irreducible quadratic polynomial. We further distinguish between *imaginary quadratic fields* $\mathbb{Q}(\sqrt{D})$, $D < 0$, and *real quadratic fields* $\mathbb{Q}(\sqrt{D})$, $D > 0$. The study of both types of fields is related to that of Gauss' theory of binary quadratic forms $Ax^2 + Bxy + Cy^2$, $A, B, C \in \mathbb{Z}$. He considered sets of forms with the same *discriminant*, where the discriminant is defined to be $\Delta = B^2 - 4AC$. (We define the discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$ to be $\Delta = D$ if $D \equiv 1 \pmod 4$ and $\Delta = 4D$ otherwise.) Gauss defined the idea of equivalence of forms, and the class number of sets of forms with a particular discriminant as the number of equivalence classes they form. There is a simple relationship relating this class number to the class number of the quadratic field with the same discriminant.

Arithmetic in quadratic fields has led to the development of new integer factoring algorithms. It is known that if Δ is composite, then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ must be even. Shanks [Sha71] has shown that one can factor the discriminant Δ if one can compute the class number of $\mathbb{Q}(\sqrt{-D})$, and in particular a field element of order 2. Such elements correspond to *ambiguous* binary quadratic forms, those forms that are equal to their inverses. He also gave an analogous method of searching for ambiguous forms in real quadratic fields.

Despite being the simplest type of algebraic number fields, there are still many difficult and unsolved problems relating to quadratic fields, such as the famous Gauss conjecture which states that there are infinitely many real quadratic fields that have class number one. Also, class numbers in both real and imaginary quadratic fields can be rather difficult to compute. Currently, the best unconditional algorithm has complexity $O\left(D^{1/2+\epsilon}\right)$. However, computing with quadratic field elements and ideals is relatively easy compared to doing these things in fields of higher degree; thus, quadratic fields are a good testing ground for conjectures and algorithms, as numerical evidence can be more readily obtained.

The apparent difficulty of computing class numbers in quadratic fields has given rise to a number of cryptographic applications involving arithmetic in these fields [BW90]. For example, key exchange protocols have been proposed using both imaginary [BW88] and real quadratic fields [BW89a, Sch93]. The security of these schemes depends upon the choice of field, so knowledge about structures of quadratic fields is needed.

1.1 Organization of the Thesis

The main goal of this thesis is to provide extensive numerical evidence supporting some unresolved conjectures related to quadratic fields. The most important tasks in obtaining these numerical results were computing the class number h of both real and imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ and a quantity called the regulator R of real quadratic fields.

In Chapter 2 we formally define quadratic fields, class numbers, and regulators and give the necessary background pertaining to our investigations, including ideals and infrastructure. In addition, we present two well-known algorithms related to ideals in quadratic fields that are needed for our numerical experiments, the continued fraction expansion algorithm and the ideal multiplication and reduction algorithm. We also define the Dirichlet L-function $L(s,\chi)$ and the analytic class number formula, both of which are essential to our class number algorithms. We briefly discuss the Extended Riemann Hypothesis (ERH), since many of the conjectures and algorithms relating to quadratic fields are dependent on its truth.

We describe our algorithm for computing the regulator and class number of a real quadratic field in Chapter 3. We use the techniques due to Buchmann and Williams [BW89b], given for the real quadratic case in [MW92], which compute h and R in at most $O\left(D^{1/5+\epsilon}\right)$ operations. We also employ a new averaging technique for estimating Euler products developed by Bach [Bac94] which has a better error estimate than the traditional truncated product method. Comparisons between the performance of our algorithm using Bach's idea and truncated products are provided. A few other modifications which result in better performance are also described and implemented.

The first conjectures we consider are the Cohen-Lenstra Heuristics [CL83, CL84]. Since the heuristics pertaining to imaginary quadratic fields have been dealt with in great detail elsewhere (see, for example, Buell [Bue84]) we focus our attention in Chapter 4 on the real case. In particular, we examine the prediction that the odd part of the class group of a real quadratic field has some order l with some definite non-zero probability. For example, fields with odd part of the class group equal to one should occur approximately 75.446% of the time. We also derive another result based on this prediction, which states that the probability of the odd part of the class group being greater than x is $1/(2x) + O\left(\log x/x^2\right)$. These results suggest that class numbers are most likely to be small. In order to test these conjectures we computed class numbers of all the fields $\mathbb{Q}(\sqrt{p})$ for primes $p < 10^9$ and and all fields $\mathbb{Q}(\sqrt{D})$ for square-free $D < 10^8$ using the

techniques of Chapter 3. We then checked whether the actual proportions of fields with class numbers of certain sizes corresponded with the heuristic predictions. We also used this data to test a conjecture of Hooley which states that the sum of class numbers of fields $\mathbb{Q}(\sqrt{p})$ where $p \equiv 1 \pmod 4$, $p < x$ is approximately $x/8$.

In Chapter 5 we turn our attention to the size of another important invariant of real quadratic fields, the regulator. By the results of Chapter 4 we expect that class numbers of real quadratic fields are most likely small, so by examining the analytic class number formula we see that fields with large $L(1,\chi)$ values should often have large regulators. Under the ERH, Littlewood [Lit28] derived bounds on $L(1,\chi)$ which are much tighter than any of the existing unconditional bounds. We used a new sieving device, the MSSU [LPW, LPW95, Luk95] to compute thousands of numbers which should provide values of $L(1,\chi)$ which are close to the local maxima of $L(1,\chi)$. We then used the method of Chapter 3 to evaluate h, R, and $L(1,\chi)$ in an attempt to find values of $L(1,\chi)$ which are as close to Littlewood's bounds as possible. Based on our numerical evidence, we are able to conjecture that $R \gg \sqrt{\Delta}\log\log\Delta$ for an infinite set of discriminants Δ.

Since Euler's time, prime producing polynomials have been of considerable interest to number theorists. A special version of Hardy and Littlewood's Conjecture F [HL23] allows us to predict which polynomials of the form x^2+x+A will have high asymptotic densities of prime values by evaluating the quantity $C(D)$, where $D = 1-4A$. We describe a method of evaluating $C(D)$ to 8 significant digits, which depends on evaluating class numbers and is conditional on the ERH. Using the MSSU, we searched for values of D which we would expect to have locally extreme values of $C(D)$ and used our technique to evaluate $C(D)$ for each of the thousands of solutions we obtained. We considered both positive and negative values of D, and we discuss the method we used to evaluate h in imaginary quadratic fields, which makes use of the well-known ideas of Lenstra [Len82] and Shanks' baby step-giant step algorithm [Sha71]. We were able to find several polynomials which have higher asymptotic densities than any other currently known polynomials of this type.

Finally, in Chapter 7 we briefly discuss some of the other aspects of quadratic fields we have not looked at, including the recent development of subexponential algorithms for computing class numbers.

1.2 Frequently Used Notation

Some of the symbols used frequently throughout this thesis are defined as follows:

- $\mathbb{Z}$ — the integers
- $\mathbb{Q}$ — the rationals
- $\mathbb{C}$ — the complex numbers
- $\log$ — logarithm base e
- $\exp(x)$ — e^x
- $\log_2$ — logarithm base 2
- $[x]$ — integer part of $x \in \mathbb{Q}$, satisfies $x - 1 < [x] \leq x$.
- $\mathrm{Ne}(x)$ — nearest integer to $x \in \mathbb{Q}$, $\mathrm{Ne}(x) = \left[x + \frac{1}{2}\right]$
- $\Re(s)$ — real part of $s \in \mathbb{C}$
- $\mathrm{Prob}(x)$ — probability that proposition x is true
- $f(n)$ is $O(g(n))$ — $f(n) \leq cg(n)$ for some constant c and sufficiently large n
- $f(n)$ is $o(g(n))$ — $f(n)$ is much smaller than $g(n)$, or more formally

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

We use the following symbols pertaining to quadratic fields:

- $\mathcal{K}$ — an arbitrary quadratic field
- $\mathbb{Q}(\sqrt{-D})$ — an arbitrary imaginary quadratic field
- $\mathbb{Q}(\sqrt{D})$ — an arbitrary real quadratic field
- $\mathbb{Q}(\sqrt{p})$ — an arbitrary real quadratic field whose radicand is prime
- D, p — radicand of $\mathcal{K}$ (p if prime)
- Δ — discriminant of $\mathcal{K}$ (Theorem 2.1)
- $\mathcal{O}_{\mathcal{K}}$ — ring of integers in $\mathcal{K}$ (maximal order)
- Cl — class group of $\mathcal{K}$
- h — class number of $\mathcal{K}$ (Definition 2.5)
- ε_0 — fundamental unit of $\mathbb{Q}(\sqrt{D})$ (Definition 2.1)
- R — regulator of $\mathbb{Q}(\sqrt{D})$ (Definition 2.2).

For α an arbitrary quadratic number we define the following:

- $\overline{\alpha}$ – conjugate of α
- $\mathrm{Tr}\,(\alpha)$ — trace of α
- $N(\alpha)$ — norm of α

For $\mathfrak{a}$, $\mathfrak{b}$ arbitrary integral ideals of $\mathcal{O}_{\mathcal{K}}$ (Definition 2.3) we define

- $\overline{\mathfrak{a}}$ — conjugate of $\mathfrak{a}$
- $N(\mathfrak{a})$ — norm of $\mathfrak{a}$
- $L(\mathfrak{a})$ — least positive rational integer in $\mathfrak{a}$

- $\mathfrak{a} \sim \mathfrak{b}$ — ideal equivalence (Definition 2.4)
- $\mathfrak{a} * \mathfrak{b}$ — ideal multiplication followed by reduction (Algorithm 2.4 for imaginary quadratic fields and Algorithm 2.8 for real quadratic fields)
- $\delta(\mathfrak{b}, \mathfrak{a})$ — distance from $\mathfrak{a}$ to $\mathfrak{b}$ (Definition 2.9)
- δ_m — distance from (1) to $\mathfrak{a}_m$ (Definition 2.9)
- $\delta_{\mathfrak{a}}$ — distance associated with $\mathfrak{a}$, either from (1) or another ideal.

Chapter 2

Introduction to Quadratic Fields

Most of the material in this chapter can be found in basic number theory text books, especially [HW62], [Hua82] and [Coh93]. The results on reduced ideals in imaginary quadratic fields can be found in [BW88] and the corresponding results for real quadratic fields can be found in [MW92]. For proofs of the following well-known results and a more definitive treatment of the subject the interested reader should consult these references.

Let ϱ be a zero of a quadratic polynomial that is irreducible over $\mathbb{Q}$. Then the aggregate of all algebraic numbers of the form

$$\xi = b_0 + b_1\varrho,$$

$b_0, b_1 \in \mathbb{Q}$ forms an algebraic number field of degree 2 denoted by $\mathbb{Q}(\varrho)$. Since ϱ is a root of a quadratic polynomial, we can write

$$\varrho = \frac{a + b\sqrt{D}}{c}$$

for $a, b, c, D \in \mathbb{Z}$. Also,

$$\sqrt{D} = \frac{c\varrho - a}{b}$$

where we can assume without loss of generality that D is square-free. In fact, we can

represent any element $\xi \in \mathbb{Q}(\varrho)$ as

$$\xi = \frac{a + b\sqrt{D}}{c},$$

so the fields $\mathbb{Q}(\varrho)$ and $\mathbb{Q}(\sqrt{D})$ are identical. Hence, it is sufficient to only consider fields $\mathbb{Q}(\sqrt{D})$ for square-free integers D, positive or negative. We call D the *radicand* of the quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{D})$. From now on, we will let $\mathcal{K}$ represent an arbitrary quadratic field.

The *conjugate* of $\xi = (a + b\sqrt{D})/c \in \mathcal{K}$ is denoted by

$$\overline{\xi} = \frac{a - b\sqrt{D}}{c}.$$

In imaginary quadratic fields this is simply complex conjugation, but in the real case the meaning is different. The *trace* and *norm* of $\xi \in \mathcal{K}$ are given by

$$\mathrm{Tr}\,(\xi) = \xi + \overline{\xi} = \frac{2a}{c}$$

and

$$N(\xi) = \xi\overline{\xi} = \frac{a^2 - Db^2}{c^2}$$

respectively. It is easy to show that for $\alpha, \beta \in \mathcal{K}$,

$$\mathrm{Tr}\,(\alpha + \beta) = \mathrm{Tr}\,(\alpha) + \mathrm{Tr}\,(\beta)$$

and

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Every element $\xi \in \mathcal{K}$ is the zero of a quadratic polynomial with integer coefficients, since for

$$\xi = \frac{a + b\sqrt{D}}{c}$$

we have $(c\xi - a)^2 = Db^2$; hence ξ is a zero of

$$c^2x^2 - 2acx + a^2 - Db^2. \tag{2.1}$$

Thus, every element $\xi \in \mathcal{K}$ is either a rational or a quadratic number. An *algebraic integer* is defined as a root of a monic quadratic polynomial in $\mathbb{Z}[x]$. Let

$$\vartheta = \frac{a + b\sqrt{D}}{c}$$

with $a, b, c \in \mathbb{Z}$ be an integer in $\mathcal{K}$. We can assume here that $c > 0$ and $(a, b, c) = 1$. If we divide (2.1) by c^2 then we obtain a monic quadratic polynomial

$$x^2 - \frac{2a}{c}x + \frac{a^2 - Db^2}{c^2}.$$

Since it can be shown using the quadratic formula that ϑ is a zero of this polynomial, and since we have defined ϑ to be a zero of a monic quadratic polynomial in $\mathbb{Z}[x]$, $\frac{2a}{c}$ and $\frac{a^2-Db^2}{c^2}$ must be integers and we have that $c \,|\, 2a$ and $c^2 \,|\, (a^2 - Db^2)$. If $d = (a, c)$, then $d^2 \,|\, a^2$ and $d^2 \,|\, c^2$. Also, $d^2 \,|\, (a^2 - Db^2)$, and since $d^2 \,|\, a^2$ we must have $d^2 \,|\, Db^2$. Since D has no square factors, this implies that $d \,|\, b$. However, $(a, b, c) = 1$ so we have $(a, c) = 1$, and since $c \,|\, 2a$, $c = 1$ or $c = 2$. If $c = 2$, then a is odd and $Db^2 \equiv a^2 \equiv 1 \pmod 4$ so b is also odd and $D \equiv 1 \pmod 4$. Therefore, we must distinguish between two cases. If $D \equiv 1 \pmod 4$, then the integers of $\mathcal{K}$ are of the form

$$\vartheta = \frac{a + b\sqrt{D}}{2} \tag{2.2}$$

where $a, b \in \mathbb{Z}$. If $D \equiv 2, 3 \pmod 4$, then the integers of $\mathbb{Q}(\sqrt{D})$ are of the form

$$\vartheta = a + b\sqrt{D} \tag{2.3}$$

where $a, b \in \mathbb{Z}$. As in the case of the rationals, the set of integers of $\mathcal{K}$ forms a ring which we will denote as $\mathcal{O}_\mathcal{K}$, the *maximal order* of $\mathcal{K}$.

If every integer $\vartheta \in \mathcal{O}_\mathcal{K}$ can be uniquely expressed as

$$\vartheta = a_1\omega_1 + a_2\omega_2$$

where $a_i \in \mathbb{Z}, \omega_i \in \mathcal{O}_\mathcal{K}$, then we call ω_1, ω_2 an *integral basis* for $\mathcal{K}$, and we denote $\mathcal{O}_\mathcal{K}$ by the $\mathbb{Z}$-module

$$[\omega_1, \omega_2] = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}.$$

Every algebraic number field has an integral basis, and in quadratic fields it is especially easy to give one. If $D \equiv 2, 3 \pmod 4$, then from (2.3) it is obvious that

$$\omega_1 = 1, \quad \omega_2 = \sqrt{D}$$

is an integral basis. If $D \equiv 1 \pmod 4$, then from (2.2) we see that

$$\vartheta = \frac{a-b}{2} + b\frac{1+\sqrt{D}}{2},$$

so

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{D}}{2}$$

is an integral basis. The *discriminant* of $\mathcal{K}$ is defined as

$$\Delta = \begin{vmatrix} \omega_1 & \overline{\omega_1} \\ \omega_2 & \overline{\omega_2} \end{vmatrix}^2,$$

so for $D \equiv 1 \pmod 4$ we have $\Delta = D$ and for $D \equiv 2, 3 \pmod 4$ we have $\Delta = 4D$. We summarize this in the following theorem:

Theorem 2.1 *Let D be a square-free integer, positive or negative, and define*

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

Then the discriminant Δ of $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ is given by

$$\Delta = \frac{4D}{r^2},$$

and $\{1, \omega\}$, where

$$\omega = \frac{r-1+\sqrt{D}}{r},$$

is an integral basis of $\mathcal{K}$. □

Since it can be shown that Δ is independent of the choice of basis, Δ is an invariant of the field $\mathcal{K}$. Also, since $\{1, \omega\}$ is an integral basis, any integer $\vartheta \in \mathcal{O}_\mathcal{K}$ can be represented as

$$\vartheta = a + b\omega,$$

where $a, b \in \mathbb{Z}$.

2.1 Units and Prime Factorization in $\mathcal{O}_\mathcal{K}$

We say that for $\alpha, \beta \in \mathcal{O}_\mathcal{K}$, α is *divisible* by β, or $\beta \mid \alpha$, if there exists $\gamma \in \mathcal{O}_\mathcal{K}$ such that $\alpha = \beta\gamma$. This is analogous to the definition of divisibility in $\mathbb{Z}$. A *unit* ε is defined to be a divisor of the integer 1, and hence of every integer in the field. However, unlike $\mathbb{Z}$, in quadratic fields we may also have the existence of non-trivial units, i.e., units other than ± 1. The trivial units ± 1 exist in every quadratic field. For $\xi \in \mathcal{O}_\mathcal{K}$, we call the numbers $\varepsilon\xi$ *associates* of ξ. Thus any multiple of ξ by a unit is an associate of ξ. Also, $\xi \in \mathcal{O}_\mathcal{K}$ is called *prime* if it is divisible only by the units of $\mathcal{O}_\mathcal{K}$ and its associates. The norm of a prime in $\mathcal{O}_\mathcal{K}$ is a prime in $\mathbb{Z}$.

It is easy to show that for any unit ε we have $N(\varepsilon) = \pm 1$. Hence, $\varepsilon = a + b\omega$ is a unit if and only if the equation

$$\begin{cases} a^2 - Db^2 = 1 & \text{when } D \equiv 2, 3 \pmod 4 \\ \left(a + \frac{b}{2}\right)^2 - \frac{1}{4}Db^2 = 1 & \text{when } D \equiv 1 \pmod 4 \end{cases} \tag{2.4}$$

holds. If $D < 0$, then (2.4) has a finite number of solutions. If $D = -1$, then there are 4 solutions, and if $D = -3$ there are 6; hence $\mathbb{Q}(\sqrt{-1})$ has 4 units and $\mathbb{Q}(\sqrt{-3})$ has 6 units. If $D < -3$, then the only solutions are given by $a = \pm 1$, $b = 0$ so there are only 2 units. If $D > 0$, then (2.4) has an infinitude of solutions which can be represented as $\pm\varepsilon_0^n$ where $n \in \mathbb{Z}$ and ε_0 is the smallest solution that is greater than 1.

Definition 2.1 *We call* ε_0 *the* fundamental unit *of* $\mathbb{Q}(\sqrt{D})$.

Definition 2.2 *The* regulator *is defined as* $R = \log \varepsilon_0$.

Every integer in $\mathcal{O}_\mathcal{K}$ can be expressed as a product of primes. However, as illustrated in Chapter 1, this representation is not necessarily unique. We say that $\mathcal{O}_\mathcal{K}$ is a *unique factorization domain* (UFD) if every element that is not zero and not a unit can be uniquely represented as a product of primes. In other words, $\mathcal{O}_\mathcal{K}$ is a UFD if the fundamental theorem of arithmetic is true for its elements. It is known that there are a finite

number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ whose maximal orders are UFD's, the one with the smallest discriminant being $\mathbb{Q}(\sqrt{-163})$. Computational evidence suggests that there are infinitely many real quadratic fields whose maximal orders are UFD's, but this has yet to be proved.

2.2 Ideals and the Class Group

To overcome the problems caused by fields where unique factorization does not hold, Kummer invented the notion of ideal numbers, a concept that was later modified by Dedekind to what today we call *ideals.*

Definition 2.3 *We say that a subset* $\mathfrak{a}$ *of* $\mathcal{O}_K$ *is an* integral ideal *if the following two properties hold:*

1. *If* $\alpha, \beta \in \mathfrak{a}$, *then* $\alpha \pm \beta \in \mathfrak{a}$.
2. *If* $\alpha \in \mathfrak{a}$ *and* $\eta \in \mathcal{O}_K$ *then* $\eta\alpha \in \mathfrak{a}$.

Similarly, we can define *fractional ideals* but they are less convenient to work with from a computational point of view. Therefore, we will restrict our discussion to integral ideals, and from now on we will use the term ideal to mean an integral ideal of $\mathcal{O}_K$.

If $\alpha, \beta \in \mathcal{O}_K$, then the set $\{\eta_1\alpha + \eta_2\beta | \eta_i \in \mathcal{O}_K\}$ is clearly an ideal. We say that $\mathfrak{a} = (\alpha, \beta)$ is the ideal generated by α and β. It is known that no more than two generators are needed to generate any ideal of $\mathcal{O}_K$. We can give a standard basis for any ideal in terms of the integral basis of $\mathcal{O}_K$. Any ideal $\mathfrak{a}$ can be expressed as a $\mathbb{Z}$-module

$$\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z} = [a, b + c\omega]$$

where $a, b, c \in \mathbb{Z}$, $a > 0$, $c > 0$, $c \,|\, b$, $c \,|\, a$, and $ac \,|\, N(b + c\omega)$. Furthermore, for a given ideal $\mathfrak{a}$ the integers a and c are unique and a is the least positive rational integer in $\mathfrak{a}$,

which we will denote as $L(\mathfrak{a})$. We define the norm of an ideal as the absolute value of the determinant of its standard basis coefficients, i.e.,

$$N(\mathfrak{a}) = \begin{vmatrix} a & 0 \\ b & c \end{vmatrix} = |ac|.$$

As with norms of field elements, we have here

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

An ideal $\mathfrak{a}$ is said to be *primitive* if $L(\mathfrak{a}) = N(\mathfrak{a})$; hence $c = 1$. Every primitive ideal can be uniquely given by

$$\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$$

where $b \in \mathbb{Z}$, $L(\mathfrak{a}) \,|\, N(b + \omega)$, and $-L(\mathfrak{a}) < \mathrm{Tr}\,(b + \omega) \leq L(\mathfrak{a})$; this is called the *normal presentation* of $\mathfrak{a}$. We say that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equal*, $\mathfrak{a} = \mathfrak{b}$, if they contain exactly the same elements of $\mathcal{O}_K$. The *conjugate* of $\mathfrak{a}$ is defined as

$$\bar{\mathfrak{a}} = \left[L(\mathfrak{a}), \overline{b + \omega}\right],$$

and we say that $\mathfrak{a}$ is *ambiguous* if $\mathfrak{a} = \bar{\mathfrak{a}}$. A *principal ideal* is any ideal with a single generator, denoted by $\mathfrak{a} = (\alpha)$. It can be shown that if $\mathfrak{a}$ is principal, then $N(\mathfrak{a}) = |N(\alpha)|$.

We define the product of two ideals $\mathfrak{a} = (\alpha_1, \alpha_2)$ and $\mathfrak{b} = (\beta_1, \beta_2)$ as

$$\mathfrak{ab} = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2).$$

This operation of ideal multiplication is commutative and associative. The *unit ideal* is the ideal $(1) = [1, \omega] = \mathcal{O}_K$, since it is easy to see that for any ideal $\mathfrak{a}$ we have $(1)\mathfrak{a} = \mathfrak{a}(1) = \mathfrak{a}$. We say that the ideal $\mathfrak{a}$ *divides* $\mathfrak{b}$, $\mathfrak{a} \,|\, \mathfrak{b}$, if there exists another ideal $\mathfrak{c}$ such that

$$\mathfrak{ac} = \mathfrak{b},$$

and that $\mathfrak{a}$ and $\mathfrak{c}$ are the *divisors* of $\mathfrak{b}$. It is clear that $\mathfrak{a} \,|\, \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$. We say that an ideal $\mathfrak{a}$ is *prime* if it is non-trivial, i.e., $\mathfrak{a} \neq \{0\}$ and $\mathfrak{a} \neq (1)$, and its only divisors are (1) and itself.

Theorem 2.2 (Fundamental Theorem for Ideals) *Any non-trivial, integral ideal* $\mathfrak{a}$ *can be factored into a product of prime ideals. Furthermore, apart from ordering of the factors, this factorization is unique.*

Proof: See [Hua82]. □

Thus, unique factorization is restored at the level of ideal arithmetic for quadratic fields, even if it does not hold for individual integers in the field.

The ideals of $\mathcal{O}_\mathcal{K}$ can be partitioned into equivalence classes if we use the following notion of equivalence.

Definition 2.4 *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be two ideals. If there exist two principal ideals* (α) *and* (β) *such that*

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$$

then we say that $\mathfrak{a}$ *and* $\mathfrak{b}$ *are* equivalent, *denoted by* $\mathfrak{a} \sim \mathfrak{b}$.

The set of all ideals equivalent to $\mathfrak{a}$ is called the *ideal class* of $\mathfrak{a}$. The set of all ideals equivalent to (1) is called the *principal class*, since $\mathfrak{a} \sim (1)$ if and only if $\mathfrak{a}$ is principal. It can be shown that for a particular field $\mathcal{K}$ the number of ideal equivalence classes is finite. Furthermore, they form an abelian group under the operation of ideal multiplication which we call the *class group* of $\mathcal{K}$, denoted by Cl.

Definition 2.5 *The* class number *of* $\mathcal{K}$ *is the integer* $h = |Cl|$.

If $h = 1$, then every ideal in $\mathcal{K}$ is a principal ideal and we call $\mathcal{O}_\mathcal{K}$ a *principal ideal domain* (PID). If $\mathcal{O}_\mathcal{K}$ is a PID, then the fundamental theorem for ideals implies that $\mathcal{O}_\mathcal{K}$ is also a UFD. Thus unique factorization holds in any field with $h = 1$.

As mentioned in Chapter 1, there is a relationship between the class number of a quadratic field and the number of equivalence classes of quadratic forms of the same

discriminant. Two forms $(a,b,c) = ax^2 + bxy + cy^2$ and $(d,e,f) = dx^2 + exy + fy^2$ are equivalent if there exists a substitution $x = uX + vY$, $y = wX + zY$ such that the determinant of the substitution $uz - vw = 1$, and that when applied to (a,b,c) yields (d,e,f). The set of all forms equivalent to (a,b,c) is an equivalence class, and the number of these equivalence classes is denoted by h_0. For any ideal $\mathfrak{a} = [\alpha_1, \alpha_2]$ of the quadratic field $\mathcal{K}$ with discriminant Δ such that $\alpha_1\overline{\alpha}_2 - \overline{\alpha}_1\alpha_2 = N(\mathfrak{a})\Delta$, we can generate a quadratic form (a,b,c) with discriminant Δ by setting

$$a = \frac{N(\alpha_1)}{N(\mathfrak{a})},$$

$$b = \frac{N(\alpha_1 + \alpha_2) - N(\alpha_1) - N(\alpha_2)}{N(\mathfrak{a})},$$

$$c = \frac{N(\alpha_2)}{N(\mathfrak{a})}.$$

We call (a,b,c) the quadratic form belonging to the ideal $\mathfrak{a}$. If (a,b,c) belongs to $\mathfrak{a}$ then every form equivalent to (a,b,c) also belongs to $\mathfrak{a}$. However, there may be two different ideals to which (a,b,c) belongs.

Definition 2.6 *We say that two ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are* equivalent in the narrow sense *if there exist principal ideals* (α) *and* (β) *such that* $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ *and* $N(\alpha\beta) > 0$. *We denote this by* $\mathfrak{a} \simeq \mathfrak{b}$.

Equivalent quadratic forms belong to ideals which are equivalent in the narrow sense, and conversely, quadratic forms belonging to ideals which are equivalent in the narrow sense are equivalent forms. Thus, under the notion of narrow equivalence of ideals there is a one-to-one correspondence between ideal equivalence classes and quadratic form equivalence classes. It can be shown that h_0 is related to h by

$$h = \begin{cases} h_0 & D < 0 \\ h_0 & D > 0, N(\varepsilon_0) = -1 \\ \frac{h_0}{2} & D > 0, N(\varepsilon_0) = 1 \end{cases}$$

Thus, if we know the class number of $\mathcal{K}$ and, in the case that $\mathcal{K}$ is a real quadratic field, we also know the norm of its fundamental unit, then we can immediately compute the number of equivalence classes of forms with discriminant Δ, where Δ is the discriminant of $\mathcal{K}$. Unfortunately, no simple criterion for determining $N(\varepsilon_0)$ is currently known.

When actually computing products of ideals, it is more convenient to represent primitive ideals as

$$\mathfrak{a} = \left[\frac{Q}{r}, \frac{P+\sqrt{D}}{r}\right]$$

where

$$\begin{aligned} P &= r(b+\omega) - \sqrt{D} \\ &= rb + r - 1 \end{aligned}$$

and

$$Q = rL(\mathfrak{a}).$$

Since $r \mid Q$ and $L(\mathfrak{a}) \mid N\,(b+\omega) = N\left((P+\sqrt{D})/r\right)$ we must have $rQ \mid D - P^2$. This allows us to represent the primitive ideal $\mathfrak{a}$ as the ordered pair (P,Q), where $P, Q \in \mathbb{Z}$. Using this notation, the conjugate of $\mathfrak{a} = (P,Q)$ is simply $\bar{\mathfrak{a}} = (-P,Q)$, and $(1) = (r-1, r)$. If $\mathfrak{a} = (P,Q)$ and $\mathfrak{a}' = (P',Q')$, then $\mathfrak{a} = \mathfrak{a}'$ if $Q = Q'$ and $P \equiv P' \pmod{Q}$.

We can use Algorithm 2.1 to compute a primitive ideal equivalent to the product of two primitive ideals. This algorithm is essentially that of Shanks [Sha71] for the composition of two quadratic forms, and is the same for both imaginary and real quadratic fields.

Algorithm 2.1 (Product of ideals)

INPUT: Primitive ideals $\mathfrak{a} = (P_\mathfrak{a}, Q_\mathfrak{a})$ and $\mathfrak{b} = (P_\mathfrak{b}, Q_\mathfrak{b})$
OUTPUT: $\mathfrak{c} = (P_\mathfrak{c}, Q_\mathfrak{c})$, $U \in \mathbb{Z}$ such that $\mathfrak{c}$ is primitive and $\mathfrak{ab} = (U)\mathfrak{c}$

1. Compute $G = \gcd(Q_\mathfrak{a}/r, Q_\mathfrak{b}/r)$ and x_1 by solving the linear congruence $\frac{Q_\mathfrak{a}}{r}x_1 \equiv G \pmod{\frac{Q_\mathfrak{b}}{r}}$ with the Extended Euclidean Algorithm.
2. Compute $U = \gcd((P_\mathfrak{a}+P_\mathfrak{b})/r, G)$, x_2, and y_2 by solving $\frac{P_\mathfrak{a}+P_\mathfrak{b}}{r}x_2 + Gy_2 = U$ with the Extended Euclidean Algorithm.
3. Set $X \equiv y_2x_1(P_\mathfrak{b} - P_\mathfrak{a}) + x_2\frac{D-P_\mathfrak{a}^2}{Q_\mathfrak{a}} \pmod{\frac{Q_\mathfrak{b}}{U}}$.
4. Set $Q_\mathfrak{c} = \frac{Q_\mathfrak{a}Q_\mathfrak{b}}{rU^2}$ and $P_\mathfrak{c} \equiv P_\mathfrak{a} + X\frac{Q_\mathfrak{a}}{rU} \pmod{Q_\mathfrak{c}}$.

End of Algorithm

2.3 Reduced Ideals in Imaginary Quadratic Fields

The idea of ideal reduction is quite old, and is related to the idea of reducing binary quadratic forms. It gives us a convenient method for giving representatives of ideal equivalence classes.

Definition 2.7 *We say that* $\mathfrak{a}$ *is a* reduced ideal *if* $\mathfrak{a}$ *is primitive and there does not exist a non-zero* $\alpha \in \mathfrak{a}$ *such that both* $|\alpha| < L(\mathfrak{a})$ *and* $|\overline{\alpha}| < L(\mathfrak{a})$ *hold.*

It is known that every ideal class of $\mathbb{Q}(\sqrt{-D})$ contains exactly one reduced ideal. Thus, in the imaginary case we can confine arithmetic in the class group of $\mathcal{K}$ to arithmetic between reduced ideals. The following theorems give some criteria for determining whether an ideal is reduced in imaginary quadratic fields.

Theorem 2.3 *If* $\mathfrak{a}$ *is a reduced ideal in* $\mathbb{Q}(\sqrt{-D})$, *then* $L(\mathfrak{a}) < \sqrt{\frac{|\Delta|}{3}}$. □

Theorem 2.4 *If* $\mathfrak{a}$ *is a primitive ideal in* $\mathbb{Q}(\sqrt{-D})$ *and* $L(\mathfrak{a}) < \frac{\sqrt{|\Delta|}}{2}$, *then* $\mathfrak{a}$ *is reduced.*

□

We can use Algorithm 2.2 taken from [BW88] to compute a reduced ideal equivalent to $\mathfrak{a}$ in imaginary quadratic fields. The proof of correctness of Algorithm 2.2 can be found in [BW88]. However, Algorithm 2.3, also from [BW88], is a more efficient version, and this is the one we use in practice.

Algorithm 2.2 (Ideal Reduction in $\mathbb{Q}(\sqrt{-D})$)

INPUT: Primitive ideal $\mathfrak{a} = (P, Q)$
OUTPUT: Reduced ideal $\mathfrak{a}' = (P', Q')$ such that $\mathfrak{a} \sim \mathfrak{a}'$

1. Set $P_0 = P$, $Q_0 = Q$, $i = 0$.
2. Compute

$$\begin{aligned} q_i &= \mathrm{Ne}(P_i/Q_i), \\ P_{i+1} &= q_i Q_i - P_i, \\ Q_{i+1} &= (P_{i+1}^2 - D)/Q_i, \end{aligned}$$

   where by $\mathrm{Ne}(x)$ we mean the nearest integer to x.
3. If $Q_{i+1} < Q_i$, set $i = i + 1$ and go to 2. Otherwise, set $P' = P_i$ and $Q' = Q_i$.

End of Algorithm

We can give an upper bound on the number of iterations made by these algorithms before a reduced ideal is found.

Theorem 2.5 *In Algorithm 2.2 and Algorithm 2.3, we get $Q_{i+1} \geq Q_i$ for some i such that*

$$i \leq \left[\frac{1}{2} \log_2 \left(\frac{3Q_0}{5\sqrt{|D|}} \right) \right].$$

Proof: See [BW88]. □

Thus, given a primitive ideal we can find a reduced ideal equivalent to it quite rapidly.

Algorithm 2.3 (Efficient Ideal Reduction in $\mathbb{Q}(\sqrt{-D})$)

INPUT: Primitive ideal $\mathfrak{a} = (P, Q)$
OUTPUT: Reduced ideal $\mathfrak{a}' = (P', Q')$ such that $\mathfrak{a} \sim \mathfrak{a}'$

1. Set $P_0 = P$, $Q_0 = Q$, $T_0 = |P_0|$, $t_0 = P_0/T_0$, $Q_{-1} = (P_0^2 - D)/Q_0$, and $i = 0$.
2. Compute

$$\begin{aligned} s_i &= [T_i/Q_i], \\ R_i &= T_i \bmod Q_1, \\ M_i &= Q_i - 2R_i. \end{aligned}$$

3. If $M_i \geq 0$ then set

$$\begin{aligned} T_{i+1} &= R_i, \\ Q_{i+1} &= Q_{i-1} - s_i(R_i + T_i), \\ t_{i+1} &= -t_i; \end{aligned}$$

if $M_i < 0$ then set

$$\begin{aligned} T_{i+1} &= R_i + M_i, \\ Q_{i+1} &= Q_{i-1} - s_i(R_i + T_i) + M_i, \\ t_{i+1} &= t_i. \end{aligned}$$

4. If $Q_{i+1} < Q_i$, set $i = i + 1$ and go to 2. Otherwise, set $P' = t_i T_i$ and $Q' = Q_i$.

End of Algorithm

Algorithm 2.4 (Ideal Multiplication and Reduction in $\mathbb{Q}(\sqrt{-D})$)

INPUT: Primitive ideals $\mathfrak{a}$ and $\mathfrak{b}$
OUTPUT: $\mathfrak{c}$ and $U \in \mathbb{Z}$, such that $\mathfrak{c}$ is the reduced ideal given by $(U)\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

1. Compute $(U)\mathfrak{c}' = \mathfrak{a}\mathfrak{b}$ with Algorithm 2.1.
2. Compute the reduced ideal $\mathfrak{c} \sim \mathfrak{c}'$ with Algorithm 2.3.

End of Algorithm

We can use Algorithm 2.4 to compute the reduced ideal equivalent to the product of any two primitive ideals.

Definition 2.8 *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are primitive ideals in* $\mathbb{Q}(\sqrt{-D})$, *then*

$$\mathfrak{c} = \mathfrak{a} * \mathfrak{b}$$

is the reduced ideal equivalent to $\mathfrak{ab}$ *given by Algorithm 2.4.*

We can consider $*$ as the group operator of the class group of imaginary quadratic fields, since each ideal class can be represented by a unique reduced ideal, and $\mathfrak{c} = \mathfrak{ab}$ is the unique reduced ideal of the ideal class containing $\mathfrak{ab}$.

2.4 Reduced Ideals in Real Quadratic Fields

The definition of reduced ideals in real quadratic fields is the same as in the imaginary case. However, the situation in real quadratic fields is somewhat more complicated because each ideal class contains a cycle of reduced ideals. We have the following analogues to Theorem 2.3 and Theorem 2.4:

Theorem 2.6 *If* $\mathfrak{a}$ *is a reduced ideal in* $\mathbb{Q}(\sqrt{D})$, *then* $L(\mathfrak{a}) < \sqrt{\Delta}$. □

Theorem 2.7 *If* $\mathfrak{a}$ *is a primitive ideal in* $\mathbb{Q}(\sqrt{D})$ *and* $L(\mathfrak{a}) < \frac{\sqrt{\Delta}}{2}$, *then* $\mathfrak{a}$ *is reduced.* □

To apply these theorems, we first need some results on the continued fraction expansion of elements in $\mathbb{Q}(\sqrt{D})$. Recall that we can represent any real number ϕ as

$$\phi = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_m + \cfrac{1}{\phi_{m+1}}}}}$$

Algorithm 2.5 (Continued Fraction Expansion)

INPUT: $\phi = \frac{P+\sqrt{D}}{Q}$, where $P, Q \in \mathbb{Z}, Q \mid D - P^2$
OUTPUT: $\phi_i = \frac{P_i+\sqrt{D}}{Q_i}$ and q_i from the continued fraction expansion of ϕ

1. Set $P_0 = P$, $Q_0 = Q$, $q_0 = \left\lfloor (P + \sqrt{D})/Q \right\rfloor$, and $i = 0$.
2. Compute

$$\begin{aligned} P_{i+1} &= q_i Q_i - P_i \\ Q_{i+1} &= \frac{D - P_{i+1}^2}{Q_i} \\ \phi_{i+1} &= \frac{P_{i+1} + \sqrt{D}}{Q_{i+1}} \\ q_{i+1} &= [\phi_{i+1}]. \end{aligned}$$

3. $i = i + 1$, go to 2

End of Algorithm

where $q_1, q_2, \ldots, q_m \in \mathbb{Z}$. We call this the *simple continued fraction expansion* of ϕ, which we will denote by

$$\phi = \langle q_0, q_1, q_2, \ldots, q_m, \phi_{m+1} \rangle .$$

$C_m = \langle q_0, q_1, q_2, \ldots, q_m \rangle$ is called a *convergent* of ϕ. If we define

$$A_{i+1} = q_{i+1} A_i + A_{i-1}$$

and

$$B_{i+1} = q_{i+1} B_i + B_{i-1}$$

where $A_{-2} = B_{-1} = 0$ and $A_{-1} = B_{-2} = 1$, then $C_m = A_m / B_m$. We can expand elements

$$\phi = \frac{P + \sqrt{D}}{Q} \in \mathbb{Q}(\sqrt{D})$$

where $P, Q \in \mathbb{Z}$ and $Q \mid D - P^2$ with Algorithm 2.5. In practice we use Algorithm 2.6, a modified version due to Tenner which is more efficient.

Algorithm 2.6 (Efficient Continued Fraction Expansion)

INPUT: $\phi = \frac{P+\sqrt{D}}{Q}$, where $P, Q \in \mathbb{Z}, Q \mid D - P^2$

OUTPUT: $\phi_i = \frac{P_i+\sqrt{D}}{Q_i}$ and q_i from the continued fraction expansion of ϕ

1. Set $d = \left\lfloor \sqrt{D} \right\rfloor$, $P_0 = P$, $Q_0 = Q$, $Q_{-1} = (D - P_0^2)/Q_0$, $q_0 = \left\lfloor (P + \sqrt{D})/Q \right\rfloor$,

$$s_0 = \begin{cases} 0 & \text{when } Q_0 > 0 \\ 1 & \text{when } Q_0 < 0, \end{cases}$$

$R_0 = P_0 + d + s_0 - q_0 Q_0$, and $i = 0$.

2. Compute

$$\begin{aligned} P_{i+1} &= d + s_i - R_i \\ Q_{i+1} &= Q_{i-1} - q_i(P_{i+1} - P_i) \\ q_{i+1} &= \left\lfloor \frac{P_{i+1} + d + s_{i+1}}{Q_{i+1}} \right\rfloor \\ R_{i+1} &= P_{i+1} + d + s_{i+1} - q_{i+1} Q_{i+1} \\ \phi_{i+1} &= \frac{P_{i+1} + \sqrt{D}}{Q_{i+1}} \end{aligned}$$

using

$$s_{i+1} = \begin{cases} 0 & \text{when } Q_0 > 0 \\ 1 & \text{when } Q_0 < 0. \end{cases}$$

3. $i = i + 1$, go to 2

End of Algorithm

If $\mathfrak{a} = \mathfrak{a}_0 = (P, Q)$, then it can be shown that if we set $\phi = (P + \sqrt{D})/Q$ and $\phi_m = (P_m + \sqrt{D})/Q_m$ is found by expanding ϕ into a continued fraction, then

$$\mathfrak{a}_m = (P_m, Q_m) = \left[\frac{Q_m}{r}, \frac{P_m + \sqrt{D}}{r}\right]$$

is an ideal in the same equivalence class as $\mathfrak{a}$. Also, if $\mathfrak{a}$ is primitive, then $\mathfrak{a}_m$ is a reduced ideal equivalent to $\mathfrak{a}$ for the least m such that $Q_m \leq \left[\sqrt{D}\right]$.

Theorem 2.8 *$\mathfrak{a}_m$ is a reduced ideal whenever*

$$m > \max\left\{2, 4 + \log\left(\frac{|Q_0|}{2\sqrt{D}}\right)\frac{1}{2\log\tau}\right\},$$

where $\tau = \left(1 + \sqrt{5}\right)/2$. □

This theorem tells us that if $\mathfrak{a}$ is not reduced, then the continued fraction algorithm will rapidly produce a reduced ideal, and then produce all the reduced ideals equivalent to it. In fact, if $\mathfrak{a}$ is reduced, then the continued fraction expansion algorithm will produce all the reduced ideals equivalent to $\mathfrak{a}$.

It can be shown that there exists a least positive $p \in \mathbb{Z}$ such that $\mathfrak{a}_0 = \mathfrak{a}_p$ where $\mathfrak{a}_p$ is found by expanding the continued fraction associated with a reduced ideal $\mathfrak{a}_0$. Thus, the reduced ideals in any ideal class form a cycle of period p. Furthermore, if we define

$$\Psi_i = \prod_{j=1}^{i} \psi_j$$

where $\Psi_0 = 1$ and

$$\psi_j = \frac{P_j + \sqrt{D}}{Q_{j-1}}$$

then it can be shown that

$$\varepsilon_0 = \Psi_p$$

and

$$R = \log \Psi_p.$$

The cycle of reduced ideals in a particular ideal class exhibits symmetry, since we have that

$$\overline{\mathfrak{a}}_{p-i} = \mathfrak{a}_i.$$

This gives us the following result (see, for example, [MW92]).

Theorem 2.9 *If s is the least positive integer such that $P_s = P_{s+1}$, then*

$$\varepsilon_0 = \frac{\Psi_s}{\left|\overline{\Psi}_s\right|},$$

$$R = 2\log\Psi_s + \log\frac{Q_0}{Q_s},$$

and $p = 2s$. If $D > 5$ and t is the least positive integer such that $Q_t = Q_{t+1}$, then

$$\varepsilon_0 = \frac{\Psi_{t+1}}{\left|\overline{\Psi}_t\right|},$$

$$R = 2\log\Psi_t + \log\frac{Q_0\psi_t}{Q_t},$$

and $p = 2t + 1$. □

Thus, we only have to look half-way through the cycle of principal ideals in order to compute ε_0 and R.

2.5 Infrastructure of the Principal Class

Shanks [Sha72] noticed that the cycle of reduced ideals of any ideal class has certain additional structural properties, which he called the *infrastructure*. We will confine our discussion here to the cycle of the principal class

$$\mathfrak{a}_0 = (1), \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{p-1}, \mathfrak{a}_p = \mathfrak{a}_0,$$

which we will call the *principal cycle*, although these principles certainly apply in other ideal classes.

Definition 2.9 *Let* $\mathfrak{a}_m$ *and* $\mathfrak{a}$ *be two reduced ideals such that* $\mathfrak{a}_m \sim \mathfrak{a}$ *and* $\mathfrak{a}_m$ *is found by expanding the continued fraction corresponding to* $\mathfrak{a}$. *Then the* distance *from* $\mathfrak{a}$ *to* $\mathfrak{a}_m$ *is defined as*

$$\delta(\mathfrak{a}_m, \mathfrak{a}) = \log \Psi_m.$$

We also define

$$\delta_m = \delta(\mathfrak{a}_m, (1)).$$

It can be shown that δ_m is a strictly increasing function of m and $\delta_p = R$. Also, if $k \in \mathbb{Z}$ and $\delta_m = kR + \delta_s$ for ideals $\mathfrak{a}_m$ and $\mathfrak{a}_s$, then $\mathfrak{a}_m = \mathfrak{a}_s$. We will use $\delta_\mathfrak{a}$ to denote the distance associated with the ideal $\mathfrak{a}$ in the cases where it can be either the distance from (1) or from another ideal. Algorithm 2.7 is an extension of Algorithm 2.6 which, in addition to generating each ideal found by expanding the continued fraction corresponding to the initial ideal, computes their distances.

Let $\mathfrak{a}_s$ and $\mathfrak{a}_t$ be two ideals found by expanding the continued fraction corresponding to (1) using Algorithm 2.7, and let $\mathfrak{c}$ be defined by using Algorithm 2.1 to compute

$$(U)\mathfrak{c} = \mathfrak{a}_s\mathfrak{a}_t.$$

If $\mathfrak{c} = (P_0, Q_0)$, then we can compute a reduced ideal $\mathfrak{c}' = (P_m, Q_m)$ equivalent to $\mathfrak{c}$ by expanding the continued fraction corresponding to $\mathfrak{c}$ using Algorithm 2.6 until we have $Q_m \leq \left\lfloor \sqrt{D} \right\rfloor$. Since $\mathfrak{c}'$ is reduced and in the principal class, we must have $\mathfrak{c}' = \mathfrak{a}_k$ for some $k \geq 0$. Furthermore, we can show that

$$\Psi_k = \Psi_s \Psi_t \frac{\Psi_m}{U},$$

so if we set $\kappa = \log(\Psi_m/U)$ we have

$$\delta_k = \delta_s + \delta_t + \kappa. \tag{2.5}$$

It can also be shown that $-\log 4D < -\log Q_s Q_t < \kappa < \log 2$, so $\delta_k \approx \delta_s + \delta_t$. By a result of Lévy, we would expect that $\delta_m \approx m\gamma$ where $\gamma = \pi^2/(12\log 2) \approx 1.186569111$.

Algorithm 2.7 (Efficient Continued Fraction Expansion with Distances)

INPUT: $\mathfrak{a} = (P, Q)$ with distance $\delta_{\mathfrak{a}}$
OUTPUT: $\mathfrak{a}_i$, with distance δ_i

1. Set $d = \left\lfloor \sqrt{D} \right\rfloor$, $P_0 = P$, $Q_0 = Q$, $Q_{-1} = (D - P_0^2)/Q_0$, $q_0 = \left\lfloor (P + \sqrt{D})/Q \right\rfloor$,

$$s_0 = \begin{cases} 0 & \text{when } Q_0 > 0 \\ 1 & \text{when } Q_0 < 0, \end{cases}$$

$R_0 = P_0 + d + s_0 - q_0 Q_0$, $\delta_0 = \delta_{\mathfrak{a}}$, and $i = 0$.

2. Compute

$$\begin{aligned} P_{i+1} &= d + s_i - R_i \\ Q_{i+1} &= Q_{i-1} - q_i(P_{i+1} - P_i) \\ q_{i+1} &= \left\lfloor \frac{P_{i+1} + d + s_{i+1}}{Q_{i+1}} \right\rfloor \\ R_{i+1} &= P_{i+1} + d + s_{i+1} - q_{i+1} Q_{i+1} \end{aligned}$$

using

$$s_{i+1} = \begin{cases} 0 & \text{when } Q_0 > 0 \\ 1 & \text{when } Q_0 < 0. \end{cases}$$

3. Set

$$\mathfrak{a}_{i+1} = (P_{i+1}, Q_{i+1})$$

$$\delta_{i+1} = \delta_i + \log\left(\frac{P_{i+1} + \sqrt{D}}{Q_i} \right)$$

4. $i = i + 1$, go to 2

End of Algorithm

Thus, for any two reduced ideals in the principal cycle $\mathfrak{a}_s$ and $\mathfrak{a}_t$, we can find an ideal $\mathfrak{a}_k$ such that $k \approx s + t$ and $\delta_k \approx \delta_s + \delta_t$. This allows us to find an ideal with distance δ by performing about δ/δ_s of these multiply-reduction steps using an ideal $\mathfrak{a}_s$ with distance δ_s, as opposed to δ/γ continued fraction steps.

Algorithm 2.8 (Ideal Multiplication and Reduction in $\mathbb{Q}(\sqrt{D})$)

INPUT: Primitive ideals $\mathfrak{a}$ and $\mathfrak{b}$ with distances $\delta_\mathfrak{a}$ and $\delta_\mathfrak{b}$
OUTPUT: $\mathfrak{c}$, $\delta_\mathfrak{c}$

1. Compute $(U)\mathfrak{c}' = \mathfrak{a}\mathfrak{b}$ with Algorithm 2.1.
2. Compute a reduced ideal $\mathfrak{c} = (P_m, Q_m)$ and $\delta(\mathfrak{c}, \mathfrak{c}')$ by expanding the continued fraction corresponding to $\mathfrak{c}' = (P_0, Q_0)$ with Algorithm 2.7 until $Q_m \leq \left[\sqrt{D}\right]$. Set $\kappa = \delta(\mathfrak{c}, \mathfrak{c}') - \log U$.
3. Set $\delta_\mathfrak{c} = \delta_\mathfrak{a} + \delta_\mathfrak{b} + \kappa$.

End of Algorithm

Algorithm 2.8 computes a reduced ideal $\mathfrak{c}$ equivalent to the product of two primitive ideals $\mathfrak{a}\mathfrak{b}$ as well as $\delta_\mathfrak{c}$, the distance of $\mathfrak{c}$. Note that while the continued fraction algorithm produces an infinitude of reduced ideals equivalent to $\mathfrak{c}$, only one of these has distance $\delta_\mathfrak{c}$.

Definition 2.10 *If $\mathfrak{a}$ and $\mathfrak{b}$ are primitive ideals in $\mathbb{Q}(\sqrt{D})$, then*

$$\mathfrak{c} = \mathfrak{a} * \mathfrak{b}$$

is the reduced ideal equivalent to $\mathfrak{a}\mathfrak{b}$ given by Algorithm 2.8.

If $\mathfrak{a} = \mathfrak{a}_s$ and $\mathfrak{b} = \mathfrak{a}_t$ are in the principal class, then $\mathfrak{c} = \mathfrak{a} * \mathfrak{b} = \mathfrak{a}_k$ is also principal and $\delta_\mathfrak{c} = \delta_k$. If we ignore the distances, then we can use $*$ to compute among the equivalence classes since $\mathfrak{a} * \mathfrak{b}$ gives us one of the reduced ideals in the equivalence class of $\mathfrak{a}\mathfrak{b}$.

2.6 $L(1,\chi)$ and the Analytic Class Number Formula

In much of what follows, especially in our algorithms for computing class numbers, we will be concerned with certain values of a function called the *Dirichlet L-function*. We first need the following two definitions relating to characters.

Definition 2.11 *Let* $\mathbf{G}$ *be any group. A complex valued function* f *defined on* $\mathbf{G}$ *is called a* character *of* $\mathbf{G}$ *if*

$$f(ab) = f(a)f(b)$$

for all $a, b \in \mathbf{G}$ *and* $f(c) \neq 0$ *for some* $c \in \mathbf{G}$.

Definition 2.12 *Let* $\mathbf{G}$ *be the group of reduced residue classes modulo* m. *Corresponding to each character* f *of* $\mathbf{G}$ *we define an arithmetical function* $\chi = \chi_f$ *as follows:*

$$\chi(n) = \begin{cases} f(n \bmod m) & \text{if } (n,m) = 1, \\ 0 & \text{if } (n.m) > 1. \end{cases}$$

This function χ *is called a* Dirichlet character modulo m.

Definition 2.13 *The* Dirichlet L-function *is defined for* $s \in \mathbb{C}$, χ *a Dirichlet character modulo* Δ *by*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

if $\Re(s) > 1$ *and by analytic continuation otherwise.*

It can be shown that $L(s,\chi)$ converges absolutely for all $s > 0$.

We will be dealing with L-functions defined for a special Dirichlet character called the *Kronecker symbol*. Recall that if p is any prime, $p \nmid a$, and there exists a value of x such that

$$x^2 \equiv a \pmod{p},$$

then we say that a is a *quadratic residue* of p; otherwise we say that a is a *quadratic non-residue* of p. Recall also that the *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p \end{cases}$$

and the *Jacobi symbol* is defined by

$$\left(\frac{a}{P}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

where

$$P = \prod_{i=1}^{m} p_i^{\alpha_i}$$

is the prime power factorization of P.

Definition 2.14 *The* Kronecker symbol $\left(\frac{a}{n}\right)$ *is defined by the Jacobi symbol if* $n > 2$ *and by*

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 4 \\ 1 & \text{if } a \equiv 1 \pmod 8 \\ -1 & \text{if } a \equiv 5 \pmod 8 \end{cases}$$

when $n = 2$.

If $a = \Delta$ is the discriminant of a quadratic field, then it can be shown that

$$\chi(n) = \left(\frac{\Delta}{n}\right)$$

where $\left(\frac{\Delta}{n}\right)$ is the Kronecker symbol and $n > 0$ is, in fact, a Dirichlet character modulo Δ. The Kronecker symbol $\left(\frac{\Delta}{p}\right)$ indicates how the principal ideal (p), p prime, factors in the quadratic field with discriminant Δ.

Theorem 2.10 *Let* Δ *be the discriminant of a quadratic field* $\mathcal{K}$ *and let* $\mathfrak{p}$ *and* $\mathfrak{q}$ *denote prime ideals in* $\mathcal{K}$ *with norm equal to* p. *Then for any prime* p *we have three possible factorizations:*

1. $(p) = \mathfrak{p}$ *if* $(\frac{\Delta}{p}) = -1$. *We say that* p *is* inert *in* $\mathcal{K}$.

2. $(p) = \mathfrak{pq}$ *if* $(\frac{\Delta}{p}) = 1$. *We say that* p *is* split *in* $\mathcal{K}$.

3. $(p) = \mathfrak{p}^2$ *if* $(\frac{\Delta}{p}) = 0$. *We say that* p *is* ramified *in* $\mathcal{K}$.

Proof: See [Hua82]. □

Recall that the *Riemann zeta function* is defined for a complex variable s by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{2.6}$$

when $\Re(s) > 1$ and by analytic continuation otherwise. We can also define the zeta function over a quadratic field $\mathcal{K}$ by

$$\zeta_{\mathcal{K}}(s) = \sum \frac{1}{N(\mathfrak{a})^s} \tag{2.7}$$

where the sum is taken over the norms of all the ideals, excluding the zero ideal, in $\mathcal{O}_{\mathcal{K}}$. We can write $L(s, \chi)$ in terms of zeta functions as

$$L(s, \chi) = \frac{\zeta_{\mathcal{K}}(s)}{\zeta(s)}.$$

At $s = 1$ we also have

$$L(1, \chi) = \lim_{s \to 1}(s - 1)\zeta_{\mathcal{K}}(s).$$

The *analytic class number formula* relates the class number and regulator of the quadratic field of discriminant Δ to the value of $L(1, \chi)$.

Definition 2.15 *The* analytic class number formula *is defined as*

$$L(1, \chi) = \frac{2hR}{\sqrt{\Delta}}$$

for real quadratic fields of discriminant Δ *and as*

$$L(1, \chi) = \frac{2\pi h}{w\sqrt{|\Delta|}}$$

for imaginary quadratic fields of discriminant Δ *with* w *units.*

Thus, evaluating $L(1,\chi)$ gives us the value of h in imaginary quadratic fields and the value of hR in real quadratic fields. Using Gauss sums, one can derive closed forms of $L(1,\chi)$. For imaginary quadratic fields this is given by

$$L(1,\chi) = -\frac{\pi}{|\Delta|^{3/2}} \sum_{j=1}^{|\Delta|} \left(\frac{\Delta}{j}\right) j \tag{2.8}$$

and for real quadratic fields by

$$L(1,\chi) = -\frac{1}{\sqrt{\Delta}} \sum_{j=1}^{\Delta} \left(\frac{\Delta}{j}\right) \log \sin \frac{\pi j}{\Delta}. \tag{2.9}$$

Together with the analytic class number formula, these allow us to compute the class number using a finite sum. For imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ with $D < -3$ we have

$$h = -\frac{1}{|\Delta|} \sum_{j=1}^{|\Delta|} \left(\frac{\Delta}{j}\right) j \tag{2.10}$$

and for real quadratic fields we have

$$h = -\frac{1}{2R} \sum_{j=1}^{\Delta} \left(\frac{\Delta}{j}\right) \log \sin \frac{\pi j}{\Delta}. \tag{2.11}$$

Unfortunately these sums involve Δ terms, and are therefore impractical for large values of Δ. Hence, we try to approximate $L(1,\chi)$ to sufficient accuracy such that h can be computed. Most of the methods for approximating $L(s,\chi)$ make use of the Euler product representation. Using the Euler product formula we can write $L(s,\chi)$ as the infinite product

$$L(s,\chi) = \prod_p \frac{p^s}{p^s - \left(\frac{\Delta}{p}\right)} = \prod_p \left(1 - \frac{\left(\frac{\Delta}{p}\right)}{p^s}\right)^{-1} \tag{2.12}$$

taken over all primes p. For $s > 1$ this product converges fairly quickly, but at $s = 1$ the convergence is very slow.

Since the time of Riemann it has been conjectured that if s is any non-trivial zero of $\zeta(s)$ then $\Re(s)$ must be $1/2$. An equivalent statement is that $\zeta(s) \neq 0$ for any value of s such that $\Re(s) > 1/2$. This is a famous hypothesis known as the Riemann Hypothesis. Although there is an overwhelming amount of numerical support for the Riemann

hypothesis, no one has yet been able to prove it. An analogous conjecture, the Generalized Riemann Hypothesis states the same thing for $\zeta_{\mathcal{K}}$. We will make extensive use of the version of the Riemann Hypothesis that pertains to $L(s,\chi)$, the Extended Riemann Hypothesis, or ERH for short.

Conjecture 2.1 (Extended Riemann Hypothesis) *For any character* χ,

$$L(s,\chi) > 0$$

for any value of s *such that* $\Re(s) > 1/2$.

The assumption of the truth of the ERH allows us to give much tighter bounds on $L(s,\chi)$ and in turn better estimates of the error in our approximations of it.

Chapter 3

Computing R and h in Real Quadratic Fields

There are approximately 50 million primes less than 10^9 and 60 million square-free integers less than 10^8, so computing all of the corresponding class numbers was a rather large project. Much careful consideration had to be taken as to how to carry out the computations as efficiently and expeditiously as possible. We used, for the most part, the techniques due to Buchmann and Williams [BW89b], given for the real case in [MW92], which evaluate h in at most $O\left(D^{1/5+\epsilon}\right)$ operations. It should be recalled that the correctness of these techniques is conditional on the truth of the Extended Riemann Hypothesis.

We divided the problem into subproblems of computing class numbers for all primes in intervals of length 10^6, and all square-free integers in intervals of length 10^5. Our algorithms were coded in C and run on a DECStation 5000/200. All class numbers and regulators were stored on a tape back-up, so the actual computation only had to be performed once.

The main idea of our algorithm was to make use of the analytic class number formula

defined in Section 2.6

$$L(1,\chi) = \frac{2hR}{\sqrt{\Delta}}, \tag{3.1}$$

where Δ is the discriminant of the field $\mathbb{Q}(\sqrt{D})$. To compute h using this formula, one must first compute the regulator R and then estimate $L(1,\chi)$ to sufficient accuracy that the unique integer h can be determined.

3.1 Estimating $L(1,\chi)$

For each radicand D in a given interval of length 10^5, or 10^6 when restricting to prime radicands, we first computed an estimate of $L(1,\chi)$. Here, instead of using a truncated Euler product and Oesterlé's results [Oes79] to estimate the error as in [MW92], we use an idea due to Bach [Bac94]. This is based on using a weighted average of truncated Euler products to compute an approximation $S(Q,\Delta)$ of $\log L(1,\chi)$ which, under the ERH, has relative error $O\left(\log\Delta/(\sqrt{Q}\log Q)\right)$. For some pre-selected value of Q we compute

$$C(Q) = \sum_{i=0}^{Q-1}(i+Q)\log(i+Q) = \sum_{i=Q}^{2Q-1} i\log i$$

and weights

$$a_j = \frac{(Q+j)\log(Q+j)}{C(Q)}.$$

According to the explicit version of Theorem 9.2 of [Bac94], under the ERH we have

$$\left|\log L(1,\chi) - \sum_{i=0}^{Q-1} a_i \log B(Q+i)\right| \le A(Q,\Delta), \tag{3.2}$$

where

$$A(Q,\Delta) = \frac{A\log\Delta + B}{\log Q\sqrt{Q}}. \tag{3.3}$$

A and B can be determined, depending on the value of Q, by using Table 3.1 taken from [Bac94]. If we select the A and B values corresponding to Q_{min}, then (3.2) holds for $Q \ge Q_{min}$. Also, $B(x)$ is defined by the truncated Euler product

$$B(x) = \prod_{p<x}\left(1 - \frac{(\Delta/p)}{p}\right)^{-1},$$

where the product is taken over all primes $p < x$.

Q_{min}	A	B
5	16.397	47.183
10	12.170	38.831
50	8.628	29.587
100	7.962	27.145
500	7.106	22.845
1000	6.897	21.528
5000	6.593	19.321
10000	6.510	18.606
50000	6.378	17.397
100000	6.338	17.031
500000	6.269	16.409
1000000	6.246	16.217

Table 3.1: A and B values for $A(Q, \Delta)$

One of the real bottlenecks in computing estimates like

$$S(Q, \Delta) = \sum_{i=0}^{Q-1} a_i \log B(Q+i)$$

is the evaluation of the many Kronecker (Legendre) symbols $(\frac{\Delta}{q})$. In order to accelerate this process, we first note that it is easy to show that

$$S(Q, \Delta) = \sum_{p \leq 2Q-1} w(p) g(p),$$

where

$$g(p) = \log \left(1 - \frac{(\frac{\Delta}{p})}{p} \right)^{-1}$$

and

$$w(p) = \begin{cases} 1 & p < Q \\ \sum_{p-Q+1}^{Q-1} a_j & Q \leq p < 2Q-1. \end{cases}$$

This method is given in Algorithm 3.1. Our technique of determining $S(Q, \Delta)$ consisted of computing and storing the list of quadratic residues and nonresidues and the values of

$$w(p) \log \left(\frac{p}{p-1} \right),$$

Algorithm 3.1 (Estimate of $\log L(1,\chi)$)

INPUT: Q
OUTPUT: $S(Q,\Delta)$, an estimate of $\log L(1,\chi)$

1. Compute
$$C = \sum_{i=Q}^{2Q-1} i \log i.$$
2. Compute weights
$$w(p) = \begin{cases} 1 & p < Q \\ \sum_{p-Q+1}^{Q-1} a_j & Q \le p < 2Q-1 \end{cases}$$
where
$$a_j = \frac{(Q+j)\log(Q+j)}{C}.$$
3. Set
$$S(Q,\Delta) = \prod_{p \le 2Q-1} w(p) \log\left(\frac{p}{p - \left(\frac{\Delta}{p}\right)}\right).$$

End of Algorithm

$$w(p)\log\left(\frac{p}{p+1}\right)$$

for all the primes $p \le 10000$ in a large table. We could then find the value of

$$w(p)\log\left(\frac{p}{p-\left(\frac{\Delta}{p}\right)}\right)$$

by little more than a single table look-up for each prime $p \le 10000$; thus, we could easily evaluate

$$S(Q,\Delta) = \sum_{p \le 2Q-1} w(p)\log\left(\frac{p}{p-\left(\frac{\Delta}{p}\right)}\right)$$

and then compute an estimate of $L(1,\chi)$ by a single exponentiation.

After conducting some preliminary experiments we found that a value of $Q = 2000$ was very often sufficient to estimate $L(1,\chi)$ (for $\Delta < 10^9$) in order to establish $h = 1$. This is a huge improvement over the truncated product method used in Stephens and Williams

[SW88], where all primes less than 18000 had to be used in the estimate (compared with only 4000 using Bach's method). In fact, we found that using $Q = 5000$ (i.e., primes less than 10000) was often sufficient to establish $h \leq 3$ and that this resulted in the best performance of our algorithm.

3.2 Evaluation of R

Once the initial $L(1,\chi)$ estimates were computed our next step was to evaluate the regulator R of each field $\mathbb{Q}(\sqrt{D})$ for prime D in the current interval. If, for any fixed Q and Δ, we put

$$E = \frac{\sqrt{\Delta}\exp(S(Q,\Delta))}{2},$$

then $hR \approx E$. By using (3.1) and (3.2) we know (under the ERH) that

$$|E - hR| < L^2, \tag{3.4}$$

where

$$L^2 = E\max\left\{e^{A(Q,\Delta)} - 1, 1 - e^{-A(Q,\Delta)}\right\}.$$

In order to determine some indication of the growth rate of L ($Q = 5000$), we evaluated it for prime radicands D only, in various intervals. Here, and in the sequel, interval i represents the set of all prime values of D such that $(i-1) \times 10^6 < D < i \times 10^6$. In Table 3.2 avg( ) denotes the average of the values found in interval i.

With the value of L as computed above we calculated the regulator by using a modified version of the second algorithm in Section 7 of [MW92]. We compute a list $\mathcal{T}$ of all reduced principal ideals whose distance functions δ are less than $L + \log 2$ by developing the continued fraction expansion corresponding to $\mathfrak{a}_0 = (1)$ using Algorithm 2.7. We store each ideal $\mathfrak{a}_i = \left[\frac{Q_i}{r}, \frac{P_i+\sqrt{D}}{r}\right]$ as a triple (P_i, Q_i, δ_i) in a list ordered by the Q values. If during the computation of the list we find some $P_n = P_{n+1}$ then by Theorem 2.9 we can immediately set

$$R = 2\log\Psi_n + \log\frac{Q_0}{Q_n}.$$

interval	max (L)	avg(L)
1	26.01440	10.73694
101	99.76966	50.64988
201	120.47460	61.27755
301	135.44843	68.64010
401	146.94061	74.26657
501	157.06318	78.86076
601	166.13391	82.86471
701	172.31836	86.53736
801	176.91473	89.52843
901	183.47702	92.59853
1000	191.06620	95.27484

Table 3.2: Growth of L

If $Q_m = Q_{m+1}$ then, also by Theorem 2.9,

$$R = 2\log\Psi_m + \log\frac{Q_0\psi_m}{Q_m}.$$

In either case, we terminate the algorithm.

We used hashing techniques to store these ideals since access times for hash tables are generally faster than ordered lists. Since we know that there are approximately L reduced principal ideals with distance less than L, we were easily able to store the entire list in the hash table because our values of L were never larger than 200 (see Table 3.2). We used a hash table of size 2048 so that the number of collisions during insertion would be small. Our hash function was simply $Q_i \pmod{2048}$.

We now use Algorithm 3.2 to find a reduced ideal $\mathfrak{a}_m = \left[\frac{Q_m}{r}, \frac{P_m+\sqrt{D}}{r}\right]$ with $\delta_m \approx E$. If $2^k < E < 2^{k+1}$, then we can use k "doubling" steps to find $\mathfrak{a}_m$ by selecting some $\mathfrak{a}_s(=\mathfrak{b}_0)$ with $\delta_s \approx \frac{E}{2^k}$ and computing $\mathfrak{b}_{j+1} = \mathfrak{b}_j * \mathfrak{b}_j$ until we get $\mathfrak{b}_k = \mathfrak{a}_m$. At each step, after we compute the product $\mathfrak{a} = \mathfrak{b}_j * \mathfrak{b}_j$ we move through the cycle of principal ideals from $\mathfrak{a}$ until we find some $\mathfrak{a}_i$ such that $\delta_i \leq \frac{E}{2^{k-j}} < \delta_{i+1}$ and set $\mathfrak{b}_{j+1} = \mathfrak{a}_i$. We do this so that each ideal $\mathfrak{b}_{j+1}$ has distance as close to $\frac{E}{2^{k-j}}$ as possible. We can then use this ideal $\mathfrak{a}_m$ to compute a value for h^*R, where h^* is some positive integer, as follows. Select the

Algorithm 3.2 (Compute $\mathfrak{a}_m$ with $\delta_m \approx E$)

INPUT: $E, \mathcal{T}$
OUTPUT: $\mathfrak{a}_m$

1. Determine k such that $2^k < E < 2^{k+1}$.
2. Select $\mathfrak{a}_s$ from $\mathcal{T}$ such that $\delta_s < \frac{E}{2^k} < \delta_{s+1}$.
3. Set $\mathfrak{b}_0 = \mathfrak{a}_s$, $j = 0$.
4. Compute $\mathfrak{a} = \mathfrak{b}_j * \mathfrak{b}_j$.
5. Expand the continued fraction corresponding to $\mathfrak{a}$ using Algorithm 2.7 until we find $\mathfrak{a}_i$ with $\delta_i < \frac{E}{2^{k-j}} < \delta_{i+1}$.
6. Set $\mathfrak{b}_{j+1} = \mathfrak{a}_i$, $\delta_j + 1 = \delta_i$, and $j = j + 1$. If $j < k$ then go to 4.
7. Set $\mathfrak{a}_m = \mathfrak{b}_j$.

End of Algorithm

reduced principal ideal $\mathfrak{a}_t$ from the list $\mathcal{T}$ such that $\delta_t < L < \delta_{t+1}$. Set $\mathfrak{c}_0 = \mathfrak{a}_m$, $\mathfrak{d}_0 = \bar{\mathfrak{a}}_m$ and compute $\mathfrak{c}_{i+1} = \mathfrak{c}_i * \mathfrak{a}_t$ and $\mathfrak{d}_{i+1} = \mathfrak{d}_i * \mathfrak{a}_t$ until we find some $\mathfrak{c}_j$ or $\mathfrak{d}_j$ in $\mathcal{T}$. If $\mathfrak{c}_j = \mathfrak{a}_k$ where $\mathfrak{a}_k \in \mathcal{T}$, $\mathfrak{c}_j$ has distance δ_j, and $\mathfrak{a}_k$ has distance δ_k then

$$h^*R = \delta_j - \delta_k.$$

If $\mathfrak{d}_j = \mathfrak{a}_k$ where $\mathfrak{d}_j$ has distance δ_j from $\mathfrak{d}_0$ then

$$h^*R = \delta_m - (\delta_j - \delta_k) - \log \frac{Q_m}{r}.$$

Notice that h^* is not necessarily the class number of $\mathbb{Q}(\sqrt{D})$, but it is at least a rational integer.

Using our value of h^*R, we must now compute R. We first check whether $R < \frac{E}{\sqrt{L}}$ by using a technique similar to that for finding h^*R. As above, select the reduced principal ideal $\mathfrak{a}_t$ from $\mathcal{T}$ such that $\delta_t < L < \delta_{t+1}$. Set $\mathfrak{c}_1 = \mathfrak{a}_t$ and compute $\mathfrak{c}_{i+1} = \mathfrak{c}_i * \mathfrak{a}_t$. If for some $\mathfrak{c}_j$ with distance δ_j we get $\delta_j \geq \frac{E}{\sqrt{L}}$, then we know that $R \geq \frac{E}{\sqrt{L}}$. However, if $\mathfrak{c}_j = \mathfrak{a}_k$ where $\mathfrak{a}_k \in \mathcal{T}$, then

$$R = \delta_j - \delta_k.$$

If $\bar{\mathfrak{c}}_j = \mathfrak{a}_k$ then

$$R = \delta_j + \delta_k - \log \frac{Q_j}{r}.$$

In either case we can terminate the algorithm.

In the case where $R \geq \frac{E}{\sqrt{L}}$, we must find h^*. The main idea, as stated in [MW92], is to check for all primes $q < B = \sqrt{L} + L^2\sqrt{L}/E$ whether the ideal $\mathfrak{a}$ at distance $\frac{h^*R}{q}$ from (1) is such that $\mathfrak{a} = (1)$. If so, then we know that $q \mid h^*R$ and we check the ideals at distance $\frac{h^*R}{q^2}$, $\frac{h^*R}{q^3}$, etc... until we find one equal to (1) at distance $\frac{h^*R}{q^{\alpha_i}}$ but not at $\frac{h^*R}{q^{\alpha_i+1}}$. Then we have q^{α_i} as the highest power of q that divides h^*. If there are n primes $< B$, we have

$$h^* = \prod_{i=1}^{n} q_i^{\alpha_i}$$

and R can be computed easily.

The technique we actually implemented to find h^*, Algorithm 3.3, was presented in [Fun90], and is a more efficient modification of the above procedure (see Table 3.3). Although this technique was developed for pure cubic fields, it can easily be applied to the real quadratic case. We first compute a list $\mathcal{I}$ of reduced ideals $\mathfrak{a}_{t_0}, \mathfrak{a}_{t_1}, \ldots, \mathfrak{a}_{t_n}$ where $\mathfrak{a}_{t_0} = \mathfrak{a}_t$, $\mathfrak{a}_{t_j} = \mathfrak{a}_{t_{j-1}} * \mathfrak{a}_{t_{j-1}}$ and $\delta_{t_{n-1}} < \frac{h^*R}{2} < \delta_{t_n}$. We then produce a list of all primes $q < B$ in decreasing order. For each prime q_s, we must find a reduced ideal $\mathfrak{a}_e$ with distance δ_e such that

$$\frac{h^*R}{q_s} < \delta_e < \frac{h^*R}{q_s} + \delta_t.$$

From the preceding prime q_{s+1} $(> q_s)$ we have an ideal $\mathfrak{a}_m$ such that

$$\frac{h^*R}{q_{s+1}} < \delta_m < \frac{h^*R}{q_{s+1}} + \delta_t.$$

We notice that if we find an ideal $\mathfrak{a}_s$ with distance δ_s such that

$$\delta_s \approx \frac{h^*R}{q_s} - \delta_m$$

and

$$\frac{h^*R}{q_s} < \delta_s + \delta_m \leq \frac{h^*R}{q_s} + \delta_t$$

Algorithm 3.3 (Compute h^* given h^*R)

INPUT: $h^*R, L, \mathcal{T}$, and $\mathfrak{a}_t$ with distance δ_t
OUTPUT: h^*

1. Set $B = \sqrt{L} + \frac{L^2\sqrt{L}}{E}$. Compute a list $\mathcal{P}$ containing all the primes less than B. Set $n = |\mathcal{P}|$. Set $R = h^*R$.
2. Compute a list $\mathcal{I}$ containing the reduced ideals $\mathfrak{a}_{t_i}$ where

$$\mathfrak{a}_{t_0} = \mathfrak{a}_t,$$

$$\mathfrak{a}_{t_j} = \mathfrak{a}_{t_{j-1}} * \mathfrak{a}_{t_{j-1}},$$

$$\delta_{t_{n-1}} < \frac{h^*R}{2} < \delta_{t_n}.$$

3. Set $h^* = 1, \mathfrak{a}_m = (1), \delta_m = 0, s = n$, and let p_s be the s^{th} prime in $\mathcal{P}$.
4. Set

$$r = \frac{R}{p_s} - \delta_m$$

and

$$q = \left\lfloor \frac{r}{\delta_t} \right\rfloor + 1.$$

Compute the binary representation of q, $q = b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_0$, and set

$$\mathfrak{a}_e = \prod_{j=0}^{k} \mathfrak{a}_{t_j}^{b_j}.$$

5. If $\mathfrak{a}_e = \mathfrak{a}_j \in \mathcal{T}$ and $\delta_e = \frac{h^*R}{p_s} + \delta_j$, then set $h^* = h^*q$, $R = R/q$, $\mathfrak{a}_m = (1)$, and go to 4.
6. If $\mathfrak{a}_e \neq \mathfrak{a}_j$ for all the $\mathfrak{a}_j \in \mathcal{T}$, then set $s = s - 1$. If $s > 0$, then set $\mathfrak{a}_m = \mathfrak{a}_e$ and go to 4.

End of Algorithm

then we can set $\mathfrak{a}_e = \mathfrak{a}_s * \mathfrak{a}_m$ with $\delta_e \approx \delta_s + \delta_m$. To find $\mathfrak{a}_s$, we first put $r\delta_t = \frac{h^*R}{q_s} - \delta_m$ for some real number r. We then have $\delta_s \approx q\delta_t$ where $q = [r] + 1$. If we represent q in binary as

$$q = b_k 2^k + b_{k-1} 2^{k-1} + \ldots + b_0$$

where $b_k = 1$ and $b_j = 0,\ 1\ (j < k)$ then we have

$$q\delta_t = b_k 2^k \delta_t + b_{k-1} 2^{k-1} \delta_t + \ldots + b_0 \delta_t.$$

In our list $\mathcal{I}$, we have $\delta_{t_k} \approx 2^k \delta_t$ so we can find $\mathfrak{a}_s$ with distance $\delta_s \approx q\delta_t$ by simply computing a reduced ideal equivalent to

$$\prod_{j=0}^{k} \mathfrak{a}_{t_j}^{b_j}.$$

Once $\mathfrak{a}_e$ has been determined, we check whether there is an ideal $\mathfrak{a}_j \in \mathcal{T}$ with distance δ_j such that $\mathfrak{a}_e = \mathfrak{a}_j$ and $\delta_e = \frac{h^*R}{q_s} + \delta_j$. If so, then $q_s \mid h^*$ and we repeat the above process to determine the precise power α_s of q_s that divides h^*. After the above process has been performed for all $q_s < B$, we have

$$h^* = \prod_{i=1}^{s} q_i^{\alpha_i}$$

and we can compute R.

Table 3.3 shows run-times in minutes on an IBM RS6000/590 for various intervals. By t_i we mean the time required to evaluate R, given an estimate E of hR, for all prime values of D in the specified interval. Algorithm 7.1 from [MW92] which computes R with complexity $O\left(D^{1/4+\epsilon}\right)$ was used to compute the times t_1. Algorithm 3.4 using the simple method for computing h^* was used for t_2, and Algorithm 3.4 using Algorithm 3.3 to compute h^* was used for t_3. The modified algorithm (t_3) was always faster than the unmodified version, and except for the smallest values of D was the fastest overall. Algorithm 7.1 was the best for very small D.

Algorithm 3.4 (Regulator of $\mathbb{Q}(\sqrt{D})$)

INPUT: $S(Q,\Delta)$
OUTPUT: R, h^*

1. Compute $A(Q,\Delta)$, an estimate of the error of $S(Q,\Delta)$, using (3.3).
2. Set
$$E = \frac{\sqrt{\Delta}\exp\left(S(Q,\Delta)\right)}{2},$$
$$L = \sqrt{E\max\left\{\exp(A(Q,\Delta)) - 1, 1 - \exp(-A(Q,\Delta))\right\}}.$$
3. Compute a list $\mathcal{T}$ of the reduced principal ideals $\mathfrak{a}_i$ with $\delta_i < L + \log 2$ by expanding the continued fraction of $\mathfrak{a}_0 = (1)$ using Algorithm 2.7.
4. Compute a_m with $\delta_m \approx E$ using Algorithm 3.2.
5. Select $\mathfrak{a}_t$ from $\mathcal{T}$ such that $\delta_t < L < \delta_{t+1}$.
6. Compute h^*R.
   (a) Set $\mathfrak{c}_0 = \mathfrak{a}_m$, $\mathfrak{d}_0 = \overline{\mathfrak{a}}_m$, $i = j = 0$, $\delta_i = \delta_m$ and $\delta_j = \delta(\mathfrak{d}_j, \mathfrak{d}_0)$.
   (b) Compute $\mathfrak{c}_{i+1} = \mathfrak{c}_i * \mathfrak{a}_t$ and $\mathfrak{d}_{j+1} = \mathfrak{d}_j * \mathfrak{a}_t$. Set $i = i+1$ and $j = j+1$.
   (c) If $\mathfrak{c}_i = \mathfrak{a}_k \in \mathcal{T}$, then set $h^*R = \delta_i - \delta_k$ and go to 7. If $\mathfrak{d}_j = \mathfrak{a}_k \in \mathcal{T}$, then set $h^*R = \delta_m - (\delta_j - \delta_k) - \log\frac{Q_m}{r}$ and go to 7. Otherwise go to b.
7. Check whether $R < E/\sqrt{L}$.
   (a) Set $\mathfrak{c}_0 = \mathfrak{a}_t$, $i = 0$, $\delta_i = \delta\left(\mathfrak{c}_i, (1)\right)$.
   (b) Compute $\mathfrak{c}_{i+1} = \mathfrak{c}_i * \mathfrak{a}_t$ and set $i = i+1$.
   (c) If $\mathfrak{c}_i = \mathfrak{a}_k \in \mathcal{T}$, then set $R = \delta_i - \delta_k$, $h^* = 1$ and terminate. If $\overline{\mathfrak{c}}_i = \mathfrak{a}_k \in \mathcal{T}$, then set $R = \delta_i + \delta_k - \log\frac{Q_i}{r}$, $h^* = 1$ and terminate.
   (d) If $\delta_j > E/\sqrt{L}$ go to 8. Otherwise go to b.
8. $R > E/\sqrt{L}$, so compute h^* and R using Algorithm 3.3.

End of Algorithm

interval	t_1	t_2	t_3
1	0.3	1.0	0.6
101	0.9	2.0	0.8
201	1.1	2.2	0.9
301	1.2	2.4	0.9
401	1.3	2.4	0.9
501	1.4	2.5	1.0
601	1.4	2.6	1.0
701	1.5	2.6	1.0
801	1.5	2.6	1.0
901	1.5	2.7	1.0
1000	1.6	2.7	1.0

Table 3.3: Times for computing R using various algorithms

3.3 Finding a divisor of h

From Section 3.1 we know that our estimate of $L(1,\chi)$ is accurate enough to determine whether $h \leq 3$ for any field $\mathbb{Q}(\sqrt{D})$ with $D < 10^9$. If $h > 3$, it is advisable to find an integer h_1 that divides h, since if $h_2 = h/h_1 \leq 3$, then our estimate of $L(1,\chi)$ is accurate enough to determine that $h = h_1 h_2$. Otherwise, we are forced to compute a more accurate estimate of $L(1,\chi)$ in order to prove (under the ERH) that h is the class number. In our implementation, we set

$$\tilde{h} = \mathrm{Ne}\left(\frac{\sqrt{\Delta}\exp\left(S(Q,\Delta)\right)}{2R}\right),$$

where by $\mathrm{Ne}(x)$ we mean the nearest integer to x, and computed $h_1 > \tilde{h}/3$ for all fields with $\tilde{h} \geq 3$ so that in Algorithm 3.6 we rarely had to improve our estimate of $L(1,\chi)$.

We used Algorithm 3.5 to find h_1. We first select an ideal $\mathfrak{a} = \left[\frac{Q}{r}, \frac{P+\sqrt{D}}{r}\right]$ by setting $Q/r = q$, a prime such that $\left(\frac{D}{q}\right) = 1$ finding a solution x of

$$x^2 \equiv D \pmod{q}$$

Algorithm 3.5 (Divisor of h for $\mathbb{Q}(\sqrt{D})$)

INPUT: h^*, max
OUTPUT: h_1, such that $h_1 \mid h$

1. Set $h_1 = 1$.
2. Set $\mathfrak{a} = (P, Q)$ where $Q = rp$ for some prime p such that $(\frac{D}{p}) = 1$ and $P \equiv x \pmod{p}$, $P \equiv r - 1 \pmod{r}$ where $x^2 \equiv D \pmod{p}$.
3. Set $i = 0$ and compute $\mathfrak{b}_{h^*} = \mathfrak{a}^{h^*}$. If $\mathfrak{b}_{h^*} \sim (1)$, set $m = h^*$ and go to 6.
4. Set
$$\mathfrak{b}_{h^*+i} = \mathfrak{b}_{h^*+(i-1)} * \mathfrak{a},$$
$$\mathfrak{b}_{h^*-i} = \mathfrak{b}_{h^*-(i-1)} * \overline{\mathfrak{a}}.$$
5. If $\mathfrak{b}_{h^*+i} \sim (1)$, then set $m = h^* + i$ and go to 6. If $\mathfrak{b}_{h^*-i} \sim (1)$, then set $m = h^* - i$ and go to 6. Otherwise, set $i = i + 1$ and go to 4.
6. Determine e, the smallest divisor of m such that $\mathfrak{a}^e \sim (1)$.
7. Set $h_1 = \mathrm{LCM}(h_1, e)$. If $h_1 > \frac{\tilde{h}}{3}$ or we have used more than max ideals, terminate. Otherwise, select a new value of p such that $(\frac{D}{p}) = 1$ and go to 2.

End of Algorithm

and then putting $P \equiv r-1 \pmod{r}$, $P \equiv x \pmod{q}$. We then attempt to find an exponent $m \approx \tilde{h}$ such that $\mathfrak{a}^m$ is principal. First, we compute a reduced ideal $\mathfrak{b}_{\tilde{h}} \sim \mathfrak{a}^{\tilde{h}}$ using a fast exponentiation algorithm like those in [Knu81] and check whether it is principal. Often, $\mathfrak{b}_{\tilde{h}}$ will be principal and we can set $m = \tilde{h}$. If it is not we set $i = 1$ and then compute $\mathfrak{b}_{\tilde{h}+i} = \mathfrak{b}_{\tilde{h}+(i-1)} * \mathfrak{a}$ and $\mathfrak{b}_{\tilde{h}-i} = \mathfrak{b}_{\tilde{h}-(i-1)} * \overline{\mathfrak{a}}$ until we get $m = \tilde{h} + i$ or $m = \tilde{h} - i$ such that $\mathfrak{b}_m$ is principal. The value of m found here is in most cases the class number. However, since this is not always the case, we take $h_1 = e_1$, the largest divisor of m such that the reduced ideal $\mathfrak{b} \sim \mathfrak{a}^{e_1}$ is principal. If h_1 is not large enough, we repeat the above process with different ideals and take as h_1 the least common multiple of all divisors found until we have one that is large enough. As shown in Table 3.4, we seldom had to use more than one ideal but sometimes as many as 12 were required. This algorithm is somewhat naive because if, for example, the class group $Cl = C(3) \times C(3) \times C(3) \times \cdots \times C(3)$, the largest

value we could ever find for h_1 would be 3. However, such fields are extremely rare so this is not a problem for $D < 10^9$. In our implementation, if we do not find $h_1 > \tilde{h}/3$ after trying a certain number of ideals, then we give up and take the largest value of h_1 that we are able to obtain.

interval	max	avg
1	10	1
101	12	1
201	12	1
301	12	1
401	11	1
501	11	1
601	11	1
701	11	1
801	11	1
901	11	1
1000	11	1

Table 3.4: Number of ideals used to compute h_1

Since we were interested only in fields with $D < 10^9$, we were able to check whether ideals were principal by simply searching an ordered list of all the ideals in the principal class. We computed this list once for each D with $\tilde{h} \geq 3$. The use of this technique was feasible here because fields with large class numbers have relatively few principal ideals; furthermore, as shown in Table 3.5, we only had to compute h_1 for approximately 12% of all the fields we examined.

Upon further investigation we found that using h^* rather than $\tilde{h}$ was slightly faster in the above algorithm. For fields with large h, the value of h^* found by the regulator algorithm is usually a better approximation than $\tilde{h}$, so fewer ideal multiplications are necessary to determine m. However, the savings in time is small because the regulators for fields with large class numbers are usually found without computing h^*. In these cases, we were forced to use $\tilde{h}$ as detailed above.

interval	# of fields	# of h_1	%
1	78498	7088	9.03
101	54208	6394	11.80
201	52326	6090	11.64
301	51300	6016	11.73
401	50426	5815	11.53
501	49918	5845	11.71
601	49623	5934	11.96
701	49058	5742	11.70
801	48848	5861	12.00
901	48676	5697	11.70
1000	47957	5704	11.89

Table 3.5: How often h_1 was calculated

For square-free D, we can often do a little more. It is well-known ([MW92]) that

$$2^{t-\lambda} \mid h \tag{3.5}$$

where

$$t = \text{number of distinct prime factors of } \Delta$$

and

$$\lambda = \begin{cases} 1 & \text{if all prime factors of } D \text{ are congruent to } 1, 2 \bmod 4 \\ 2 & \text{otherwise.} \end{cases}$$

We can easily compute t and λ for each square-free D in a specific interval during the sieving process used to generate them, so we get this extra information almost for free.

3.4 Evaluation of h

Once the regulator and a sufficiently large divisor have been determined, it is a straightforward matter to determine the class number. We used Algorithm 3.6 due essentially to Buchmann and Williams (see [MW92]). It was very rarely necessary to go beyond the $Q = 5000$ used in the initial approximation to $\log L(1, \chi)$ in order for this algorithm

Algorithm 3.6 (Class Number of $\mathbb{Q}(\sqrt{D})$)

INPUT: D and Δ, the radicand and discriminant of a real quadratic field.
OUTPUT: h and R

1. Put $Q = 5000$. Compute $S(Q, \Delta)$ using Algorithm 3.1, R and h^* using Algorithm 3.4, and h_1 using Algorithm 3.5.
2. Compute
$$F = \frac{\sqrt{\Delta}\exp(S(Q,\Delta))}{2Rh_1}$$
3. $\tilde{h}_2 = \mathrm{Ne}(F)$, $\kappa = F - \tilde{h}_2$
4. If
$$A(Q,\Delta) < \log\left(\frac{\tilde{h}_2 + 1}{\tilde{h}_2 + |\kappa|}\right),$$
then $h = \tilde{h}_2 h_1$ and the algorithm terminates.
5. Otherwise, set $Q = Q + 5000$, recompute $S(Q, \Delta)$, and go to 2.

End of Algorithm

to compute h. In fact it was typically necessary to go beyond this for less than 10 out of approximately 50000 fields examined in each interval. As shown in Tables 3.6 and 3.7 this is an improvement over the truncated product method. A more significant improvement is that the maximum value of Q required in an interval is much smaller than that required by the truncated product method. This is important because Bach's method requires the whole approximation to be recomputed in these cases, whereas a truncated product approximation can be improved simply by adding more terms. However, since we rarely require more accuracy and, if we do, the Q value needed is usually fairly small, our algorithm still runs faster using Bach's method. In these cases we used the usual Jacobi algorithm to evaluate the Legendre symbols (Δ/q). It must be emphasized here that, although the values of the regulators are unconditionally correct, the values of these class numbers are dependent on the truth of the ERH, since the estimate $A(Q, \Delta)$ of the error in our approximation of $L(1, \chi)$ is conditional on the ERH. However, given the

discussion in Shanks [Sha71], it would be a most unusual event, should the ERH be false, for any of the class numbers computed by this technique to be incorrect, assuming that the calculations are carried out correctly.

interval	# of fields	$Q > 18000$	%	$\max(Q)$	$\text{avg}(Q)$
1	78498	61	0.08	127913	18017
101	54208	103	0.19	177841	18100
201	52326	79	0.15	337661	18090
301	51300	106	0.21	197807	18139
401	50426	89	0.18	327667	18126
501	49918	92	0.18	177841	18110
601	49623	104	0.21	807127	18162
701	49058	85	0.17	567377	18113
801	48848	113	0.23	207799	18154
901	48676	119	0.24	1036883	18184
1000	47957	106	0.22	207799	18159

Table 3.6: How often $Q > 18000$ was required (truncated product method)

interval	# of fields	$Q > 18000$	%	$\max(Q)$	$\text{avg}(Q)$
1	78498	2	0.00	10000	5000
101	54208	3	0.00	10000	5000
201	52326	4	0.00	15000	5000
301	51300	8	0.02	10000	5000
401	50426	9	0.02	15000	5000
501	49918	2	0.00	10000	5000
601	49623	7	0.01	35000	5001
701	49058	2	0.00	25000	5000
801	48848	6	0.01	10000	5000
901	48676	6	0.01	40000	5001
1000	47957	7	0.01	10000	5000

Table 3.7: How often $Q > 5000$ was required (Bach method)

The algorithms for determining h_1 and h were also coded in C and run on an IBM RS6000/590. Tables 3.8 and 3.9 show run-times in minutes required to evaluate h for all prime radicands in various intervals using truncated Euler products and Bach's weighted average technique. The time taken to compute $E \approx hR$ for each field in the interval is denoted by t_F, t_R is the time taken to evaluate R, t_h is the time taken to evaluate h, and t is the total time required for all computations in the interval. Using Bach's method, our algorithms executed about 1.5 times as fast as they did using the truncated Euler product method.

interval	t_F	t_R	t_h	t
1	1.3	0.7	0.1	2.1
101	0.9	0.9	0.3	2.1
201	0.9	1.0	0.3	2.2
301	0.9	1.0	0.4	2.3
401	0.9	1.0	0.4	2.3
501	0.9	1.0	0.5	2.4
601	0.9	1.0	0.6	2.5
701	0.9	1.0	0.6	2.5
801	0.9	1.0	0.7	2.6
901	0.9	1.1	0.7	2.7
1000	0.9	1.1	0.8	2.8

Table 3.8: Times for computing h (truncated products Q=18000)

interval	t_F	t_R	t_h	t
1	0.8	0.6	0.0	1.4
101	0.6	0.8	0.1	1.5
201	0.6	0.9	0.1	1.6
301	0.6	0.9	0.1	1.6
401	0.6	0.9	0.1	1.6
501	0.6	1.0	0.1	1.7
601	0.6	1.0	0.1	1.7
701	0.6	1.0	0.1	1.7
801	0.6	1.0	0.2	1.8
901	0.6	1.0	0.2	1.8
1000	0.6	1.0	0.2	1.8

Table 3.9: Times for computing h (Bach's method Q=5000)

Chapter 4

The Cohen-Lenstra Heuristics

Let Cl be the class group of $\mathbb{Q}(\sqrt{D})$ and let Cl^* be the odd part of Cl. In [CL83] and [CL84] Cohen and Lenstra provide some heuristics on the distribution of various Cl^*. For example, if we define $h^* = |Cl^*|$, then the probability that $h^* = 1$ is approximately $\text{Prob}\,(h^* = 1) = 0.75446$, a figure supported by the computations is [SW88].

The fundamental heuristic assumption in [CL83] and [CL84] comes from the observation that if one only looks at the odd part of the class group of imaginary quadratic fields, cyclic groups occur much more frequently than non-cyclic groups. One explanation of this phenomenon is the fact that the automorphism group of a cyclic group is smaller than that of any other abelian group of the same size. This leads to the assumption that each isomorphism class of an abelian group $\mathbf{G}$ has a "weight" associated with it proportional to $1/|\text{Aut}\,(\mathbf{G})\,|$, where $|\text{Aut}\,(\mathbf{G})\,|$ is the order of the automorphism group of $\mathbf{G}$.

We define

$$w(n) = \sum_{\substack{\mathbf{G} \\ |\mathbf{G}|=n}} \frac{1}{\text{Aut}\,(\mathbf{G})}$$

where the sum is taken over all abelian groups of order n up to isomorphism. We have

the following results on w from [CL84]:

$$w(n) = \prod_{p^\alpha \| n} \left(p^\alpha \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^\alpha}\right)\right)^{-1}, \tag{4.1}$$

$$\sum_{d|n} w(d) = nw(n), \tag{4.2}$$

$$\sum_{n \geq 1} \frac{w(n)}{n^s} = \zeta(s+1)\zeta(s+2)\cdots \tag{4.3}$$

where $s > 0$, and

$$\frac{A}{\phi(n)} < w(n) < \frac{B}{\phi(n)} \tag{4.4}$$

where A and B are constants such that $0 < A < B$. For real quadratic fields, we assign the weight $w(n)/n$ to those Cl^* with $|Cl^*| = n$. Dividing by n can be justified by the fact that the ideal classes of real quadratic fields partition themselves into h distinct cycles of reduced ideals, and that each of these cycles exhibits a group-like structure under the operation $*$ defined in Definition 2.10. In fact, the only group axiom that does not hold is associativity. $w(n)$ is the sum of the weights of all groups $\mathbf{G}$ of order n up to isomorphism, so since we are considering real quadratic field class groups we divide $w(n)$ by n because we do not want to count the n "groups" corresponding to the n ideal classes. Further justification of this is provided in [CL83].

4.1 Heuristic Results

Our first heuristic result, found in [CL83] and [CL84], is a result on the probability that $h^* = l$. If the weight $w(n)/n$ is assigned to those Cl^* with $h^* = n$, then we would expect that

$$\text{Prob}\,(h^* = l) = \frac{\frac{w(l)}{l}}{\sum_{\substack{d=1 \\ d \text{ odd}}}^{\infty} \frac{w(d)}{d}}.$$

This is simply the weight assigned to groups with $|\mathbf{G}^*| = l$ divided by the sum of the weights of groups of all odd orders.

We first need to compute an approximation of the function

$$\eta_\infty(p) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

at $p = 2$. An identity of Euler (see, for example, [Hua82, p. 194]) allows us to express functions of the form

$$\frac{1}{(1-ax)(1-ax^2)\cdots(1-ax^i)\cdots}$$

as the more rapidly converging

$$1 + \frac{ax}{1-x} + \frac{a^2x^2}{(1-x)(1-x^2)} + \frac{a^3x^3}{(1-x)(1-x^2)(1-x^3)} + \cdots.$$

At $a = 1$, $x = 1/2$ this gives us

$$\frac{1}{\eta_\infty(2)} = 1 + \frac{1}{2(1-1/2)} + \frac{1}{4(1-1/2)(1-1/4)} + \frac{1}{8(1-1/2)(1-1/4)(1-1/8)} + \cdots$$

and we can compute

$$\eta_\infty(2) = 0.288788095\ldots,$$

an approximation correct to nine digits.

Consider the sum

$$\sum_{d=1}^{\infty} \frac{w(d)}{d}.$$

Since $w(d)/d$ is multiplicative and $\sum w(d)/d$ converges absolutely, we can apply the Euler product formula, yielding

$$\begin{aligned} \sum_{d=1}^{\infty} \frac{w(d)}{d} &= \prod_{p} \left(\sum_{i=0}^{\infty} \frac{w(p^i)}{p^i} \right) \\ &= \sum_{i=0}^{\infty} \frac{w(2^i)}{2^i} \sum_{\substack{d=1 \\ d \text{ odd}}}^{\infty} \frac{w(d)}{d}. \end{aligned}$$

From (4.3) we have

$$\sum_{d=1}^{\infty} \frac{w(d)}{d} = \zeta(2)\zeta(3)\cdots$$

which is precisely the constant

$$C_\infty = 2.294856589\ldots.$$

Also, from (4.1) we have

$$\sum_{i=0}^{\infty} \frac{w(2^i)}{2^i} = \sum_{i=0}^{\infty} \frac{1}{2^{2i}(1-1/2)(1-1/2^2)\cdots(1-1/2^i)}$$

Applying Euler's identity with $a = 1/2$, $x = 1/2$ gives us

$$\begin{aligned} \sum_{i=0}^{\infty} \frac{w(2^i)}{2^i} &= \frac{1}{(1-1/2^2)(1-1/2^3)(1-1/2^4)\cdots} \\ &= \frac{1}{2\eta_\infty(2)}. \end{aligned}$$

Hence,

$$\sum_{\substack{d=1 \\ d \text{ odd}}}^{\infty} \frac{w(d)}{d} = 2\eta_\infty(2)C_\infty. \tag{4.5}$$

If we set

$$C = \frac{1}{2\eta_\infty(2)C_\infty} = 0.754458173\ldots$$

then we can state our first heuristic result as a conjecture.

Conjecture 4.1 *The probability that $h^* = l$ is given by*

$$\text{Prob}\,(h^* = l) = C\frac{w(l)}{l}.$$

This gives us $\text{Prob}\,(h^* = 1) = 0.754458173\ldots$, $\text{Prob}\,(h^* = 3) = 0.125743028\ldots$, and $\text{Prob}\,(h^* = 5) = 0.037722908\ldots$ for the first few values of l.

Our second heuristic result is on the probability that $h^* > x$. By Conjecture 4.1 we would expect this to be given by

$$\text{Prob}\,(h^* > x) = C \sum_{\substack{j>x \\ j \text{ odd}}} \frac{w(j)}{j}. \tag{4.6}$$

In order to analyze the sum in (4.6), we need some additional results on $w(n)$. It is known [Lan36] that

$$\sum_{d>x} \frac{1}{d\,\phi(d)} = O\left(\frac{1}{x}\right),$$

$$\sum_{d>x} \frac{\log d}{d\,\phi(d)} = O\left(\frac{\log x}{x}\right),$$

$$\sum_{\substack{d\le x\\(d,l)=1}} \frac{1}{\phi(d)} = O\left(\log x\right),$$

and

$$\sum_{\substack{d\le x\\(d,l)=1}} \frac{1}{d} = \frac{\phi(l)}{l}\log x + E_0(l) + O\left(\frac{1}{x}\right), \tag{4.7}$$

where $E_0(l)$ is a constant which only depends on l; for example, $E_0(1) = \gamma$. From (4.4), then, it follows that

$$\sum_{d>x} \frac{w(d)}{d} = O\left(\frac{1}{x}\right), \tag{4.8}$$

$$\sum_{d>x} \frac{w(d)\log d}{d} = O\left(\frac{\log x}{x}\right), \tag{4.9}$$

and

$$\sum_{\substack{d\le x\\(d,l)=1}} w(d) = O\left(\log x\right). \tag{4.10}$$

Now if we define

$$W(x) = \sum_{\substack{n\le x\\ n \text{ odd}}} w(n), \tag{4.11}$$

then we can show the following:

Theorem 4.1 *There exist constants E_1, and E_2 such that*

$$W(x) = E_1 \log x + E_2 + O\left(\frac{\log x}{x}\right)$$

where

$$E_1 = \frac{1}{2C} = \eta_\infty(2)C_\infty.$$

Proof: Let

$$\Omega(x,l) = \sum_{\substack{n\le x\\(n,l)=1}} w(n).$$

We apply standard analytic methods similar to those employed by Landau [Lan36]. From (4.2) we have

$$\begin{aligned}\Omega(x,l) &= \sum_{\substack{n\le x\\(n,l)=1}} \frac{1}{n}\sum_{d\mid n} w(d)\\ &= \sum_{\substack{d\le x\\(d,l)=1}} w(d) \sum_{\substack{n\le x, d\mid n\\(n,l)=1}} \frac{1}{n}\\ &= \sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)}{d} \sum_{\substack{m\le x/d\\(m,l)=1}} \frac{1}{m}\end{aligned}$$

and from (4.7) we have

$$\begin{aligned}\Omega(x,l) &= \sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)}{d}\left(\frac{\phi(l)}{l}\log\frac{x}{d} + E_0(l) + O\left(\frac{d}{x}\right)\right)\\ &= \sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)}{d}\frac{\phi(l)}{l}\log\frac{x}{d} + E_0(l)\sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)}{d} + O\left(\frac{1}{x}\sum_{\substack{d\le x\\(d,l)=1}} w(d)\right).\end{aligned}$$

By (4.10) we can set

$$O\left(\frac{1}{x}\sum_{\substack{d\le x\\(d,l)=1}} w(d)\right) = O\left(\frac{\log x}{x}\right),$$

so we now have

$$\begin{aligned}\Omega(x,l) &= \frac{\phi(l)}{l}\log x \sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)}{d} - \frac{\phi(l)}{l}\sum_{\substack{d\le x\\(d,l)=1}} \frac{w(d)\log d}{d}\\ &\quad + E_0(l)\left(\sum_{\substack{d=1\\(d,l)=1}}^{\infty} \frac{w(d)}{d} - \sum_{\substack{d>x\\(d,l)=1}} \frac{w(d)}{d}\right) + O\left(\frac{\log x}{x}\right)\\ &= \frac{\phi(l)}{l}\log x\left(\sum_{\substack{d=1\\(d,l)=1}}^{\infty} \frac{w(d)}{d} - \sum_{\substack{d>x\\(d,l)=1}} \frac{w(d)}{d}\right)\\ &\quad - \frac{\phi(l)}{l}\left(\sum_{\substack{d=1\\(d,l)=1}}^{\infty} \frac{w(d)\log d}{d} - \sum_{\substack{d>x\\(d,l)=1}} \frac{w(d)\log d}{d}\right)\end{aligned}$$

$$+E_0(l)\left(\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)}{d}-\sum_{\substack{d>x\\(d,l)=1}}\frac{w(d)}{d}\right)+O\left(\frac{\log x}{x}\right).$$

Since $\phi(l)/l$ and $E_0(l)$ are constants depending only on l, we can use (4.8) and (4.9) to obtain

$$\Omega(x,l)=\frac{\phi(l)}{l}\log x\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)}{d}-\frac{\phi(l)}{l}\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)\log d}{d}+E_0(l)\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)}{d}+O\left(\frac{\log x}{x}\right).$$

Put

$$E_2(l)=E_0(l)\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)}{d}-\frac{\phi(l)}{l}\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)\log d}{d}$$

and

$$E_1(l)=\frac{\phi(l)}{l}\sum_{\substack{d=1\\(d,l)=1}}^{\infty}\frac{w(d)}{d}.$$

Then we have

$$\Omega(x,l)=E_1(l)\log x+E_2(l)+O\left(\frac{\log x}{x}\right).$$

Now $W(x)=\Omega(x,2)$ so if we set $E_1=E_1(2)$ and $E_2=E_2(2)$ then

$$W(x)=E_1\log x+E_2+O\left(\frac{\log x}{x}\right).$$

Furthermore, using (4.5) it follows that

$$\begin{aligned}E_1 &= E_1(2)\\ &= \frac{\phi(2)}{2}\sum_{\substack{d=1\\d\ \text{odd}}}^{\infty}\frac{w(d)}{d}\\ &= \frac{1}{2}\left(2\eta_\infty(2)C_\infty\right)\\ &= \frac{1}{2C}.\end{aligned}$$

□

Using this result, we can derive the following:

Theorem 4.2 *For n, x both odd*

$$\sum_{n>x} \frac{w(n)}{n} = \frac{E_1}{x} + O\left(\frac{\log x}{x^2}\right).$$

Proof: Consider the sum

$$\sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{w(n)}{n}. \tag{4.12}$$

Using the fact

$$w(2j+1) = W(2j+1) - W(2j-1),$$

we apply partial summation to (4.12) and obtain

$$\begin{aligned}
\sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{w(n)}{n} &= \sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{1}{n}(W(n) - W(n-2)) \\
&= -\frac{W(2r+1)}{2r+3} + \sum_{\substack{n>2r+1 \\ n \text{ odd}}} W(n)\left(\frac{1}{n} - \frac{1}{n+2}\right) \\
&= -\frac{W(2r+1)}{2r+3} + 2\sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{W(n)}{n(n+2)}.
\end{aligned}$$

Now consider

$$2\sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{W(n)}{n(n+2)}.$$

By Theorem 4.1 we have

$$\sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{W(n)}{n(n+2)} = E_1 \sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{\log n}{n(n+2)} + E_2 \sum_{\substack{n>2r+1 \\ n \text{ odd}}} \frac{1}{n(n+2)} + O\left(\sum_{n>x} \frac{\log n}{n^2(n+2)}\right) \tag{4.13}$$

We know that

$$\sum_{n>x} \frac{\log n}{n^3} = O\left(\int_x^\infty \frac{\log t}{t^3} dt\right) = O\left(\frac{\log x}{x^2}\right)$$

so

$$\sum_{n>x} \frac{\log n}{n^2(n+2)} = O\left(\frac{\log x}{x^2}\right). \tag{4.14}$$

Since

$$\sum_{\substack{n>2r+1\\ n \text{ odd}}} \frac{1}{n(n+2)} = \frac{1}{2(2r+3)}$$

we can write

$$\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{1}{n(n+2)} = \frac{1}{2x} + O\left(\frac{1}{x^2}\right). \tag{4.15}$$

From

$$\frac{\log n}{n^2} - \frac{2\log n}{n(n+2)} = \frac{2\log n}{n^2(n+2)}$$

we have by (4.14)

$$\begin{aligned}\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n^2} - 2\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n(n+2)} &= \sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n^2(n+2)} \\ &= O\left(\frac{\log x}{x^2}\right).\end{aligned}$$

Thus

$$\begin{aligned}2\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n(n+2)} &= \sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n^2} + O\left(\frac{\log x}{x^2}\right) \\ &= \int_{\frac{x+1}{2}}^{\infty} \frac{\log(2t+1)}{(2t+1)^2} dt + O\left(\frac{\log x}{x^2}\right)\end{aligned}$$

and by evaluating the integral we obtain

$$2\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{\log n}{n(n+2)} = \frac{1}{2}\left(\frac{\log x+2}{x+2} + \frac{1}{x+2}\right) + O\left(\frac{\log x}{x^2}\right). \tag{4.16}$$

Substituting (4.14), (4.15), and (4.16) into (4.13) yields

$$2\sum_{\substack{n>2r+1\\ n \text{ odd}}} \frac{W(n)}{n(n+2)} = E_1\frac{\log x+2}{x+2} + \frac{E_1}{x+2} + \frac{E_2}{x} + O\left(\frac{\log x}{x^2}\right). \tag{4.17}$$

We now apply Theorem 4.1 to

$$-\frac{W(2r+1)}{2r+3} = -\frac{W(x)}{x+2}$$

and combine the result with (4.17) giving us

$$\begin{aligned}\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{w(n)}{n} &= \frac{-E_1 \log x}{x+2} + \frac{E_1 \log x + 2}{x+2} + \frac{E_1}{x+2} - \frac{E_2}{x+2} + \frac{E_2}{x} + O\left(\frac{\log x}{x^2}\right) \\ &= \frac{E_1(\log(x+2) - \log x + 1)}{x+2} + O\left(\frac{\log x}{x^2}\right) \\ &= \frac{E_1}{x+2} + \frac{E_1 \log(1+2/x)}{x+2} + O\left(\frac{\log x}{x^2}\right)\end{aligned}$$

Finally, since

$$\log\left(1+\frac{2}{x}\right) = O\left(\frac{1}{x}\right)$$

we have

$$\sum_{\substack{n>x\\ n,x \text{ odd}}} \frac{w(n)}{n} = \frac{E_1}{x} + O\left(\frac{\log x}{x^2}\right)$$

and the theorem is proved. □

We are now in a position to state our second heuristic result. Combining (4.6) and Theorem 4.2 gives us

$$\begin{aligned}C \sum_{\substack{j>x\\ j \text{ odd}}}^{\infty} \frac{w(j)}{j} &= C\left(\frac{E_1}{x} + O\left(\frac{\log x}{x^2}\right)\right) \\ &= C\frac{1}{2Cx} + O\left(\frac{\log x}{x^2}\right) \\ &= \frac{1}{2x} + O\left(\frac{\log x}{x^2}\right)\end{aligned}$$

and we have

Conjecture 4.2 *The probability that $h^* > x$ is given by*

$$\text{Prob}\,(h^* > x) = \frac{1}{2x} + O\left(\frac{\log x}{x^2}\right).$$

Thus, under the Cohen-Lenstra heuristics we would expect that h^* is most likely to be small. Since $\text{Prob}\,(h^* = 1) \approx 3/4$, we will write this as

$$1 - \text{Prob}\,(h^* \leq x) = \frac{1}{2x+2} + O\left(\frac{\log x}{x^2}\right).$$

Thus, we would expect that

$$k+1=\frac{1}{2}\left(\frac{1}{1-\text{Prob}\,(h^*\leq k)}\right)+O\left(\frac{\log k}{k^2}\right), \tag{4.18}$$

a result that can be used to test the accuracy of Conjecture 4.2.

Let $h(p)$ be the class number of the field $\mathbb{Q}(\sqrt{p})$ where p is a prime. By using some further assumptions, Cohen was able to show the following:

Conjecture 4.3 *For* $p\equiv 1 \pmod 4$,

$$\sum_{p\leq x} h(p)\sim\frac{x}{8}.$$

This result was conjectured by Hooley [Hoo84] at about the same time.

4.2 Numerical Experiments

In order to test the conjectures stated in Section 4.1 we used the techniques of Chapter 3 to compute the class numbers for all fields $\mathbb{Q}(\sqrt{D})$ where $D<10^8$ and all fields $\mathbb{Q}(\sqrt{p})$ where p is prime and $p<10^9$. This computation required just under 4 weeks on a DECStation 5000/200. The class numbers are stored on 8mm tape along with their corresponding radicands and regulators in TAR format.

We use the notation of [JLW94] to describe our results. For a finite group $\mathbf{G}$ we define

$$f_k(\mathbf{G})=\begin{cases}1 & \text{when } |\mathbf{G}|=k,\\ 0 & \text{otherwise.}\end{cases}$$

Let D denote any square-free, positive integer and let $Cl^*(D)$ represent the odd part of the class group of $\mathbb{Q}(\sqrt{D})$. Put

$$\begin{aligned}\mathcal{D}_1(x) &= \{D\leq x \mid D\equiv 1 \pmod 4\}\\ \mathcal{D}_2(x) &= \{D\leq x \mid D\not\equiv 1 \pmod 4\}\end{aligned}$$

$$\begin{aligned}\mathcal{P}_1(x) &= \{p \le x \mid p \equiv 1 \pmod 4,\ p \text{ prime}\}\\ \mathcal{P}_2(x) &= \{p \le x \mid p \equiv 3 \pmod 4,\ p \text{ prime}\}\end{aligned}$$

For each $\mathcal{D}(x) \in \{\mathcal{D}_1(x), \mathcal{D}_2(x), \mathcal{P}_1(x), \mathcal{P}_2(x)\}$, we define

$$\begin{aligned}r_i(x) &= \sum_{D\in\mathcal{D}(x)} f_i(Cl^*(D)) \Big/ \sum_{D\in\mathcal{D}(x)} 1,\\ q_i(x) &= r_i(x)i/(Cw(i)),\\ s_i(x) &= \sum_{j\le i} r_i(x),\\ t_i(x) &= \frac{1}{2}\left(\frac{1}{1-s_i(x)}\right).\end{aligned}$$

Also, put

$$H^*(x) = \sum_{D\in\mathcal{D}(x)} h^*(D).$$

In Tables 4.1 through 4.4 we provide values of $q_i(x)$ for various values of i and x, $\mathcal{D}(x) = \mathcal{D}_1(x),\ \mathcal{D}_2(x),\ \mathcal{P}_1(x),\ \mathcal{P}_2(x)$. If Conjecture 4.1 is correct, we would expect the values of $q_i(x)$ to converge to 1 as x increases. Figures 4.1 through 4.4 show the values of $q_1(x)$ plotted against x. In all cases the values of $q_i(x)$ do seem to be converging to 1, although the apparent convergence is very slow.

Tables 4.5 through 4.8 contain values of $t_i(x)$, again for various values of i and x, $\mathcal{D}(x) = \mathcal{D}_1(x),\ \mathcal{D}_2(x),\ \mathcal{P}_1(x),\ \mathcal{P}_2(x)$. We expect, because of Conjecture 4.2 and (4.18), that $t_i(x)$ will approach $i+1$ for each i as x increases. Figures 4.5 through 4.8 show the values of $t_1(x)$ plotted against x. Our results seem to indicate that $t_i(x)$ does indeed approach $i+1$, but as in the case of the $q_i(x)$ values, the convergence is slow.

In Tables 4.9 and 4.10 we provide values of $H^*(x)$ and $8H^*(x)/x$ for $\mathcal{D}(x) = \mathcal{P}_1(x)$ and $\mathcal{P}_2(x)$. By Conjecture 4.3 we expect that $8H^*(x)/x$ will approach 1 as x increases for $D \in \mathcal{P}_1(x)$. Figure 4.9 shows the values of $y = 8H^*(x)/x$ plotted against x. It appears that the values of y are in fact approaching 1, but very slowly. Not surprisingly, the

same phenomenon appears to happen for the case where $D \in \mathcal{P}_2(x)$ (Table 4.10 and Figure 4.10).

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.06119	0.85263	0.95644	0.94918	0.70424	0.90228	0.47347
10000000	1.03676	0.89604	0.99125	0.99564	0.83023	0.97519	0.69086
20000000	1.03178	0.90683	0.99465	1.00142	0.84625	0.98812	0.74718
30000000	1.02923	0.91246	0.99592	1.00250	0.85705	0.99247	0.76587
40000000	1.02752	0.91613	0.99663	1.00194	0.86264	0.99791	0.78753
50000000	1.02634	0.91893	0.99664	1.00315	0.86638	0.99846	0.79660
60000000	1.02541	0.92078	0.99588	1.00446	0.87092	0.99982	0.80705
70000000	1.02461	0.92235	0.99632	1.00504	0.87567	1.00148	0.81494
80000000	1.02389	0.92374	0.99637	1.00623	0.87874	1.00372	0.82014
90000000	1.02333	0.92480	0.99702	1.00608	0.88182	1.00418	0.82863
100000000	1.02284	0.92605	0.99695	1.00581	0.88409	1.00528	0.83205

Table 4.1: $q_i(x)$ for $\Delta \equiv 1 \pmod 4$

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.05492	0.88695	0.98805	0.98292	0.74471	0.89756	0.45440
10000000	1.03283	0.91646	1.00575	1.01113	0.84605	0.99578	0.72188
20000000	1.02840	0.92278	1.00558	1.01101	0.87155	1.00547	0.77881
30000000	1.02602	0.92657	1.00659	1.01256	0.88017	1.00613	0.80868
40000000	1.02444	0.92959	1.00629	1.01317	0.88575	1.00535	0.81575
50000000	1.02329	0.93152	1.00573	1.01367	0.89055	1.00847	0.82751
60000000	1.02239	0.93313	1.00569	1.01364	0.89438	1.00911	0.83671
70000000	1.02169	0.93456	1.00496	1.01327	0.89749	1.00864	0.84090
80000000	1.02108	0.93571	1.00449	1.01288	0.89939	1.00894	0.84989
90000000	1.02057	0.93680	1.00413	1.01286	0.90080	1.00935	0.85503
100000000	1.02013	0.93773	1.00406	1.01266	0.90285	1.00939	0.85902

Table 4.2: $q_i(x)$ for $\Delta \equiv 0 \pmod 4$

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.03912	0.87049	0.98999	1.05015	0.74868	0.89694	0.80228
10000000	1.02286	0.91026	1.00832	1.00988	0.89654	1.00820	0.83991
20000000	1.01992	0.91885	1.01125	1.01036	0.89047	1.00770	0.87678
30000000	1.01878	0.92317	1.00562	1.02080	0.89756	1.00138	0.88219
40000000	1.01746	0.92762	1.00621	1.02143	0.89815	1.01307	0.89369
50000000	1.01679	0.93026	1.00793	1.01899	0.90235	1.01437	0.89445
60000000	1.01614	0.93257	1.00686	1.01727	0.90852	1.01408	0.90140
70000000	1.01563	0.93519	1.00600	1.01803	0.91051	1.01274	0.90768
80000000	1.01515	0.93662	1.00488	1.01891	0.91308	1.01263	0.90514
90000000	1.01493	0.93712	1.00600	1.01489	0.91691	1.01078	0.89925
100000000	1.01468	0.93864	1.00478	1.01335	0.91944	1.00665	0.90274
200000000	1.01314	0.94558	1.00057	1.01216	0.92337	1.00713	0.90869
300000000	1.01241	0.94866	1.00118	1.00676	0.92586	1.00590	0.91010
400000000	1.01169	0.95144	1.00229	1.00406	0.92779	1.00362	0.91560
500000000	1.01122	0.95334	1.00100	1.00519	0.93096	1.00409	0.91528
600000000	1.01077	0.95493	1.00120	1.00534	0.93239	1.00461	0.92144
700000000	1.01045	0.95583	1.00199	1.00608	0.93323	1.00523	0.92348
800000000	1.01020	0.95683	1.00179	1.00619	0.93468	1.00506	0.92527
900000000	1.00998	0.95777	1.00186	1.00629	0.93499	1.00509	0.92732
1000000000	1.00976	0.95830	1.00239	1.00646	0.93604	1.00508	0.92706

Table 4.3: $q_i(x)$ for $p \equiv 1 \pmod 4$

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.03169	0.88645	1.00516	1.06462	0.87370	1.05674	1.05168
10000000	1.01961	0.92914	1.00096	1.01608	0.88639	1.04657	0.92562
20000000	1.01729	0.93251	1.00361	1.01853	0.90461	1.04376	0.94236
30000000	1.01601	0.93806	1.00252	1.01969	0.90604	1.02475	0.92939
40000000	1.01510	0.94106	1.00413	1.02069	0.90458	1.01667	0.90934
50000000	1.01414	0.94392	1.00371	1.02162	0.91150	1.02266	0.90975
60000000	1.01373	0.94516	1.00376	1.02286	0.91323	1.01674	0.91555
70000000	1.01339	0.94591	1.00271	1.02380	0.91663	1.01399	0.91383
80000000	1.01315	0.94704	1.00186	1.01999	0.91465	1.01691	0.90890
90000000	1.01318	0.94739	1.00096	1.01841	0.91495	1.01658	0.90364
100000000	1.01282	0.94863	1.00277	1.01841	0.91523	1.01206	0.90528
200000000	1.01125	0.95343	1.00129	1.01415	0.92563	1.01600	0.91863
300000000	1.01053	0.95553	1.00120	1.01083	0.93371	1.01677	0.91909
400000000	1.01000	0.95730	1.00000	1.00955	0.93646	1.01743	0.92316
500000000	1.00952	0.95938	1.00057	1.00996	0.93687	1.01306	0.92387
600000000	1.00916	0.96067	1.00087	1.01030	0.93849	1.01272	0.92674
700000000	1.00897	0.96160	0.99977	1.00988	0.94034	1.01177	0.93430
800000000	1.00878	0.96248	0.99929	1.00930	0.94228	1.01058	0.93566
900000000	1.00860	0.96303	0.99942	1.00942	0.94350	1.01118	0.93528
1000000000	1.00844	0.96357	0.99976	1.00902	0.94452	1.01033	0.93923

Table 4.4: $q_i(x)$ for $p \equiv 3 \pmod 4$

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.50786	5.42530	8.91565	12.81041	17.88166	22.96408	109.6509
10000000	2.29561	4.75574	7.38079	10.02841	13.58368	16.60010	55.01249
20000000	2.25667	4.64952	7.14116	9.61024	12.91103	15.64977	48.43620
30000000	2.23723	4.59746	7.02378	9.40226	12.59204	15.19731	45.43814
40000000	2.22443	4.56286	6.94593	9.26159	12.36781	14.88841	43.53718
50000000	2.21560	4.54032	6.89384	9.17287	12.22767	14.68742	42.23651
60000000	2.20874	4.52115	6.84708	9.09414	12.10904	14.52054	41.36938
70000000	2.20287	4.50462	6.81076	9.03188	12.02043	14.39801	40.61104
80000000	2.19765	4.48987	6.77728	8.97656	11.93639	14.28389	39.94645
90000000	2.19354	4.47810	6.75275	8.93314	11.87337	14.19501	39.48465
100000000	2.18998	4.46955	6.73308	8.89798	11.82131	14.12367	39.02412

Table 4.5: $t_i(x)$ for $D \equiv 1 \pmod 4$

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.44971	5.40084	9.04060	13.28036	19.27199	25.26746	149.0036
10000000	2.26478	4.73781	7.39709	10.11513	13.83783	17.06305	60.93412
20000000	2.23102	4.62625	7.12805	9.61830	13.05984	15.92912	51.83881
30000000	2.21324	4.57025	6.99969	9.39093	12.68762	15.38094	48.02569
40000000	2.20163	4.53657	6.91991	9.24978	12.45849	15.04308	45.68878
50000000	2.19330	4.51119	6.85904	9.14283	12.28799	14.80457	44.11769
60000000	2.18672	4.49165	6.81385	9.06263	12.16136	14.62304	42.90773
70000000	2.18168	4.47761	6.77904	9.00007	12.06317	14.47996	41.96801
80000000	2.17735	4.46517	6.74894	8.94596	11.97473	14.35356	41.23261
90000000	2.17371	4.45532	6.72525	8.90433	11.90654	14.25684	40.59847
100000000	2.17054	4.44663	6.70522	8.86869	11.85193	14.17872	40.07697

Table 4.6: $t_i(x)$ for $D \equiv 0 \pmod 4$

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.31449	4.69162	7.22253	9.92777	12.95470	15.41109	55.48867
10000000	2.19018	4.39240	6.59663	8.67220	11.47744	13.64301	36.38335
20000000	2.16904	4.34869	6.50789	8.52074	11.18966	13.23712	34.28533
30000000	2.16105	4.33701	6.46395	8.47241	11.13404	13.14434	33.69292
40000000	2.15178	4.32065	6.42954	8.41497	11.03731	13.03696	32.98149
50000000	2.14711	4.31417	6.42053	8.39339	11.01621	13.01053	32.63839
60000000	2.14260	4.30673	6.40077	8.35532	10.97404	12.95108	32.35346
70000000	2.13905	4.30460	6.39342	8.34469	10.96322	12.93295	32.21378
80000000	2.13576	4.29791	6.37521	8.31590	10.92319	12.87703	32.04356
90000000	2.13419	4.29391	6.36986	8.29684	10.90465	12.84707	31.84695
100000000	2.13247	4.29399	6.36629	8.28698	10.89705	12.82721	31.69778
200000000	2.12197	4.28339	6.33025	8.22313	10.80130	12.69580	30.99612
300000000	2.11706	4.27754	6.31934	8.19169	10.75619	12.63083	30.63904
400000000	2.11217	4.27035	6.30698	8.16446	10.71624	12.57083	30.40868
500000000	2.10902	4.26615	6.29396	8.14535	10.69473	12.54227	30.24493
600000000	2.10600	4.26107	6.28353	8.12824	10.67037	12.50989	30.15319
700000000	2.10388	4.25650	6.27594	8.11728	10.65447	12.48937	30.07765
800000000	2.10222	4.25425	6.27045	8.10837	10.64429	12.47502	30.02542
900000000	2.10075	4.25251	6.26689	8.10267	10.63557	12.46310	29.98853
1000000000	2.09927	4.24886	6.26053	8.09245	10.62169	12.44402	29.92182

Table 4.7: $t_i(x)$ for $p \equiv 1 \pmod 4$

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.25600	4.53855	6.92045	9.41168	12.69270	15.55459	52.99461
10000000	2.16684	4.38914	6.56524	8.63461	11.37025	13.58834	36.30384
20000000	2.15056	4.33875	6.46149	8.46233	11.14409	13.25980	34.39996
30000000	2.14165	4.32863	6.43567	8.42106	11.07814	13.12147	33.53834
40000000	2.13541	4.31723	6.41548	8.38905	11.01726	13.01735	32.87498
50000000	2.12880	4.30357	6.38408	8.33777	10.95500	12.94427	32.59799
60000000	2.12603	4.29800	6.37199	8.32023	10.93125	12.89761	32.39932
70000000	2.12369	4.29195	6.35549	8.29445	10.89947	12.84714	32.03312
80000000	2.12206	4.29051	6.34975	8.27530	10.85909	12.79765	31.81470
90000000	2.12227	4.29298	6.35243	8.27594	10.86131	12.79998	31.75285
100000000	2.11984	4.28880	6.34878	8.26975	10.85169	12.77651	31.62821
200000000	2.10924	4.26748	6.29775	8.17314	10.72340	12.60762	30.75279
300000000	2.10442	4.25731	6.27535	8.12757	10.67391	12.54094	30.39120
400000000	2.10089	4.25097	6.25804	8.09554	10.62850	12.47970	30.07747
500000000	2.09769	4.24728	6.25172	8.08593	10.61340	12.44959	29.97066
600000000	2.09527	4.24322	6.24381	8.07351	10.59775	12.42734	29.90209
700000000	2.09401	4.24225	6.23848	8.06361	10.58721	12.41083	29.80571
800000000	2.09274	4.24103	6.23443	8.05550	10.58005	12.39850	29.75144
900000000	2.09156	4.23869	6.22975	8.04796	10.57134	12.38781	29.69179
1000000000	2.09053	4.23690	6.22690	8.04226	10.56509	12.37742	29.66390

Table 4.8: $t_i(x)$ for $p \equiv 3 \pmod 4$

x	$H^*(x)$	$8H^*(x)/x$
1000000	97521	0.78017
10000000	990162	0.79213
20000000	1988884	0.79555
30000000	2976321	0.79369
40000000	3984781	0.79696
50000000	4987508	0.79800
60000000	5987504	0.79833
70000000	6987254	0.79854
80000000	7972707	0.79727
90000000	8997355	0.79976
100000000	10010538	0.80084
200000000	20090934	0.80364
300000000	30153902	0.80410
400000000	40367003	0.80734
500000000	50551652	0.80883
600000000	60651064	0.80868
700000000	70801346	0.80916
800000000	80950648	0.80951
900000000	91082121	0.80962
1000000000	101284007	0.81027

Table 4.9: $H^*(x)$ for $p \equiv 1 \pmod 4$

x	$H^*(x)$	$8H^*(x)/x$
1000000	97506	0.78005
10000000	972400	0.77792
20000000	1950824	0.78033
30000000	2933763	0.78234
40000000	3916578	0.78332
50000000	4897327	0.78357
60000000	5870416	0.78272
70000000	6867611	0.78487
80000000	7863314	0.78633
90000000	8845532	0.78627
100000000	9836462	0.78692
200000000	19858578	0.79434
300000000	29832040	0.79552
400000000	39891148	0.79782
500000000	49965564	0.79945
600000000	59954496	0.79939
700000000	70036400	0.80042
800000000	80044854	0.80045
900000000	90119519	0.80106
1000000000	100141354	0.80113

Table 4.10: $H^*(x)$ for $p \equiv 3 \pmod 4$

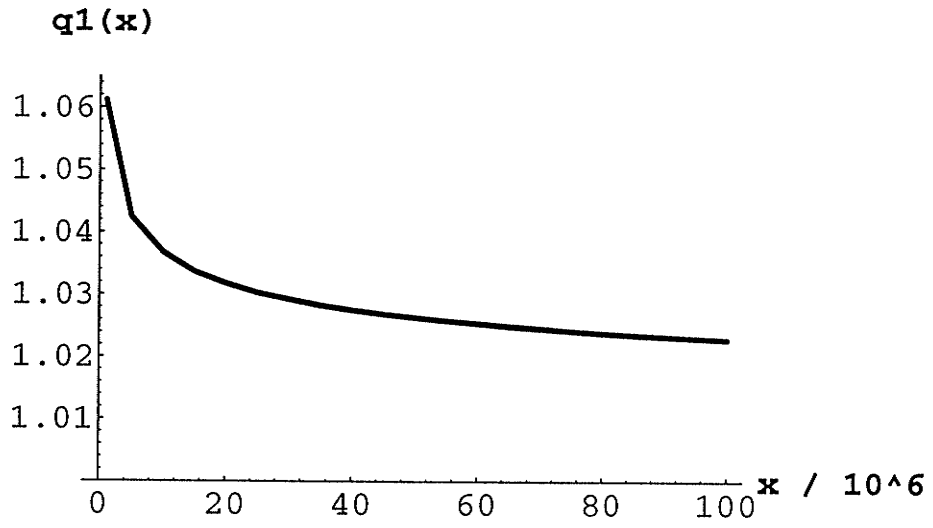

Figure 4.1: x vs. $q_1(x)$ for $\Delta \equiv 1 \pmod 4$

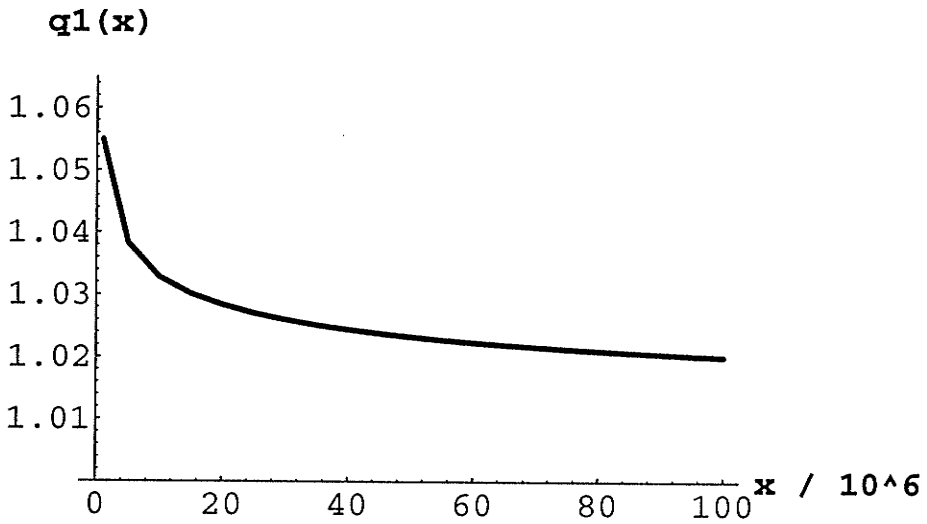

Figure 4.2: x vs. $q_1(x)$ for $\Delta \equiv 0 \pmod 4$

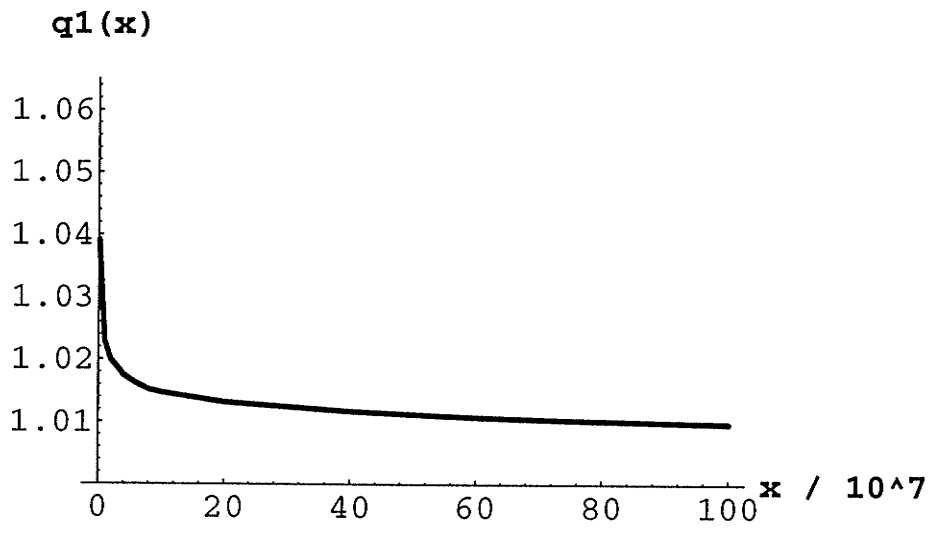

Figure 4.3: x vs. $q_1(x)$ for $p \equiv 1 \pmod 4$

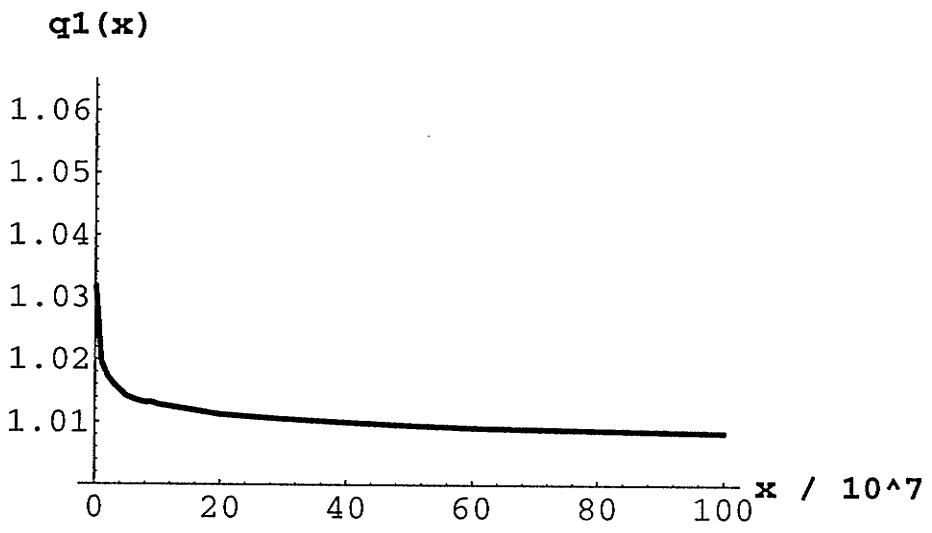

Figure 4.4: x vs. $q_1(x)$ for $p \equiv 3 \pmod 4$

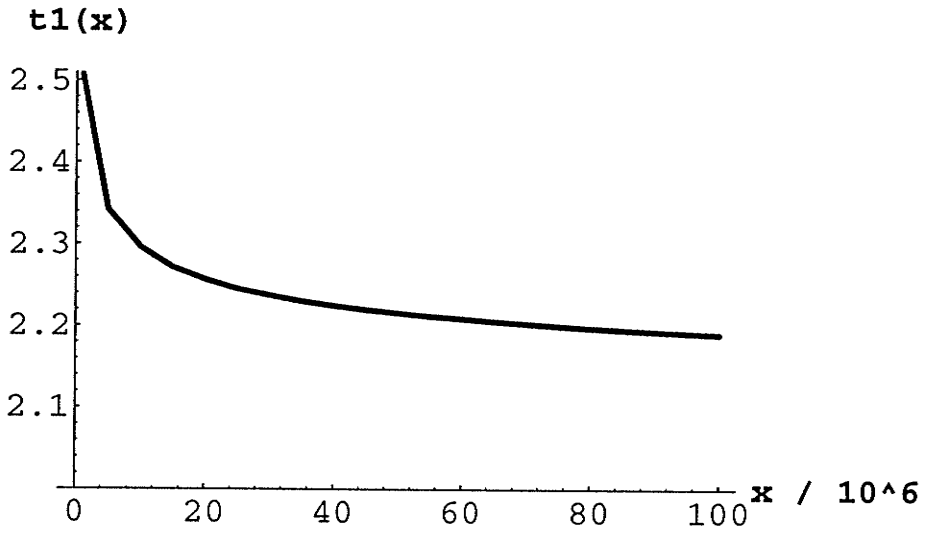

Figure 4.5: x vs. $t_1(x)$ for $\Delta \equiv 1 \pmod 4$

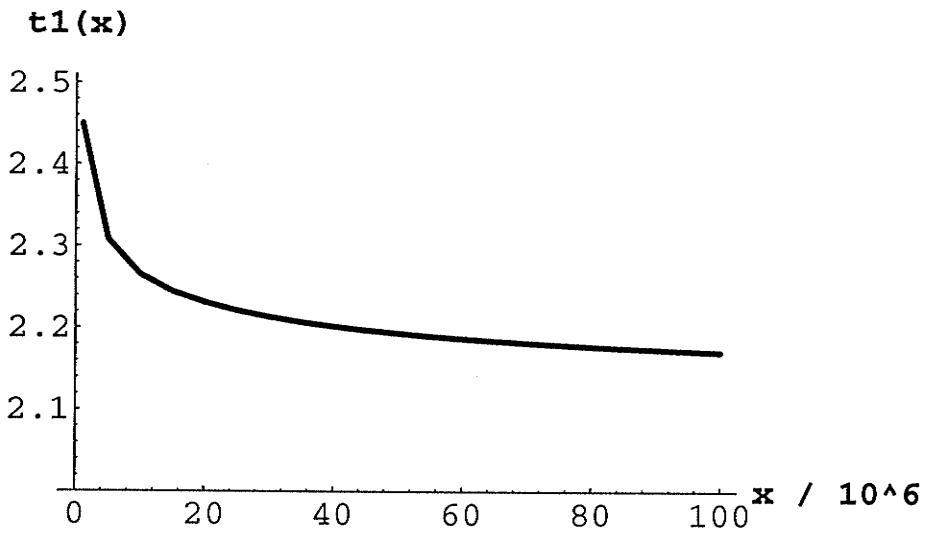

Figure 4.6: x vs. $t_1(x)$ for $\Delta \equiv 0 \pmod 4$

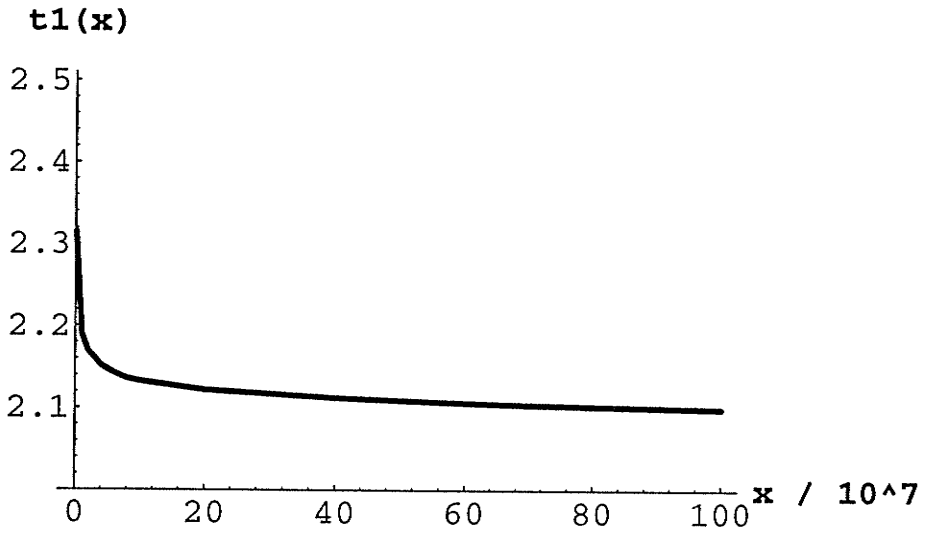

Figure 4.7: x vs. $t_1(x)$ for $p \equiv 1 \pmod 4$

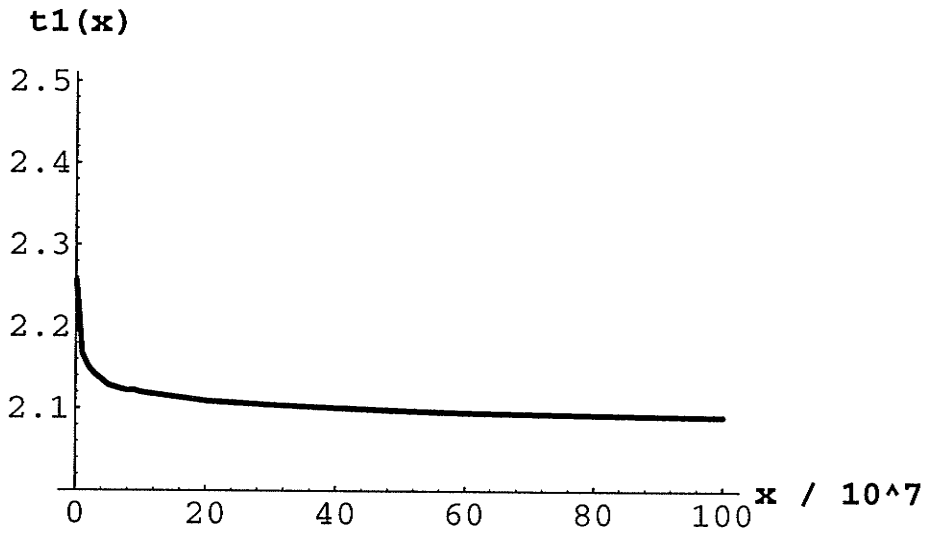

Figure 4.8: x vs. $t_1(x)$ for $p \equiv 3 \pmod 4$

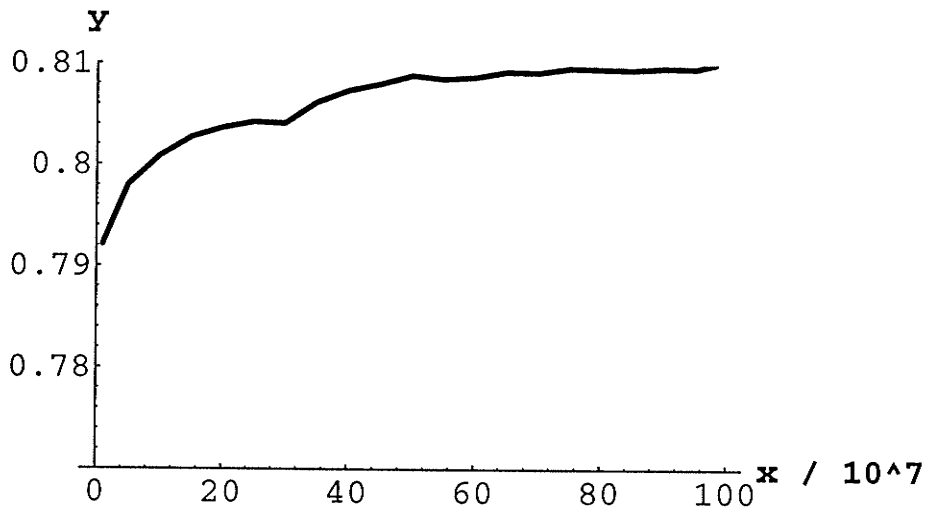

Figure 4.9: x vs. $8H^*(x)/x$ for $p \equiv 1 \pmod 4$

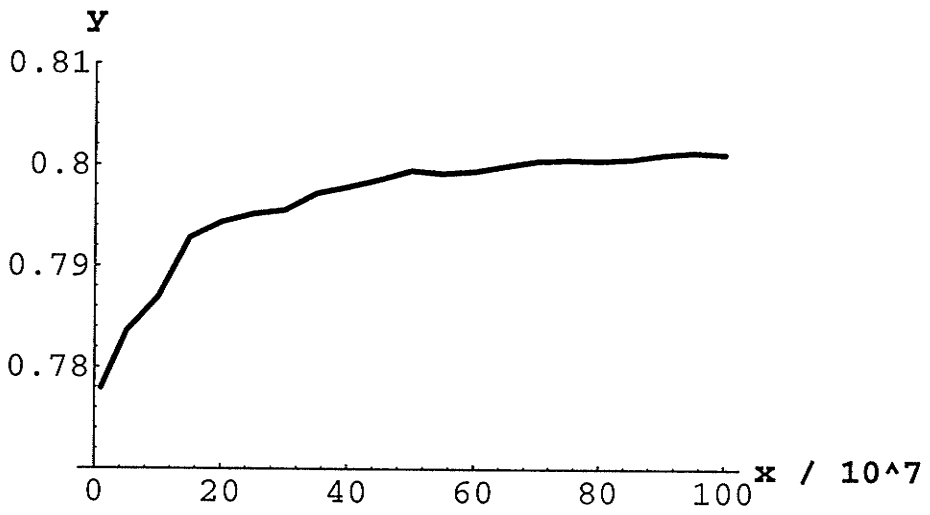

Figure 4.10: x vs. $8H^*(x)/x$ for $p \equiv 3 \pmod 4$

4.3 Conclusion

A strong indicator that the conjectures given in this chapter are likely to be valid is the fact that two particular cases of two of the other conjectures in [CL83] and [CL84] are actually theorems. Since these conjectures were developed on the same heuristic assumption as the conjectures given here, it seems likely that the conjectures of this chapter, as well as the remaining ones in [CL83] and [CL84], are true.

All of our results provide numerical support for the Cohen-Lenstra heuristics, and in particular that small values of h^* seem to occur infinitely often, even when we restrict the radicands of the fields to prime values. In these cases, of course, we have $h = h^*$, so it seems very likely that small class numbers occur infinitely often.

Chapter 5

The Size of R

Recall from Definition 2.2 that the regulator R of $\mathbb{Q}(\sqrt{D})$ is equal to $\log \varepsilon_0$ where ε_0 is the fundamental unit of $\mathbb{Q}(\sqrt{D})$. Since $\varepsilon_0 \in \mathcal{O}_\mathcal{K}$, we have $\varepsilon_0 = (x + y\sqrt{\Delta})/2$, where $x, y \in \mathbb{Z}$. Also, $|N(\varepsilon_0)| = \varepsilon_0|\overline{\varepsilon_0}| = 1$, so we have

$$\varepsilon_0 - 1 < x < \varepsilon_0 + 1$$
$$\frac{\varepsilon_0 - 1}{\sqrt{\Delta}} < y < \frac{\varepsilon_0 + 1}{\sqrt{\Delta}}.$$

Hence, $x, y > 0$ and we see that the regulator provides us with a good estimate of $\log x$ and $\log \sqrt{\Delta} y$. It is of great interest to have some idea of the size of R (and hence ε_0) since, for example, the fundamental unit is useful in characterizing all solutions of Diophantine equations of the form $N(\alpha) = k$ where $\alpha \in \mathcal{O}_\mathcal{K}$ and $k \in \mathbb{Z}$. Also, certain cryptosystems (see for example [BW89a]) require a large number of ideals in any given ideal class, and R is a measure of this.

It is easy to give a tight lower bound on R in terms of Δ. When $\Delta = x^2 + 4$ for some odd x, then it is not difficult to show that $\varepsilon_0 = (x + \sqrt{\Delta})/2$. Thus, we have $\varepsilon_0 = (\sqrt{\Delta - 4} + \sqrt{\Delta})/2$ and $R = \log(\sqrt{\Delta - 4} + \sqrt{\Delta})/2$. Since in general $\varepsilon_0 = (x + y\sqrt{\Delta})/2$ with $x, y > 0$ and $|\varepsilon_0\overline{\varepsilon_0}| = 1$, we have $x = \sqrt{y^2\Delta \pm 4}$ and

$$\varepsilon_0 = \frac{\sqrt{y^2\Delta \pm 4} + y\sqrt{\Delta}}{2} \geq \frac{\sqrt{\Delta - 4} + \sqrt{\Delta}}{2}.$$

Hence

$$R \geq \log\left(\frac{\sqrt{\Delta-4}+\sqrt{\Delta}}{2}\right) \tag{5.1}$$

It has been shown (for example, Nagell [Nag22]) that x^2+4 is square-free infinitely often for odd x. Therefore, equality in the lower bound (5.1) is achieved infinitely often.

It is a far more difficult problem to give a tight upper bound on R. By a result of Hua ([Hua82, p. 329]) we can say that

$$R < \sqrt{\Delta}\left(\frac{1}{2}\log\Delta + 1\right),$$

but this is not nearly as tight as (5.1). Thus, we are faced with two questions:

1. How large can R become as a function of Δ?

2. How often does R become that large?

Both of these problems turn out to be extremely difficult.

Recall the analytic class number formula from Section 2.6,

$$L(1,\chi) = \frac{2hR}{\sqrt{\Delta}} \tag{5.2}$$

By examining this equation we note that in order for R to be large it is necessary for h to be small and $L(1,\chi)$ to be large. The results of Chapter 4 suggest that h is small infinitely often, in fact for a large portion of all real quadratic fields. Thus, we focus our attention here on the size of $L(1,\chi)$.

5.1 Littlewood's Bounds on $L(1,\chi)$

Littlewood [Lit28] and Shanks [Sha73] have shown that under the ERH we have

$$\frac{\{1+o(1)\}}{c_1 \log\log\Delta} < L(1,\chi) < \{1+o(1)\}\, c_2 \log\log\Delta, \tag{5.3}$$

where the values of the constants c_1 and c_2 depend upon the parity of Δ,

$$c_1 = \begin{cases} \frac{8e^\gamma}{\pi^2} & \text{when } 2 \mid \Delta, \\ \frac{12e^\gamma}{\pi^2} & \text{otherwise,} \end{cases}$$

$$c_2 = \begin{cases} e^\gamma & \text{when } 2 \mid \Delta, \\ 2e^\gamma & \text{otherwise,} \end{cases}$$

and γ is Euler's constant. In his numerical examination of (5.3) Shanks [Sha73] defined for a fixed Δ the *upper* and *lower Littlewood indices* as

$$ULI = \frac{L(1,\chi)}{c_2 \log\log \Delta} \tag{5.4}$$

and

$$LLI = L(1,\chi)\, c_1 \log\log \Delta \tag{5.5}$$

If (5.3) is true, then as Δ increases, we would expect that extreme values of the ULI and LLI would tend to approach 1.

In fact, Chowla [Cho49] has shown that for any positive $\epsilon < 1$,

$$ULI > \frac{1-\epsilon}{2} \quad \text{and} \quad LLI < 2(1-\epsilon)$$

hold, each for an infinite sequence of values of Δ. Furthermore, Joshi [Jos70] showed that if c and d are relatively prime positive integers and $8 \mid d$, then as Δ runs through prime values congruent to $c \pmod d$, we have

$$ULI > \frac{1-\epsilon}{2} \prod_{p \mid d} \frac{1-1/p}{1-\left(\frac{p}{c}\right) 1/p}$$

and

$$LLI < 2(1-\epsilon) \prod_{p \mid d} \frac{1-1/p}{1-\left(\frac{p}{c}\right) 1/p}$$

infinitely often. Thus, if Δ is a prime and $\Delta \equiv 5 \pmod 8$, we would have

$$LLI < (4/3)(1-\epsilon)$$

infinitely often. Also, if Δ is a prime and $\Delta \equiv 1 \pmod 8$, we would have

$$ULI > (1/2)(1-\epsilon)$$

infinitely often. Assuming that the size of $L(1,\chi)$ and h are independent, this result (together with the Cohen-Lenstra Heuristics) suggests that we would have

$$R > (1-\epsilon)(c_2/4)\sqrt{\Delta}\log\log\Delta \tag{5.6}$$

infinitely often. In Figure 5.1 below we have plotted the frequency distribution of the values of

$$Z = \frac{R}{\sqrt{\Delta}\log\log\Delta}$$

for all prime values of $\Delta \equiv 1 \pmod 8$, where $8 \times 10^8 < \Delta < 10^9$. The vertical line on this figure intersects the Z axis at $c_2/4$. Notice that there is a small but not insignificant portion of the frequency distribution which is to the right of this line. The results of [Jos70] are not as good as the extreme values suggested by the truth of the ERH, and Figure 5.1 provides some evidence that a better result than (5.6) might hold; thus, it is of some interest to conduct a numerical investigation into how large (small) the ULI (LLI) values can be.

Shanks tested (5.3) by attempting to produce values of Δ for which he might have locally extreme values for the LLI and ULI. For example, if $\Delta \equiv 5 \pmod 8$ and $(\Delta/q) = -1$ for all of the small primes q less than some bound p, then we would expect by (5.2) that $L(1,\chi)$ would be small. On the other hand, if $\Delta/4 \equiv 7 \pmod 8$ and $(\Delta/q) = 1$ for all the primes $q \leq p$, then we would expect $L(1,\chi)$ to be large. Shanks made use of Lehmer's numerical sieving device, the DLS-157, to find such special values of Δ. He found no ULI larger than 1; in fact, the largest ULI that he found was 0.7333. Also, he found only a few LLI's less than 1 (these occurred for small values of Δ only). The values of the LLI's tended to remain stable on average, or change very slowly; whereas the ULI's tended to increase very slowly for these special Δ values; thus, these numerical trials lend support to (5.3).

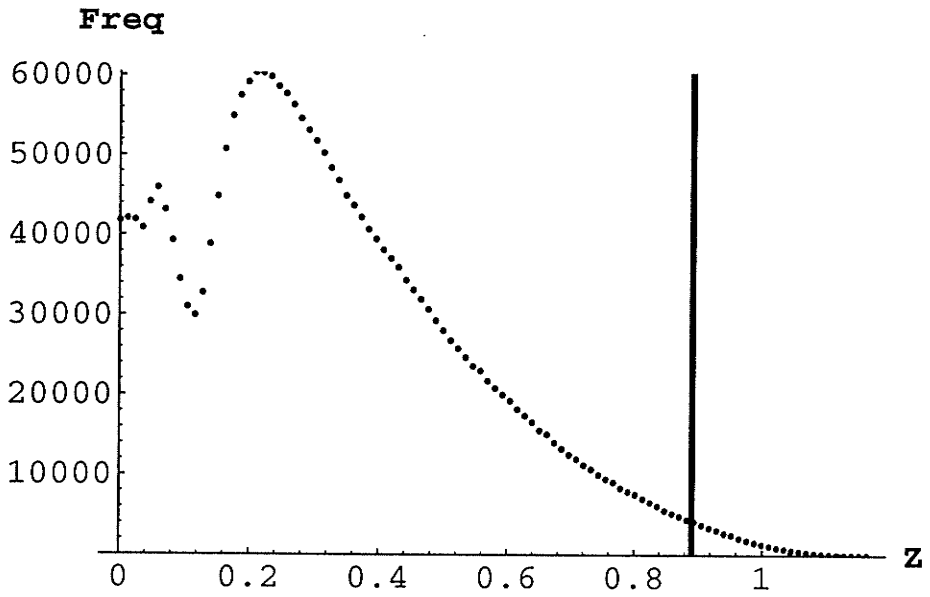

Figure 5.1: Frequency values of Z for $\Delta = p$ (prime), $8 \times 10^8 < p < 10^9$, $p \equiv 1 \pmod 8$

5.2 Numerical Experiments

We used a new sieving device, the MSSU, to extend Shanks' computations. As this instrument has been described in some detail elsewhere (see Lukes, Patterson and Williams [LPW], [LPW95] and Lukes [Luk95]), we will only mention here that it conducts its search for the kind of numbers that we sought at the rate of over 4×10^{12} per second, a considerably faster search rate than that of the DLS-157. For $D \equiv 5 \pmod 8$, we found all values of D such that $0 < D < 10^{19}$ and $(D/q) = -1$ for $q = 3, 5, 7, \ldots, 199$. For $D \equiv 1 \pmod 8$ we found all the values of D such that $0 < D < 4 \times 10^{19}$ and $(D/q) = 1$ for $q = 3, 5, 7, \ldots, 199$ and for $D \equiv 6 \pmod 8$ and $D \equiv -1 \pmod 4$ we found all the values of D such that $0 < D < 10^{19}$ and $(D/q) = 1$ for $q = 3, 5, 7, \ldots, 199$. We evaluated the class number, regulator, and $L(1, \chi)$ for each of the several thousand numbers that resulted by using the Shanks heuristic [MW92, p.283]. We then selected the "$L(1, \chi)$-lochamps" and "LLI-lochamps" from the values of $D \equiv 5 \pmod 8$, namely those D with the property that their corresponding $L(1, \chi)$ value (or LLI value) is less than that of any smaller D. From each of the other sets of D values we selected the "$L(1, \chi)$-hichamps" and "ULI-hichamps," those D with the property that their corresponding $L(1, \chi)$ value (or ULI value) is greater than that of any smaller D in the same set. For these D with the most extreme $L(1, \chi)$, LLI, and ULI values we computed h, R, and $L(1, \chi)$ using the techniques of Chapter 3. In every case the results were the same as those produced by the Shanks heuristic.

Since the techniques of Chapter 3 for computing h require the truth of the ERH, the fact that both these techniques and the Shanks heuristic give the same results increases our confidence that the computed values are correct, even if the ERH is false. Also, the Shanks heuristic is much faster than the method of Chapter 3, so it provided us with a relatively quick way to examine all the numbers produced by the sieve. Even if the class numbers computed by the Shanks heuristic are wrong, they will still be very close to the actual value, and their corresponding $L(1, \chi)$ values will be quite accurate. At any rate,

we would only expect the Shanks heuristic to give erroneous results for very large class numbers which, by the Cohen-Lenstra heuristics [CL83], are extremely rare.

Table 5.1 contains the $L(1,\chi)$-lochamps for $D \equiv 5 \pmod 8$ and Table 5.2 contains the LLI-lochamps. Tables 5.3, 5.5, and 5.7 contain the $L(1,\chi)$-hichamps for $D \equiv 1 \pmod 8$, $D \equiv 6 \pmod 8$, and $D \equiv -1 \pmod 4$ respectively and Tables 5.4, 5.6, and 5.8 contain the ULI-hichamps. The largest ULI we found is $ULI = 0.741429825\ldots$ ($L(1,\chi) = 4.98741315\ldots$, $h = 2$) for

$$D = 2323617473234474719.$$

The least LLI we found is $LLI = 1.24745080\ldots$ ($L(1,\chi) = 0.158960540\ldots$, $h = 4$) for

$$D = 18974003020179917.$$

D	R	h	$L(1,\chi)$	LLI
370095509388197	794079.6472497177	2	0.165107631	1.25601176
16710980998953317	5296924.2425040266	2	0.163901444	1.28502009
18974003020179917	2737025.3979827850	4	0.158960540	1.24745080
587108439330001613	30377994.3008864805	2	0.158584203	1.27458613
2430946649400343037	30781378.0110772471	4	0.157939344	1.28107906
3512773592849667053	146959147.1762363224	1	0.156820032	1.27494032
4927390995446922917	86988957.8224337937	2	0.156752908	1.27707402

Table 5.1: $D \equiv 5 \pmod 8$ — $L(1,\chi)$-lochamps

D	R	h	$L(1,\chi)$	LLI
370095509388197	794079.6472497177	2	0.165107631	1.25601176
18974003020179917	2737025.3979827850	4	0.158960540	1.24745080

Table 5.2: $D \equiv 5 \pmod 8$ — LLI-lochamps

D	R	h	$L(1,\chi)$	ULI
6450045516630769	90756597.6965676137	4	9.04038245	0.706023128
11641399247947921	491322389.3502864803	1	9.10739051	0.708086652
30819994040589121	807859472.4921805586	1	9.20342636	0.710441965
76885196535776281	1282736248.6860863457	1	9.25222102	0.709566435
116307279575913409	1603698785.2191524967	1	9.40479529	0.719187024
309361186961076121	659373276.4916228329	4	9.48393166	0.720412930
593648033453064769	3654584697.9672249203	1	9.48644537	0.717487068
837534463612755841	289454213.0306511549	15	9.48854860	0.716030574
986170795371327721	4740842625.4498078954	1	9.54793526	0.719747677
1289728952842378129	2716207893.5494826876	2	9.56695593	0.719933418
1378346290984666249	1404229020.6952799891	4	9.56860793	0.719750528
1625302739833637089	1220590093.7364507665	5	9.57420466	0.719412391
2001773756832589609	564658107.7859120341	12	9.57831938	0.718768069
2305984263805598401	7377563911.9100995120	1	9.71661078	0.728492958
6476334166896360649	1245808525.9986525809	10	9.79076596	0.729352585
10329119652469596889	2623785779.2277717348	6	9.79665842	0.727721514
11917728321713151001	4247532486.6139021970	4	9.84305599	0.730537438
38867746006848704401	15362673061.6274488366	2	9.85671277	0.726450543

Table 5.3: $D \equiv 1 \pmod 8$ — $L(1,\chi)$-hichamps

D	R	h	$L(1,\chi)$	ULI
6450045516630769	90756597.6965676137	4	9.04038245	0.706023128
11641399247947921	491322389.3502864803	1	9.10739051	0.708086652
30819994040589121	807859472.4921805586	1	9.20342636	0.710441965
116307279575913409	1603698785.2191524967	1	9.40479529	0.719187024
309361186961076121	659373276.4916228329	4	9.48393166	0.720412930
2305984263805598401	7377563911.9100995120	1	9.71661078	0.728492958
6476334166896360649	1245808525.9986525809	10	9.79076596	0.729352585
11917728321713151001	4247532486.6139021970	4	9.84305599	0.730537438

Table 5.4: $D \equiv 1 \pmod 8$ — ULI-hichamps

D	R	h	$L(1,\chi)$	ULI
8265289127640406	410994766.1996174020	1	4.52071643	0.697582853
9442925344429966	457439232.0709417274	1	4.70738946	0.725690793
18743664182538766	161745705.1813451513	4	4.72569296	0.724968902
30814780209680086	207679715.9624258895	4	4.73232469	0.723473149
62414818040620774	1187337674.0593696079	1	4.75259048	0.723071482
129717075149592694	431223881.0852231480	4	4.78921375	0.725087667
134132998967004766	73116855.2567294857	24	4.79138345	0.725255725
164913261020266126	1958556197.5128538633	1	4.82289989	0.729034169
306611208916703926	446668848.1319415496	6	4.83997258	0.728671899
382903329914535886	188017733.9645143813	16	4.86154405	0.730876784
574911115184562766	3718539673.4666251606	1	4.90424396	0.735394142
1730279630321324086	6453073222.6040767436	1	4.90578426	0.730605175
2103720936842562766	7123705342.1971433290	1	4.91147437	0.730581571
2249618179698381886	744815083.7612317213	10	4.96585525	0.738369948

Table 5.5: $D \equiv 6 \pmod 8$ — $L(1,\chi)$-hichamps

D	R	h	$L(1,\chi)$	ULI
8265289127640406	410994766.1996174020	1	4.52071643	0.697582853
9442925344429966	457439232.0709417274	1	4.70738946	0.725690793
164913261020266126	1958556197.5128538633	1	4.82289989	0.729034169
382903329914535886	188017733.9645143813	16	4.86154405	0.730876784
574911115184562766	3718539673.4666251606	1	4.90424396	0.735394142
2249618179698381886	744815083.7612317213	10	4.96585525	0.738369948

Table 5.6: $D \equiv 6 \pmod 8$ — ULI-hichamps

D	R	h	$L(1,\chi)$	ULI
2871159201832639	246120736.6299490883	1	4.59324455	0.714308970
5851505127988699	177728821.6530873557	2	4.64680087	0.718840689
9591413800044619	455208963.5698300412	1	4.64803608	0.716460487
11343192346627639	126443772.9651967759	4	4.74886462	0.731122630
20602619993714851	170879672.4976781991	4	4.76199755	0.730053523
51094523613269371	53964999.0328392756	20	4.77479787	0.727437404
95881886945811019	185704022.4558378132	8	4.79780962	0.727848754
108273250869863179	263663061.5874190707	6	4.80772870	0.728763306
134428259280597811	442693041.8869178770	4	4.82966935	0.731040320
170308074259332571	62365910.9078004024	32	4.83592580	0.730848871
370695282126782419	1483547793.6632413161	2	4.87329843	0.732795816
686289874744590691	4066647990.4097152107	1	4.90888418	0.735269175
1548668327679299479	3055545592.8796488176	2	4.91065649	0.731827607
1794918979479064651	3292752562.7077233152	2	4.91548830	0.731886310
2323617473234474719	3801260801.6072624237	2	4.98741315	0.741429825
4100575042219601191	5055383165.1321981459	2	4.99300144	0.739729838
7461358178243390719	1705289936.4645851663	8	4.99435342	0.737315480
9182479206058844911	3789554588.5732193340	4	5.00228212	0.737590379

Table 5.7: $D \equiv -1 \pmod 4$ — $L(1,\chi)$-hichamps

D	R	h	$L(1,\chi)$	ULI
2871159201832639	246120736.6299490883	1	4.59324455	0.714308970
5851505127988699	177728821.6530873557	2	4.64680087	0.718840689
11343192346627639	126443772.9651967759	4	4.74886462	0.731122630
370695282126782419	1483547793.6632413161	2	4.87329843	0.732795816
686289874744590691	4066647990.4097152107	1	4.90888418	0.735269175
2323617473234474719	3801260801.6072624237	2	4.98741315	0.741429825

Table 5.8: $D \equiv -1 \pmod 4$ — ULI-hichamps

Following Shanks we define the symbols aR_p (aN_p) to represent the least integers congruent to a modulo 8 such that

$$\left(\frac{aR_p}{q}\right) = 1, \qquad \left(\frac{aN_p}{q}\right) = -1$$

for all odd primes $q \leq p$. We provide tables of aR_p for $a = 1$ (the positive psuedosquares from [LPW]), $a = 6$, $a = 3$ and 7, and aN_p for $a = 5$ and also similar tables of aR_p and aN_p when we added the extra constraint that aR_p and aN_p be prime, together with the ULI and LLI values. Figure 5.2 shows the LLI values plotted for the $5N_p$ least solutions. The horizontal line is at $LLI = 4/3$. Figures 5.3, 5.4, and 5.5 show the $1 - ULI$ values plotted for the $1R_p$ least solutions, the $6R_p$ least solutions and $3R_p$ and $7R_p$ combined least solutions respectively. Notice that the tendency for the ULI's is to very slowly increase and for the LLI's is to remain stable with minor fluctuations about 4/3. Thus, the results that we have obtained completely support Shanks' earlier findings and therefore support the truth of (5.3). At least, we have not found anything that would lead us to believe that the ERH has been violated.

p	N_p	R	h	$L(1,\chi)$	LLI
3	5	0.48121	1	0.430408	0.44355
5	53	1.96572	1	0.540024	1.61246
7,11	173	2.57081	1	0.390910	1.38799
13	293	2.83665	1	0.331438	1.24669
17	437	3.04224	1	0.291060	1.13768
19,23	9173	12.47223	1	0.260446	1.24696
29	24653	5.05628	4	0.257624	1.29084
31,37,41	74093	7.21597	5	0.265098	1.38758
43	170957	16.93918	3	0.245810	1.32491
47,53,59	214037	28.95367	2	0.250333	1.35931
61	2004917	48.29722	3	0.204656	1.18549
67	44401013	352.50783	2	0.211608	1.31442
71	71148173	140.53952	6	0.199939	1.25337
73,79	154554077	694.91315	2	0.223588	1.42197
83,89,97	163520117	152.13679	9	0.214151	1.36334
101,103	261153653	512.32723	3	0.190217	1.22104
107,109,113	1728061733	4021.14004	1	0.193463	1.28086
127	9447241877	1252.37753	7	0.180389	1.22431
131	19553206613	6209.50558	2	0.177626	1.21755
137,139	49107823133	18804.68086	1	0.169715	1.17733
149,...,163	385995595277	27068.06281	2	0.174271	1.23929
167	13213747959653	330785.26635	1	0.181996	1.34325
173	14506773263237	331149.00619	1	0.173887	1.28456
179,181	57824199003317	165998.45961	4	0.174638	1.30698
191,193	160909740894437	275610.26298	4	0.173817	1.31280
197,199	370095509388197	794079.64724	2	0.165107	1.25601
211	1409029796180597	3130386.68971	1	0.166789	1.28291
223	4075316253649373	5291574.72421	1	0.165780	1.28593
227,229,233	18974003020179917	2737025.39798	4	0.158960	1.24745
239,241	224117990614052477	10257518.45839	4	0.173338	1.38422
251,257,263	637754768063384837	22908547.79705	3	0.172116	1.38410
269,...,283	4472988326827347533	14462868.44192	12	0.164121	1.33631

Table 5.9: $5N_p$ — Least Solutions

p	N_p	R	h	$L(1,\chi)$	LLI
3	5	0.48121	1	0.430408	0.44355
5	53	1.96572	1	0.540024	1.61246
7,11	173	2.57081	1	0.390910	1.38799
13	293	2.83665	1	0.331438	1.24669
17	2477	6.47234	1	0.260093	1.15802
19,23	9173	12.47223	1	0.260446	1.24696
29	61613	36.23370	1	0.291948	1.51764
31,37,41	74093	7.21597	5	0.265098	1.38758
43	170957	16.93918	3	0.245810	1.32491
47	360293	68.23691	1	0.227363	1.25504
53	679733	92.04349	1	0.223282	1.25592
59,61	2004917	48.29722	3	0.204656	1.18549
67	69009533	869.69643	1	0.209383	1.31182
71	138473837	1369.29769	1	0.232725	1.47713
73	237536213	1725.64096	1	0.223931	1.43508
79	384479933	2087.35754	1	0.212907	1.37580
83	883597853	3018.26471	1	0.203076	1.33041
89,...,113	1728061733	4021.14004	1	0.193463	1.28086
127	9447241877	1252.37753	7	0.180389	1.22431
131,137,139	49107823133	18804.68086	1	0.169715	1.17733
149	1843103135837	119080.85359	1	0.175427	1.26915
151,157	4316096218013	192239.83257	1	0.185066	1.35078
163,167	15021875771117	344898.80858	1	0.177975	1.31520
173,179	82409880589277	804942.51462	1	0.177339	1.33146
181	326813126363093	1551603.41110	1	0.171656	1.30445
191,193	390894884910197	1650908.48845	1	0.167002	1.27101
197	1051212848890277	547589.04349	5	0.168892	1.29600
199,211,223	4075316253649373	5291574.72421	1	0.165780	1.28593
227	274457237558283317	45653225.95687	1	0.174286	1.39371
229	443001676907312837	6097479.67224	9	0.164899	1.32287
233	599423482887195557	65388978.22854	1	0.168914	1.35780
239	614530964726833997	64783176.97206	1	0.165280	1.32880
241,...,263	637754768063384837	22908547.79705	3	0.172116	1.38410

Table 5.10: $5N_p$ — Least Prime Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	73	7.66669	1	1.79463	0.345928
5	241	18.77149	1	2.41835	0.398891
7	1009	6.98471	7	3.07844	0.446865
11	2641	90.12298	1	3.50736	0.477001
13	8089	178.22839	1	3.96332	0.506420
17	18001	282.97884	1	4.21828	0.518884
19	53881	541.55812	1	4.66613	0.548483
23	87481	711.16358	1	4.80886	0.555144
29	117049	846.09997	1	4.94615	0.565121
31	515761	1907.45206	1	5.31201	0.578745
37	1083289	2874.30570	1	5.52320	0.589203
41	3206641	1695.17846	3	5.67991	0.589086
43	3818929	5713.82642	1	5.84771	0.603903
47	9257329	9230.38989	1	6.06746	0.613776
53	22000801	2086.08127	7	6.22644	0.618151
59,61	48473881	22267.38552	1	6.39654	0.624945
67	175244281	8755.31433	5	6.61378	0.630779
71,73	427733329	70323.96940	1	6.80059	0.638630
79	898716289	9537.40888	11	6.99909	0.649304
83,89,97	2805544681	19261.83080	10	7.27309	0.662948
101	10310263441	380018.36474	1	7.48513	0.669642
103	23616331489	30603.44175	19	7.56741	0.669469
107,109	85157610409	571883.79118	2	7.83891	0.682242
113,127	196265095009	1724813.51799	1	7.78664	0.670905
131,137,139	2871842842801	7023729.35989	1	8.28929	0.693315
149,151	26250887023729	5468833.11462	4	8.53911	0.698741
157,163,167	112434732901969	45498659.97703	1	8.58179	0.692942
173,179	178936222537081	905318.66551	65	8.79823	0.707517
181,191	696161110209049	29450368.88199	4	8.92947	0.709822
193	2854909648103881	121507633.56511	2	9.09635	0.714897
197,199	6450045516630769	90756597.69656	4	9.04038	0.706023
211,223	11641399247947921	491322389.35028	1	9.10739	0.708086
227	190621428905186449	1011534665.99196	2	9.26733	0.706271
229	196640248121928601	2074591515.46250	1	9.35677	0.712937
233	712624335095093521	263678486.70195	15	9.37056	0.707873
239	1773855791877850321	506310756.67776	12	9.12366	0.685176
241	2327687064124474441	7232768052.87025	1	9.48139	0.710815
251	6384991873059836689	2004168448.13387	6	9.51777	0.709077
257	8019204661305419761	6728169524.19910	2	9.50366	0.707042
263,269,271	10198100582046287689	3783707520.39501	4	9.47868	0.704155

Table 5.11: $1R_p$ — Least Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	73	7.66669	1	1.79463	0.345928
5	241	18.77149	1	2.41835	0.398891
7	1009	6.98471	7	3.07844	0.446865
11	2689	90.34568	1	3.48451	0.473369
13	8089	178.22839	1	3.96332	0.506420
17	33049	395.07371	1	4.34639	0.520911
19	53881	541.55812	1	4.66613	0.548483
23	87481	711.16358	1	4.80886	0.555144
29	483289	1817.65959	1	5.22924	0.570825
31	515761	1907.45206	1	5.31201	0.578745
37	1083289	2874.30570	1	5.52320	0.589203
41,43	3818929	5713.82642	1	5.84771	0.603903
47	9257329	9230.38989	1	6.06746	0.613776
53	22000801	2086.08127	7	6.22644	0.618151
59,61	48473881	22267.38552	1	6.39654	0.624945
67	175244281	8755.31433	5	6.61378	0.630779
71,73	427733329	70323.96940	1	6.80059	0.638630
79	898716289	9537.40888	11	6.99909	0.649304
83	8114538721	331798.46946	1	7.36669	0.661246
89	9176747449	351603.83089	1	7.34072	0.657784
97,101,103	23616331489	30603.44175	19	7.56741	0.669469
107,...,127	196265095009	1724813.51799	1	7.78664	0.670905
131,137,139	2871842842801	7023729.35989	1	8.28929	0.693315
149	26437680473689	21737796.43131	1	8.45539	0.691844
151	89436364375801	13405886.42469	3	8.50530	0.688170
157,163,167	112434732901969	45498659.97703	1	8.58179	0.692942
173,179	178936222537081	905318.66551	65	8.79823	0.707517
181,191,193	6072205049848081	343020804.21265	1	8.80394	0.687875
197,...,223	11641399247947921	491322389.35028	1	9.10739	0.708086
227,229	196640248121928601	2074591515.46250	1	9.35677	0.712937
233	781158046093912369	830497955.18837	5	9.39656	0.709411
239	6938117179828687609	4215890391.93407	3	9.60328	0.715084
241	9064125655411231729	14430633177.92549	1	9.58633	0.712661
251	15559176909429792409	18941964091.64911	1	9.60421	0.711672
257	18539153100230615161	20896666758.05901	1	9.70648	0.718500

Table 5.12: $1R_p$ — Least Prime Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	22	5.97634	1	1.27416	0.477235
5,7	46	10.79281	1	1.59131	0.540989
11	214	27.96084	1	1.91136	0.561896
13	1054	36.44254	2	2.24501	0.594046
17	4174	153.01734	1	2.36845	0.584654
19	5014	86.81137	2	2.45196	0.600339
23	9454	125.42036	2	2.57982	0.615001
29	34654	508.58627	1	2.73204	0.620664
31	166846	1188.82213	1	2.91044	0.629446
37,41	189814	1283.96215	1	2.94705	0.635023
43	2185726	4732.05980	1	3.20075	0.648402
47,53	2237134	4898.78054	1	3.27523	0.663141
59	12020446	5852.61292	2	3.37613	0.659805
61	30628966	18845.36360	1	3.40516	0.653754
67	45735286	23224.68967	1	3.43418	0.654558
71	103345246	36324.19702	1	3.57314	0.671479
73	193438606	12646.28053	4	3.63706	0.676448
79	302673526	15594.73822	4	3.58550	0.662113
83	1399951606	71257.69974	2	3.80895	0.687397
89	1493483566	74632.78430	2	3.86241	0.696403
97	8813799094	370333.79740	1	3.94467	0.694310
101	8932573654	373945.60357	1	3.95658	0.696285
103	11391294814	208190.33992	2	3.90125	0.684412
107,109,113	16692514294	65489.35755	8	4.05508	0.707981
127,131	490184082166	1438149.37446	2	4.10822	0.689976
137,139	771038637814	938914.08768	4	4.27708	0.714941
149,151	1052385901774	443737.18803	10	4.32551	0.720728
157,163	27266351212006	1448975.39844	16	4.43984	0.717189
167	46075643128414	7562458.76640	4	4.45643	0.716550
173	101596847251054	11240507.75375	4	4.46072	0.712388
179	111010920394126	5975308.10095	8	4.53698	0.724024
181,191	186677562227374	10370523.26198	6	4.55413	0.723615
193	2769113411231974	9937273.14521	24	4.53218	0.705005
197	7796793440819254	15101865.90968	27	4.61781	0.712866
199	8265289127640406	410994766.19961	1	4.52071	0.697582
211	9442925344429966	457439232.07094	1	4.70738	0.725690
223	27130689396477286	127224468.66266	6	4.63437	0.709124
227	62414818040620774	1187337674.05936	1	4.75259	0.723071
229	77991421972487566	330118687.39204	4	4.72831	0.718299
233	230816476295404294	1145918413.80384	2	4.77035	0.719509
239,241	574911115184562766	3718539673.46662	1	4.90424	0.735394
251,...,269	1441979855850505414	1410649668.17247	4	4.69893	0.700582

Table 5.13: $6R_p$ — Least Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	22	5.97634	1	1.27416	0.477235
5,7	46	10.79281	1	1.59131	0.540989
11	214	27.96084	1	1.91136	0.561896
13	1486	17.45176	5	2.26360	0.587793
17	4174	153.01734	1	2.36845	0.584654
19	10774	265.96151	1	2.56230	0.607645
23	13126	298.64260	1	2.60666	0.613415
29	34654	508.58627	1	2.73204	0.620664
31	166846	1188.82213	1	2.91044	0.629446
37,41	189814	1283.96215	1	2.94705	0.635023
43	2185726	4732.05980	1	3.20075	0.648402
47,53	2237134	4898.78054	1	3.27523	0.663141
59	25056574	16886.10677	1	3.37340	0.650066
61	30628966	18845.36360	1	3.40516	0.653754
67	45735286	23224.68967	1	3.43418	0.654558
71	103345246	36324.19702	1	3.57314	0.671479
73	548033014	87004.91984	1	3.71655	0.680052
79,83,89	1998450094	55854.72123	3	3.74830	0.673048
97	8813799094	370333.79740	1	3.94467	0.694310
101	8932573654	373945.60357	1	3.95658	0.696285
103,107,109	26026453534	647111.49210	1	4.01117	0.696490
113	31416841054	723672.41556	1	4.08282	0.707314
127	762216630646	3635072.15709	1	4.16364	0.696062
131	1058804919286	4298691.69550	1	4.17761	0.696041
137	1321651385014	4795026.18085	1	4.17092	0.693363
139,149	3499659258286	2635944.01166	3	4.22711	0.695967
151	25070229597526	22138339.93304	1	4.42146	0.714755
157	48888369417694	30359479.49961	1	4.34201	0.697793
163	129143129979406	50279000.91153	1	4.42436	0.705155
167	184022456828926	12173479.56229	5	4.48693	0.713022
173	256397742215806	71809801.11098	1	4.48463	0.710716
179	600206879107606	112267896.30029	1	4.58252	0.721282
181	2457721162815286	224676759.26288	1	4.53202	0.705611
191	4142956695812806	289298680.36845	1	4.49460	0.697063
193,197	7796793440819254	15101865.90968	27	4.61781	0.712866
199	8265289127640406	410994766.19961	1	4.52071	0.697582
211	9442925344429966	457439232.07094	1	4.70738	0.725690
223,227	62414818040620774	1187337674.05936	1	4.75259	0.723071
229	150726700798733614	1854144221.59350	1	4.77582	0.722345
233,239,241	574911115184562766	3718539673.46662	1	4.90424	0.735394
251	2380303014240673006	7394016196.76485	1	4.79252	0.712353
257,263	4693358374126530406	10456361930.77094	1	4.82657	0.714498

Table 5.14: $6R_p$ — Least $2\times$ Prime Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	7	2.76865	1	1.04645	0.488140
5	19	5.82893	1	1.33724	0.512241
7	79	5.07513	3	1.71299	0.549523
11	331	36.25638	1	1.99283	0.567255
13	751	57.94214	1	2.11433	0.570617
17	1171	25.37280	3	2.22439	0.585134
19	5251	89.61570	2	2.47339	0.604359
23	10651	270.87206	1	2.62463	0.622710
29	18379	367.19773	1	2.70856	0.629349
31,37	78439	813.56346	1	2.90486	0.642576
41	399499	1890.86355	1	2.99159	0.631650
43	1234531	3537.86780	1	3.18412	0.653616
47	1394611	1901.10782	2	3.21966	0.659012
53	1427911	3841.39768	1	3.21468	0.657630
59	4355311	6958.99836	1	3.33454	0.665368
61	5715319	8109.80131	1	3.39226	0.673017
67	12807391	6078.51980	2	3.39701	0.663060
71	117678031	38495.70798	1	3.54866	0.665425
73,79	133826599	10617.14453	4	3.67110	0.686912
83	452980999	78083.74919	1	3.66877	0.673261
89,97	505313251	83941.62341	1	3.73419	0.684123
101	5273095699	144314.39229	2	3.97472	0.704318
103,107,109	9248561191	127289.80150	3	3.97079	0.698473
113	38816991931	36197.20051	22	4.04191	0.698450
127	257057640739	1042866.42766	2	4.11380	0.695714
131	348113924239	2445102.46006	1	4.14415	0.698553
137,139	782893951711	66997.96852	56	4.24031	0.708683
149,151,157	963864514519	2107959.76759	2	4.29422	0.716156
163	20044941740191	453137.89102	42	4.25086	0.688557
167	35984570527819	6600795.76612	4	4.40147	0.709247
173,179	46257585588439	30459726.68748	1	4.47852	0.720076
181,191,193	53009903964319	16254586.37321	2	4.46506	0.717062
197	2726829078460579	59344254.16218	4	4.54579	0.707203
199,...,229	2871159201832639	246120736.62994	1	4.59324	0.714308
233	97915624862375191	184534021.41965	8	4.71780	0.715612
239	286657540188128671	249648958.63100	10	4.66281	0.702304
241,...,263	632590969227841471	3833565622.42494	1	4.81993	0.722316
269,...,281	1905834685957869991	3348155946.05282	2	4.85057	0.721956

Table 5.15: $3R_p$ and $7R_p$ — Least Solutions

p	R_p	R	h	$L(1,\chi)$	ULI
3	7	2.76865	1	1.04645	0.488140
5	19	5.82893	1	1.33724	0.512241
7	79	5.07513	3	1.71299	0.549523
11	331	36.25638	1	1.99283	0.567255
13	751	57.94214	1	2.11433	0.570617
17	1171	25.37280	3	2.22439	0.585134
19	7459	73.05341	3	2.53759	0.610832
23	10651	270.87206	1	2.62463	0.622710
29	18379	367.19773	1	2.70856	0.629349
31,37	78439	813.56346	1	2.90486	0.642576
41	399499	1890.86355	1	2.99159	0.631650
43	1234531	3537.86780	1	3.18412	0.653616
47,53	1427911	3841.39768	1	3.21468	0.657630
59	4355311	6958.99836	1	3.33454	0.665368
61	5715319	8109.80131	1	3.39226	0.673017
67	49196359	24407.90384	1	3.47987	0.662406
71	117678031	38495.70798	1	3.54866	0.665425
73	180628639	49263.42426	1	3.66548	0.682492
79,83	452980999	78083.74919	1	3.66877	0.673261
89,97	505313251	83941.62341	1	3.73419	0.684123
101,...,109	9248561191	127289.80150	3	3.97079	0.698473
113	152524816291	6690.84067	239	4.09457	0.696458
113,127,131	348113924239	2445102.46006	1	4.14415	0.698553
137	916716646759	3976755.53799	1	4.15347	0.693040
139	1086257787619	637789.47424	7	4.28360	0.713513
149	4606472154439	707977.15943	13	4.28823	0.704162
151	4726529308939	9447793.54167	1	4.34569	0.713422
157	35032713351619	8533304.31730	3	4.32515	0.697114
163,...,179	46257585588439	30459726.68748	1	4.47852	0.720076
181	251274765020899	23977422.86688	3	4.53784	0.719268
191	316934672172031	81024861.17467	1	4.55127	0.720036
193,...,229	2871159201832639	246120736.62994	1	4.59324	0.714308
233,...,263	632590969227841471	3833565622.42494	1	4.81993	0.722316

Table 5.16: $3R_p$ and $7R_p$ — Least Prime Solutions

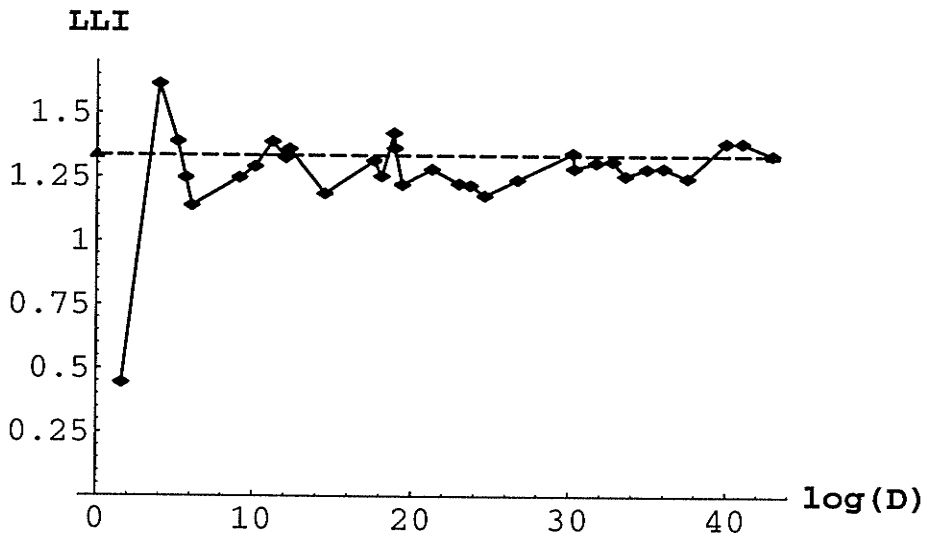

Figure 5.2: $\log 5N_p$ vs. LLI

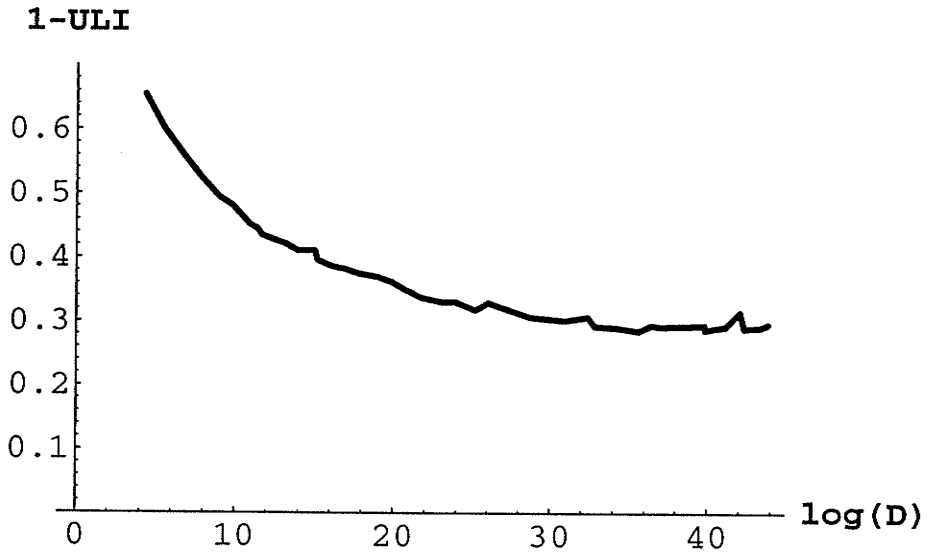

Figure 5.3: $\log 1R_p$ vs. $1 - ULI$

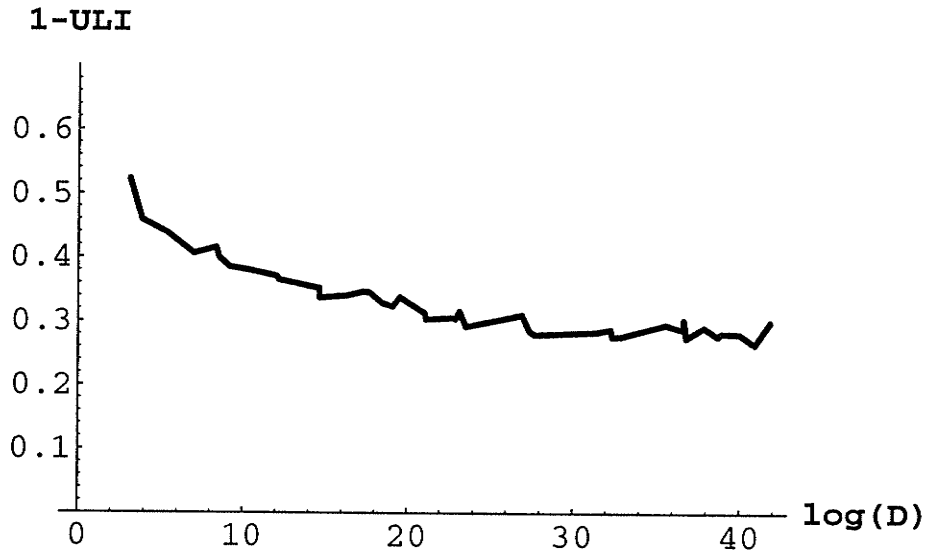

Figure 5.4: $\log 6R_p$ vs. $1 - ULI$

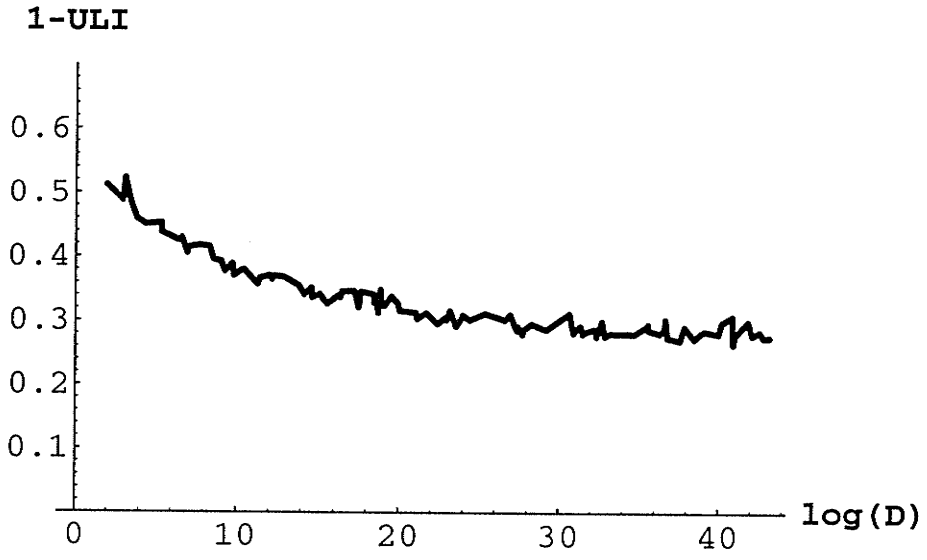

Figure 5.5: $\log 3R_p$ and $\log 7R_p$vs. $1 - ULI$

Although such values of D surely must exist, it seems to be very difficult to produce a value of D with a ULI close to 1. We attempted to do this by finding a D value with a large $L(1,\chi)$ value. We used an unpublished idea of Lehmer which he employed to find the 20 digit value of D with a small $L(1,\chi)$ value that appears in Lehmer, Lehmer, Shanks [LLS70, p. 439]. We examined numbers of the form

$$D = A + BX$$

where

$$B = \prod_{i=j}^{k} p_i,$$

p_i is the i^{th} prime, and $(A/p_i) = 1$ $(i = j, j+1, \ldots, k)$. In our case we used

$$B = 271 \cdot 277 \cdots 313 \approx 5.277 \times 10^{19}$$

and the least nonsquare value of A. We then employed the MSSU to sieve on values of X by using as moduli 8 and primes $p_1, p_2, \ldots, p_m$ with $p_m \leq 269$ such that $A + XB \equiv 6 \pmod 8$ and $((A+XB)/p_i) = 1$, $i = 1, 2, \ldots, m$. Henri Cohen used the technique of [CDyDO93] to evaluate the $L(1,\chi)$ values for some of these D values. The largest ULI occurred for

$$D = 132087087958076030335220262526122432 46,$$

where $L(1,\chi) = 5.324999338\ldots$ $(h = 1)$. This is a large $L(1,\chi)$, but when we evaluate the ULI we only get

$$ULI = 0.669706597\ldots$$

5.3 Conclusion

Elliot [Ell69] has shown that if $\epsilon > 0$ is given, then there exist constants c_3, c_4 (depending on ϵ) and a set $S = S(x)$ for $x \geq 2$, such that for all prime values of $\Delta \leq x$, $\Delta \notin S$, we have

$$\frac{c_3}{\log\log\Delta} \leq L(1,\chi) \leq c_4 \log\log\Delta.$$

Furthermore, S has cardinality at most $O(x^{\epsilon})$. In view of the Cohen-Lenstra heuristics and the numerical evidence presented above, this would seem to permit us to conjecture that there exists an infinite set of values of Δ for which

$$R \gg \frac{\sqrt{\Delta}}{\log\log\Delta}. \tag{5.7}$$

In fact it even appears that there must exist an infinite set of values of Δ such that

$$R \gg \sqrt{\Delta}\log\log\Delta.$$

At present the best result of this type is that of Halter-Koch [HK89] where it is shown that there exists an infinite set of values of Δ such that

$$R \gg (\log\Delta)^4. \tag{5.8}$$

This result is so much worse than (5.7) that it should be possible (without appealing to the ERH or the Gauss Conjecture) to get a better result than (5.8).

Chapter 6

Polynomials With High Densities of Prime Values

Consider the polynomial $f_{41}(x) = x^2 + x + 41$. Euler showed in 1772 that $f_{41}(x)$ is prime for $0 \leq x \leq 39$. To date, no one has found a polynomial of the form $f_A(x) = x^2 + x + A$ that represents distinct primes for more than the first 40 values of x. However, many more polynomials of this form with higher *asymptotic* densities of prime values have been found. An example of this is $f_{27941}(x)$, discovered by Beeger [Bee39] in 1938. If we define $P_A(n)$ as the number of prime values assumed by $f_A(x)$ for $0 \leq x \leq n$, we see that although $P_{27941}(39) = 30 < P_{41}(39)$, we nevertheless have $P_{27941}(1000000) = 286128$ whereas $P_{41}(1000000) = 261080$.

In [Leh37], Lehmer observed that if $f_A(x)$ is to represents primes, then A must be odd. Also,

$$4f_A(x) = (2x + 1)^2 - D,$$

where $D = 1 - 4A$. Thus, if q is an odd prime and the Legendre symbol $(D/q) = 1$, then there must exist some x such that $0 \leq x < q$ and $q \mid f_A(x)$. Values of D such that $(D/q) = -1$ for many values of q, particularly the small values, should therefore force the

corresponding polynomial $f_A(x)$ to take on many prime values, since these values of q are eliminated as possible divisors of $f_A(x)$. Beeger made use of this strategy in [Bee39]. He computed all positive integers $N < 10^6$, $N \equiv 3 \pmod 8$ such that $(-N/q) = -1$ for $q = 3, 5, 7, \ldots, 43$; the only such numbers are $N = 77683, 1117683, 289963$. Poletti [Pol39] computed tables of $P_A(n)$ for the corresponding values of A (19421, 27941, and 72491) and various values of n up to 11000. He discovered that f_{27941} and f_{72491} seem to have higher asymptotic densities of prime values than $f_{41}(x)$. For example, he found that $P_{41}(11000) = 4605$, whereas $P_{27941}(11000) = 4819$ and $P_{72491}(11000) = 4923$.

6.1 The Conjecture of Hardy and Littlewood

Hardy and Littlewood's Conjecture F [HL23] is a result concerning the number of prime values assumed by the quadratic polynomial $f(x) = ax^2 + bx + c$. If we denote by $\pi_f(n)$ the number of prime values assumed by $f(x)$ for $x = 0, 1, \ldots, n$, then their conjecture can be given in the form below.

Conjecture 6.1 (F) *Let $a > 0, b, c$ be integers such that $\gcd(a, b, c) = 1$, $d = b^2 - 4ac$ is not a square and $a + b$, c are not both even. Then there are infinitely many primes of the form $f(n)$ and*

$$\pi_f(n) \sim \varepsilon C_f Li(n),$$

where

$$Li(n) = \int_2^n \frac{dx}{\log x},$$

$$\varepsilon = \begin{cases} \frac{1}{2} & \text{when } 2 \nmid a + b, \\ 1 & \text{otherwise,} \end{cases}$$

and

$$C_f = \prod_{\substack{p>2 \\ p \mid (a,b)}} \frac{p}{p-1} \prod_{\substack{p>2 \\ p \nmid a}} \left(1 - \frac{\left(\frac{d}{p}\right)}{p-1}\right).$$

The products in the expression for C_f are taken over the primes only, and (d/p) denotes the Legendre symbol. Note here that εC_f is what really determines the density of prime values assumed by f, since $Li(n)$ is a function of n only.

We can derive a special version of Conjecture F which applies to $f_A(x)$:

$$P_A(n) \sim C(D)L_A(n),$$

where

$$L_A(n) = 2\int_0^n \frac{dx}{\log f_A(x)},$$

and

$$C(D) = \prod_{p\geq 3} 1 - \frac{\left(\frac{D}{p}\right)}{p-1}. \tag{6.1}$$

Here $D = 1 - 4A$. For example, when $A = 41$, we have $C(-163) = 3.3197732$, whereas Beeger's polynomials f_{27941} and f_{72491} have corresponding $C(D)$ values $C(-111763) = 3.6319998$ and $C(-289963) = 3.6947081$. These numerical values for $C(D)$ tend to confirm Poletti's observation of the superiority of Beeger's polynomials to $f_{41}(x)$ in generating primes. In fact, it seems that Conjecture F provides us with a very accurate predictor of prime densities of quadratic polynomials; the polynomials f_A corresponding to the values of D with large $C(D)$ values will have high densities of prime values. By examining (6.1), we note that the strategy for selecting values of A employed by Beeger and Lehmer has the effect of maximizing the first several terms in the infinite product $C(D)$, so we expect that these polynomials will have especially large $C(D)$ values, and therefore high asymptotic densities of prime values. Table 6.1 contains some values of D taken from Fung and Williams [FW90] and the corresponding values for $P_A(10^6)$, $C(D)$, and $P_A(10^6)/L_A(10^6)$. Note that the actual values of $P_A(10^6)/L_A(10^6)$ are quite close to those of the corresponding $C(D)$, as we would suspect if Conjecture F holds.

D	$P_A(10^6)$	$C(D)$	$P/L_A(10^6)$
-163	261080	3.3197732	3.3203421
-88507	272102	3.4643422	3.4612190
-111763	286128	3.6319998	3.6396821
-222643	293169	3.7289570	3.7293962
-1333963	300001	3.8123997	3.8169182
-9471067	312436	3.9760501	3.9764927
-10560643	315542	4.0194873	4.0161335
-60408307	318250	4.0501092	4.0531570
-171583003	320126	4.0815068	4.0796515
-269497867	322488	4.1092157	4.1112637
-398158363	325782	4.1579113	4.1548155
-643338763	335224	4.2716019	4.2775772
-1408126003	334712	4.2771747	4.2759778
-1595514187	341572	4.3616794	4.3645752
-4067175907	346057	4.4324788	4.4309683
-71837718283	354875	4.6097143	4.6090901
-85702502803	361841	4.7073044	4.7067227
-16501779755323	326605	4.7524812	4.7559512
-30059924764123	326392	4.8379057	4.8453809
-37221595794667	325086	4.8634109	4.8594354
-74210430269347	323289	4.9548401	4.9413604
-110587910656507	321488	4.9711959	4.9770300
-531497118115723	312975	5.0870883	5.0894316
-2068660612674307	300923	5.0978921	5.0976398

Table 6.1: $P_A(10^6)/L_A(10^6)$ for some values of D

6.2 Evaluation of $C(D)$

Evaluating $C(D)$ is a difficult task, since the product in (6.1) converges very slowly. Shanks [Sha60, Sha63, Sha75] has developed efficient methods for evaluating $C(D)$ to high levels of accuracy for $D < 0$. These methods all require that the function $L(s,\chi)$ be computed for various values of s. If h is the class number of $\mathbb{Q}(\sqrt{D})$, then the value of $L(s,\chi)$ can be determined fairly rapidly if the values of h Epstein zeta functions are

known. Shanks [Sha75] showed how to evaluate these Epstein zeta functions to high accuracy rapidly; therefore one can accurately determine $C(D)$ using this method. If h is large, as is often the case with large values of D, this method can be quite slow. However, it is unconditional and is the best method known for evaluating $C(D)$ to great accuracy.

Since it was necessary for us to evaluate $C(D)$ for many large values of D, some of which were positive, we decided to use a different method. We used the ideas presented in [FW90] to evaluate $C(D)$ to eight significant figures. We first note that using an idea of [Sha60] we can show that

$$\frac{C(D)L(1,\chi)L(2,\chi)}{\zeta(4)} = c \prod_{\substack{p \mid D \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right), \tag{6.2}$$

where

$$c = \begin{cases} \frac{5}{2} & \text{when } D \equiv 1 \pmod 8, \\ \frac{1}{2} & \text{when } D \equiv 5 \pmod 8, \\ \frac{15}{16} & \text{otherwise,} \end{cases}$$

$\zeta(4) = \pi^4/90$, and the second product on the right is taken over all primes q such that the Legendre symbol $(D/q) = 1$. Recall the analytic class number formula for imaginary quadratic fields from Section 2.6:

$$L(1,\chi) = \frac{2\pi h}{w\sqrt{|\Delta|}} \tag{6.3}$$

Thus, for $D < -3$ we have

$$C(D) = \frac{c\pi^3\sqrt{|\Delta|}}{90h} \cdot \frac{1}{L(2,\chi)} \prod_{\substack{p \mid D \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right). \tag{6.4}$$

Similarly, the analytic class number formula for real quadratic fields is

$$L(1,\chi) = \frac{2hR}{\sqrt{\Delta}}$$

so for $D > 0$ we have

$$C(D) = \frac{c\pi^4\sqrt{\Delta}}{180Rh} \cdot \frac{1}{L(2,\chi)} \prod_{\substack{p \mid D \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right). \tag{6.5}$$

The evaluation of h for $D > 0$ was discussed in Chapter 3 and we give a brief outline in Section 6.3 on how to determine h for $D < 0$. Thus, the only remaining problem is to estimate

$$F = \frac{1}{L(2,\chi)} \cdot \prod_{q \geq 3} \left(1 - \frac{2}{q(q-1)^2}\right) \tag{6.6}$$

to sufficient accuracy so that (6.4) and (6.5) approximate $C(D)$ to eight significant figures.

We compute an estimate of (6.6) using truncated Euler products. The function F converges much faster than $L(1,\chi)$, so it is not as important to use methods like Bach's averaging techniques. For a fixed Q, we define

$$F_1(Q) = \prod_{p \leq Q} \frac{p^2}{p^2 - \left(\frac{D}{p}\right)},$$

$$T_1(Q) = \prod_{p > Q} \frac{p^2}{p^2 - \left(\frac{D}{p}\right)},$$

and

$$F_2(Q) = \prod_{3 \leq p \leq Q} \left(1 - \frac{2}{q(q-1)^2}\right),$$

$$T_2(Q) = \prod_{p > Q} \left(1 - \frac{2}{q(q-1)^2}\right).$$

Thus, $F_2(Q)/F_1(Q)$ estimates (6.6) with error $T_2(Q)/T_1(Q)$. It is easy to show that if $Q > 10$,

$$|\log T_1(Q)| + |\log T_2(Q)| \leq \sum_{p > Q} \frac{1}{p^2} + \delta_1,$$

where $|\delta_1| < 2/Q^2$. If we set

$$B(Q) = \log|D| \left(\frac{1}{\pi \log Q} + \frac{5.3}{(\log Q)^2}\right) + \frac{4}{\log Q} + \frac{1}{\pi},$$

then by using the method of Cornell and Washington [CW85], we get

$$|\log T_1(Q)| + |\log T_2(Q)| < B(Q) \left(\frac{8 + 13 \log Q}{9Q^{3/2}}\right) + \frac{2}{Q^2} = b. \tag{6.7}$$

Now, if $b < \log((1 + \sqrt{1 + 4k})/2)$ where $k = 10^{1-r}/2$, then

$$C(D) = \frac{c\pi^3 \sqrt{|\Delta|}}{90h} \frac{F_2(Q)}{F_1(Q)} \prod_{\substack{p \mid D \\ p \text{ odd}}} \left(1 - \frac{1}{p^4}\right) \tag{6.8}$$

when $\Delta < 0$ and

$$C(D) = \frac{c\pi^4\sqrt{\Delta}}{180Rh}\frac{F_2(Q)}{F_1(Q)}\prod_{\substack{p \mid D \\ p \text{ odd}}}\left(1 - \frac{1}{p^4}\right) \tag{6.9}$$

when $\Delta > 0$ both approximate $C(D)$ to r significant figures. The D values we planned to examine were all less than 2×10^{19} in absolute value, so by (6.7) we have that $Q = 1.2\times10^6$ will yield approximations of $C(D)$ correct to eight figures. Note that the proof of the inequality in (6.7) requires the truth of the ERH, so the accuracy of the approximations (6.8) and (6.9) is contingent on the ERH as well.

6.3 Computing h in Imaginary Quadratic Fields

In the cases where $D > 0$, we can use the techniques of Chapter 3 to evaluate R and h, but a different method is required when $D < 0$. Fortunately the situation in imaginary quadratic fields is somewhat less difficult than that of real quadratic fields. We will give here a brief outline of the algorithm which executes in at most $O\left(D^{1/5+\epsilon}\right)$ operations that we used to compute h. This is basically a simple modification of the baby step-giant step method of Shanks [Sha71].

As in the case of real quadratic fields, our first step was to compute an estimate $S(Q,\Delta)$ of $\log L\,(1,\chi)$ for some fixed value of Q. We used the averaging procedure of Bach, Algorithm 3.1, which has error bounded by $A(Q,|\Delta|)$ in order to get the best accuracy possible. We used the analytic class number formula (6.3) to compute an estimate $\tilde{h}$ of h by setting

$$F = \frac{\sqrt{|\Delta|}\exp\left(S(Q,\Delta)\right)}{\pi}$$

and computing

$$\tilde{h} = \mathrm{Ne}\,(F)\,, \tag{6.10}$$

where by $\mathrm{Ne}\,(F)$ we mean the nearest integer to F. If $\tilde{h} > 3$, we attempted to find a divisor h_1 of h. Otherwise, we set $h_1 = 1$ and proceeded directly to the next part of the algorithm.

Algorithm 6.1 (Divisor of h for $\mathbb{Q}(\sqrt{-D})$)

INPUT: $\tilde{h}, max$
OUTPUT: h_1, such that $h_1 \mid h$

1. Set $h_1 = 1$, $k = |\Delta|^{1/5} + 1$
2. Set $\mathfrak{a} = (P, Q)$ where $Q = rp$ for some prime p such that $(\frac{D}{p}) = 1$ and $P \equiv x \pmod{p}$, $P \equiv r - 1 \pmod{r}$ where $x^2 \equiv D \pmod{p}$.
3. Compute a list $\mathcal{T}$ of reduced ideals $\mathfrak{a}^i$ for $0 \leq i < k$.
4. Set $q = 0$ and compute $\mathfrak{b} = \mathfrak{a}^{\tilde{h}}$.
5. If $\mathfrak{b} = \mathfrak{a}^i \in \mathcal{T}$, go to 7.
6. Set $q = q + 1$ and compute $\mathfrak{b} = \mathfrak{b} * \mathfrak{a}^k$. Go to 5.
7. Set $m = \tilde{h} + qk - i$. Determine e, the smallest divisor of m such that $\mathfrak{a}^e \sim (1)$.
8. Set $h_1 = \mathrm{LCM}(h_1, e)$. If $h_1 > |\Delta|^{2/5}$ or we have used more than max ideals, terminate. Otherwise, select a new value of p such that $(\frac{D}{p}) = 1$ and go to 2.

End of Algorithm

Since the class numbers of imaginary quadratic fields are generally much larger than those of real quadratic fields, it is important to find as large a divisor of the class number as we can. The method we used, Algorithm 6.1, is as follows. We selected an ideal $\mathfrak{a}$ at random as in Section 3.3 and computed its order in the class group, the least integer e such that $\mathfrak{a}^e \sim (1)$. We first set $k = |\Delta|^{1/5} + 1$ and computed a list $\mathcal{T}$ of the reduced ideals $\mathfrak{a}^i$, for $0 \leq i < k$, along with their corresponding values of i, ordered by the Q values of the ideals. As in Chapter 3 we used a hash table here so that access times were as fast as possible. We determined which integer q gives us $\mathfrak{a}^{\tilde{h}} * \mathfrak{a}^{qk} \sim \mathfrak{b}_i$ for some $\mathfrak{b}_i \in \mathcal{T}$. Then, we have $m = \tilde{h} + qk - i$ is a multiple of e. The actual value of e is the smallest factor of m such that $\mathfrak{a}^e \sim (1)$. We then set $h_1 = e$. If $h_1 < |\Delta|^{2/5}$, then we selected another ideal $\mathfrak{a}_2$ and computed the order of the subgroup generated by $\mathfrak{a}$ and $\mathfrak{a}_2$. We continued selecting ideals until we got a sufficiently large value of h_1. As in the real case, the class group is most often cyclic or close to it (see [CL83]), so we usually found a sufficiently large h_1

Algorithm 6.2 (Class Number of $\mathbb{Q}(\sqrt{-D})$)

INPUT: D and Δ, the radicand and discriminant of an imaginary quadratic field
OUTPUT: h

1. Put $Q = 5000$. Compute $S(Q, \Delta)$ using Algorithm 3.1, and h_1 using Algorithm 6.1.
2. Compute $F = \sqrt{|\Delta|}\exp(S(Q, \Delta))/(\pi h_1)$
3. $\tilde{h} = \mathrm{Ne}(F)$, $\kappa = F - \tilde{h}$
4. $B_1 = F\exp(A(Q, |\Delta|))$, $B_2 = |\kappa| + B_1 - F$
5. If $\tilde{h} - B_2 - [B_2 + \tilde{h}] > -1$, then $h = h_1[B_2 + \tilde{h}]$ and the algorithm terminates.
6. Otherwise, set $Q \leftarrow Q + 5000$, recompute $S(Q, \Delta)$, and go to 2.

End of Algorithm

quite rapidly. However, in the rare cases where we do not, we give up after trying a fixed number of ideals and take as h_1 the order of the largest subgroup we were able to find.

Once we have computed h_1, we can compute h using a modification of the idea of Lenstra [Len82]. If, for a fixed Q we put

$$B_1 = \frac{\sqrt{|\Delta|}\exp\left(S(Q, \Delta) + A(Q, |\Delta|)\right)}{\pi},$$

$$\kappa = F - \tilde{h},$$

and

$$B_2 = |\kappa| + B_1 - F,$$

then from (6.3), and since $|\log L(1, \chi) - S(Q, \Delta)| \leq A(Q, |\Delta|)$, we have

$$h \leq B_1,$$

and

$$|\tilde{h} - h| < B_2. \tag{6.11}$$

Thus, if

$$\frac{\tilde{h}}{h_1} - \frac{B_2}{h_1} - \left[\frac{B_2}{h_1} + \frac{\tilde{h}}{h_1}\right] > -1 \tag{6.12}$$

then $h_2 = [B_2/h_1 + \tilde{h}/h_1]$ is the only integer in the interval I given by

$$\frac{\tilde{h}}{h_1} - \frac{B_2}{h_1} < x \leq \left[\frac{B_2}{h_1} + \frac{\tilde{h}}{h_1}\right].$$

From (6.11) we have

$$\left|\frac{h}{h_1} - \frac{\tilde{h}}{h_1}\right| < \frac{B_2}{h_1},$$

so h/h_1 must be in I. It follows that $h = h_1 h_2$ when (6.12) holds. We sum up these ideas in Algorithm 6.2. Since most of the class groups of $\mathbb{Q}(\sqrt{-D})$ are cyclic or close to it (see Cohen and Lenstra [CL83]) the value of h_1 is usually relatively close to the actual value of h, and this means that this part of the algorithm executes quite rapidly. These aspects of imaginary quadratic fields have been studied elsewhere in great detail (see for example Buell [Bue84]), so we shall not pursue it here any further.

6.4 Numerical Experiments

In order to find values of D for which $C(D)$ is large, we used MSSU (see [Luk95]) to search for all values of D such that $-2\times10^{19} < D < 10^{19}$, $D \equiv 5 \pmod 8$, and $(D/p) = -1$ for all odd primes $q \leq 199$. For the several thousand numbers that resulted, we computed $C(D)$, using the Shanks heuristic [MW92, p.283] to calculate the class numbers when $D > 0$ and the technique of the previous section when $D < 0$. We then selected the $C(D)$-hichamps, $L(1,\chi)$-lochamps, and LLI-lochamps from both the positive values of D and the negative values. Here LLI is the lower Littlewood index defined in Chapter 5. The $C(D)$-hichamps are those values of D with the property that their corresponding $C(D)$ value is greater than that of any D of smaller magnitude. Similarly, the $L(1,\chi)$-lochamps and LLI-lochamps are those values of D with the property that their corresponding $L(1,\chi)$ value (or LLI value) is less than that of any D of smaller magnitude. Since all our values of D have $(D/q) = -1$ for many small primes q, we expect that in addition to giving rise to polynomials with high asymptotic densities of prime values, their $L(1,\chi)$ and LLI values should be small.

We evaluated $C(D)$ correct to 8 figures for all of these values of D with extreme $C(D)$, $L(1,\chi)$, and LLI values by using the techniques described in this chapter. We found no deviations from the results given by the Shanks heuristic. Table 6.2 contains the $C(D)$-hichamps for the negative values of D. Tables 6.4 and 6.5 contain the $L(1,\chi)$-lochamps and LLI-lochamps for the negative D values. Table 6.3 contains the $C(D)$-hichamps for the positive values of D. The $L(1,\chi)$-lochamps and LLI-lochamps for the positive D values are equivalent to Tables 5.1 and 5.2 and can be found in Chapter 5. The largest $C(D)$ value we found is

$$C(-13598858514212472187) = 5.3670819.$$

Thus, if Conjecture F holds, then then polynomial

$$x^2 + x + 3399714628553118047$$

has the largest asymptotic density of prime values for any polynomial of this type currently known. The least $L(1,\chi)$ value we found was

$$L(1,\chi) = 0.153175728\ldots$$

for $D = -13598858514212472187$ and the least LLI we found was

$$LLI = 1.24745080\ldots$$

for $D = 18974003020179917$.

D	$h(D)$	$L(1,\chi)$	$C(D)$
-4311527414591923	3791896	0.181422319	4.5293043
-5513463660887323	4214276	0.178303796	4.6086597
-8842819893041227	5188215	0.173329485	4.7414735
-11779882219755787	5904498	0.170907994	4.8086435
-14363876114143483	6478729	0.169825875	4.8393795
-15326624594334307	6664840	0.169128322	4.8590033
-30462609261723907	9340770	0.168131466	4.8883007
-32779240456803163	9520419	0.165198649	4.9753684
-50792117776428667	11782274	0.164240716	5.0043010
-221328140358231307	24591656	0.164217459	5.0050646
-234391954943494723	24980688	0.162099963	5.0706939
-369885383792662483	31346105	0.161919767	5.0766794
-441899002218793387	33684408	0.159190549	5.1635912
-554395014308976163	37602038	0.158654209	5.1814176
-803608018073876563	45224688	0.158490531	5.1864453
-2038991582966171563	71351592	0.156980541	5.2369507
-2039953459173530587	70825967	0.155787373	5.2765336
-6849319464662435083	128288704	0.153997822	5.3384020
-13598858514212472187	179800672	0.153175728	5.3670819

Table 6.2: $C(D)$-hichamps ($D < 0$)

D	$R(D)$	$h(D)$	$L(1,\chi)$	$C(D)$
370095509388197	794079.6472497177	2	0.165107631	4.9779328
16710980998953317	5296924.2425040266	2	0.163901444	5.0144216
18974003020179917	2737025.3979827850	4	0.158960540	5.1711431
587108439330001613	30377994.3008864805	2	0.158584203	5.1831340
2430946649400343037	30781378.0110772471	4	0.157939344	5.2048129
3512773592849667053	146959147.1762363224	1	0.156820032	5.2422843
4927390995446922917	86988957.8224337937	2	0.156752908	5.2437622

Table 6.3: $C(D)$-hichamps ($D > 0$)

D	$h(D)$	$L(1,\chi)$	LLI
-4311527414591923	3791896	0.181422319	1.40787380
-5513463660887323	4214276	0.178303796	1.38630189
-8842819893041227	5188215	0.173329485	1.35248742
-11779882219755787	5904498	0.170907994	1.33647203
-14363876114143483	6478729	0.169825875	1.32997574
-15326624594334307	6664840	0.169128322	1.32515102
-30462609261723907	9340770	0.168131466	1.32399013
-32779240456803163	9520419	0.165198649	1.30158515
-50792117776428667	11782274	0.164240716	1.29811022
-221328140358231307	24591656	0.164217459	1.31128005
-234391954943494723	24980688	0.162099963	1.29487549
-369885383792662483	31346105	0.161919767	1.29741290
-441899002218793387	33684408	0.159190549	1.27705715
-554395014308976163	37602038	0.158654209	1.27466700
-803608018073876563	45224688	0.158490531	1.27645643
-2038991582966171563	71351592	0.156980541	1.27188721
-2039953459173530587	70825967	0.155787373	1.26222370
-6849319464662435083	128288704	0.153997822	1.25717022
-13598858514212472187	179800672	0.153175728	1.25566335

Table 6.4: $L(1,\chi)$-lochamps ($D < 0$)

D	$h(D)$	$L(1,\chi)$	LLI
-4311527414591923	3791896	0.181422319	1.40787380
-5513463660887323	4214276	0.178303796	1.38630189
-8842819893041227	5188215	0.173329485	1.35248742
-11779882219755787	5904498	0.170907994	1.33647203
-14363876114143483	6478729	0.169825875	1.32997574
-15326624594334307	6664840	0.169128322	1.32515102
-30462609261723907	9340770	0.168131466	1.32399013
-32779240456803163	9520419	0.165198649	1.30158515
-50792117776428667	11782274	0.164240716	1.29811022
-234391954943494723	24980688	0.162099963	1.29487549
-441899002218793387	33684408	0.159190549	1.27705715
-554395014308976163	37602038	0.158654209	1.27466700
-2038991582966171563	71351592	0.156980541	1.27188721
-2039953459173530587	70825967	0.155787373	1.26222370
-6849319464662435083	128288704	0.153997822	1.25717022
-13598585514212472187	179800672	0.153175728	1.25566335

Table 6.5: LLI-lochamps ($D < 0$)

Following Lehmer [Leh37] we define the symbol N_p to represent the least positive integer congruent to 3 modulo 8 such that

$$\left(\frac{-N_p}{q}\right) = -1$$

for all odd primes $q \leq p$. Lehmer computed the first table of N_p values for $p \leq 107$. Lehmer, Lehmer, and Shanks extended these computations in [LLS70], Problem III, to values of $p \leq 163$ and Lehmer also computed the next three values up to $p = 181$, but did not publish them. We used MSSU to extend further these computations and were able to find values of N_p up to $p = 277$, and least prime solutions of N_p up to $p = 269$. Tables 6.6 and 6.7 contain all the currently known values of N_p and the least prime solutions of N_p respectively. Tables 6.10 and 6.11 give the LLI values for the N_p solutions.

Similarly, we define the symbol M_p to represent the least positive integer congruent to 5 modulo 8 such that

$$\left(\frac{M_p}{q}\right) = -1$$

for all odd primes $q \leq p$. We would expect, due to Conjecture F, that $|f_A(x)|$ will have a large density of prime values when $A = (1 - M_p)/4$. According to Poletti [Pol51], Beeger was the first to make a table of M_p values; he listed them up to $p = 59$. Lehmer, Lehmer, and Shanks [LLS70], Problem VI, extended this table in 1970 up to $p = 139$ and Lehmer produced one more value for $p = 163$, but did not publish it. We used MSSU to extend further the table to $p = 283$ and $p = 263$ for least prime solutions. Tables 6.8 and 6.9 contain all the currently known values of M_p and the least prime solutions of M_p respectively. The LLI values for the M_p solutions are equivalent to the $5R_p$ tables 5.9 and 5.10 from Chapter 5.

We can derive an upper bound on $C(D)$ from Littlewood's bound

$$L(1,\chi) > \frac{\{1 + o(1)\}}{c_1 \log\log \Delta} \tag{6.13}$$

where

$$c_1 = \begin{cases} \frac{8e^\gamma}{\pi^2} & \text{when } 2 \mid \Delta, \\ \frac{12e^\gamma}{\pi^2} & \text{otherwise} \end{cases}$$

as given in Chapter 5. We know that

$$\frac{\zeta(4)}{\zeta(2)} = \prod_p \left(1 + \frac{1}{p^2}\right)^{-1} \tag{6.14}$$

and $\zeta(2) = \pi^2/6$. Also, from the Euler product representation of $L(2,\chi)$ we have

$$L(2,\chi)^{-1} = \prod_p \left(1 + \frac{\chi(p)}{p^2}\right) < \prod_p \left(1 + \frac{1}{p^2}\right). \tag{6.15}$$

From (6.2) and (6.13) we have

$$C(D) < \{1 + o(1)\} c \cdot c_1 \log\log|\Delta| \frac{\zeta(4)}{2L(2,\chi)}$$

and from (6.14) and (6.15) we get

$$C(D) < \{1 + o(1)\} d \log\log|\Delta| \tag{6.16}$$

where

$$d = \begin{cases} 5e^\gamma & \text{when } D \equiv 1 \pmod 8, \\ e^\gamma & \text{when } D \equiv 5 \pmod 8, \\ \frac{5}{4}e^\gamma & \text{otherwise} \end{cases}$$

Tables 6.12 to 6.15 give the values of $Z(D) = C/e^\gamma \log\log|D|$ for our values of N_p and M_p. By (6.16) we would expect a very slow growth rate of $C(D)$. In fact, with the exception of $N_p = 163$, the value of Z is always less than 1, and does not vary much from 0.8. Figures 6.1 and 6.2 show the Z values plotted against the N_p and M_p solutions respectively. In each case, the horizontal line is at $Z = 0.8$.

p	N_p	$h(-N_p)$	$L(1,\chi)$	$C(-N_p)$
3	19	1	0.720730	0.94222046
5,7	43	1	0.479088	1.6297209
11,13	67	1	0.383806	2.0873308
17,...,37	163	1	0.246068	3.3197732
41,43	77683	22	0.247975	3.3003388
47	1333963	79	0.214884	3.8123997
53,59	2404147	107	0.216796	3.7793704
61	20950603	311	0.213457	3.8410195
67	36254563	432	0.225399	3.6365197
71	51599563	487	0.212988	3.8514289
73,79	96295483	665	0.212896	3.8528890
83	114148483	692	0.203479	4.0332358
89,...,103	269497867	1044	0.199789	4.1092157
107	585811843	1536	0.199371	4.1185705
109,113	52947440683	13909	0.189899	4.3245257
127	71837718283	15204	0.178209	4.6097143
131,137	229565917267	29351	0.192450	4.2679170
139	575528148427	44332	0.183583	4.4746374
149,...,163	1432817816347	70877	0.186020	4.4163429
167	6778817202523	149460	0.180342	4.5565681
173	16501779755323	223574	0.172904	4.7524812
179,181	30059924764123	296475	0.169880	4.8379057
191,193,197	110587910656507	553436	0.165334	4.9711959
199	4311527414591923	3791896	0.181422	4.5293043
211,223	10472407114788067	5798780	0.178017	4.6162389
227,...,241	22261805373620443	8035685	0.169196	4.8576312
251	132958087830686827	19412108	0.167249	4.9146545
257	441899002218793387	33684408	0.159190	5.1635913
263,269	2278509757859388307	77949544	0.162232	5.0669199
271	5694230275645018963	119705436	0.157596	5.2163043
277	9828323860172600203	156104956	0.156432	5.2552050

Table 6.6: N_p — Least Solutions

p	N_p	$h(-N_p)$	$L(1,\chi)$	$C(-N_p)$
3	19	1	0.720730	0.94222046
5,7	43	1	0.479088	1.6297209
11,13	67	1	0.383806	2.0873308
17,...,37	163	1	0.246068	3.3197732
41	222643	33	0.219714	3.7289570
43,47	1333963	79	0.214884	3.8123997
53,59	2404147	107	0.216796	3.7793704
61	20950603	311	0.213457	3.8410195
67,71	51599563	487	0.212988	3.8514289
73,79	96295483	665	0.212896	3.8528890
83	146161723	857	0.222696	3.6832906
89	1408126003	2293	0.191969	4.2771747
97,101,103	3341091163	3523	0.191477	4.2878711
107,109,113	52947440683	13909	0.189899	4.3245257
127	193310265163	26713	0.190873	4.3024065
131,137	229565917267	29351	0.192450	4.2679170
139	915809911867	59801	0.196315	4.1834705
149,...,163	1432817816347	70877	0.186020	4.4163429
167,...,181	30059924764123	296475	0.169880	4.8379057
191	3126717241727227	3201195	0.179853	4.5685162
193,197,199	8842819893041227	5188215	0.173329	4.7414735
211,223	13688678408873323	6524653	0.175196	4.6907580
227,...,241	22261805373620443	8035685	0.169196	4.8576312
251	4908856524312968467	121139393	0.171769	4.7847955
257,263,269	7961860547428719787	140879803	0.156852	5.2409110

Table 6.7: N_p — Least Prime Solutions

p	M_p	$R(M_p)$	$h(M_p)$	$L(1,\chi)$	$C(M_p)$
3	5	0.4812	1	0.430408	1.7733051
5	53	1.9657	1	0.540024	1.3831458
7,11	173	2.5708	1	0.390910	2.0427655
13	293	2.8366	1	0.331438	2.4386997
17	437	3.0422	1	0.291060	2.7933935
19,23	9173	12.4722	1	0.260446	3.1227858
29	24653	5.0562	4	0.257624	3.1631443
31,37,41	74093	7.2159	5	0.265098	3.0809338
43	170957	16.9391	3	0.245810	3.3299831
47,53,59	214037	28.9536	2	0.250333	3.2704656
61	2004917	48.2972	3	0.204656	4.0077796
67	44401013	352.5078	2	0.211608	3.8743032
71	71148173	140.5395	6	0.199939	4.1026493
73,79	154554077	694.9131	2	0.223588	3.6684052
83,89,97	163520117	152.1367	9	0.214151	3.8307572
101,103	261153653	512.3272	3	0.190217	4.3158954
107,109,113	1728061733	4021.1400	1	0.193463	4.2447622
127	9447241877	1252.3775	7	0.180389	4.5541813
131	19553206613	6209.5055	2	0.177626	4.6250203
137,139	49107823133	18804.6808	1	0.169715	4.8420287
149,...,163	385995595277	27068.0628	2	0.174271	4.7144914
167	13213747959653	330785.2663	1	0.181996	4.5147795
173	14506773263237	331149.0061	1	0.173887	4.7257867
179,181	57824199003317	165998.4596	4	0.174638	4.7059530
191,193	160909740894437	275610.2629	4	0.173817	4.7279560
197,199	370095509388197	794079.6472	2	0.165107	4.9779329
211	1409029796180597	3130386.6897	1	0.166789	4.9274990
223	4075316253649373	5291574.7242	1	0.165780	4.9577054
227,229,233	18974003020179917	2737025.3979	4	0.158960	5.1711431
239,241	224117990614052477	10257518.4583	4	0.173338	4.7415726
251,257,263	637754768063384837	22908547.7970	3	0.172116	4.7753226
269,...,283	4472988326827347533	14462868.4419	12	0.164129	5.0085747

Table 6.8: M_p — Least Solutions

p	M_p	$R(M_p)$	$h(M_p)$	$L(1,\chi)$	$C(M_p)$
3	5	0.48121	1	0.430408	1.7733051
5	53	1.96572	1	0.540024	1.3831458
7,11	173	2.57081	1	0.390910	2.0427655
13	293	2.83665	1	0.331438	2.4386997
17	2477	6.47234	1	0.260093	3.1173079
19,23	9173	12.47223	1	0.260446	3.1227858
29	61613	36.23370	1	0.291948	2.7929099
31,37,41	74093	7.21597	5	0.265098	3.0809338
43	170957	16.93918	3	0.245810	3.3299831
47	360293	68.23691	1	0.227363	3.6032397
53	679733	92.04349	1	0.223282	3.6713558
59,61	2004917	48.29722	3	0.204656	4.0077796
67	69009533	869.69643	1	0.209383	3.9166092
71	138473837	1369.29769	1	0.232725	3.5221802
73	237536213	1725.64096	1	0.223931	3.6624765
79	384479933	2087.35754	1	0.212907	3.8534093
83	883597853	3018.26471	1	0.203076	4.0411818
89,...,113	1728061733	4021.14004	1	0.193463	4.2447622
127	9447241877	1252.37753	7	0.180389	4.5541813
131,137,139	49107823133	18804.68086	1	0.169715	4.8420287
149	1843103135837	119080.85359	1	0.175427	4.6828076
151,157	4316096218013	192239.83257	1	0.185066	4.4390420
163,167	15021875771117	344898.80858	1	0.177975	4.6165765
173,179	82409880589277	804942.51462	1	0.177339	4.6336310
181	326813126363093	1551603.41110	1	0.171656	4.7874230
191,193	390894884910197	1650908.48845	1	0.167002	4.9214877
197	1051212848890277	547589.04349	5	0.168892	4.8659116
199,211,223	4075316253649373	5291574.72421	1	0.165780	4.9577054
227	274457237558283317	45653225.95687	1	0.174286	4.7155029
229	443001676907312837	6097479.67224	9	0.164899	4.9843291
233	599423482887195557	65388978.22854	1	0.168914	4.8658247
239	614530964726833997	64783176.97206	1	0.165280	4.9730080
241,...,263	637754768063384837	22908547.79705	3	0.172116	4.7753226

Table 6.9: M_p — Least Prime Solutions

p	N_p	$h(-N_p)$	$L(1,\chi)$	LLI
3	19	1	0.720730	1.68549
5,7	43	1	0.479088	1.37438
11,13	67	1	0.383806	1.19368
17,...,37	163	1	0.246068	0.86751
41,43	77683	22	0.247975	1.30022
47	1333963	79	0.214884	1.23148
53,59	2404147	107	0.216796	1.26165
61	20950603	311	0.213457	1.30576
67	36254563	432	0.225399	1.39443
71	51599563	487	0.212988	1.32691
73,79	96295483	665	0.212896	1.34226
83	114148483	692	0.203479	1.28694
89,...,103	269497867	1044	0.199789	1.28319
107	585811843	1536	0.199371	1.29743
109,113	52947440683	13909	0.189899	1.31861
127	71837718283	15204	0.178209	1.24218
131,137	229565917267	29351	0.192450	1.36038
139	575528148427	44332	0.183583	1.31143
149,...,163	1432817816347	70877	0.186020	1.34218
167	6778817202523	149460	0.180342	1.32231
173	16501779755323	223574	0.172904	1.27888
179,181	30059924764123	296475	0.169880	1.26370
191,193,197	110587910656507	553436	0.165334	1.24460
199	4311527414591923	3791896	0.181422	1.40787
211,223	10472407114788067	5798780	0.178017	1.39084
227,...,241	22261805373620443	8035685	0.169196	1.32934
251	132958087830686827	19412108	0.167249	1.33084
257	441899002218793387	33684408	0.159190	1.27705
263,269	2278509757859388307	77949544	0.162232	1.31536
271	5694230275645018963	119705436	0.157596	1.28509
277	9828323860172600203	156104956	0.156432	1.27985

Table 6.10: N_p — Least Solutions (LLI)

p	N_p	$h(-N_p)$	$L(1,\chi)$	LLI
3	19	1	0.720730	1.68549
5,7	43	1	0.479088	1.37438
11,13	67	1	0.383806	1.19368
17,...,37	163	1	0.246068	0.86751
41	222643	33	0.219714	1.19457
43,47	1333963	79	0.214884	1.23148
53,59	2404147	107	0.216796	1.26165
61	20950603	311	0.213457	1.30576
67,71	51599563	487	0.212988	1.32691
73,79	96295483	665	0.212896	1.34226
83	146161723	857	0.222696	1.41487
89	1408126003	2293	0.191969	1.26695
97,101,103	3341091163	3523	0.191477	1.28037
107,109,113	52947440683	13909	0.189899	1.31861
127	193310265163	26713	0.190873	1.34650
131,137	229565917267	29351	0.192450	1.36038
139	915809911867	59801	0.196315	1.40961
149,...,163	1432817816347	70877	0.186020	1.34218
167,...,181	30059924764123	296475	0.169880	1.26370
191	3126717241727227	3201195	0.179853	1.39220
193,197,199	8842819893041227	5188215	0.173329	1.35248
211,223	13688678408873323	6524653	0.175196	1.37154
227,...,241	22261805373620443	8035685	0.169196	1.32934
251	4908856524312968467	121139393	0.171769	1.39937
257,263,269	7961860547428719787	140879803	0.156852	1.28165

Table 6.11: N_p — Least Prime Solutions (LLI)

p	N_p	$h(-N_p)$	$C(-N_p)$	$Z(N_p)$
3	19	1	0.94222046	0.489869
5,7	43	1	1.6297209	0.690719
11,13	67	1	2.0873308	0.816008
17,...,37	163	1	3.3197732	1.144902
41,43	77683	22	3.3003388	0.765296
47	1333963	79	3.8123997	0.808827
53,59	2404147	107	3.7793704	0.789611
61	20950603	311	3.8410195	0.763442
67	36254563	432	3.6365197	0.714696
71	51599563	487	3.8514289	0.751651
73,79	96295483	665	3.8528890	0.743018
83	114148483	692	4.0332358	0.775345
89,...,103	269497867	1044	4.1092157	0.777896
107	585811843	1536	4.1185705	0.769491
109,113	52947440683	13909	4.3245257	0.757225
127	71837718283	15204	4.6097143	0.804082
131,137	229565917267	29351	4.2679170	0.734101
139	575528148427	44332	4.4746374	0.761601
149,...,163	1432817816347	70877	4.4163429	0.744205
167	6778817202523	149460	4.5565681	0.755581
173	16501779755323	223574	4.7524812	0.781222
179,181	30059924764123	296475	4.8379057	0.790747
191,193,197	110587910656507	553436	4.9711959	0.802922
199	4311527414591923	3791896	4.5293043	0.709643
211,223	10472407114788067	5798780	4.6162389	0.718381
227,...,241	22261805373620443	8035685	4.8576312	0.751730
251	132958087830686827	19412108	4.9146545	0.750954
257	441899002218793387	33684408	5.1635913	0.782600
263,269	2278509757859388307	77949544	5.0669199	0.759831
271	5694230275645018963	119705436	5.2163043	0.777780
277	9828323860172600203	156104956	5.2552050	0.780975

Table 6.12: N_p — Least Solutions ($Z(N_p) = C/e^{\gamma} \log\log N_p$)

p	N_p	$h(-N_p)$	$C(-N_p)$	$Z(N_p)$
3	19	1	0.94222046	0.489869
5,7	43	1	1.6297209	0.690719
11,13	67	1	2.0873308	0.816008
17,...,37	163	1	3.3197732	1.144902
41	222643	33	3.7289570	0.833900
43,47	1333963	79	3.8123997	0.808827
53,59	2404147	107	3.7793704	0.789611
61	20950603	311	3.8410195	0.763442
67,71	51599563	487	3.8514289	0.751651
73,79	96295483	665	3.8528890	0.743018
83	146161723	857	3.6832906	0.704877
89	1408126003	2293	4.2771747	0.787974
97,101,103	3341091163	3523	4.2878711	0.779661
107,109,113	52947440683	13909	4.3245257	0.757225
127	193310265163	26713	4.3024065	0.741531
131,137	229565917267	29351	4.2679170	0.734101
139	915809911867	59801	4.1834705	0.708391
149,...,163	1432817816347	70877	4.4163429	0.744205
167,...,181	30059924764123	296475	4.8379057	0.790747
191	3126717241727227	3201195	4.5685162	0.717582
193,197,199	8842819893041227	5188215	4.7414735	0.738812
211,223	13688678408873323	6524653	4.6907580	0.728517
227,...,241	22261805373620443	8035685	4.8576312	0.751730
251	4908856524312968467	121139393	4.7847955	0.714092
257,263,269	7961860547428719787	140879803	5.2409110	0.779847

Table 6.13: N_p — Least Prime Solutions ($Z(N_p) = C/e^{\gamma} \log\log N_p$)

p	M_p	$R(M_p)$	$h(M_p)$	$C(M_p)$	$Z(M_p)$
3	5	0.4812	1	1.7733051	2.092183
5	53	1.9657	1	1.3831458	0.563212
7,11	173	2.5708	1	2.0427655	0.699503
13	293	2.8366	1	2.4386997	0.788281
17	437	3.0422	1	2.7933935	0.868910
19,23	9173	12.4722	1	3.1227858	0.793029
29	24653	5.0562	4	3.1631443	0.767562
31,37,41	74093	7.2159	5	3.0809338	0.715664
43	170957	16.9391	3	3.3299831	0.751166
47,53,59	214037	28.9536	2	3.2704656	0.732303
61	2004917	48.2972	3	4.0077796	0.841225
67	44401013	352.5078	2	3.8743032	0.758355
71	71148173	140.5395	6	4.1026493	0.795721
73,79	154554077	694.9131	2	3.6684052	0.701320
83,89,97	163520117	152.1367	9	3.8307572	0.731614
101,103	261153653	512.3272	3	4.3158954	0.817468
107,109,113	1728061733	4021.1400	1	4.2447622	0.779529
127	9447241877	1252.3775	7	4.5541813	0.815848
131	19553206613	6209.5055	2	4.6250203	0.820377
137,139	49107823133	18804.6808	1	4.8420287	0.848648
149,...,163	385995595277	27068.0628	2	4.7144914	0.806057
167	13213747959653	330785.2663	1	4.5147795	0.743744
173	14506773263237	331149.0061	1	4.7257867	0.777800
179,181	57824199003317	165998.4596	4	4.7059530	0.764536
191,193	160909740894437	275610.2629	4	4.7279560	0.761111
197,199	370095509388197	794079.6472	2	4.9779329	0.795616
211	1409029796180597	3130386.6897	1	4.9274990	0.778891
223	4075316253649373	5291574.7242	1	4.9577054	0.777103
227,229,233	18974003020179917	2737025.3979	4	5.1711431	0.801187
239,241	224117990614052477	10257518.4583	4	4.7415726	0.721922
251,257,263	637754768063384837	22908547.7970	3	4.7753226	0.722002
269,...,283	4472988326827347533	14462868.4419	12	5.0085747	0.747919

Table 6.14: M_p — Least Solutions ($Z(M_p) = C/e^{\gamma} \log\log M_p$)

p	M_p	$R(M_p)$	$h(M_p)$	$C(M_p)$	$Z(M_p)$
3	5	0.4812	1	1.7733051	2.092183
5	53	1.9657	1	1.3831458	0.563212
7,11	173	2.5708	1	2.0427655	0.699503
13	293	2.8366	1	2.4386997	0.788281
17	2477	6.4723	1	3.1173079	0.851276
19,23	9173	12.4722	1	3.1227858	0.793029
29	61613	36.2337	1	2.7929099	0.653242
31,37,41	74093	7.2159	5	3.0809338	0.715664
43	170957	16.9391	3	3.3299831	0.751166
47	360293	68.2369	1	3.6032397	0.793664
53	679733	92.0434	1	3.6713558	0.793592
59,61	2004917	48.2972	3	4.0077796	0.841225
67	69009533	869.6964	1	3.9166092	0.760081
71	138473837	1369.2976	1	3.5221802	0.674707
73	237536213	1725.6409	1	3.6624765	0.694854
79	384479933	2087.3575	1	3.8534093	0.725036
83	883597853	3018.2647	1	4.0411818	0.750003
89,...,113	1728061733	4021.1400	1	4.2447622	0.779529
127	9447241877	1252.3775	7	4.5541813	0.815848
131,137,139	49107823133	18804.6808	1	4.8420287	0.848648
149	1843103135837	119080.8535	1	4.6828076	0.786992
151,157	4316096218013	192239.8325	1	4.4390420	0.739455
163,167	15021875771117	344898.8085	1	4.6165765	0.759569
173,179	82409880589277	804942.5146	1	4.6336310	0.750373
181	326813126363093	1551603.4111	1	4.7874230	0.765977
191,193	390894884910197	1650908.4884	1	4.9214877	0.786230
197	1051212848890277	547589.0434	5	4.8659116	0.770986
199,211,223	4075316253649373	5291574.7242	1	4.9577054	0.777103
227	274457237558283317	45653225.9568	1	4.7155029	0.716970
229	443001676907312837	6097479.6722	9	4.9843291	0.755419
233	599423482887195557	65388978.2285	1	4.8658247	0.735985
239	614530964726833997	64783176.9720	1	4.9730080	0.752074
241,...,263	637754768063384837	22908547.7970	3	4.7753226	0.722002

Table 6.15: M_p — Least Prime Solutions ($Z(M_p) = C/e^{\gamma} \log\log M_p$)

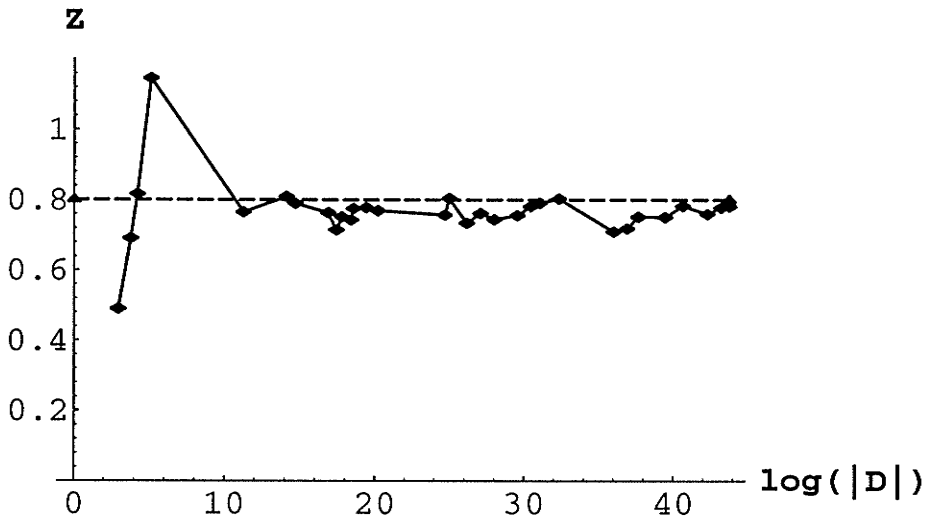

Figure 6.1: N_p vs. $C/e^{\gamma} \log\log N_p$

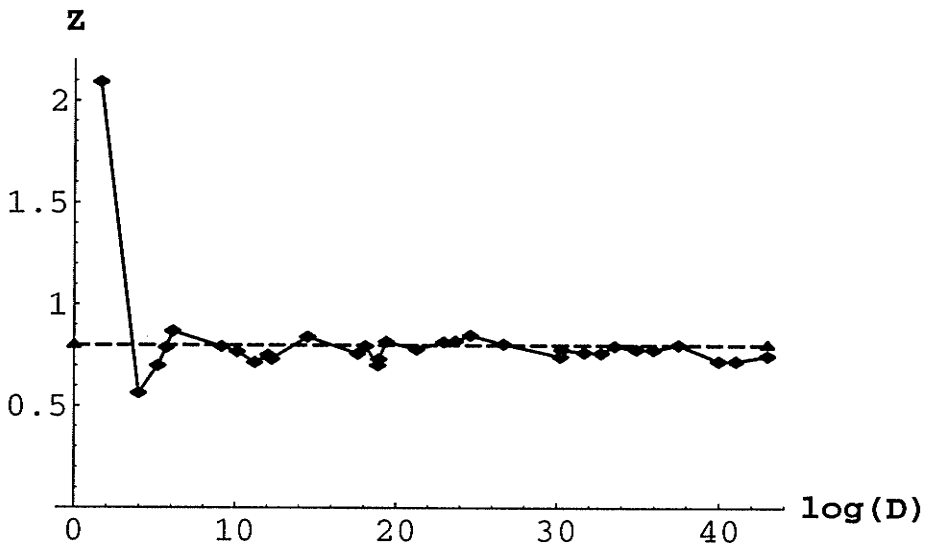

Figure 6.2: M_p vs. $C/e^{\gamma} \log\log M_p$

6.5 Conclusion

Almost certainly none of our D values computed here violates the ERH, but at first glance it appears that $N_p = 163$ might, since its LLI value is less than 1 and its $C/e^{\gamma}\log\log|D|$ value is greater than 1. However, as pointed out in Shanks [Sha73], this is almost certainly not the case. The apparent discrepancy is most likely accounted for by the $o(1)$ term that is ignored in the Littlewood indices and $C/e^{\gamma}\log\log|D|$.

Shanks' analysis of this is as follows. He first notes that Littlewood's lower bound on $L(1,\chi)$ can be written as

$$[\{1+o(1)\}B(x)]^{-1} < L(1,\chi) \tag{6.17}$$

where

$$B(x) = \exp\sum_{p^m \le x}\frac{(-1)^{m+1}}{mp^m},$$

and

$$x = (\log|\Delta|)^{2(1+4\epsilon)} \tag{6.18}$$

for some $\epsilon > 0$. Littlewood's analysis in [Lit28] leading to (6.17) shows that the $o(1)$ term depends only on our choice of ϵ. We define $b(x)$ by writing

$$B(x) = \left(1+\frac{b(x)}{\sqrt{x}\log x}\right)\frac{6e^{\gamma}}{\pi^2}\log x.$$

As $x \to \infty$, $b(x)/(\sqrt(x)\log x) \to 0$, and the first approximation made in [Lit28] replaces this quantity by 0. The second approximation sets $\epsilon = 0$ in (6.18) so (6.17) becomes

$$\left[\{1+o(1)\}\frac{12e^{\gamma}}{\pi^2}\log\log\Delta\right]^{-1} < L(1,\chi). \tag{6.19}$$

For $\Delta = -163$, if we set $\epsilon = 0$ in (6.18) we get

$$x = (\log 163)^2 = 25.9463,$$

$$B(x) = 3.7601,$$

and

$$\frac{6e^{\gamma}}{\pi^2}\log x = 3.4853.$$

Although $B(x)^{-1} > L(1,\chi)$ for $\Delta = -163$, we do have

$$B(x) > \frac{6e^{\gamma}}{\pi^2}\log x.$$

Thus, the two leading terms in the approximations leading to Littlewood's bounds are of the sign needed to convince us that -163 almost certainly does not violate the ERH, even though they are not of sufficient magnitude for it to be completely exhonerated.

Also, as mentioned in [LLS70], our values of D relate to an investigation of Ayoub, Chowla, and Walum [ACW67] involving sums of quadratic characters. It is known that the class number $h(-q)$ for primes $q \equiv 3 \pmod 4$ can be obtained from the sums

$$S_1(q) = \sum_{v=1}^{q-1} v\left(\frac{v}{q}\right) = -qh(-q)$$

and

$$S_2(q) = \sum_{v=1}^{q-1} v^2\left(\frac{v}{q}\right) = -q^2h(-q).$$

Since $h(-q)$ is always positive, $S_1(q)$ and $S_2(q)$ must therefore be negative. However, in [ACW67] it is proven that

$$S_3(q) = \sum_{v=1}^{q-1} v^3\left(\frac{v}{q}\right)$$

is positive for infinitely many primes q. In fact, we also have

$$S_3(q) = \frac{q^3\sqrt{q}}{\pi}\left[\frac{3}{2\pi^2}L(3,\chi) - L(1,\chi)\right]$$

where

$$L(3,\chi) = \prod_{p=2}^{\infty}\frac{p^3}{p^3 - \left(\frac{-q}{p}\right)}.$$

Now

$$L(3,\chi) > \prod_{p=2}^{\infty}\frac{p^3}{p^3+1} = \frac{\zeta(6)}{\zeta(3)},$$

so, as pointed out in [LLS70], to obtain a positive value of $S_3(q)$ it would suffice if

$$L(1,\chi) < \frac{3}{2\pi^2}\frac{\zeta(6)}{\zeta(3)} = \frac{\zeta(6)}{4\zeta(2)\zeta(3)} = 0.12863. \tag{6.20}$$

Our D values are selected such that their $L(1,\chi)$ functions are unusually small, but our smallest value of

$$L(1,\chi) = 0.154498922\ldots$$

for the prime

$$D = -19701513057844219387$$

($h = 218285743$, $C(D) = 5.3209478$) still does not satisfy (6.20). However, it suggests that the chance of actually finding a value of q such that $S_3(q) > 0$ may not be too remote.

Chapter 7

Conclusion

An interesting aspect regarding the computation of class numbers in quadratic fields is that there is no unconditional algorithm known that has complexity better than $O\left(D^{1/2+\epsilon}\right)$. The most direct approach is to simply count every ideal equivalence class in the field. In imaginary quadratic fields this essentially means counting the number of reduced ideals and leads to an algorithm with complexity $O\left(|D|^{1/2}\right)$ (see [Coh93]). In real quadratic fields this means counting the number of ideal class cycles. It is not immediately obvious, but this method can be organized into an algorithm with complexity $O\left(D^{1/2+\epsilon}\right)$ (cf. [MW92]). In both cases the value of h is certainly unconditionally correct.

The finite sums (2.10) and (2.11) given in Section 2.6 can be given using half the summands for imaginary quadratic fields by

$$h = -\frac{1}{2-\left(\frac{\Delta}{2}\right)} \sum_{j=1}^{|\Delta|/2} \left(\frac{\Delta}{j}\right)$$

and for real quadratic fields by

$$h = -\frac{1}{R} \sum_{j=1}^{\lfloor(\Delta-1)/2\rfloor} \left(\frac{\Delta}{j}\right) \log \sin \frac{\pi j}{\Delta}.$$

These sums also give us an unconditionally correct value of h, but they require $O\left(|D|^{1+\epsilon}\right)$ operations and are therefore impractical for large values of D. However, if we make use of the functional equation defining $L(1,\chi)$ we can derive for imaginary quadratic fields

$$h = \sum_{n\geq 1}\left(\frac{\Delta}{n}\right)\left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|\Delta|}}\right) + \frac{\sqrt{|\Delta|}}{\pi n}\exp\left(\frac{-\pi n^2}{|\Delta|}\right)\right)$$

and for real quadratic fields

$$h = \frac{1}{2R}\sum_{n\geq 1}\left(\frac{\Delta}{n}\right)\left(\frac{\sqrt{\Delta}}{n}\operatorname{erfc}\left(n\sqrt{\frac{\pi}{\Delta}}\right) + E_1\left(\frac{\pi n^2}{\Delta}\right)\right),$$

where

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty \exp\left(-t^2\right)dt$$

and

$$E_1(x) = \int_x^\infty \frac{\exp(-t)}{t}dt.$$

It can be shown that if we sum $O\left(|D|^{1/2}\right)$ terms, then the closest integer to the value of these sums is equal to h. The functions $\operatorname{erfc}(x)$ and $E_1(x)$ can be computed rapidly enough so that the overall complexity of the algorithms using these formulae is $O\left(|D|^{1/2+\epsilon}\right)$, but the constant implicit in the O-notation is too large to make this method practical for large radicands.

The best conditional algorithms currently known for computing class numbers have subexponential complexity $O\left(L(|D|)^{c+o(1)}\right)$ where $L(D) = \exp\left(\sqrt{\log D \log\log D}\right)$. For imaginary quadratic fields $c = \sqrt{2}$ and for real quadratic fields $c \approx 1.44$. The algorithm in the imaginary case is due to Haffner and McCurley [HM89] and has been implemented by Stephan Düllmann [Dül91] with great success. This algorithm has been generalized to arbitrary number fields by Buchmann [Buc89] and dealt with extensively in the real quadratic case by Abel [Abe94]. Cohen, Diaz y Diaz, and Olivier [CDyDO93, CDyDO94] have implemented this algorithm, as well as that for imaginary quadratic fields.

The basic ideas behind these subexponential algorithms are fairly straightforward. For an imaginary quadratic field $\mathcal{K}$ of discriminant Δ, Bach [Bac90], under the ERH, has

has shown that the class group can be generated by all prime ideals of norm less than $6\log^2|\Delta|$. If we denote by $\mathcal{P}$ the set of all such prime ideals $\mathfrak{p}_i$ in $\mathcal{K}$ and set $n = |\mathcal{P}|$, then the map

$$\phi : \mathbb{Z}^n \to Cl$$
$$(x_1, \ldots, x_n) \mapsto \prod_{i=1}^{n} \mathfrak{p}_i^{x_i}$$

is a surjective group homomorphism. The kernel Λ of ϕ is a sublattice of $\mathbb{Z}^n$, and hence

$$\mathbb{Z}^n/\Lambda \simeq Cl.$$

Also, if by $\det(\Lambda)$ we denote the determinant of any integral basis of Λ, then

$$|\det(\Lambda)| = h.$$

To compute h, we generate many random relations of the form

$$\prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i} \sim (1),$$

where $\alpha_i \in \mathbb{Z}$. We then compute a basis for the lattice generated by these relations by computing the Hermite normal form of the matrix L of their exponents. We use the analytic class number formula to check whether $\tilde{h} = \det L$ is within a factor of 2 of the actual value of h. If so, then this basis generates Λ and $\tilde{h} = h$. Otherwise, we add more relations until we obtain a full basis of Λ. Once we have computed h, we determine the structure of Cl as a direct sum of cyclic subgroups

$$Cl = \bigoplus \mathbb{Z}/d_i\mathbb{Z},$$

where the d_i are the diagonal elements greater than 1 found in the Smith normal form of L. With extra complications, this method can be extended to real quadratic fields, yielding an algorithm which simultaneously computes h and R.

Unlike the algorithms we use in this thesis, the subexponential algorithms are not deterministic. Also, the value of R which we compute is unconditionally correct, whereas

the correctness of R, h, and the complexity result are all conditional on the truth of the ERH in the subexponential algorithms. However, the subexponential algorithms are certainly faster for very large values of D. The values of D for which we computed R and h were sufficiently small that very little would have been gained by using the subexponential algorithms, although it is not clear exactly where the trade-off point is.

Another advantage of the subexponential algorithms is that they compute the structure of the class group as a direct product of cyclic subgroups for little additional cost. The algorithms presented here can be extended to compute the structure of the class group as well, but the complexity of the resulting algorithm decreases to $O\left(D^{1/4+\epsilon}\right)$. We did not implement an algorithm to do this, since the conjectures we wished to test did not require knowledge of the structure of the class group, only the class number.

Buchmann and Williams [BW89c] have shown that a short proof of the value of R and h in real quadratic fields exists, i.e., the computation of R and h is in $\mathcal{NP}$. Also, using so-called short representations for quadratic integers, Buchmann, Thiel, and Williams [BTW95] have shown that norms, signs, products, and inverses of numbers in $\mathcal{O}_K$ and of principal ideals can be computed in polynomial time and that principal ideal testing is in $\mathcal{NP}$. These short representations are necessary since, for example, fundamental units require at least $\sqrt{\Delta}/(9h\log\Delta)$ bits for a standard representation, and since we have shown that h is probably often small it is therefore impossible to give ε_0 in standard representation for the majority of real quadratic fields.

Finally, we wish to emphasize that none of the conjectures we have tested has been proved. In fact, the correctness of the algorithms we used to test them is itself conditional on an unproved hypothesis. However, during the course of our experiments we have found nothing to suggest that any of these conjectures is false, and hopefully formal proofs of them will one day appear.

Bibliography

[Abe94] C.S. Abel, *Ein algorithmus zur berechnung der klassenzahl und des regulators reellquadratischer ordnungen*, Ph.D. thesis, Universität des Saarlandes, Saarbrücken, Germany, 1994.

[ACW67] R. Ayoub, S. Chowla, and H. Walum, *On sums involving quadratic characters*, J. London Math. Soc. **42** (1967), 152–154.

[Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380.

[Bac94] E. Bach, *Improved approximations for Euler products*, Unpublished MS., 1994.

[Bee39] N.G.W.H. Beeger, *Report on some calculations of prime numbers*, Nieuw Archief voor Wiskunde (2) **20** (1939), 48–50.

[BTW95] J. Buchmann, C. Thiel, and H.C. Williams, *Short representation of quadratic integers*, Computational Algebra and Number Theory, Mathematics and its Applications **325**, Kluwer, Dordrecht, 1995, pp. 159–185.

[Buc89] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres (Paris), 1988-89, pp. 27–41.

[Bue84] D.A. Buell, *The expectation of success using a Monte-Carlo factoring method — Some statistics on quadratic class numbers*, Math. Comp. **43** (1984), 313–327.

[BW88] J. Buchmann and H.C. Williams, *A key-exchange system based on imaginary quadratic fields*, Journal of Cryptology 1 (1988), 107–118.

[BW89a] J. Buchmann and H.C. Williams, *A key-exchange system based on real quadratic fields*, Lecture Notes in Computer Science **435** (1989), 335–343.

[BW89b] J. Buchmann and H.C. Williams, *On the computation of the class number of an algebraic number field*, Math. Comp. **53** (1989), 679–688.

[BW89c] J. Buchmann and H.C. Williams, *On the existence of a short proof for the value of the class number and regulator of a real quadratic field*, Proc. NATO ASI on Number Theory and Applications, Kluwer Academic Press, 1989, pp. 327–345.

[BW90] J. Buchmann and H.C. Williams, *Quadratic fields and cryptography*, Number Theory and Cryptography, London Math. Soc. Lecture Note Series **154** (1990), 9–26.

[CDyDO93] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Calculs de nombres de classes et de régulateurs de corps quadratiques en temps sous-exponentiel*, Séminaire de Théorie des Nombres (Paris), 1993, pp. 35–46.

[CDyDO94] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Subexponential algorithms for class group and unit computations*, Unpublished manuscript, 1994.

[Cho49] S. Chowla, *Improvement of a theorem of Linnik and Walfisz*, Proc. London Math. Soc. **50** (1949), 423–429.

[CL83] H. Cohen and H.W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory, Lecture notes in Math., vol. 1068, Springer-Verlag, New York, 1983, pp. 33–62.

[CL84] H. Cohen and H.W. Lenstra, Jr., *Heuristics on class groups*, Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1052, Springer-Verlag, New York, 1984, pp. 26–36.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[CW85] G. Cornell and L.C. Washington, *Class numbers of cyclotomic fields*, J. Number Theory **21** (1985), 260–274.

[Dül91] S. Düllmann, *Ein algorithmus zur bestimmung der klassengruppe positiv definiter binärer quadratischer formen*, Ph.D. thesis, Universität des Saarlandes, Saarbrücken, Germany, 1991.

[Ell69] P.D.T.A. Elliot, *On the size of* $L(1,\chi)$, J. reine angew. Math. **236** (1969), 26–36.

[Fun90] G.W. Fung, *Computational problems in complex cubic fields*, Ph.D. thesis, University of Manitoba, Winnipeg, Manitoba, 1990.

[FW90] G.W. Fung and H.C. Williams, *Quadratic polynomials which have a high density of prime values*, Math. Comp. **55** (1990), 345–353.

[HK89] F. Halter-Koch, *Reell-quadratischer Zahlkörper mit groszer Grundeinheit*, Abh. Math. Sem. Univ. Hamburg **59** (1989), 171–181.

[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.

[HM89] J.L. Hafner and K.S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, Tech. report, IBM Research Report, San Jose, CA, 1989.

[Hoo84] C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. reine angew. Math. **353** (1984), 98–131.

[Hua82] L.K. Hua, *Introduction to number theory*, Springer-Verlag, New York, 1982.

[HW62] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fourth ed., Oxford University Press, London, 1962.

[JLW94] M.J. Jacobson, Jr., R.F. Lukes, and H.C. Williams, *Some numerical experiments concerning quadratic fields*, Unpublished manuscript, 1994.

[Jos70] P.T. Joshi, *The size of $L(1,\chi)$ for real nonprincipal residue characters χ with prime modulus*, J. Number Theory **2** (1970), 58–73.

[Knu81] D.E. Knuth, *The art of computer programming, vol. ii: Seminumerical algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

[Lan36] E. Landau, *On a Titchmarsh-Estermann sum*, J. London Math. Soc. **II** (1936), 242–245.

[Leh37] D.H. Lehmer, *On the function $x^2 + x + A$*, Sphinx **6** (1937), 212–214, 1936 and 7:40.

[Len82] H.W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, London Math. Soc. Lecture Note Series **56** (1982), 123–150.

[Lit28] J.E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$*, Proc. London Math. Soc. **27** (1928), 358–372.

[LLS70] D.H. Lehmer, E. Lehmer, and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. **24** (1970), 433–451.

[LPW] R.F. Lukes, C.D. Patterson, and H.C. Williams, *Some results on pseudosquares*, Math. Comp. To appear.

[LPW95] R.F. Lukes, C.D. Patterson, and H.C. Williams, *Numerical sieving devices: Their history and some applications*, Nieuw Archief voor Wiskunde (4) **13** (1995), 113–139.

[Luk95] Richard F. Lukes, *A very fast electronic number sieve*, Ph.D. thesis, University of Manitoba, Winnipeg, Manitoba, 1995.

[MW92] R.A. Mollin and H.C. Williams, *Computation of the class number of a real quadratic field*, Utilitas Mathematica **41** (1992), 259–308.

[Nag22] T. Nagell, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 179–194.

[Oes79] J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée*, Astérisque **61** (1979), 165–167.

[Pol39] L. Poletti, *Au sujet de la décomposition des termes de la série* $z = x^2 + x + 146452961$, Sphinx **9** (1939), 83–85.

[Pol51] L. Poletti, *Il contributo italiano alla tavola dei numeri primi*, Rivista di Matematica della Università di Parma **2** (1951), 417–434.

[Sch93] R. Scheidler, *Applications of algebraic number theory to cryprography*, Ph.D. thesis, University of Manitoba, Winnipeg, Manitoba, 1993.

[Sha60] D. Shanks, *On the conjecture of Hardy and Littlewood concerning the number of primes of the form* $n^2 + a$, Math. Comp. **14** (1960), 320–332.

[Sha63] D. Shanks, *Supplementary data and remarks concerning a Hardy - Littlewood conjecture*, Math. Comp. **17** (1963), 188–193.

[Sha71] D. Shanks, *Class number, a theory of factorization and genera*, Proc. Symp. Pure Math. 20, AMS, Providence, R.I., 1971, pp. 415–440.

[Sha72] D. Shanks, *The infrastructure of real quadratic fields and its applications*, Proc. 1972 Number Theory Conf., Boulder, Colorado, 1972, pp. 217–224.

[Sha73] D. Shanks, *Systematic examination of Littlewood's bounds on* $L(1, \chi)$, Proc. Sympos. Pure Math, AMS, Providence, R.I., 1973, pp. 267–283.

[Sha75] D. Shanks, *Calculation and applications of Epstein zeta functions*, Math. Comp. **29** (1975), 271–287.

[SW88] A.J. Stephens and H.C. Williams, *Computation of real quadratic fields with class number one*, Math. Comp. **51** (1988), 809–824.