UNRAMIFIED ELLIPTIC UNITS

by

Farshid Hajir

B.A., Mathematics
Princeton University, 1988

Submitted to the Department of Mathematics
in Partial Fulfillment of the Requirements for the
Degree of

Doctor of Philosophy
in Mathematics

at the

Massachusetts Institute of Technology
June 1993

©Farshid Hajir 1993, All rights reserved

The author hereby grants to MIT permission to reproduce and to distribute publicly
copies of this thesis document in whole or in part

Signature of Author ____________________________________________

Department of Mathematics
May 13, 1993

Certified by ___________________________________________________

Harold M. Stark
Professor of Mathematics
Thesis Supervisor

Accepted by ___________________________________________________

Professor Sigurdur Helgason
Director of Graduate Studies
UNRAMIFIED ELLIPTIC UNITS

by

Farshid Hajir

Submitted to the Department of Mathematics on May 13, 1993
in partial fulfillment of the requirements for the Degree of
Doctor of Philosophy in Mathematics

Abstract

Let $K$ be an abelian unramified extension of degree $n$ over $k$, a complex quadratic
field with discriminant $-D$ and class number $h$. Let $H$ and $E_K$ be the class number
and unit group of $K$, respectively. If $K$ is not a cyclic extension of $k$, assume that there
are only two roots of unity in $K^*$. We define a subgroup $E_K$ of $E_K$ (by specifying a
minimal set of generators $\varepsilon_1, \ldots, \varepsilon_{n-1}$ for its free part) whose index in $E_K$ is $H/(h/n)$.
The "elliptic units" $\varepsilon_i$ are given explicitly in terms of the Dedekind eta function. An
algorithm for computing the elliptic units and using them to determine the class
number $H$ and a set of fundamental units of $K$ is discussed, with improvements in
the case that $n$ is an odd prime. This algorithm was implemented on a computer to
investigate the parity of $H$ when $h$ is an odd prime less than 23 and $D < 15000$. For
these fields, a table of the minimal polynomial of an elliptic unit whose conjugates
generate $E_K$ is given. An interesting example is the quadratic field with discriminant
$-14947$: the ideal class group of its Hilbert class field contains a subgroup isomorphic
to $(\mathbb{Z}/2\mathbb{Z})^8$.

Thesis Supervisor: Harold M. Stark

Title: Professor of Mathematics
ACKNOWLEDGEMENTS

My first thanks are to my advisor, Harold Stark, who managed to oversee my progress from 3000 miles away: I am very grateful to him for the many trips he made to Boston, and for his hospitality during my visits in San Diego. Anyone familiar with his work will recognize that this thesis owes the light of day to the insights he shared generously with me.

With hindsight, a great benefit of my advisor being away was that I had an excuse to bug Dick Gross from time to time; he has been a great teacher and motivator, one whose enthusiasm for mathematics is contagious. I have been very fortunate to benefit from his advice and his positive view of my work.

I am very grateful to Fernando Rodriguez Villegas who is always full of interesting mathematical ideas, many of which he has generously shared with me. I also learned a lot from Glenn Stevens and other participants of the Boston University Algebra Seminar. I would like to thank Mike Hopkins for his encouragement, advice, and interesting mathematical discussions, as well as his expert analysis of The Simpsons. Many thanks also to Bob MacPherson for enlightening discussions and encouraging words.

It has been a great pleasure for me to teach at MIT: my thanks to the math department for its support, the Interphase program and the Concourse program for giving me the opportunity to teach their students, and to Arthur Mattuck whose exemplary teaching and supervision have had a positive influence on my teaching. The staff of the Undergraduate Math Office, Joanne, John, and Anna, has provided great friendship, advice, and laughs, not to mention lots of colored chalk.

I would like to acknowledge the financial assistance I received from the Starr Foundation, and I thank Phyllis Ruby for her expert guidance regarding the administrative intricacies of MIT.

Fellow graduate students and housemates Matthew, Rick, David, Alan: thanks for teaching me lots of beautiful mathematics and feeding me lots of tasty food. Rick and Alan have to be doubly thanked because they also put up with me at the office. I thank Siman Wong for the many questions he posed and the great many more he answered. Officemate Jim Turner has to be credited with not losing his patience with me after infinitely many interruptions of his work caused by my chatter, and for the semi-permanent loans from the number theory archives of the "Turner Library."

My debt to my parents, whose dedication to my education has been extraordinary and who have sacrificed so much to make it possible, is immense.

Finally, just as my parents are largely responsible for my reaching graduate school, Janice is largely responsible for my completing it, by setting an inspiring example, and sharing in my successes and failures; I thank her for her constant love and support, her jokes, and her culinary wizardry. This thesis is dedicated to her.
"...Out of this grew the idea that the division of elliptic functions with complex multiplication must play the same role, for the corresponding imaginary quadratic fields, as the division of the circle plays for \( \mathbb{Q} \), and that of the lemniscate for \( \mathbb{Q}(i) \)....This, as [Kronecker] wrote later to Dedekind, had been the most cherished dream of his youth ("mein liebster Jugendtraum"; Werke V, p.455).

Frequently this has been taken to mean no more than the extension to imaginary quadratic fields of his existence theorem of 1853 for \( \mathbb{Q} \), or in other words the conjecture that the division of elliptic functions with complex multiplication supplies all the abelian extensions of such fields. But this seems too restrictive an interpretation.

... the conjecture may well have been only part of the dream, perhaps no more than its beginning. It was the whole work of Kummer on the factors of the class-numbers of cyclotomic fields and on their \( p \)-adic properties that he wished to extend to all imaginary quadratic fields and their abelian extensions. Such seems to have been the huge program which Kronecker was planning to carry out ... A whole galaxy of later writers, H. Weber, Fueter, Hasse, Hecke, C. Meyer, Siegel, K. Ramachandra, have taken it up since, perhaps without exhausting even the purely arithmetical problems."

Contents

0.1 Introduction .................................................. 7
0.2 Notation ..................................................... 10

1 Complex Multiplication ......................................... 11
   1.1 Facts from Complex Multiplication ......................... 11
   1.2 Stark's "Algebraic Lemma" ................................ 12
   1.3 An Explicit 12th Root of $\Delta(m)/\Delta(n)$ in $F^*$ .... 13
   1.4 Unit Delta Quotients ...................................... 18
   1.5 Unit Eta Quotients ........................................ 19

2 L-series .......................................................... 21
   2.1 Zeta and L-functions ...................................... 21
   2.2 Imprimitive L-functions .................................... 22
   2.3 Kronecker's Limit Formula .................................. 24
   2.4 Interlude on Stark's Conjecture ......................... 25

3 Cyclic Extensions ................................................. 27
   3.1 The Group Determinant ..................................... 27
   3.2 Transforming $A$ Into A Regulator Matrix .................. 29
   3.3 Reducing the Index ....................................... 31

4 The Main Theorem ................................................ 34
   4.1 Sums of Imprimitive L-functions ......................... 34
   4.2 The S-unit $\delta$ .......................................... 35
   4.3 Making Units from $\delta$ .................................. 36
5 Computational Techniques

5.1 Calculating the Elliptic Units ........................................ 42
  5.1.1 Evaluating the Dedekind Eta Function ......................... 42
  5.1.2 Ideal Bases ...................................................... 43
5.2 Calculating the Index of Elliptic Units .............................. 44
  5.2.1 Checking for $p$th Powers .................................... 44
  5.2.2 The Algorithm .................................................. 45
  5.2.3 An Upper Bound for the Index .................................. 47
5.3 Extensions of Prime Degree .......................................... 47
  5.3.1 $E_K/W_K$ as $\mathcal{O}_t$-module ................................ 47
  5.3.2 Special Minkowski Units ....................................... 48
  5.3.3 The Gras-Gras Lemma .......................................... 48
5.4 Computations and Tables ............................................. 50
  5.4.1 Four Fields of Even Class Number ............................. 50
  5.4.2 Tables .......................................................... 52
0.1 Introduction

This thesis grew out of a need to compute the class number of certain number fields. In general, given a number field $K$, it is a difficult and fundamental problem of algebraic number theory to determine its unit group $E_K$ and its ideal class group $\text{Cl}(K)$, or less ambitiously, its class number $h_K = |\text{Cl}(K)|$. However, if $K$ is a normal extension of $k$ with abelian Galois group $G$, where $k$ is a complex quadratic field, then a large subgroup of $E_K$ (composed of “elliptic units”) is readily available: this goes a long way toward the determination of $h_K$ because if one has an explicit basis for $E_K$, then computing the class number becomes much easier, via the analytic class number formula, for example. Elliptic units are special values of certain modular functions (with origins in the theory of elliptic curves) which are in some sense analogous to the exponential function, which provides “cyclotomic” units in abelian extensions of $\mathbb{Q}$. One feature of the elliptic case which is different from the cyclotomic one is that there exists a rich supply of examples where $K$ is unramified over the base field $k$, (assuming $k$ is not one of the nine complex quadratic fields of class number one). Our aim here is to refine the theory of elliptic units under the assumption that $K$ is an unramified extension of $k$. This leads to results concerning the class number of $K$, including an efficient algorithm for computing it, which at the same time, produces a basis for $E_K$.

Let $k$ be a complex quadratic field of class number $h > 1$ and $K$ a proper abelian unramified extension of $k$, i.e. $k \subset K \subset F$, where $F$ is the Hilbert class field of $k$. One knows that $h_K$ is divisible by $[F : K]$, and that $h_K/[F : K]$ divides $h_F$. It has been known for some time how to define a group of elliptic units of $K$ whose index in $E_K$ is finite. The interesting fact that this index is related to the class number $h_K$ is also well understood: it is an algebraic reflection of analytic properties of the zeta and L-functions associated to number fields (e.g. the analytic class number and Kronecker limit formulae). By virtue of the finiteness of the index, these units can be used to compute $E_K$ and $h_K$.

The elliptic units of $K$ may be expressed as quotients of values of the Dedekind eta function, defined for complex $z$ with positive imaginary part by the convergent product

$$\eta(z) = e^{\pi iz/12} \prod_{n \geq 1} (1 - e^{2\pi inz}).$$

Siegel [Si] has defined elliptic units $\omega_1, \ldots, \omega_{n-1} \in E_K$ which, together with the roots of unity of $K$ generate a subgroup $\Omega$ of $E_K$ of index

$$[E_K : \Omega] = n^{n-2} 12^{n-1} h_K / [F : K].$$

Siegel’s result can be used to compute $h_K$ as follows. If $\alpha$ is an integer of $K$, and the numerical value of all of its conjugates is known with sufficient accuracy, then for any positive integer $m$, one can determine if some $m$th root of $\alpha$ is in $K$ or not. The
elliptic units (and their conjugates) may be approximated via the Fourier expansion of $\eta(z)$. Therefore one may, in principle, determine $[E_K : \Omega]$, and thereby $h_K$, as long as there is an upper bound for this index; the latter is easily obtained, for instance, via standard lower bounds for the regulator of $K$. Using the structure of $E_K$ as a $\mathbb{Z}[G]$-module, one can make this procedure more practical by using ideas of Gras-Gras [Gr].

In practice, however, Siegel’s group often proves unwieldy in computations. For example, one needs to extract many square, cube and $h$th roots just to arrive at the point where one can investigate the divisibility of $h_K$ by 2, 3 and the prime divisors of $h$. Furthermore, and much more significantly, Siegel’s units are “large” in the sense that some of their conjugates are huge, while others of them are very nearly zero, (in other words, their minimal polynomials have large height) forcing us to keep track of many digits, thereby rendering the computations more time-consuming and in some cases impossible.

Our main result is an index formula for a refined (larger) group of elliptic units with an index formula of the same shape as above, but devoid of all “parasitic” factors; for the reasons discussed above, this group is more conducive to efficient computation.

**Theorem 0.1.1** Let $k$ and $K$ be as above, and set $n = [K : k]$. If $K/k$ is not cyclic, assume that the only roots of unity in $K$ are $\pm 1$. Then there exist elliptic units $\varepsilon_1, \ldots, \varepsilon_{n-1}$ in $E_K$ (with explicit expression in terms of the Dedekind eta function) which, together with the roots of unity of $K$, generate a subgroup $E_{K}$ of $E_K$ of index $h_K/[F : K]$. If $K/k$ is cyclic, and the discriminant of $k$ is prime to 6, these units may be chosen in such a way that they are all conjugate to each other over $k$.

Many partial results of this type have been obtained (e.g. [Ra], [Ro1], [Sc], [Gi-Ro], [Ha1]); most notably Kersey [Ku-La, Chapter 9] has found an elliptic group of index $h_K/[F : K]$ for an arbitrary unramified abelian extension $K$ of $k$, however his group (which has rank $n - 1$) is defined as the span of $n(n - 1)/2$ generators, whereas we provide a minimal basis for our elliptic group. From a computational point of view, the difficulties caused by the lack of a minimal basis for the elliptic group are far more unpleasant than those caused by the parasitic factors in Siegel’s index formula.

The main difficulty in the proof of Theorem 0.1.1 is showing that certain combinations of values of $\eta$ are in $F$. In particular, when the discriminant of $k$ is prime to 6, we prove an explicit formula (due to Villegas) for a generator of $a$ (considered as an ideal of $F$) where $a$ is any ideal of $k$ prime to 6. The outline of the proof of Theorem 0.1.1 is classical, i.e. not essentially different from Siegel’s, though the minor variations, such as the evaluation of L-series at $s = 0$ instead of $s = 1$, and the use of imprimitive L-series (both of which have been pioneered by Stark), simplify some of the steps.

When $K/k$ is not cyclic and $D$ is divisible by 2 or 3, our group has an extra factor
of $(W/2)^{n-2}$ in its index, where $W$ is the number of roots of unity in $K$. The present
techniques will hopefully prove to be sufficient for removing this factor.

A program for calculating the elliptic units appearing in the above theorem was
implemented on two different systems. In particular, I investigated the parity of the
class number of the Hilbert class field of complex quadratic fields of odd prime class
number less than 23.

**Theorem 0.1.2** Suppose $k$ is a complex quadratic field with odd prime class number
less than 23. Let $D$ be the absolute value of the discriminant of $k$ and assume $D <
15000$. Then $h_F$ is odd unless $D$ is 283, 331, 643, or 14947. In the first three cases,
h = 3 and Cl$(F)$ is the Klein four group; in the last case, $h = 17$ and the 2-Sylow
subgroup of Cl$(F)$ contains an elementary abelian subgroup of rank 8.

The chapters are organized as follows. Some facts from the theory of complex
multiplication are recalled and used to investigate properties of certain elliptic units.
The main result is the formula of Villegas (Theorem 1.3.2) mentioned above. Its
proof illustrates the use of the reciprocity law of complex multiplication à la Stark.
The second chapter provides the analytic tools (special values of L-series) one needs
to link arithmetic information with the elliptic units. In the third chapter, we treat
the case of cyclic $K/k$, since we can prove slightly more specialized results under that
assumption, while in chapter four, we use the same techniques to prove Theorem 0.1.1
in general. Chapter 5 contains a detailed discussion of algorithms for computing the
elliptic units and using them to determine $h_K$ and fundamental units for $E_K$. A more
efficient algorithm, based on the $\mathbb{Z}[G]$-struture of $E_K$, is discussed when $n$ is an odd
prime. Finally, we provide tables for the minimal polynomial of the elliptic units for
the fields appearing in Theorem 0.1.2.
0.2 Notation

\[ k = \mathbb{Q}(\sqrt{-D}) \] complex quadratic field
\[ -D \] discriminant of \( k \)
\( F \) Hilbert class field of \( k \)
\( K \) abelian unramified extension of \( k, k \subset K \subset F \)
\( G \) \( \text{Gal}(K/k) \)
\( n \) \(|G| = [K : k]\)
\( \mathcal{E}_K \) group of elliptic units
\( K^+ \) a maximal real subfield of \( K \)
\( M \) arbitrary number field
\( \mathcal{O}_M \) ring of integers of \( M \)
\( E_M \) group of units of \( M \), i.e. \( \mathcal{O}_M^* \)
\( \text{Cl}(M) \) the ideal class group of \( M \)
\( h_M \) \(|\text{Cl}(M)| \), class number of \( M \)
\( R_M \) regulator of \( M \)
\( \mathcal{W}_M \) the group of roots of unity in \( M^* \)
\( h \) \( h_k \)
\( H \) \( h_K \)
\( R \) \( R_K \)
\( W \) \(|\mathcal{W}_K| \), the number of roots of unity in \( K^* \)
\( S \) subgroup of \( \text{Cl}(k) \) isomorphic to \( \text{Gal}(F/K) \) under the Artin map
\( \omega \) \((1 + \sqrt{-D})/2 \) for odd \( D \) and \( \sqrt{-D}/4 \) for even \( D \)
\( \sigma \) \( \mathcal{O}_k = [\omega, 1] \)
\( e(z) \) \( \exp(2\pi i z) \)
\( e_m(z) \) \( \exp(2\pi i z/m) \)
\( \ell \) an odd prime
\( 2 \) an even prime
\( \zeta_\ell \) a primitive \( \ell \)th root of 1
\( \mathcal{O}_\ell \) \( \mathbb{Z}[[\zeta_\ell]] \)
\( [a] \) the image of \( a \) in \( \text{Cl}(k) \)
\( \{a\} \) the image of \([a]\) in \( \text{Cl}(k)/S \)
\( \sigma \) the Artin-Frobenius symbol
\( \eta(z) \) Dedekind eta function
\( \Delta(z) \) \( \eta(z)^{24} \)
Chapter 1

Complex Multiplication

1.1 Facts from Complex Multiplication

Fix a complex quadratic field $k$, and let $F$ be its Hilbert class field, i.e. the maximal abelian unramified extension of $k$, which we embed in $\mathbb{C}$. Let $K$ be a subfield of $F$ containing $k$, with relative degree $n = [K : k]$. Let $h = h_k, H = h_K$ be the class number of $k$ and $K$ respectively. Let $R = R_K$ be the regulator of $K$. The number of roots of unity in $K$, call it $\mathcal{W}$, is a divisor of 12 [Ku-La, p.272]. We assume throughout that $K \neq k$, so, in particular, $k$ is not one of the nine complex quadratic fields of class number one, and the only roots of unity in $k$ are $\pm 1$.

Unless the prefix "integral" is used, by "ideal" we shall always mean "fractional ideal." For a prime ideal $\mathfrak{p}$ of $k$, let $\sigma(\mathfrak{p})$ denote the corresponding Frobenius automorphism of $F/k$; it depends only on the ideal class $[\mathfrak{p}]$ of $\mathfrak{p}$ and gives rise to an isomorphism $\sigma : \text{Cl}(k) \cong \text{Gal}(F/k)$. The group $\text{Gal}(F/K)$, when considered as a subgroup of $\text{Gal}(F/k)$, corresponds, via $\sigma^{-1}$, to a subgroup $S$ of $\text{Cl}(k)$, so that $\sigma$ induces an isomorphism $\text{Cl}(k)/S \cong \text{Gal}(K/k)$, which we also denote by $\sigma$. A character $\chi$ of $\text{Gal}(K/k)$, therefore, may be viewed as a character of $\text{Cl}(k)$ which is trivial on $S$. For an ideal $\mathfrak{a}$ of $k$, let $\{\mathfrak{a}\}$ denote the image of $[\mathfrak{a}]$ in $\text{Cl}(k)/S$.

Throughout, we use the abbreviations $e(z) = \exp(2\pi i z), e_m(z) = e(z/m)$.

For an ideal $\mathfrak{b}$ of $k$, with $\mathbb{Z}$-basis $[\omega_1, \omega_2]$, satisfying $\Im(\frac{\omega_1}{\omega_2}) > 0$, define

$$\Delta(b) = \left(\frac{2\pi}{\omega_2}\right)^{12} \Delta\left(\frac{\omega_1}{\omega_2}\right),$$

where

$$\Delta(z) = \eta(z)^{24},$$

and

$$\eta(z) = e(z/24) \prod_{m \geq 1} (1 - e(mz)).$$
It is well known that $\Delta(z)$ does not vanish on the upper half plane and is a modular form of weight 12 for $SL(2, \mathbb{Z})$. Thus, $\Delta(b)$ does not depend on the choice of basis. We recall the following facts from the theory of complex multiplication [St].

**Lemma 1.1.1** For any pair of ideals $m, n$ of $k$, $\alpha = \Delta(m)/\Delta(n)$ is in $F^*$ and generates the ideal $(\alpha)O_F = (n/m)^{12}$. The conjugates of $\alpha$ are given explicitly by the reciprocity law:

$$\left(\frac{\Delta(m)}{\Delta(n)}\right)^\sigma(a) = \frac{\Delta(ma)}{\Delta(na)},$$

for any ideal $a$ of $k$.

### 1.2 Stark’s “Algebraic Lemma”

**Lemma 1.2.1** Let $m$ be a positive integer. Let $\bar{K}/k$ be an abelian extension with conductor $\mathfrak{f}$. Let $\bar{W}$ be the number of roots of unity in $\bar{K}$. Suppose that $\delta \neq 0$ is a number such that $\alpha = \delta^m$ is in $\bar{K}$ and $\bar{K}(\delta)$ is abelian over $k$. If $q$ is a prime ideal of $k$ of norm $q$ relatively prime to $ma\mathfrak{f}$, then $\alpha^q / \alpha^{\sigma(q)}$ and $\alpha^{(\bar{W}, m)}$ are $m$th powers in $\bar{K}$ itself, where $\sigma(q)$ denotes the Frobenius automorphism of $q$ in $\bar{K}/k$.

**Proof.** This is (a weak version of) [St, Lemma 6].

**Lemma 1.2.2** With $\alpha$ as in Lemma 1.1.1, let $\beta = N_{\bar{K}/K}(\alpha)$. For $p$ any prime ideal of $k$ of degree one and norm $p$ prime to $6Dmn$,

(i) $\beta$ is a square in $K^*$;

(ii) $\beta^W$ is a 24th power in $K^*$;

(iii) $\beta^p / \beta^{\sigma(p)}$ is a 24th power in $K^*$;

(iv) $(\beta / \beta^{\sigma(p)})^W$ is a 48th power in $K^*$;

(v) if 4 does not divide $W$, then $(\beta / \beta^{\sigma(p)})^{W/2}$ is a 24th power in $K^*$.

**Proof.** For (i), see [Ku-La, p.238]. The key fact (see [St]) is that when $m,n$ are ideals of $k$, adjoining any 24th root of $\Delta(m)/\Delta(n)$ to $k$ yields an abelian extension of $k$. Then, (ii) and (iii) are immediate consequences of Lemma 1.2.1. Since $p$ is odd and $W$ is even, $(\beta^p / \beta^{\sigma})^W$ and $\beta^{W(1-p)}$ are 48th powers in $K^*$. Part (iv) follows because $(\beta / \beta^{\sigma(p)})^W$ is the product of these numbers. Assume (v) is false, so that
\(-\left(\frac{\beta}{\beta^p}\right)^{W/2}\) is a 24th power in \(K^*\). But by (i), \(\beta/\beta^p\) is a square in \(K^*\), so this exhibits \(-1\) as a square in \(K^*\), contradicting the assumption that 4 does not divide \(\mathcal{W}\).

1.3 An Explicit 12th Root of \(\Delta(m)/\Delta(n)\) in \(F^*\)

Recall that \(F\), the Hilbert class field of \(k\), is embedded in \(\mathbb{C}\). In the last section, we saw that \(\Delta(m)/\Delta(n)\) is in \(F^{*r}\) for some \(r \geq 2\) dividing 24. As will be clear from the proof of the theorem in this section, once this is known, finding which \(r\)th root lies in \(F^*\) requires only a single application of the reciprocity law of complex multiplication, which, using Stark’s formulation for example, is easy to carry out. Under the assumption that the discriminant of \(k\) is prime to 6, it is even possible to write down a simple, explicit formula for a 12th root of \(\Delta(m)/\Delta(n)\) in \(F^*\). This formula is due to Villegas [Vi] though the proof given here is different from his. I would like to express my thanks for his permission to include this formula here. Finally, Robert [Ro2] has provided an alternate recipe for determining which roots of \(\Delta\)-quotients land in the Hilbert class field.

Assumption. Throughout this section, we take \(K = F\), and assume that the discriminant \(-D\) of the complex quadratic field \(k\) is prime to 6, so that \(\mathcal{W} = 2\).

Definition 1.3.1 (Villegas) Suppose \(m\) is a primitive (i.e., not divisible by a rational integer \(> 1\)) integral ideal of \(k\) of norm \(m\) prime to \(6D\), with \(\mathcal{I}\)-basis \([\omega - t, m]\) for some integer \(t\) and \(\omega = (1 + \sqrt{-D})/2\). Let \(\mathfrak{o} = [\omega, 1]\) be the ring of integers of \(k\). For \(m\) as above, set

\[
\eta(m) = e_{24}(m(2 - t)) \eta\left(\frac{t - \overline{\omega}}{m}\right),
\]

and

\[
\overline{\eta}(m) = e_{24}(m(t - 2)) \eta\left(\frac{\omega - t}{m}\right).
\]

Using the modular property: \(\eta(z + 1) = e_{24}(1)\eta(z)\), and the fact that \(m^2 \equiv 1 \mod 24\), it is easy to see that the above definition is independent of the choice of \(t\).

Theorem 1.3.2 With the above assumptions on \(D\) and \(m\),

\[
\left(\frac{\eta(m)}{\eta(\mathfrak{o})}\right)^2 \in F^*.
\]

and its 12th power is \(m^{12}\Delta(\mathfrak{m})/\Delta(\mathfrak{o})\).
<table>
<thead>
<tr>
<th>$D \mod 48$</th>
<th>$r$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7$</td>
<td>$3-2t$</td>
<td>$2$</td>
</tr>
<tr>
<td>$11$</td>
<td>$8-t$</td>
<td>$1$</td>
</tr>
<tr>
<td>$19$</td>
<td>$10-t$</td>
<td>$1$</td>
</tr>
<tr>
<td>$23$</td>
<td>$1-2t$</td>
<td>$2$</td>
</tr>
<tr>
<td>$31$</td>
<td>$3-2t$</td>
<td>$2$</td>
</tr>
<tr>
<td>$35$</td>
<td>$11-t$</td>
<td>$1$</td>
</tr>
<tr>
<td>$43$</td>
<td>$-t$</td>
<td>$1$</td>
</tr>
<tr>
<td>$47$</td>
<td>$1-2t$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

Table 1

Proof. Define $\theta = t - \omega$ and $N = N(\theta) = t^2 - t + (1 + D)/4$. Note that $m$ divides $N$. Let $g(z) = \eta(z/m)/\eta(z)$ and $f(z) = g(z)^2$. If one uses the basis $\sigma = [\omega - t, 1]$,

$$
\left( \frac{\eta(m)}{\eta(\sigma)} \right)^2 = e_{12}((m - 1)(2 - t))f(\theta).
$$

By Lemma 1.2.2, $(\Delta(\overline{m})/\Delta(\sigma))^2$ is a 24th power in $F^*$ and $\Delta(\overline{m})/\Delta(\sigma)$ is a square in $F^*$. Since $W = 2$, it follows that some twelfth root $\delta$ of $\Delta(\overline{m})/\Delta(\sigma)$ is in $F^*$. If we now let $\alpha = \delta m$, it is an immediate consequence of the definition of $\Delta$ that for some integer $\ell$,

$$
\alpha = e_{12}(\ell)f(\theta).
$$

Since $\pm \alpha \in F^*$, to prove the theorem it suffices to prove that

$$
2\ell \equiv 2(m - 1)(2 - t) \mod 12. \tag{1.1}
$$

We do this by computing the action on $\alpha$ of the Frobenius automorphism of some principal prime ideal of norm $\equiv 11 \mod 12$, using [St, Theorem 3]. We can always find an integer $\kappa_0 = r_0 + s_0\theta$ with $s_0 \neq 0$ such that $N(\kappa_0) \equiv 11 \mod 12$. There are then infinitely many $\kappa = r + s\theta$ such that $(r, s) \equiv (r_0, s_0) \mod 12$ and $(\kappa)$ is a prime ideal of norm $q \equiv 11 \mod 12$ so we may even choose $q$ to be prime to $a$. Some appropriate choices of $r, s \mod 12$ for each equivalence class of $D$ modulo 48 are given in Table 1. According to [St, Theorem 3],

$$
\alpha^{\sigma((\kappa))} = e_{12}(\ell q)(f \circ qB^{-1})(\theta),
$$

where

$$
B = \begin{pmatrix} r & sN \\ -s & r + s(2t - 1) \end{pmatrix},
$$

$$
qB^{-1} = \begin{pmatrix} r + s(2t - 1) & -sN \\ s & r \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} r + s(2t - 1) & -sN \\ sq^* & rq^* \end{pmatrix} \mod 24m,
$$

\[\text{14}\]
where $q^*$ is any integer satisfying $qq^* \equiv 1 \mod 24m$. Let $\Gamma^0(m)$ be the group of integral $2 \times 2$ matrices \[
\begin{pmatrix} a & b \\ c & d \end{pmatrix}\] that satisfy \(b \equiv 0 \mod m\), and \(ad \equiv 1 \mod m\).

**Lemma 1.3.3** If \(U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(m)\), then

\[(g \circ U)(z) = \epsilon e_{24}(j)g(z),\]

and

\[(f \circ U)(z) = e_{12}(j)f(z),\]

where

\[
\epsilon = \begin{cases} 
\left( \frac{d}{c} \right) \left( \frac{d}{cm} \right) & \text{if } c \text{ is odd and positive} \\
\left( \frac{c}{d} \right) \left( \frac{cm}{d} \right) & \text{if } d \text{ is odd and positive}
\end{cases}
\]

(\(\left( \frac{\cdot}{\cdot} \right)\) denotes the Jacobi Symbol with \(\left( \frac{9}{1} \right) = 1\)), and the value of \(j = j_U \mod 24\) is given by:

\[
j = \begin{cases} 
(m - 1)[c(d + a - 3) - bmd(mc^2 + 1)] & \text{if } c \text{ is odd and positive} \\
(m - 1)[-d(c + bm) - (d^2 - 1)ac] & \text{if } d \text{ is odd and positive}
\end{cases}
\]

**Proof.** Let \(U' = \begin{pmatrix} a & b/m \\ cm & d \end{pmatrix}\). Then

\[
(g \circ U)(z) = \frac{\eta \left( \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \right) \circ z}{\eta(U \circ z)}
= \frac{\xi(U', z/m)}{\xi(U, z)}g(z),
\]

where \(\xi(Y, z) = \eta(Y \circ z)/\eta(z)\) for an integral matrix \(Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}\) of determinant 1 is given explicitly by Weber [We, p. 126]:

\[
\xi(Y, z) = \begin{cases} 
\left( \frac{y_4}{y_3} \right) e_{24}(v_1) \sqrt{e_{24}(3)(y_3z + y_4)} & \text{if } y_3 \text{ is odd and positive} \\
\left( \frac{y_3}{y_4} \right) e_{24}(v_2) \sqrt{y_3z + y_4} & \text{if } y_4 \text{ is odd and positive}
\end{cases}
\]

where

\[
v_1 = 3 + y_3(y_4 + y_1 - 3) - (y_3^2 - 1)y_2y_4 \\
v_2 = -3 + y_4(y_2 - y_3 + 3) + (y_4^2 - 1)y_1y_3.
\]

The square root here is the usual branch with non-negative real part. The lemma follows easily.
Lemma 1.3.4 The function $f(z)$ is invariant under $\Gamma(6m)$.

Proof. This follows easily from the above lemma.

Let $A$ be the following matrix:

$$
A = \begin{pmatrix}
    r + s(2t - 1) & -sN \\
    sq^* & rq^*
\end{pmatrix}.
$$

If $A \equiv U \mod 6m$ for $U \in \Gamma^0(m)$, then $f \circ A = f \circ U$. Since $f$ has rational Fourier coefficients,

$$(f \circ qB^{-1})(z) = (f \circ A)(z).$$

Since $\alpha \in F$, we know that $\alpha = \alpha^{e((\tau))}$. Therefore,

$$e_{12}(\ell)f(\theta) = e_{12}(\ell q)e_{12}(j)f(\theta),$$

where $j = j_A$ is given by the lemma. It then follows that

$$2\ell \equiv j \mod 12$$

since $q \equiv 11 \mod 12$. We see from (1.1) that the theorem will follow once we establish:

$$j \equiv 2(m - 1)(2 - t) \mod 12. \tag{1.2}$$

Now using the values of $r, s$ in the above table, we compute $j$ from the lemma and verify (1.2) in each case. Note that since the value of $j$ is only determined modulo 12, we may replace the $q^*$ in $A$ with $q$ when we compute $j_A$. First, consider the four cases where $s = 1$:

$$j \equiv (m - 1)[-(-r + r + 2t - 1 - 3)] + (m - 1)[-bmd(m + 1)] \mod 12$$

$$\equiv (m - 1)(4 - 2t) \mod 12,$$

the second congruence following from the useful fact that $m^2 \equiv 1 \mod 24$. When $s = 2$,

$$j \equiv 2(m - 1)[2 - 4t - 2r - mNr - 2r^2 + 4tr^2 + r^3] \mod 12$$

$$\equiv 2(m - 1)(2 - t) + 2(m - 1)[r^3 + (4t - 2)r^2 - r(mN + 2)] \mod 12.$$

In all cases, the second term in the above sum is congruent to 0 modulo 12 because

$$r^3 + (4t - 2)r^2 - r(mN + 2) \equiv \begin{cases}
    (m + 1)(2t^3 + t^2 + t) \mod 3 & \text{if } D \equiv 7 \mod 24 \\
    (m + 1)(2t^3 + t) \mod 3 & \text{if } D \equiv 23 \mod 24
\end{cases}.$$

This completes the proof of the theorem.

16
Corollary 1.3.5 With $D$ and $m$ as above,

$$
\left( \frac{\eta(m)}{\eta(o)} \right)^2 \in F^*,
$$

and its 12th power is $m^{12}\Delta(m)/\Delta(o)$.

**Proof.** It is enough to note that since $\eta(z) = \eta(-z)$, $\eta(m) = \eta(m)$.

Corollary 1.3.6 With $D$ and $m$ as above, $(\eta(m)/\eta(o))^2$ and $(\eta(m)/\eta(o))^2$ are generators of $m\mathcal{O}_F$ and $\bar{m}\mathcal{O}_F$, respectively.

**Proof.** This is clear from the proof of Theorem 1.3.2.

Another measure of the naturality of Villegas' eta-quotients is that they transform nicely under the Frobenius automorphism.

Lemma 1.3.7 Let $q$ and $m$ (of norm $q$ and $m$, respectively) be integral ideals of $k$ prime to $6D$ such that $mq$ and $m\bar{q}$ are primitive. Let $\sigma(q)$ denote the Frobenius automorphism of $q$ in $\text{Gal}(k^a/k)$. Then

$$
\left( \frac{\eta(m)}{\eta(o)} \right)^{\sigma(q)} = \frac{\eta(mq)}{\eta(q)},
$$

$$
\left( \frac{\eta(m)}{\eta(o)} \right)^{\sigma(q)} = \frac{\eta(m\bar{q})}{\eta(\bar{q})}.
$$

**Proof.** This is another exercise in the use of the reciprocity law [St, Theorem 3]. Of course, the two formulations are equivalent. Let us use the first one. Since $\sigma$ is multiplicative, we may assume without loss of generality that $q$ is a prime ideal. Choose a basis of the form $[\omega - t, mq]$ for $mq$ so that $[\omega - t, m]$ and $[\omega - t, q]$ are bases for $m$ and $q$, respectively. Let $\theta = t - \bar{\omega}$ and recall that $g(z) = \eta(z/m)/\eta(z)$. Then

$$
\eta(mq) = e_{24}\left[ q(2 - t)(m - 1) \right] g(\theta/q),
$$

$$
\eta(m) = e_{24}\left[ (2 - t)(m - 1) \right] g(\theta).
$$

When we apply the reciprocity law, we find:

$$
\left( \frac{\eta(m)}{\eta(o)} \right)^{\sigma(q)} = e_{24}\left[ q(2 - t)(m - 1) \right] g(\theta)(g \circ qB^{-1})(B \circ \theta)
$$

17
with
\[ B = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}, \quad qB^{-1} = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}. \]

Writing
\[ qB^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & q^* \end{pmatrix} \pmod{24m}, \]

we note once again that \( \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \) acts trivially on \( g(z) \) and in fact so does \( \begin{pmatrix} q & 0 \\ 0 & q^* \end{pmatrix} \), as is easily seen from Lemma 1.3.3 (using \( q^* \equiv q \pmod{24} \)). In conclusion,
\[ (g \circ qB^{-1})(z) = g(z). \]

The lemma follows since \( B \circ \theta = \theta/q \).

### 1.4 Unit Delta Quotients

We now define and explore basic properties of some units in the Hilbert class field expressed as product of \( \Delta \)-quotients.

**Lemma 1.4.1** Suppose \( m, n \) are ideals of \( k \) with \( [m] = [n] \). Then \( \Delta(m)/\Delta(n) \in k^* \).

**Proof.** Write \( m = (\alpha)n \), with \( \alpha \in k^* \). Then, \( \Delta(m)/\Delta(n) = \alpha^{-12} \).

**Lemma 1.4.2** If \( [b] \in S \), then \( N_{F/K}(\Delta(o)/\Delta(b)) \in k^* \).

**Proof.** Say \([m_1], \ldots, [m_{h/n}]\) are the elements of \( S \). Then so are \([bm_1], \ldots, [bm_{h/n}]\). Hence the product
\[ N_{F/K} \frac{\Delta(o)}{\Delta(b)} = \prod_{j=1}^{h/n} \frac{\Delta(m_j)}{\Delta(bm_j)}, \]
can be rearranged into a product of terms like \( \Delta(m)/\Delta(n) \) with \( [m] = [n] \). Therefore the lemma is reduced to the previous one.

**Definition 1.4.3** For ideals \( a_1, \ldots, a_r \) of \( k \), write \( \sigma_i = \sigma(\{\bar{a}_i\}) \in \text{Gal}(K/k) \) for \( i = 1, \ldots, r \). Let
\[ V(a_1, \ldots, a_r) = N_{F/K} \frac{\Delta(a_1) \cdots \Delta(a_r)}{\Delta(o)^{r-1} \Delta(a_1 \cdots a_r)}. \]
Lemma 1.4.4  (i) \( V(a_1, \ldots, a_r) = \)
\[
\left( N_{F/K} \frac{\Delta(a_1)}{\Delta(o)} \right)^{1-\sigma_2} \left( N_{F/K} \frac{\Delta(a_1a_2)}{\Delta(o)} \right)^{1-\sigma_3} \cdots \left( N_{F/K} \frac{\Delta(a_1 \cdots a_{r-1})}{\Delta(o)} \right)^{1-\sigma_r};
\]

(ii) \( V(a_1, \ldots, a_r) \in E_K \) and \( N_{K/k} V(a_1, \ldots, a_r) = 1; \)

(iii) \( V(a_1, \ldots, a_r)^W \in E_{K^2}; \) if \( W = 2, V(a_1, \ldots, a_r) \in E_K^2; \)

(iv) If \( a'_1, \ldots, a'_r \) are ideals of \( k, \) satisfying \( \{a'_i\} = \{a_i\} \) for \( i = 1, \ldots, r, \) then
\[
V(a'_1, \ldots, a'_r) = V(a_1, \ldots, a_r).
\]

Proof. (i) Apply Lemma 1.1.1 and multiply out the telescoping product. (ii) is clear from Lemma 1.1.1 and (i). (iii) is a direct consequence of Lemma 1.2.2 applied to each term appearing in (i). For (iv), note that, by (i), the general case is reduced to \( r = 2 \) (\( r = 1 \) being trivial). Write \( a'_i = a_i b_i \) with \([b_i] \in S\). Then
\[
\frac{V(a_1, a_2)}{V(a'_1, a'_2)} = \left( \frac{N_{F/K} \Delta(a_1)}{\Delta(a'_1)} \right)^{1-\sigma_2}
= \left( \frac{N_{F/K} \Delta(o)}{\Delta(b_1)} \right)^{(1-\sigma_2)^{\sigma_1}}
= 1,
\]
because \( N_{F/K}(\Delta(o)/\Delta(b_1)) \in k^* \) by Lemma 1.4.2.

1.5 Unit Eta Quotients

In this section, we assume that \( D \) is prime to 6. Our goal is to write down an explicit 24th root of \( V. \)

Lemma 1.5.1 Suppose \( a, b \) are integral ideals of \( k \) prime to \( 6D \) such that \( ab \) is primitive. Let \( \sigma \) be as in Lemma 1.3.7. Then,
\[
\left( \frac{\overline{\eta}(a)}{\overline{\eta}(o)} \right)^{1-\sigma(b)} = \frac{\overline{\eta}(a)\overline{\eta}(b)}{\overline{\eta}(o)\overline{\eta}(ab)} \in E_F,
\]

and
\[
\left( \frac{\overline{\eta}(a)\overline{\eta}(b)}{\overline{\eta}(o)\overline{\eta}(ab)} \right)^{24} = \left( \frac{\Delta(a)}{\Delta(o)} \right)^{1-\sigma(b)}.
\]
Proof. Let $\alpha = \overline{\eta}(a)/\overline{\eta}(\sigma)$. By Theorem 1.3.2, $\alpha^2 \in F^*$, and $\alpha^{24} = N_{A^2}(a)/\Delta(a)$. By Lemma 1.3.7,

$$\alpha^{1-\sigma(\delta)} = \frac{\overline{\eta}(a)\overline{\eta}(b)}{\overline{\eta}(\sigma)\overline{\eta}(ab)},$$

hence $(\alpha^{1-\sigma(\delta)})^2 \in E_F$ and its 24th power is $(\Delta(a)/\Delta^{(a)})^{1-\sigma(\delta)}$. Thus, it remains only to show that $(\alpha^{1-\sigma(\delta)})^2$ is a square in $F^*$. By Lemma 1.2.2, $(\Delta(a)/\Delta^{(a)})^{1-\sigma(\delta)}$ is the 24th power of some $\beta \in F^*$, therefore $\alpha^{1-\sigma(\delta)} = \zeta / \beta$ for some 24th root of unity $\zeta$. But

$$\left(\frac{\alpha^{1-\sigma(\delta)}}{\beta}\right)^2 = \zeta^2 \in F^*,$$

hence $\zeta = \pm 1$ (recall that $W = 2$ since $D$ is prime to 6), and $\alpha^{1-\sigma(\delta)} = \pm \beta \in F^*$.

**Lemma 1.5.2** Suppose $a_1, \ldots, a_r$ are integral ideals of $k$ prime to $6D$ such that $a_1 \cdots a_r$ is primitive. Let $\sigma$ be as in Lemma 1.3.7. Then,

$$\frac{\overline{\eta}(a_1) \cdots \overline{\eta}(a_r)}{\overline{\eta}(\sigma)^{(r-1)}} = \frac{\overline{\eta}(a_1) \cdots \overline{\eta}(a_r)}{\overline{\eta}(\sigma)} \in E_F.$$  

**Proof.** The equality is easily checked by using Lemma 1.3.7 to expand the right hand side into a telescoping product. Then, each of the terms in the product is in $E_F$ by the previous lemma.

**Definition 1.5.3** For integral ideals $a_1, \ldots, a_r$ of $k$, prime to $6D$, and such that $a_1 \cdots a_r$ is primitive, let

$$v(a_1, \ldots, a_r) = N_{K^F}(\overline{\eta}(a_1) \cdots \overline{\eta}(a_r))/\overline{\eta}(\sigma)^{(r-1)}.$$  

**Lemma 1.5.4** (i) $v(a_1, \ldots, a_r)^{24} = V(a_1, \ldots, a_r)$. (ii) If $a'_1, \ldots, a'_r$ are ideals of $k$, satisfying $\{a'_i\} = \{a_i\}$ for $i = 1, \ldots, r$, then

$$v(a'_1, \ldots, a'_r) = v(a_1, \ldots, a_r).$$  

**Proof.** (i) is clear from Lemma 1.5.2 and Lemma 1.4.4. The proof of (ii) is exactly analogous to that of Lemma 1.4.4.iv and is left to the reader.
Chapter 2

L-series

2.1 Zeta and L-functions

For an arbitrary number field $M$, with $r_1$ real and $r_2$ pairs of complex conjugate embeddings, let $O_M, \text{Cl}(M), h_M, R_M, \mathcal{W}_M$ and $w_M$ denote the ring of integers, ideal class group, class number, regulator, and the group of roots of unity of $M$, respectively. Let $w_M$ be the cardinality of $\mathcal{W}_M$. For an ideal class $C$ of $M$, and complex $s$ with $\Re(s) > 1$, the partial zeta function is defined by

$$\zeta_M(s, C) = \sum_{a \subseteq O_M, [a] = C} N(a)^{-s},$$

where the sum is over non-zero integral ideals $a$ of $k$, $[a]$ is the ideal class of $a$, and $N$ denotes the absolute norm; it has a meromorphic continuation to the complex plane. For a character $\chi$ of the class group $\text{Cl}(M)$, we define the L-function

$$L(s, \chi) = \sum_{C \in \text{Cl}(M)} \chi(C)\zeta_M(s, C).$$

Finally, for the trivial character $\chi_1$, $L(s, \chi_1)$ is the Dedekind zeta function of $M$, denoted by $\zeta_M(s)$. We continue to use the abbreviation $e(z) = \exp(2\pi iz)$.

The work of Dirichlet and Dedekind on zeta functions culminated in the determination of the first non-zero term in the Taylor expansion of $\zeta_M(s, C)$ at $s = 1$. Hecke’s functional equation allows one to carry out the expansion at $s = 0$:

$$\zeta_M(s, C) = -\frac{R_M}{w_M} s^{r_1 + r_2 - 1} + O(s^{r_1 + r_2}). \quad (2.1)$$

Since the leading term is independent of the ideal class $C$,

$$\zeta_M(s) = -\frac{h_M R_M}{w_M} s^{r_1 + r_2 - 1} + O(s^{r_1 + r_2}). \quad (2.2)$$

Let $k, F, K, R, W$ be as in chapter one.
Definition 2.1.1 For an ideal class $C$ of $k$, let $\lambda(C) = \zeta_k(0, C)$.

Lemma 2.1.2 With the above notation,

$$-\frac{HR}{W} = L(0, \chi_1) \prod_{\chi \neq \chi_1} L'(0, \chi),$$

(2.3)

where the product is over those non-trivial characters $\chi$ of $\text{Cl}(k)$ which are trivial on $S$.

Proof. Class field theory furnishes the factorization of the Dedekind zeta function of $K$ into $L$-functions:

$$\zeta_K(s) = \prod_{\chi} L(s, \chi).$$

(2.4)

Here, and in all that is to follow, $\prod_{\chi}$ means the product over all $n$ characters of $\text{Cl}(k)$ which are trivial on $S$. Applying (2.1) and (2.2) to $k$, and $K$, respectively, we obtain:

$$\zeta_k(s, C) = -\frac{1}{2} + \lambda(C)s + O(s^2)$$

(2.5)

and

$$\zeta_K(s) = -\frac{HR}{W} s^{n-1} + O(s^n).$$

(2.6)

Using (2.5) and the orthogonality relation of characters, we get an expansion for the $L$-functions of $k$:

$$L(s, \chi) = \begin{cases} 
-\frac{1}{2} + O(s) & \text{if } \chi = \chi_1 \\
\left(\sum_{C \in \text{Cl}(k)} \chi(C)\lambda(C)\right)s + O(s^2) & \text{if } \chi \neq \chi_1
\end{cases}$$

(2.7)

Finally if we use (2.6) and (2.7) to expand the right and left hand sides of (2.4) at $s = 0$ and equate the coefficients of $s^{n-1}$, we arrive at the desired result.

2.2 Imprimitive L-functions

Recall that for an ideal $a$ of $k$, $[a]$ denotes the ideal class of $a$ in $\text{Cl}(k)$, and $\{a\}$ denotes the image of $[a]$ in $\text{Cl}(k)/S$. Throughout this chapter, $p$ denotes an arbitrary prime ideal of $k$.

It will be extremely advantageous to modify the $L$-functions slightly so that they all vanish at $s = 0$. In addition, the expression for the derivative of the $L$-functions at 0 coming from the Kronecker limit formula will be greatly simplified as a result of
this modification. For any character $\chi$ of $\text{Cl}(k)$, and any prime ideal $p$ of $k$, define

$$L(s, \chi, p) = L(s, \chi) \left(1 - \chi([p])Np^{-s}\right).$$

This is the imprimitive $L$-function attached to $\chi$ viewed as a ray class character modulo $p$. It is clear that $L(0, \chi, p) = 0$ for all $\chi$, including $\chi_1$, and

$$L'(0, \chi, p) = \begin{cases} L(0, \chi_1) \log Np & \text{if } \chi = \chi_1, \\ L'(0, \chi)(1 - \chi([p])) & \text{if } \chi \neq \chi_1. \end{cases} \quad (2.8)$$

Recall that $\lambda(C) = \zeta_k(0, C)$, and define

$$\lambda(C, p) = \lambda(C) - \lambda(C[p]^{-1}) - \frac{1}{2} \log Np, \quad (2.9)$$

$$\lambda_k(\{C\}, p) = \sum_{C' \in S} \lambda(CC', p). \quad (2.10)$$

**Lemma 2.2.1** (i) For all $\chi$,

$$L'(0, \chi, p) = \sum_{C \in \text{Cl}(k)} \chi(C)\lambda(C, p);$$

(ii) For those $\chi$ which are trivial on $S$,

$$L'(0, \chi, p) = \sum_{\{C\} \in \text{Cl}(k)/S} \chi(\{C\})\lambda_k(\{C\}, p).$$

**Proof.** Using the definition of $L(s, \chi)$, and expanding the Euler $p$-factor $1 - \chi([p])Np^{-s}$ as $1 - \chi([p])(1 - s \log Np + O(s^2))$, the Taylor expansion of $L(s, \chi, p)$ at $s = 0$ may be written:

$$L(s, \chi, p) = \sum_{C \in \text{Cl}(k)} \chi(C) \left[\zeta_k(s, C) - \zeta_k(s, C[p]^{-1}) + s\zeta_k(s, C[p]^{-1}) \log Np\right] + O(s^2).$$

Evaluating the derivative at $s = 0$ is then a simple matter:

$$L'(0, \chi, p) = \sum_{C \in \text{Cl}(k)} \chi(C) \left[\zeta_k(0, C) - \zeta_k(0, C[p]^{-1}) + \zeta_k(0, C[p]^{-1}) \log Np\right].$$

Since by (2.5), $\zeta_k(0, C') = -1/2$ for any class $C' \in \text{Cl}(k)$, we have:

$$L'(0, \chi, p) = \sum_{C \in \text{Cl}(k)} \chi(C) \lambda(C) - \lambda(C[p]^{-1}) - \frac{1}{2} \log Np$$

$$= \sum_{C \in \text{Cl}(k)} \chi(C)\lambda(C, p).$$
For a character $\chi$ which is trivial on $S$, we may rewrite the above sum as a sum over $\text{Cl}(k)/S$ as follows:

$$L'(0, \chi, p) = \sum_{\{C\} \in \text{Cl}(k)/S} \chi(\{C\}) \sum_{C' \in S} \lambda(CC', p)$$

$$= \sum_{\{C\} \in \text{Cl}(k)/S} \chi(\{C\}) \lambda_K(\{C\}, p).$$

(2.11)

2.3 Kronecker’s Limit Formula

Kronecker’s first limit formula provides the key link between L-series (whose special values are related to the arithmetic invariants of $K$) and elliptic modular functions whose special values are numbers in $K^*$.

**Lemma 2.3.1 (Kronecker’s First Limit Formula)** For any $C \in \text{Cl}(k)$,

$$\lambda(C) = -\frac{1}{24} \log \left| \mathcal{N}(b)^6 \Delta(b) \right|^2$$

where $b$ is any ideal of $k$ with $[b] = C^{-1}$.

For a proof, see [Si] or [St]. The left hand side shows that the right hand side is independent of the choice of the ideal $b$ in $C^{-1}$, which can also be checked via the modular properties of $\Delta$.

**Lemma 2.3.2** Whenever $[b] = C^{-1}$,

$$\lambda_K(\{C\}, p) = -\frac{1}{24} \log \left| \mathcal{N}_{F/K} \left( \frac{\Delta(b)}{\Delta(bp)} \right) \right|^2$$

$$= -\frac{1}{24} \log \left| \mathcal{N}_{F/K} \left( \frac{\Delta(o)}{\Delta(p)} \right) \right|^{\sigma(C)}.$$

**Proof.** We apply the limit formula (Lemma 2.3.1) to compute $\lambda(C, p)$ and $\lambda_K(\{C\}, p)$, defined in (2.9) and (2.10):

$$\lambda(C, p) = -\frac{1}{24} \log \left| \mathcal{N}(b)^6 \Delta(b) \right|^2 + \frac{1}{24} \log \left| \mathcal{N}(bp)^6 \Delta(bp) \right|^2 - \frac{1}{24} \log \left| \mathcal{N}p^6 \right|^2$$

$$= -\frac{1}{24} \log \left| \frac{\Delta(b)}{\Delta(bp)} \right|^2,$$
and

\[ \lambda_K(\{C\}, p) = \sum_{C' \in S} -\frac{1}{24} \log \left| \frac{\Delta(bb')}{\Delta(bb'p)} \right|^2 \]

\[ = -\frac{1}{24} \log \left| \prod_{C' \in S} \frac{\Delta(bb')}{\Delta(bb'p)} \right|^2, \quad (2.12) \]

with \([b] = C^{-1}\) and \([b'] = C'^{-1}\). Next, we use Lemma 1.1.1 to investigate the \(\Delta\)-quotient in (2.12):

\[ \frac{\Delta(bb')}{\Delta(bb'p)} = \left( \frac{\Delta(b)}{\Delta(bp)} \right)^{\sigma(b')} = \left( \frac{\Delta(b)}{\Delta(bp)} \right)^{\sigma(C')} \]

since \([b'] = [b']^{-1} = C'\). Recalling that \(\sigma\) maps \(S\) isomorphically to \(\text{Gal}(F/K)\), we recognize the expression appearing inside the absolute values in (2.12) as a relative norm from \(F\) to \(K\):

\[ \prod_{C' \in S} \frac{\Delta(bb')}{\Delta(bb'p)} = \prod_{C' \in S} \left( \frac{\Delta(b)}{\Delta(bp)} \right)^{\sigma(C')} = \mathcal{N}_{F/K} \left( \frac{\Delta(b)}{\Delta(p)} \right) = \mathcal{N}_{F/K} \left( \frac{\Delta(\phi)}{\Delta(p)} \right)^{\sigma(C')} \]

The lemma is proved.

2.4 Interlude on Stark’s Conjecture

The results of this section are essentially known, and proved in [St]. They concern Stark’s conjecture in the only case where an auxiliary prime must be added to the set \(S_\infty\) in order for the conjecture to make sense, namely with \(K\) an abelian unramified extension of a complex quadratic field \(k\). We give a slightly different formulation for the units involved, and point out the connection with the index formulae to be proved in subsequent chapters. For background and details, the reader is referred to Stark’s papers and Tate’s book, especially [St, Conjecture 1], and [Ta, Conjecture IV.2.2]. I would like to thank John Tate for having brought this question to my attention.

Theorem 2.4.1 Stark’s conjecture \(St(K/k, \{\infty, p\})\) is true where \(p\) is any prime ideal of \(k\).

Proof. Putting together Lemma 2.2.1 and Lemma 2.3.2, we have

\[ L'(0, \chi, p) = -\frac{1}{24} \sum_{\{C\} \in \text{Cl}(k)/S} \chi(\{C\}) \log |\delta_p^\sigma(C)|^2, \]

25
where

$$\delta_p = N_{F/K} \left( \frac{\Delta(o)}{\Delta(p)} \right).$$

By Lemma 1.2.2, there exits a number $\epsilon_p \in K^*$ satisfying

$$\epsilon_p^{24} = \delta_p^W.$$

By Lemma 1.1.1, any such $\epsilon_p$ generates $p^{\nu h/(2n)}$ in $\mathcal{O}_K$, hence is a $p$-unit of $K^*$. Furthermore, any $W$th root of $\epsilon_p$ generates an abelian extension of $k$ by the theory of complex multiplication. If we identify $\text{Cl}(k)/S$ with $\text{Gal}(K/k)$ via the Artin map $\sigma$, then we conclude:

$$L'(0, \chi, p) = -\frac{1}{W} \sum_{g \in \text{Gal}(K/k)} \chi(g) \log |\epsilon_p^g|^2,$$

which is one version of Stark's conjecture for $K/k$. When $D$ is prime to 6, Theorem 1.3.2 gives $\epsilon_p$ more explicitly:

$$\epsilon_p = Np^{h/n}N_{F/K} \left( \frac{\eta(o)}{\eta(p)} \right)^2.$$

Note that the units $\epsilon_p^{1-g}$ which intervene in the expression for the difference of two $L$-series at zero are the units $\nu^2$ from the previous chapter; their square roots will play a key role in the refined index formula we are seeking.
Chapter 3

Cyclic Extensions

In this chapter, we assume that $K$ is a cyclic unramified extension of $k$. Recall that for an ideal $a$ of $k$, $[a]$ denotes the ideal class of $a$ in $\text{Cl}(k)$, and $\{a\}$ denotes the image of $[a]$ in $\text{Cl}(k)/S$. Since there are infinitely many prime ideals of degree one in every ideal class, we let $\mathfrak{p}$ be an unramified prime ideal of degree one and norm $p > 3$ such that $\{\mathfrak{p}\}$ generates the cyclic group $\text{Cl}(k)/S$.

3.1 The Group Determinant

In this section, we recall the group determinant formula of Dedekind-Frobenius and use it to transform the right hand side in the following lemma into the determinant of a matrix whose entries are defined in terms of the derivative of the partial zeta functions of $k$ at zero.

Lemma 3.1.1

$$-\frac{HR}{W} n \log p = \prod_{\chi} L'(0, \chi, \mathfrak{p}).$$

Proof. Recall that $\prod_{\chi}$ means the product over those characters which are trivial on $S$. Using 2.8, we have:

$$\prod_{\chi} L'(0, \chi, \mathfrak{p}) = \left\{ L(0, \chi_1) \prod_{\chi \neq \chi_1} L'(0, \chi) \right\} \log p \prod_{\chi \neq \chi_1} (1 - \chi([\mathfrak{p}])).$$

Since the set of characters of $\text{Cl}(k)$ which are trivial on $S$ coincides with the set of characters of $\text{Cl}(k)/S$, a cyclic group of order $n$ with generator $\{\mathfrak{p}\}$, we easily evaluate $\prod_{\chi \neq \chi_1} (1 - \chi([\mathfrak{p}])) = \prod_{j=1}^{n-1} (1 - e(j/n)) = n$. The equality we seek is then a consequence of Lemma 2.1.2.
Lemma 3.1.2 (Dedekind-Frobenius) Let \( g_1, \ldots, g_n \) be the elements of an abelian group \( G \) of order \( n \), and assign a complex number \( \Lambda(g) \) to each \( g \in G \). Then the group determinant of \( G \) satisfies:

\[
\det \left( \Lambda(g_i^{-1}g_j) \right)_{1 \leq i, j \leq n} = \prod_{\psi} \sum_{g \in G} \psi(g) \Lambda(g),
\]

where \( \psi \) runs through all characters of \( G \).

**Proof.** See, for example, [La, p.282].

**Definition 3.1.3** For any integer \( m \), define \( C_m = [p]^m \), so that \( \{C_1\}, \ldots, \{C_n\} \) are the \( n \) elements of \( \text{Cl}(k)/S \).

**Lemma 3.1.4**

\[
-\frac{HR}{W} n \log p = \det \left( \lambda_K(\{C_i^{-1}C_j\}, p) \right)_{1 \leq i, j \leq n}.
\]

**Proof.** This follows immediately from Lemma 3.1.1, Lemma 3.1.2 and Lemma 2.2.1.

Recall that whenever \([b] = C^{-1}\),

\[
\lambda_K(\{C_i\}, p) = -\frac{1}{24} \log \left| N_{F/K} \left( \frac{\Delta(b)}{\Delta(bp)} \right) \right|^2,
\]

and that we have defined \( C_m = [p]^m \) for any integer \( m \). With the choice \( b_m = p^{-m} \),

\[
\lambda_K(\{C_m\}, p) = -\frac{1}{24} \log \left| N_{F/K} \left( \frac{\Delta(p^{-m})}{\Delta(p^{1-m})} \right) \right|^2.
\]

**Definition 3.1.5** Let \( a_{ij} = \lambda_K(\{C_i^{-1}C_j\}, p) \) for \( 1 \leq i, j \leq n \) and let \( A \) denote the \( n \times n \) matrix whose entry in the \( i \)th row and \( j \)th column is \( a_{ij} \). Also, define

\[
\alpha(i, j) = N_{F/K} \left( \frac{\Delta(p^{i-j})}{\Delta(p^{i-j+1})} \right).
\]

Since \( \{C_i^{-1}C_j\} = \{C_{j-i}\} \),

\[
a_{ij} = -\frac{1}{24} \log |\alpha(i, j)|^2.
\]

**Lemma 3.1.6**

\[
-\frac{HR}{W} n \log p = \det A.
\]

**Proof.** This is simply a rephrasing of the previous lemma.
3.2 Transforming $A$ Into A Regulator Matrix

For any number $\gamma \in K$, let $\gamma^{(1)}, \ldots, \gamma^{(n)}$ be its conjugates over $k$ in some fixed order. Suppose $\varepsilon_1, \ldots, \varepsilon_{n-1}$ are units of $K$. Let us call the $n \times n$ matrix $\mathcal{R}(\varepsilon_1, \ldots, \varepsilon_{n-1}) = R$ whose $ij$th entry is $\log |\varepsilon_i^{(j)}|^2$, the "regulator matrix" of these units. Its determinant is non-zero if and only if $\varepsilon_1, \ldots, \varepsilon_{n-1}$ generate, together with the roots of unity in $K$, a subgroup of $E_K$ of finite index, and moreover this index is then precisely the quotient $|\det \mathcal{R}|/R$ where $R$ is the regulator of $K$ [Wa, Lemma 4.15]. Therefore, to obtain an index formula involving $H$, we would like to transform Lemma 3.1.6 into $HR = (h/n)|\det \mathcal{R}|$ for some regulator matrix $\mathcal{R}$. The tools we need to accomplish this were developed in the first chapter.

**Definition 3.2.1** For any integer $i$, define

$$\alpha_i = N_{F/K} \left( \frac{\Delta(p^i)}{\Delta(p^{i+1})} \right).$$

For any $\gamma \in K$, let $\gamma^{(j)} = \gamma^{(j)}(\varepsilon_1, \ldots, \varepsilon_{n-1})$ for $j = 1, \ldots, n$. Then $\gamma^{(1)}, \ldots, \gamma^{(n)}$ are the conjugates of $\gamma$ over $k$ with $\gamma = \gamma^{(n)}$.

**Lemma 3.2.2** The quotient of any two $\alpha(i, j)$'s is a unit of $K$, and

$$\alpha(i, j) = \alpha_{i}^{(j)}$$

for $1 \leq i, j \leq n$.

**Proof.** By Lemma 1.1.1, for all $i, j$, $\Delta(p^{i-j})/\Delta(p^{i-j+1})$ generates the ideal $p^{12}$ in $\mathcal{O}_F$, hence $\alpha(i, j)$ generates $p^{12h/n}$ in $\mathcal{O}_K$, which is independent of $i, j$. The first claim follows. The second claim is any easy consequence of Lemma 1.1.1 and the fact that the class of the conjugate of an ideal in a complex quadratic field is the inverse of the class of the ideal.

It is clear from the above lemma that $A$ is almost a regulator matrix; as such, it has three shortcomings: first, the numbers inside the absolute value signs are not units; second, the dimension of $A$ is $n$ not $n - 1$; third, every entry has an extra factor of $-1/24$.

**Definition 3.2.3** For $i = 1, \ldots, n - 1$, let

$$\beta_i = \frac{\alpha_i}{\alpha_{i+1}}. \tag{3.1}$$

Define the matrix

$$B = \left( \frac{-1}{24} \log |\beta_i^{(j)}|^2 \right)_{1 \leq i, j \leq n-1}. $$
Lemma 3.2.4 For every $i, j$, $\beta_i^{(j)} \in E_K$.

Proof. By the previous lemma,
\[ \beta_i^{(j)} = \frac{\alpha_i^{(j)}}{\alpha_{i+1}^{(j)}} = \frac{\alpha(i, j)}{\alpha(i + 1, j)} \]
is a unit of $K$.

Lemma 3.2.5
\[ \frac{W \det B}{2} \frac{R}{R} = \frac{H}{h/n}. \]

Proof. Let $B'$ be the $n \times n$ matrix whose $ij$th entry $b_{ij}$ is given by:
\[ b_{ij} = \begin{cases} a_{ij} - a_{i+1,j} & \text{for } i = 1, \ldots, n - 1 \\ \sum_{\ell=1}^n a_{\ell j} & \text{for } i = n. \end{cases} \]

Then it is an easy exercise in linear algebra to verify that
\[ \det B' = n \det A. \quad (3.2) \]

We now examine the matrix $B'$. In the first $n - 1$ rows of $B'$, the entries are:
\[ b_{ij} = -\frac{1}{24} \log |\alpha(i, j)/\alpha(i + 1, j)|^2 = -\frac{1}{24} \log |\beta_i^{(j)}|^2. \]

On the other hand, recalling that $a_{ij} = \lambda_K(\{C_i^{-1}C_j\}, p)$, we compute the last row of $B'$:
\[ b_{nj} = \sum_{i=1}^n \lambda_K(\{C_i^{-1}C_j\}, p) = \sum_{m=1}^n \Lambda(\{C_m\}) \]
\[ = L'(0, \chi_1, p) = L(0, \chi_1) \log p = -\frac{h}{2} \log p, \]
the last three equalities being due in turn to (2.11), (2.8), and (2.7).

In short,
\[ B' = \begin{pmatrix} -\frac{1}{24} \log |\beta_1^{(1)}|^2 & \cdots & -\frac{1}{24} \log |\beta_1^{(n)}|^2 \\ \vdots & \ddots & \vdots \\ -\frac{1}{24} \log |\beta_{n-1}^{(1)}|^2 & \cdots & -\frac{1}{24} \log |\beta_{n-1}^{(n)}|^2 \\ -\frac{h}{2} \log p & \cdots & -\frac{h}{2} \log p \end{pmatrix}. \]

It is clear that $B$ is the matrix that results by deleting the last row and last column of $B'$. Furthermore,
\[ \det B' = -\frac{h}{2} n \log p \det B. \quad (3.3) \]
To see this, we add the first $n - 1$ columns of $B'$ to the last column, which then becomes:

\[
\begin{pmatrix}
-\frac{1}{24} \log |N_{K/k}(\beta_1)|^2 \\
\vdots \\
-\frac{1}{24} \log |N_{K/k}(\beta_{n-1})|^2 \\
-\frac{1}{2} \frac{n}{2} \log p
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
\vdots \\
0 \\
-\frac{1}{2} \log p
\end{pmatrix},
\]

the last equality owing to the fact that $N_{K/k}(\beta_i)$ is a unit of $k$ and hence has absolute value 1. The lemma follows by combining (3.2) and (3.3) with Lemma 3.1.6.

3.3 Reducing the Index

In order to eliminate the factors of $-1/24$ in $B$, we use Lemma 1.2.2 to show that certain combinations of the $\beta_i$ are high powers in $K^*$.

**Lemma 3.3.1** For each $i$, $\beta_i^W \in E_K^4$. 

**Proof.** Thanks to Lemma 1.2.2, we need only observe from (3.1) and Lemma 1.1.1 that $\beta_i = \alpha_i/\alpha_i^{(p)}$.

**Definition 3.3.2** Let $\rho_1$ be a unit of $K$ such that

\[\rho_1^{-48} = \beta_1^W,\]

and define for $i = 2, \ldots, n - 1,$

\[\rho_i = \rho_1^{(C_{i-1})},\]

so that

\[\rho_i^{-48} = \beta_i^W.\]

We can now write

\[B = \left( \frac{2}{W} \log |\rho_i^{(j)}|_1^2 \right)_{1 \leq i, j \leq n-1},\]

which is very close to being a regulator matrix and in fact is one whenever $W = 2$. The other two possibilities are $W = 4$, $W = 6$, ($W = 12$ requires a non-cyclic extension of $k$).

**Lemma 3.3.3** For each $i$, $\rho_i/\rho_{i+1} \in E_K^{W/2}$. 

**Proof.** Apply Lemma 1.2.1 and note that $\rho_{i+1}^{(p)} = \rho_i$.  

31
Definition 3.3.4 Let $\gamma_1$ be some unit of $K$ satisfying

$$\gamma_1^{\frac{W}{2}} = \frac{\rho_1}{\rho_2},$$

and define for $i = 2, \ldots, n - 2$,

$$\gamma_i = \gamma_1^{\sigma(C_{i-1})},$$

so that

$$\gamma_i^{\frac{W}{2}} = \frac{\rho_i}{\rho_{i+1}}.$$

Theorem 3.3.5 Let $\mathcal{E}_K = \langle W_K, \gamma_1, \ldots, \gamma_{n-2}, \rho_{n-1} \rangle$ be the subgroup of $E_K$ generated by the elliptic units $\varepsilon_1, \ldots, \varepsilon_{n-1}$, together with the roots of unity of $K$. Note that when $W = 2$, $\mathcal{E}_K = \langle -1, \rho_1, \ldots, \rho_{n-1} \rangle$. The index of this subgroup is:

$$[E_K : \mathcal{E}] = \frac{H}{h/n}.$$

Proof. Let $R_1, \ldots, R_{n-1}$ be the rows of $B$. Let $\mathcal{R'}$ be the $n - 1 \times n - 1$ matrix whose rows $R'_1, \ldots, R'_{n-1}$ are given by

$$R'_1 = R_1 - pR_2$$
$$R'_2 = R_2 - pR_3$$
$$\vdots$$
$$R'_{n-2} = R_{n-2} - pR_{n-1}$$
$$R'_{n-1} = R_{n-1}.$$

Then $\det \mathcal{R'} = \det B$, and

$$\mathcal{R'} = \begin{pmatrix}
\log |\gamma_1^{(1)}|^2 & \cdots & \log |\gamma_1^{(n-1)}|^2 \\
\vdots & & \vdots \\
\log |\gamma_{n-2}^{(1)}|^2 & \cdots & \log |\gamma_{n-2}^{(n-1)}|^2 \\
\frac{2}{W} \log |\rho_{n-1}^{(1)}|^2 & \cdots & \frac{2}{W} \log |\rho_{n-1}^{(n-1)}|^2
\end{pmatrix}.$$

Now define the regulator matrix

$$\mathcal{R} = \begin{pmatrix}
\log |\gamma_1^{(1)}|^2 & \cdots & \log |\gamma_1^{(n-1)}|^2 \\
\vdots & & \vdots \\
\log |\gamma_{n-2}^{(1)}|^2 & \cdots & \log |\gamma_{n-2}^{(n-1)}|^2 \\
\log |\rho_{n-1}^{(1)}|^2 & \cdots & \log |\rho_{n-1}^{(n-1)}|^2
\end{pmatrix},$$

32
so that by Lemma 3.2.5,
\[ \frac{H}{h/n} = \frac{\det \mathcal{R}}{R}. \]  
(3.5)

This completes the proof of the theorem.

We conclude with a more explicit version of Theorem 3.3.5.

**Theorem 3.3.6** Suppose \( k \) is a complex quadratic field of discriminant \(-D\) prime to 6. Denote the Hilbert class field of \( k \) by \( F \). Let \( K \) be a cyclic unramified extension of degree \( n \) over \( k \). Let \( h \) and \( H \) be the class numbers of \( k \) and \( K \), respectively. Let \( \sigma \) be as in Lemma 1.3.7. Choose an unramified prime ideal \( p \) in \( k \) of degree one and norm \( p > 3 \) such that the image of \( \sigma(p) \) in \( \text{Gal}(K/k) \) is a generator. Choose a basis 
\[ [\omega - t, p^{n+1}] \] 
for \( p^{n+1} \). For \( i = 0, \ldots, n - 1 \), define:
\[ U_i = e_{24}[(2 - t)p^i(p - 1)^2] \frac{\eta(\frac{\omega - t}{p^{i+1}})^2}{\eta(\frac{\omega - t}{p^i})\eta(\frac{\omega - t}{p^{i+2}})}. \]

Then \( U_0, \ldots, U_{n-1} \in E_F \) are conjugate units. If \( u_i = N_{F/K}(U_i) \), then \( u_0, \ldots, u_{n-1} \in E_K \) are conjugate units and
\[ [E_K : <-1, u_1, \ldots, u_{n-1}>] = \frac{H}{h/n}. \]

**Proof.** Let \( \alpha = \frac{\eta(p^i)}{\eta(p^{i+1})} \) and \( \sigma = \sigma(p) \). By Lemma 1.5.1, \( \alpha^\sigma/\alpha = U_i \in E_F \). The remaining conclusions follow from Theorem 3.3.5 and the observation that, up to a factor of \( \pm 1 \), \( u_i \) is the unit \( \rho_i \).

We point out an immediate corollary of the above theorem.

**Corollary 3.3.7** Suppose \( K \) is a cyclic extension of \( k \) of arbitrary degree \( n \), and the only roots of unity in \( K \) are \( \pm 1 \). Suppose the "new class number" of \( K \) is 1, i.e. \( H = h/n \). Then \( K \) possesses a special Minkowski unit, i.e. a unit whose conjugates over \( k \) form a fundamental system for \( E_K \).

**Proof.** The unit \( u_1 \) is such a unit. Let us note here that its conjugates over \( k \) are all of its conjugates, i.e. \( u_1 \) has a real conjugate, thus lies in a maximal real subfield of \( K \). In fact,
\[ u_{n-1} = N_{F/K} \left( \frac{\eta(p^n)\eta(p^n)}{\eta(p^{n-1})\eta(p^{n+1})} \right) \]
\[ = N_{F/K} \left( \frac{\eta(p^n)}{\eta(p^{n-1})} \right) N_{F/K} \left( \frac{\eta(\sigma)}{\eta(p)} \right) \]
\[ = v(p, p^{n-1})^{-1}, \]
since \( \sigma(\{p^n\}) = \sigma(\{p\}) \). By Lemma 1.5.4, \( v(p, p^{n-1}) = v(p, p) \) since \( [p] = [\bar{p}] \). But \( v(p, \bar{p}) = v(\bar{p}, p) = v(p, p) \), hence \( u_{n-1} = u_{n-1} \).
Chapter 4

The Main Theorem

4.1 Sums of Imprimitive L-functions

Choose prime ideals $p_1, \ldots, p_n$ (prime to $6D$ and of degree one) such that $\{p_1\}, \ldots, \{p_n\}$ are the $n$ elements of $\text{Cl}(k)/S$ and assume that $[p_n] \in S$. For $j = 1, \ldots, n$, let $C_j = [p_j]$ and $p_j = N(p_j)$.

**Definition 4.1.1** For each character $\chi$ of $\text{Cl}(k)$ trivial on $S$, let

$$Z(\chi) = \sum_{j=1}^{n} L'(0, \chi, p_j).$$

(4.1)

**Lemma 4.1.2**

$$-\frac{HR}{W} n^{n-1} \log(p_1 \cdots p_n) = \prod_{\chi} Z(\chi).$$

**Proof.** If $\chi$ is trivial on $S$,

$$Z(\chi) = \begin{cases} L(0, \chi_1) \log(p_1 \cdots p_n) & \text{if } \chi = \chi_1, \\ nL'(0, \chi) & \text{if } \chi \neq \chi_1, \end{cases}$$

(4.2)

by (2.8) and the orthogonality relation for characters of $\text{Cl}(k)/S$. Taking the product of $Z(\chi)$ over those $\chi$ which are trivial on $S$ yields:

$$\prod_{\chi} Z(\chi) = n^{n-1} \log(p_1 \cdots p_n) L(0, \chi_1) \prod_{\chi \neq \chi_1} L'(0, \chi).$$

The equality we seek then follows from Lemma 2.1.2.
4.2 The S-unit $\delta$

Definition 4.2.1 Let

$$\Lambda(\{C\}) = \sum_{j=1}^{n} \lambda_{K}(\{C\}, p_j).$$

Lemma 4.2.2

$$-\frac{H R}{W} n^{n-1} \log(p_1 \cdots p_n) = \det \left( \Lambda(\{C^{-1}_i C_j\}) \right)_{1 \leq i, j \leq n}.$$

Proof. For a character $\chi$ which is trivial on $S$, we use Definition 4.2.1 to write

$$\sum_{j=1}^{n} L'(0, \chi, p_j) = \sum_{j=1}^{n} \sum_{\{C\} \in Cl(k)/S} \chi(\{C\}) \lambda_{K}(\{C\}, p_j)$$

$$= \sum_{\{C\} \in Cl(k)/S} \chi(\{C\}) \Lambda(\{C\}).$$

The previous lemma when combined with Lemma 4.1.2 and Lemma 3.1.2 yields the result.

Definition 4.2.3 Let

$$\delta = N_{F/K} \left( \frac{\Delta(\{C\})}{\Delta(p_j)} \right)$$

$$= \prod_{j=1}^{n} \delta_{p_j}.$$

Lemma 4.2.4 For any $C \in Cl(k)$, $\Lambda(\{C\}) = -\frac{1}{24} \log |\delta^{s(C)}|^2$.

Proof. By Lemma 2.3.2 and Definition 4.2.1, if $b$ is an ideal of $k$ with ideal class $[b] = C^{-1}$,

$$\Lambda(\{C\}) = -\frac{1}{24} \log \left| N_{F/K} \left( \prod_{j=1}^{n} \frac{\Delta(b)}{\Delta(bp_j)} \right) \right|^2$$

$$= -\frac{1}{24} \log \left| N_{F/K} \left( \prod_{j=1}^{n} \frac{\Delta(b)}{\Delta(p_j)} \right)^{s(C)} \right|^2$$

$$= -\frac{1}{24} \log |\delta^{s(C)}|^2.$$
4.3 Making Units from $\delta$

It will be convenient to work in the group ring $\mathbb{Z}[G]$ where $G = \text{Gal}(K/k)$ is identified with $\text{Cl}(k)/S$ via the Artin map $\sigma$. Recall that the degree map $\deg : \mathbb{Z}[G] \to \mathbb{Z}$ is defined by $\deg(\sum c_g g) = \sum c_g$.

Throughout this section, we suppose $g_1, \ldots, g_r$ are arbitrary non-trivial elements of $G$ and fix the following element $\mu$ of $\mathbb{Z}[G]$:

$$\mu = g_1 + \cdots + g_r - g_1 \cdots g_r - r + 1.$$  

Choose integral ideals $a_1, \ldots, a_r$ of $k$ prime to $6D$ satisfying $\sigma((\bar{a}_i)) = g_i$ for $i = 1, \ldots, r$. If $D$ is prime to 6, assume in addition that $a_1 \cdots a_r$ is primitive.

**Definition 4.3.1** Let

$$V_\mu = V(a_1, \ldots, a_r).$$

If $D$ is prime to 6, let

$$v_\mu = v(a_1, \ldots, a_r).$$

By Lemma 1.4.4 and Lemma 1.5.4, $V_\mu, v_\mu$ do not depend on the choice of ideal representatives for $g_1, \ldots, g_r$.

**Lemma 4.3.2**

(i) $\delta^\mu = V_\mu^n$;

(ii) If $D$ is prime to 6, $\delta^\mu = v_\mu^{24n}$.

**Proof.** Begin by observing that for any pair of ideals $m, n$ of $k$,

$$\left( \frac{\Delta(m)}{\Delta(o)} \right)^{1-\sigma(\bar{m})} = \left( \frac{\Delta(n)}{\Delta(o)} \right)^{1-\sigma(\bar{n})}.$$  

Thus, for $1 \leq i \leq r$,

$$\delta^{g_{i-1}} = N_{F/K} \prod_{j=1}^{n} \left( \frac{\Delta(p_j)}{\Delta(o)} \right)^{1-\sigma(\bar{p}_j)}$$

$$= N_{F/K} \prod_{j=1}^{n} \left( \frac{\Delta(a_i)}{\Delta(o)} \right)^{1-\sigma(\bar{a}_i)}$$

$$= \frac{N_{F/K} (\Delta(a_i)/\Delta(o))^n}{N_{F/K} (\Delta(a_i)/\Delta(o))}.$$  

Similarly,

$$\delta^{g_1 \cdots g_r} = \frac{N_{F/K} (\Delta(a_1 \cdots a_r)/\Delta(o))}{N_{F/K} (\Delta(a_1 \cdots a_r)/\Delta(o))^{24n}}.$$  

36
Putting all of this together, we have:

$$\delta^\mu = \delta^{g_1 \cdots g_r} \cdots \delta^{g_{r-1}} \delta^{1 \cdots g_r}$$

$$= N_{F/K} \left( \frac{\Delta(a_1) \cdots \Delta(a_r)}{\Delta(o)^{r-1} \Delta(a_1 \cdots a_r)} \right)^n N_{F/k} \left( \frac{\Delta(a_1) \cdots \Delta(a_r)}{\Delta(o)^{r-1} \Delta(a_1 \cdots a_r)} \right)^{-1}$$

$$= \frac{V^n}{N_{K/k} V^\mu}.$$ 

But by Lemma 1.4.4, $N_{K/k} V^\mu = 1$, so (i) is proved. (ii) is a consequence of (i) and Lemma 1.5.4.

### 4.4 The Main Theorem

The abelian group Cl$k/S$ can be decomposed into a product of $r$ cyclic components where $r$ is its rank. Suppose the elements $\{C_1\}, \ldots, \{C_n\}$ have been ordered in such a way that $\{C_{s+1}\}, \ldots, \{C_{n-1}\}$ is a minimal set of generators of Cl$k/S$. Here, $s = n - r - 1$. To ease the notation, we will continue to work with $G$: thus, for $1 \leq i \leq n$, write $g_i = \sigma(i_i)$; also, let $f_i$ be the order of $g_i$ in $G$. Recall that $g_n$ is the identity of $G$.

**Definition 4.4.1** For $i = 1, \ldots, n - 1$, $g_i$ has a unique representation

$$g_i = \prod_{j=1}^r g_{s+j}^{m(i,j)},$$

with $0 \leq m(i,j) < f_{s+j}$.

For $i = 1, \ldots, s$, define $\xi_i \in I[G]$ by

$$\xi_i = \sum_{j=1}^r m(i,j) g_{s+j}.$$  

Also, define

$$\mu_i = \begin{cases} 
\deg(\xi_i) - 1 + g_i - \xi_i & 1 \leq i \leq s \\
 f_i - f_i g_i & s + 1 \leq i \leq n - 1 \\
 1 & i = n
\end{cases}.$$  

**Lemma 4.4.2** For $i = 1, \ldots, n - 1$, there exists a unit $\varepsilon_i \in E_K$ such that

$$\delta^{-W_{\mu_i}} = \varepsilon_i^{48n}.$$  

**Proof.** By Lemma 4.3.2, $\delta^{-W_{\mu_i}} = V_{-\mu_i}^W$, and $V_{-\mu_i}^W \in E_K^{48}$ by Lemma 1.4.4.
Definition 4.4.3 Let $E_K$ be the group generated by the roots of unity in $K$ and any set of $n-1$ units $\varepsilon_1, \ldots, \varepsilon_{n-1} \in E_K$ satisfying the condition of the above lemma. Since for each $i$, the various choices of $\varepsilon_i$ differ only by a root of unity in $K$, $E_K$ does not depend on the choice of $\varepsilon_i$. Set $\varepsilon_n = \delta$.

Theorem 4.4.4 The index of the elliptic group $E_K$ is

$$[E_K : E_K] = \left( \frac{W}{2} \right)^{n-2} \frac{H}{h/n}.$$  

In particular, if $W = 2$, this index is precisely the new class number of $K$.

The proof is based on massaging the matrix in Lemma 4.2.2 into a regulator matrix.

Let $I_s$ be the $s \times s$ identity matrix. Define $N$ to be the following $(r+1) \times (r+1)$ matrix:

$$N = \begin{pmatrix} -f_{s+1} & f_{s+1} \\ \vdots & \vdots \\ -f_{n-1} & f_{n-1} \end{pmatrix}.$$  

So far, $m(i, j)$ has been defined with $1 \leq j \leq r$ only. For $1 \leq i \leq s$, we define

$$m(i, r+1) = 1 - \sum_{t=1}^{r} m(i, t).$$

Let $M = (m(i, j))_{1 \leq i \leq s, 1 \leq j \leq r+1}$, and put together an $n \times n$ matrix $A_0$ with the block representation

$$A_0 = \begin{pmatrix} I_s & -M \\ O & N \end{pmatrix},$$

where $O$ is the $(r+1) \times s$ zero matrix. Now let $A = (\Lambda(\{C_i^{-1}C_j\}))_{1 \leq i, j \leq n}$ and consider the product $B = A_0A$.

Lemma 4.4.5

$$|\det B| = \frac{HR}{W} n^n \log(p_1 \cdots p_n).$$

38
**Proof.** It is clear that \( \det \mathcal{A}_0 = \det \mathcal{N} \). But \( |\det \mathcal{N}| = \Pi_{j=1}^n f_{r+j} = n \), since \( g_{n+1}, \ldots, g_{n-1} \) form a minimal generating set for \( G \). The lemma now follows because we have computed \( \det \mathcal{A} \) in Lemma 4.2.2.

Using the fact that

\[
\Lambda(\{C_i^{-1}C_j\}) = -\frac{1}{24} \log \left| (\delta^o(C_i)\delta^o(C_j)) \right|^2,
\]

(see Lemma 4.2.4) and the definition of \( \mu_i \), it can be seen upon multiplying \( \mathcal{A}_0 \) by \( \mathcal{A} \) that the \( i \)th row, \( j \)th column entry of \( \mathcal{B} \) is

\[
b_{ij} = -\frac{1}{24} \log \left| (\delta^o(C_i)) \right|^2 = \begin{cases} \frac{2n}{W} \log \left| \epsilon_i^{o(C_j)} \right|^2 & 1 \leq i \leq n-1 \\ \Lambda(\{C_j\}) & i = n \end{cases} \quad (4.3)
\]

Define \( \mathcal{R} \) to be the following regulator matrix of \( \epsilon_1, \ldots, \epsilon_{n-1} \):

\[
\mathcal{R} = (\log \left| \epsilon_i^{o(C_j)} \right|^2)_{1 \leq i, j \leq n-1},
\]

and let \( \mathcal{B}_0 = (2n/W)\mathcal{R} \). It is clear that \( \mathcal{B}_0 \) is the matrix that is left when the \( n \)th row and \( n \)th column of \( \mathcal{B} \) are deleted.

**Lemma 4.4.6**

\[
\det \mathcal{B} = -\frac{h}{2} \log(p_1 \cdots p_n) \det \mathcal{B}_0.
\]

**Proof.** Let \( \mathcal{A}_1 \) be the following \( n \times n \) matrix:

\[
\mathcal{A}_1 = \begin{pmatrix}
1 & 1 & 1 \\
1 & 1 & 1 \\
\vdots & \ddots & \vdots \\
1 & 1 & 1 \\
1 & 1 & 1
\end{pmatrix}
\]

First note that \( \det(\mathcal{B} \mathcal{A}_1) = \det \mathcal{B} \). Then, keeping in mind (4.3), and using the fact that \( N_{K/k}(\epsilon_i) \) is a root of unity, we compute the last column of \( \mathcal{B} \mathcal{A}_1 \) to be:

\[
\begin{pmatrix}
\frac{2n}{W} \log \left| N_{K/k}(\epsilon_1) \right|^2 \\
\vdots \\
\frac{2n}{W} \log \left| N_{K/k}(\epsilon_{n-1}) \right|^2 \\
\sum_{j=1}^{n} \Lambda(\{C_j\})
\end{pmatrix}
= \begin{pmatrix}
0 \\
\vdots \\
0 \\
\sum_{j=1}^{n} L'(0, \chi_j, \psi_j)
\end{pmatrix}
\]

39
The lemma follows upon noting that
\[ \sum_{j=1}^{n} L'(0, \chi_j, p_j) = \sum_{j=1}^{n} \frac{h}{2} \log p_j, \]
by (2.8).

**Lemma 4.4.7**
\[ |\det \mathcal{R}| = \left( \frac{W}{2} \right)^{n-2} \frac{HR}{h/n}. \]

**Proof.** We put together the above lemmas:
\[ |\det \mathcal{R}| = \left( \frac{W}{2n} \right)^{n-1} |\det B_0| \]
\[ = \left( \frac{W}{2n} \right)^{n-1} \left( \frac{h}{2} \log(p_1 \cdots p_n) \right)^{-1} |\det B| \]
\[ = \left( \frac{W}{2n} \right)^{n-1} \left( \frac{h}{2} \log(p_1 \cdots p_n) \right)^{-1} \left( \frac{HR}{W} n \log(p_1 \cdots p_n) \right) \]
\[ = \left( \frac{W}{2} \right)^{n-2} \frac{HR}{h/n}. \]

**Proof of Theorem 4.4.4.** The theorem is equivalent to the above lemma by [Wa, Lemma 4.15].

### 4.5 Explicit Generators for the Elliptic Group

In this section, we assume that \( D \) is prime to 6. We are now able to write a completely explicit formula for \( n - 1 \) elliptic units generating a group of index \( H/(h/n) \) in \( E_K \).

**Theorem 4.5.1** Suppose \( D \) is prime to 6. Assume \( \prod_{j=1}^{n-1} p_j \) is primitive. Let \( v_i = v_{-\mu_i} \) for \( i = 1, \ldots, n - 1 \). Thus, for \( i = 1, \ldots, s \),
\[ v_i = N_{F/K} \frac{\prod_{j=1}^{i} \pi_j^{m(i,j)}}{\pi(\alpha)^{\deg(\xi_i)-1} \eta \left( \prod_{j=1}^{i} \pi_j^{m(i,j)} \right)}, \]
and for \( i = s + 1, \ldots, n - 1 \),
\[ v_i = N_{F/K} \frac{\eta(\pi_i)^{f_i}}{\eta(\alpha)^{f_i-1} \eta(\pi_i^{f_i})}. \]

Then,
\[ [E_K : \langle \pm 1, v_1, \ldots, v_{n-1} \rangle] = \frac{H}{h/n}. \]
Proof. This an immediate consequence of Theorem 4.4.4 and the fact that the units $v_1,\ldots,v_{n-1}$ satisfy the condition of Lemma 4.4.2, hence generate the free part of $E_K$. 
Chapter 5

Computational Techniques

In this chapter, we discuss how to compute the elliptic units defined above and how to use them to compute the class number and full unit group of $K$. We discuss a general algorithm, as well as simplifications in the special case where the degree of the extension $K/k$ is an odd prime.

5.1 Calculating the Elliptic Units

To compute the units generating the elliptic group, we need to know how to compute $\eta$-values accurately. Most of the arithmetic information in $k$ we will need, such as finding ideals which generate the class group can be handled by elementary means, such as reduction of binary quadratic forms (which is equivalent to the algorithm given in the next paragraph). We discuss briefly how to compute suitable bases for ideals of $k$.

5.1.1 Evaluating the Dedekind Eta Function

The Dedekind eta function is calculated efficiently and accurately using its Fourier expansion (stemming from the Pentagonal Number Theorem of Euler):

$$\eta(z) = e^{2\pi i} \left\{ 1 + \sum_{n=1}^{\infty} (-1)^n [e_2(n(3n-1)z) + e_2(n(3n+1)z)] \right\}.$$  

This series converges very quickly for $z \in \mathcal{F}$ where

$$\mathcal{F} = \left\{ z : \sqrt{3} \leq \Re(z) \leq \frac{1}{2}, \Im(z) \geq \frac{\sqrt{3}}{2} \right\}.$$
is the usual "fundamental domain" for the action of $SL(2, \mathbb{Z})$ on the upper half-plane $\mathcal{H}$. The two matrices

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

generate $SL(2, \mathbb{Z})$. If $z \in \mathcal{H}$ is given, one may find a point in $\mathcal{F}$ equivalent to $z$ by the well-known two step algorithm:

Step 1. If $|\Re(z)| > 1/2$, replace $z$ by an equivalent point $T^j z$ with $|\Re(T^j z)| \leq 1/2$.

Step 2. If $|z| \geq 1$, $z \in \mathcal{F}$. Else, replace $z$ by $S z$. Go to Step 1.

Each time $S$ or $T$ is applied, we keep track of how the value of $\eta(z)$ is transformed via the modular properties of $\eta$:

$$\eta(Tz) = e_{2a}(1)\eta(z), \quad \eta(Sz) = \sqrt{e_4(3)}z \eta(z)$$

where the branch of the square root is the one taking positive real values on the positive imaginary axis. As a point of reference, with $z \in \mathcal{F}$, truncating the Fourier series of $\eta(z)$ at $n = 10$ gives an error of less than $10^{-150}$.

5.1.2 Ideal Bases

We will also need a procedure for finding a suitable basis for a given ideal of $k$. If $-D$ is the discriminant of $k$, we define

$$\omega = \begin{cases} (1 + \sqrt{-D})/2 & \text{if } D \text{ is odd} \\ \sqrt{-D/4} & \text{if } D \text{ is even} \end{cases}$$

whose minimal polynomial is

$$f_\omega(x) = \begin{cases} x^2 - x + (1 + D)/4 & \text{if } D \text{ is odd} \\ x^2 + D/4 & \text{if } D \text{ is even} \end{cases}$$

If $q$ is a rational prime that splits into distinct prime ideals in $k$, and $t$ is an integer satisfying the congruence $f_\omega(t) \equiv 0 \mod q$, then $[q, \omega - t]$ is a $\mathbb{Z}$-basis for one of the divisors $q$ of $(q)$. A basis for the other factor $q'$ is then given by $[q, \omega + t']$ where

$$t' = \begin{cases} t - 1 & \text{if } D \text{ is odd} \\ t & \text{if } D \text{ is even} \end{cases}$$

Similarly, a basis for $q^j (j > 1)$ is given by $q^j = [q^j, \omega - t_j]$, where $f_\omega(t_j) \equiv 0 \mod q^j$, and $t_j \equiv t \mod q$.  

43
More generally, suppose $a = [a, \omega - r], b = [b, \omega - s]$ with $a = Na, b = Nb$. If $ab$ is primitive, a basis for $ab$ is $[ab, \omega - t]$ where $t \equiv r \mod a, t \equiv s \mod b$ and $f_\omega(t) \equiv 0 \mod ab$. It is not difficult to solve such congruences.

If $D$ is prime to 6, calculating each elliptic unit $\varepsilon_j$ (or $u_j$ in the cyclic case) is straightforward by using the formula in Theorem 4.4.4 (Theorem 3.3.6 in the cyclic case). If $D$ is not prime to 6, finding which $48/W$th root of each appropriate delta quotient lies in $K$ is easy following the procedure prescribed in the proof of Theorem 1.3.2 for applying the reciprocity law. Once the units are known to high accuracy (we used about 50 digits), one may determine their minimal polynomial exactly, since they have integral coefficients (see Tables).

5.2 Calculating the Index of Elliptic Units

Calculating the index is by far the most time-consuming part of our algorithm for computing the class number of $K$. Since one may find an explicit upper bound $B_K$ for this index (see below) one may proceed by checking the divisibility of the index one prime at a time. There are three components to the algorithm: (1) deciding which units to test for being a $p$th power; (2) checking whether a given unit is a $p$th power; (3) keeping track of the index. A basic approach would be as follows: for each prime $p < B_K$, one checks whether each product

$$\zeta \prod_{j=1}^{n-1} \varepsilon_j^{t_j}, \quad 0 \leq t_j < p, \zeta \in \mathcal{W}_K,$$  \hspace{1cm} (5.1)

of the basis elements for the elliptic group is a $p$th power in $K^*$ or not. The index is divisible by $p$ if and only of one of these is a $p$th power. If some of these units are $p$th powers, it is potentially complicated to determine the exact power of $p$ dividing the index in this way. We use an idea outlined by Hayashi [Ha2] to develop a better algorithm (see Lemma 5.2.4 below).

5.2.1 Checking for $p$th Powers

There are several ways to check if a given number in a number field of degree $n$ is a $p$th power in the same field. For example, if the value of each conjugate of the number is known with sufficient accuracy, one may consider all $n$-tuples of $p$th roots of conjugates of the number and check the integrality of symmetric polynomials in $n$ letters evaluated at these $n$-tuples (see [Ha1] for a more precise statement). If the number in question actually generates the field, another (often more efficient) procedure is given by the following lemma.
Lemma 5.2.1 Let $M = \mathbb{Q}(\alpha)$ for some algebraic integer $\alpha$ of degree $n > 1$ with conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$, $n = [M : \mathbb{Q}]$. Let $f_\alpha(x) = \prod_{j=1}^{n}(x - \alpha^{(j)})$ be the minimal polynomial of $\alpha$. For any positive integer $m$, $\alpha \in M^{*m}$ if and only if $f_\alpha(x^m)$ has an irreducible factor in $\mathbb{Z}[x]$ whose degree is a positive divisor of $n$.

Proof. Let $g(x) = f_\alpha(x^m)$; it is a polynomial of degree $mn$. Suppose first that $\alpha = \beta^m$ for some $\beta \in M$. Since $g(\beta) = 0$, $g(x)$ must be divisible by the minimal polynomial of $\beta$, $f_\beta(x)$, which has degree dividing $n$. Conversely, suppose $g(x)$ has an irreducible factor $\tilde{g}(x) \in \mathbb{Z}[x]$ whose degree is a positive divisor of $n$. Let $\tilde{\beta}$ be a root of $\tilde{g}(x)$. Then

$$g(\tilde{\beta}) = \prod_{j=1}^{n}(\tilde{\beta}^m - \alpha^{(j)}) = 0.$$

Hence, $\tilde{\beta}^m = \alpha^{(j)}$ for some $j$. In particular, $\mathbb{Q}(\alpha^{(j)}) \subseteq \mathbb{Q}(\tilde{\beta})$. Since the degree of $\tilde{\beta}$ is at most $n$, it follows that $\mathbb{Q}(\alpha^{(j)}) = \mathbb{Q}(\tilde{\beta})$. Therefore, some other root $\beta$ of $\tilde{g}$ (i.e. a conjugate of $\tilde{\beta}$) satisfies $\tilde{\beta}^m = \alpha$ and $\beta \in \mathbb{Q}(\alpha)$. Note that $\tilde{g}(x)$ is the minimal polynomial of an $m$th root of $\alpha$.

If the particular unit we are testing has a real conjugate, then our labor can be reduced by carrying out the computations in $K^+$, a maximal real subfield of $K$. Let us note that when $K/k$ is cyclic and $D$ is prime to 6, the generators $u_i$ of $E_K$ have a real embedding (see Corollary 3.3.7).

Lemma 5.2.2 Let $p$ be any prime, $\varepsilon \in E_{K^+}$. Then $\varepsilon \in E_{K}^p$ if and only if $\varepsilon \in E_{K^+}^p$ or $-\varepsilon/D \in E_{K^+}^p$.

Proof. Assume $\varepsilon$ is not a $p$th power in $E_{K^+}$ but $\varepsilon = \tilde{\varepsilon}^p$ with $\tilde{\varepsilon} \in E_K$. Since $K/K^+$ is a quadratic extension, $p$ must be 2. The lemma follows since $K^+ = K^+(\tilde{\varepsilon}) = K^+/(\sqrt{-D})$.

Lemma 5.2.3 Suppose $D$ is a prime number and $\mathbb{Q}(\varepsilon)$ is a maximal real subfield of $K$ for some unit $\varepsilon \in E_K$. Let $f_\varepsilon(x)$ be the minimal polynomial of $\varepsilon$. Then, for any prime $p$, $\varepsilon \in E_K^p$ if and only if $f_\varepsilon(x^p)$ has an irreducible factor in $\mathbb{Z}[x]$ whose degree is a positive divisor of $n$.

Proof. Since some prime ideal of $K^+$ prime to 2 ramifies in $K/K^+$, one can show that $\varepsilon \in E_K^p$ if and only if $\varepsilon \in E_{K^+}^p$. The lemma now follows from the previous two lemmas.

5.2.2 The Algorithm

Recall that $E_K = < W_K, \varepsilon_1, \ldots, \varepsilon_{n-1} >$. 

45
Lemma 5.2.4 (Hayashi) Let \( t = n - 1 \) be the unit rank of \( K \). There exist generators \( \nu_1, \ldots, \nu_t \) of \( E_K \), roots of unity \( \zeta_1, \ldots, \zeta_t \in \mathcal{W}_K \), and integers \( b_{ij} \) with \( b_{ij} < b_{ii} \) for \( 1 \leq j < i \leq t \) such that

\[
\begin{align*}
\varepsilon_1 & = \zeta_1 \nu_1^{b_{11}} \\
\varepsilon_2 & = \zeta_2 \nu_1^{b_{21}} \nu_2^{b_{22}} \\
& \quad \vdots \\
\varepsilon_t & = \zeta_t \nu_1^{b_{11}} \cdots \nu_t^{b_{tt}}.
\end{align*}
\]

Then, \( [E_K : \mathcal{E}_K] = |b_{11} \cdots b_{tt}|. \)

**Proof.** This follows easily from the fact that the (integral) matrix transforming any column vector of logarithms of absolute values of fundamental units of \( K \) into the logarithm of absolute values of the basis elements of \( \mathcal{E}_K \) has non-zero determinant (equal to the index \( [E_K : \mathcal{E}_K] \), in fact) and therefore can be decomposed into the product of a lower triangular integral matrix and an integral matrix of determinant \( \pm 1. \)

We proceed as follows to determine the \( p \)-part of the index:

**Step 1.** Test \( \varepsilon_1 \in \mathcal{W}_K E^K_p. \) If the answer is no, let \( \theta_1 = \varepsilon_1. \) If the answer is yes, test \( \tilde{\varepsilon}_1 \in \mathcal{W}_K E^K_p \) where \( \tilde{\varepsilon}_1 \in E_K \) is such that \( \tilde{\varepsilon}_1^p = \zeta \varepsilon_1 \) for some \( \zeta \in \mathcal{W}_K \); continue in this way until it is determined that \( \varepsilon_1 \) is in \( \mathcal{W}_K E^K_{p^{i_1}} \) but not in \( \mathcal{W}_K E^K_{p^{i_1+1}}. \) Let \( \theta_1 \in E_K \) be such that \( \theta_1^{p^{i_1}} = \zeta \varepsilon_1 \) for some \( \zeta \in \mathcal{W}_K. \)

**Step 2.** Suppose \( \theta_{m-1} \) has been found. Find the largest integer \( j_m \) such that there exist integers \( c_1, \ldots, c_{m-1} \) satisfying \( 0 \leq c_i \leq p^{m-1} - 1, \) and

\[
\varepsilon_m^{-1} \theta_1^{c_1} \cdots \theta_{m-1}^{c_{m-1}} \in \mathcal{W}_K E^K_{p^{m}}.
\]

Let \( \theta_m \) be any unit of \( E_K \) satisfying \( \theta_m^{p^m} = \zeta \varepsilon_m \theta_1^{-c_1} \cdots \theta_{m-1}^{-c_{m-1}} \) for some \( \zeta \in \nu \mathcal{W}_K. \)

**Step 3.** The \( p \)-part of \( [E_K : \mathcal{E}_K] \) is \( p^{i_1} \cdots p^{i_t}, \) and \( < \mathcal{W}_K, \theta_1, \ldots, \theta_{n-1} > \) has index \( [E_K : \mathcal{E}_K]/(p^{i_1} \cdots p^{i_t}) \).

We apply the above procedure starting with the smallest prime and working up to last prime less than \( B_K. \) It would be advantageous, after testing each prime, to use the newly found larger group of units generated by \( \theta_1, \ldots, \theta_t \) as the known group and to find its index in \( E_K. \) In this way, when the last prime has been tested, not only will we know the index (as the product of the \( p \)-parts) but we will also have found fundamental units \( \nu_1, \ldots, \nu_{n-1} \) for \( E_K. \)
5.2.3 An Upper Bound for the Index

The index we wish to compute can be written as a quotient of regulators:

$$[E_K : \mathcal{E}_K] = \frac{|\det \mathcal{R}|}{R},$$

where $\det \mathcal{R}$ is the regulator of the elliptic group $\mathcal{E}_K$. Since generators for $\mathcal{E}_K$ are explicitly known, computing $\det \mathcal{R}$ is straightforward. Hence, an upper bound for the index $[E_K : \mathcal{E}_K]$ can be achieved via a lower bound for the regulator $R$ of the field $K$. The cheapest lower bound for $R$ is the universal one due to Friedman [Fr]: the regulator of every number field (other than three exceptional cases) is at least $1/4$. Thus, we can take $B_K = 4|\det \mathcal{R}|$. Of course, one can do much better, especially by studying specific properties of $K$ (for example see [Ha1], [Ha2]), but we will content ourselves here with this very crude bound, just to show that our algorithm for computing the class number of $K$ using elliptic units is effective, and in the computations below, we will concentrate on the 2-part of the index. It should also be mentioned that when $D$ is small, the discriminant bounds of Odlyzko [Od] lead to good upper bounds for the class number of $K$.

5.3 Extensions of Prime Degree

In this section, we assume that $n$, the degree of $K/k$ is an odd prime $\ell$. We will exploit the following simplifications: $K/k$ is cyclic; $D$ is prime; $W = 2$; $\mathcal{E}_K/\pm 1$ is generated by conjugate units $u_1, \ldots, u_n$, and exactly one of these units (call it $u$) is real; we have

$$\mathcal{E}_K = \pm u \mathbb{Z}[\mathcal{C}], \quad \quad [E_K : \mathcal{E}_K] = \frac{H}{h/\ell}.$$

Furthermore, Hayashi has pointed out that the work of Gras-Gras on real abelian extensions of $\mathbb{Q}$ carries over to the elliptic case to make the computation of the index more efficient still. Let $\zeta_\ell$ be a fixed $\ell$th root of unity and denote the ring of integers of $\mathbb{Q}(\zeta_\ell)$ by $\mathcal{O}_\ell = \mathbb{Z}[\zeta_\ell]$.

5.3.1 $E_K/\mathcal{W}_K$ as $\mathcal{O}_\ell$-module

The following observation was made by Brumer [Br] in the case of cyclic extensions of prime degree over $\mathbb{Q}$.

Lemma 5.3.1 (Brumer) Let $K/k$ be cyclic of odd prime degree $\ell$. Let $\sigma$ be a generator of $G = \text{Gal}(K/k)$. In the group ring $\mathbb{Z}[G]$, define

$$s = 1 + \sigma + \cdots + \sigma^{\ell-1}.$$
Then the homomorphism $\iota : \mathcal{Z}[G] \to \mathcal{O}_\ell$ defined by mapping $\sigma \mapsto \zeta_\ell$ extends uniquely to an isomorphism (also denoted by $\iota$)

$$\mathcal{Z}[G]/(s)\mathcal{Z}[G] \cong \mathcal{O}_\ell.$$  

In this way, one may give $E_K/\mathcal{W}_K$ the structure of a (finitely generated) $\mathcal{O}_\ell$-module.

**Proof.** The map

$$\iota \left( \sum_{i=0}^{\ell-1} a_i \sigma^i \right) = \sum_{i=0}^{\ell-1} a_i \zeta_\ell^i$$

is clearly a surjective ring homomorphism whose kernel contains $s\mathcal{Z}[G]$ since $\sum_{i=0}^{\ell-1} \zeta_\ell^i = 0$. To see that the kernel is $s\mathcal{Z}[G]$, suppose $\sum_{i=0}^{\ell-1} a_i \zeta_\ell^i = 0$, with $a_i \in \mathcal{Z}$. Then the polynomial $g(x) = \sum_{i=0}^{\ell-1} a_i x^i$ has $\zeta_\ell$ as a root, hence is divisible by the minimal polynomial of $\zeta_\ell$ which is $\sum_{i=0}^{\ell-1} x^i$. Therefore, $a_0 = a_1 = \cdots = a_{\ell-1}$, and $\sum_{i=0}^{\ell-1} a_i \sigma^i \in (s)\mathcal{Z}[G]$. By Galois theory, $\mathcal{Z}[G]$ acts on $E_K$, preserving $\mathcal{W}_K$. For any $\varepsilon \in E_K$, $\varepsilon^s = N_{K/k}(\varepsilon) \in \mathcal{W}_K$, hence $\mathcal{Z}[G]/(s)\mathcal{Z}[G]$ acts on $E_K/\mathcal{W}_K$. We give $E_K/\mathcal{W}_K$ the structure of an $\mathcal{O}_\ell$-module via the inverse of $\iota$.

### 5.3.2 Special Minkowski Units

In connection with Corollary 3.3.7, note that $E_K/\mathcal{W}_K$ has free-rank one as $\mathcal{O}_\ell$-module (i.e. is generated, up to torsion, over $\mathcal{O}_\ell$ by a single element); furthermore, $E_K/\mathcal{W}_K$ is $\mathcal{O}_\ell$-free precisely when $K$ possesses a so-called "special Minkowski unit." In this direction, we have the following result, due, independently, to Moser and Gillard.

**Lemma 5.3.2 (Moser/Gillard)** There is an ideal $A^+_K$ of $\mathcal{Q}(\zeta_\ell + \zeta_\ell^{-1})$ such that $E_K/\mathcal{W}_K$ is $\mathcal{O}_\ell$-isomorphic to $(1 - \zeta_\ell)^e A^+_K \mathcal{O}_\ell$ with $e = 0$ or 1. Hence, if $\mathcal{Q}(\zeta_\ell + \zeta_\ell^{-1})$ has class number one, then $K$ has a special Minkowski unit, i.e. a unit $\varepsilon$ such that

$$E_K = \pm \varepsilon \mathcal{Z}[G].$$

**Proof.** See [Mo] or [Gi].

**Remark.** The smallest known prime $\ell$ for which $\mathcal{Q}(\zeta_\ell + \zeta_\ell^{-1})$ has class number larger than one is $\ell = 163$, and on the Generalized Riemann Hypothesis, there is no smaller $\ell$ with this property [vdL]. It would be interesting to investigate examples with $\ell = 163$.

### 5.3.3 The Gras-Gras Lemma

Checking the $p$-divisibility of the index is time-consuming because a priori, one must check many different products of type (5.1) for being a $p$th power in $E_K$. A clever
device of Gras-Gras allows us to single out only a few of these (at most \(n-1\) of them, in fact!) one of which must be a \(p\)th power if \(p\) divides the index. The utility of the following lemma in the elliptic case was pointed out by Hayashi [Ha1].

**Lemma 5.3.3 (Gras-Gras)** Suppose \(\ell\) is an odd prime, and let \(\Gamma = \text{Gal}(\mathbb{Q}(\zeta_{\ell})/\mathbb{Q})\). Recall that our elliptic group \(E_K\) is generated over \(\mathbb{Z}[\Gamma]\) by a single real elliptic unit \(u\), together with the roots of unity in \(K\). By multiplying \(u\) by \(-1\) if necessary, we may assume that \(N_{K^+/\mathbb{Q}}(u) = 1\). Suppose \(p\) is a prime different from \(\ell\) and let \(f = f_p\) be the order of \(p\) in \((\mathbb{Z}/\ell\mathbb{Z})^*\). Then the following are equivalent:

(i) \(p\) divides \([E_K : E_K]\);

(ii) \(p^f\) divides \([E_K : E_K]\);

(iii) there is a prime ideal \(\mathfrak{P}\) above \(p\) in \(\mathcal{O}_\ell\) such that for any \(\kappa \in \mathcal{O}_\ell\) and any prime ideal \(\mathfrak{F}\) of \(\mathcal{O}_\ell\) prime to \(p\) satisfying

\[
\mathfrak{F} \prod_{\gamma \in \Gamma, \gamma \neq 1} \mathfrak{P}^\gamma = (\kappa),
\]

there exists a \(\hat{u} \in E_K\) with

\[
u^\kappa = \hat{u}^{p^f}.
\]

**Proof.** See [Gr].

**Lemma 5.3.4** Suppose \(p\) is a prime primitive root modulo the odd prime \(\ell\). Let \(f_u(x)\) be the minimal polynomial of \(u\). Then \(p\) divides \([E_K : E_K]\) if and only if \(u \in E_K^\ell\).

**Proof.** Since \(p\) is inert in \(\mathbb{Q}(\zeta_{\ell})/\mathbb{Q}\), the prime \(\mathfrak{P}\) in \(\mathcal{O}_\ell\) above \(p\) is principal. Thus, by Lemma 5.3.3, \(p\) divides the index if and only if there is a unit \(\hat{u} \in E_K\) such that \(u^{p^{\ell-2}} = \hat{u}^{p^{f-1}}\), which is the case if and only if \(u\) is a \(p\)th power in \(E_K\) (recall the assumption \(N_{K^+/\mathbb{Q}}(u) = 1\)).

The following group-theoretical result gives another explanation for why \(p^f\) divides \([E_K : E_K]\) = \(H/(h/\ell)\), whenever \(p\) does.

**Lemma 5.3.5 (Iwasawa)** Suppose \(M/L\) is an extension of number fields of prime degree \(\ell = [M : L]\). Suppose \(p\) is a prime which does not divide \(\ell h_L\). Let \(f\) be the order of \(p\) in \((\mathbb{Z}/\ell\mathbb{Z})^*\). Let \(d_p(\text{Cl}(M))\) denote the \(p\)-rank of the ideal class group of \(M\), i.e. \(\dim_{\mathbb{Z}/p\mathbb{Z}} \text{Cl}(M)/\text{Cl}(M)^p\). Then,

\[
d_p(\text{Cl}(M)) \equiv 0 \mod f.
\]

In particular, if \(p\) divides \(h_M\), then the \(p\)-rank of the class group of \(M\) is at least \(f\).

**Proof.** This is a special case of [Iw, Theorem 1].
5.4 Computations and Tables

We used two systems to implement computation of the elliptic units and the 2-part of the class number of the Hilbert class field of complex quadratic fields of class number \( h = 3, 5, 7, 11, 13, 17, 19 \) and discriminant \(-D > -15,000\). There are 202 such fields. We found only four Hilbert class fields with even class number, three of which occur at \( h = 3 \) and one at \( h = 17 \). A heuristic argument for the scarcity of even class numbers in this situation can be given using the above theorem of Iwasawa and the Cohen-Lenstra philosophy: if the class number of one of our Hilbert class fields is even, then its 2-class group has large rank. But such groups have a lot of automorphisms, hence, according to Cohen-Lenstra, should occur in class groups only rarely.

Note that 2 is a primitive root modulo 3, 5, 11, 13, 19 so we need only check whether \( f_u(x) \) factors over \( \mathbb{Z} \) by Lemma 5.3.4 in these cases. For \( h = 7, 17 \), it is easily seen that (2) splits into two primes in \( \mathbb{Q}(\zeta_6) \), with generators \((1 \pm \sqrt{-7})/2\) and \((3 \pm \sqrt{17})/2\), respectively. So it is easy to find the two elements \( \kappa \) in Lemma 5.3.3; for example, with \( \ell = 7, p = 2, \kappa = 1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 \) or \(-\zeta_7 - \zeta_7^2 - \zeta_7^4\).

The two systems used were: Mathematica (Wolfram Research, Inc.) on a Sun Sparc Station 1 (Sun Microsystems, Inc.), and Kida's UBasic on an IBM PC 386. The latter turned out to be much faster at carrying out the 50-100 digit arithmetic operations, though the former was more useful for working with the minimal polynomial of the elliptic units.

5.4.1 Four Fields of Even Class Number

We found four fields whose Hilbert class field has even class number. We discuss each example briefly; the first three fields were investigated originally in 1927 by Berwick [Be], but the fourth seems to be new. Recall that \( \omega = (1 + \sqrt{-D})/2 \).

**D=283**

The class group of \( k \) has order 3 and is generated by \( \mathfrak{p}_7 = [7, \omega - 3] \). We compute the conjugates of \( u \):

\[
\begin{align*}
    u_0 &\approx -4.03032351377707122729135412114477529338499601085 - 0.49532479917720100350469615720595894487883684245i \\
    u_1 &\approx -4.03032351377707122729135412114477529338499601085 + 0.49532479917720100350469615720595894487883684245i \\
    u_2 &\approx 0.0606470275541424545827082422895505867699920217047.
\end{align*}
\]

The minimal polynomial of \( u \) is \( f_u(x) = -1 + 16x + 8x^2 + x^3 \). By Lemma 5.3.4, \( h_F \) is even if and only if \( u \) is a square in \( E_K \). We factor \( f_u(x^2) = (-1 + 4x + x^2)(1 + 4x + x^3) \). Thus, the minimal polynomial for a square root in \( E_K \) of \( u \) is \(-1 + 4x + x^3 \) (which
has discriminant $-283$), and $4$ divides $h_F = [E_K : E_K]$. By Lemma 5.3.5, $\text{Cl}(F)$ has a subgroup of type $(2, 2)$. In fact, with a little more work, one shows that $\text{Cl}(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**D=331**

The class group of $k$ has order 3 and is generated by $p_5 = [5, \omega + 3]$. We compute the conjugates of $-u$:

$$-u_0 \approx -2.024751904406922411856442095569075817493017806842 + 4.012585897889663610480129653092814851279162530312i$$

$$-u_1 \approx -2.024751904406922411856442095569075817493017806842 - 4.012585897889663610480129653092814851279162530312i$$

$$-u_2 \approx 0.0495038088138448237128841911381516349860356136834.$$  

The minimal polynomial of $-u$ is $f_{-u}(x) = -1 + 20x + 4x^2 + x^3$. By Lemma 5.3.4, $h_F$ is even if and only if $-u$ is a square in $E_K$. We factor $f_{-u}(x^2) = (1 + 4x - 2x^2 + x^3)(-1 + 4x + 2x^2 + x^3)$. Thus, the minimal polynomial for a square root in $E_K$ of $-u$ is $-1 + 4x + 2x^2 + x^3$ (with discriminant $-331$), and $4$ divides $[E_K : E_K]$. By Lemma 5.3.5, $\text{Cl}(F)$ has a subgroup of type $(2, 2)$. In fact, with a little more work, one shows that $\text{Cl}(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**D=643**

The class group of $k$ has order 3 and is generated by $p_7 = [7, \omega - 1]$. We compute the conjugates of $u$:

$$u_0 \approx 7.995530008666907553694259930125930861810659730623 + 6.92304413398995342636358956431991312817585993247i$$

$$u_1 \approx 7.995530008666907553694259930125930861810659730623 - 6.92304413398995342636358956431991312817585993247i$$

$$u_2 \approx 0.008939982661849826114801397481382763768680538753691.$$  

The minimal polynomial of $u$ is $f_u(x) = -1 + 112x - 16x^2 + x^3$. By Lemma 5.3.4, $h_F$ is even if and only if $u$ is a square in $E_K$. We factor $f_u(x^2) = (1 + 10x - 6x^2 + x^3)(-1 + 10x + 6x^2 + x^3)$. Thus, the minimal polynomial for a square root in $E_K$ of $u$ is $-1 + 10x + 6x^2 + x^3$ (with discriminant $-643$), and $4$ divides $[E_K : E_K]$. By Lemma 5.3.5, $\text{Cl}(F)$ has a subgroup of type $(2, 2)$. Once again, one shows that $\text{Cl}(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**D=14947**

Here the class group of $k$ has order 17, and is generated by $p_{13} = [13, \omega + 4]$. The minimal polynomial of $u$ is listed in the tables. Since $2$ has order 8 modulo 17, there are two elements $\kappa, \kappa' \in \mathbb{Z}[\zeta]$ of norm $2^8$ coming from Lemma 5.3.3:

$$\kappa = 1 - \zeta_{17} - \zeta_{17}^2 - \zeta_{17}^4 - \zeta_{17}^8 - \zeta_{17}^9 - \zeta_{17}^{13} - \zeta_{17}^{15} - \zeta_{17}^{16}$$

51
\( \kappa' = 2 + \zeta_{17} + \zeta_{17}^2 + \zeta_{17}^4 + \zeta_{17}^8 + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16}. \)

The class number of \( F \) is even if and only if either \( u^e \) or \( u^{e'} \) is a square in \( E_K \) (or \( E_{K^+} \) by Lemma 5.2.3). While \( u^{e'} \) is not a square in \( E_K \), we check that \( f_{u^{e'}}(x^2) = -g(-x)g(x) \) where

\[
g(x) = -1 - 2300086x - 2344251342340x^2 - 134648877974326133x^3 - 400429981823620601601338x^4 - 203270153155618791507589468x^5 + 2027349707638309969640000265801x^6 + 539542835710852062090192093800284x^7 - 2815299784245479575058878508234384417x^8 - 1159772563649201912351047755153096481x^9 - 1670938340840402395547665773430708410x^{10} - 6005391952134971058362418722142373x^{11} - 9051641052483621324452851774544x^{12} - 5656085682390322547297038398x^{13} - 12670151804875560451800219x^{14} - 1903320295284742610x^{15} - 1223647520068x^{16} + x^{17}.
\]

As a slight check on the calculations, one verifies that the discriminant of \( g(x) \) is divisible by 149478. By Lemma 5.2.3, \( u^e \) is a square in \( E_{K^+} \) so in fact, by Lemma 5.3.3, it is an eighth power in \( E_K \), although it is not even a fourth power in \( E_{K^+} \). At any rate, the class number of \( F \) is even, hence by Lemma 5.3.5, \( \text{Cl}(F) \) has a subgroup isomorphic to \((\mathbb{Z}/2\mathbb{Z})^8\). It is not clear, though it is likely, that \( K \) has an infinite 2-class field tower. By a result of Bond [Bo] the class group of the 2-class field of \( F' \) has 2-rank at least 11.

### 5.4.2 Tables

The tables are arranged according to \( h \), the class number of \( k \), and each table shows the absolute value of the discriminant, \( D \) (in increasing order), and the minimal polynomial \( f_u(x) \) of an elliptic unit \( u \in E_{K^+} \) with \( N_{K^+/\mathbb{Q}}(u) = 1 \) which, together with its conjugates, generates an elliptic group of index \( h_F \) in \( E_K \).
<table>
<thead>
<tr>
<th>$D$</th>
<th>$f_u(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>$-1 + x^2 + x^3$</td>
</tr>
<tr>
<td>31</td>
<td>$-1 + x + x^3$</td>
</tr>
<tr>
<td>59</td>
<td>$-1 + 2x + x^3$</td>
</tr>
<tr>
<td>83</td>
<td>$-1 + 2x + 2x^2 + x^3$</td>
</tr>
<tr>
<td>107</td>
<td>$-1 + 4x - 2x^2 + x^3$</td>
</tr>
<tr>
<td>139</td>
<td>$-1 + 6x - 4x^2 + x^3$</td>
</tr>
<tr>
<td>211</td>
<td>$-1 + 10x - 6x^2 + x^3$</td>
</tr>
<tr>
<td>283</td>
<td>$-1 + 16x + 8x^2 + x^3$</td>
</tr>
<tr>
<td>307</td>
<td>$-1 + 19x + 5x^2 + x^3$</td>
</tr>
<tr>
<td>331</td>
<td>$-1 + 20x + 4x^2 + x^3$</td>
</tr>
<tr>
<td>379</td>
<td>$-1 + 26x + 10x^2 + x^3$</td>
</tr>
<tr>
<td>499</td>
<td>$-1 + 48x + 6x^2 + x^3$</td>
</tr>
<tr>
<td>547</td>
<td>$-1 + 79x - 15x^2 + x^3$</td>
</tr>
<tr>
<td>643</td>
<td>$-1 + 112x - 16x^2 + x^3$</td>
</tr>
<tr>
<td>883</td>
<td>$-1 + 364x - 10x^2 + x^3$</td>
</tr>
<tr>
<td>907</td>
<td>$-1 + 402x - 28x^2 + x^3$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>47</td>
<td>$-1 - 2x - 2x^2 - x^3 + x^5$</td>
</tr>
<tr>
<td>79</td>
<td>$-1 + x - x^2 + 2x^3 - 3x^4 + x^5$</td>
</tr>
<tr>
<td>103</td>
<td>$-1 - 2x - 3x^2 - 3x^3 - x^4 + x^5$</td>
</tr>
<tr>
<td>127</td>
<td>$-1 + x + 2x^2 - x^3 - 3x^4 + x^5$</td>
</tr>
<tr>
<td>131</td>
<td>$-1 - x + x^2 + 3x^3 - 5x^4 + x^5$</td>
</tr>
<tr>
<td>179</td>
<td>$-1 + 2x - 5x^2 + x^3 - 6x^4 + x^5$</td>
</tr>
<tr>
<td>227</td>
<td>$-1 + 5x - 9x^2 + 9x^3 - 9x^4 + x^5$</td>
</tr>
<tr>
<td>347</td>
<td>$-1 - 7x - 21x^2 - 27x^3 - 13x^4 + x^5$</td>
</tr>
<tr>
<td>443</td>
<td>$-1 + 4x + 3x^2 - 17x^3 - 22x^4 + x^5$</td>
</tr>
<tr>
<td>523</td>
<td>$-1 - 6x - 59x^2 + x^3 - 64x^4 + x^5$</td>
</tr>
<tr>
<td>571</td>
<td>$-1 + 8x - 41x^2 - 45x^3 - 66x^4 + x^5$</td>
</tr>
<tr>
<td>619</td>
<td>$-1 + 11x + -51x^2 - 77x^3 - 81x^4 + x^5$</td>
</tr>
<tr>
<td>683</td>
<td>$-1 - 6x + 5x^2 + 41x^3 - 56x^4 + x^5$</td>
</tr>
<tr>
<td>691</td>
<td>$-1 - 18x - 85x^2 - 3x^3 - 110x^4 + x^5$</td>
</tr>
<tr>
<td>739</td>
<td>$-1 + 18x - 117x^2 + 161x^3 - 134x^4 + x^5$</td>
</tr>
<tr>
<td>787</td>
<td>$-1 - 12x - 293x^2 - 329x^3 - 238x^4 + x^5$</td>
</tr>
<tr>
<td>947</td>
<td>$-1 - 5x - 7x^2 + 103x^3 - 125x^4 + x^5$</td>
</tr>
<tr>
<td>1051</td>
<td>$-1 - 4x - 239x^2 - 585x^3 - 396x^4 + x^5$</td>
</tr>
<tr>
<td>1123</td>
<td>$-1 + 9x - 518x^2 - 74x^3 - 697x^4 + x^5$</td>
</tr>
<tr>
<td>1723</td>
<td>$-1 + 65x - 5097x^2 - 1023x^3 - 5885x^4 + x^5$</td>
</tr>
<tr>
<td>1747</td>
<td>$-1 + 167x - 7235x^2 + 4143x^3 - 7209x^4 + x^5$</td>
</tr>
<tr>
<td>1867</td>
<td>$-1 - 2x - 4281x^2 - 6423x^3 - 6142x^4 + x^5$</td>
</tr>
<tr>
<td>2203</td>
<td>$-1 - 144x - 7327x^2 + 20235x^3 - 14180x^4 + x^5$</td>
</tr>
<tr>
<td>2347</td>
<td>$-1 - 213x - 36007x^2 + 42771x^3 - 37073x^4 + x^5$</td>
</tr>
<tr>
<td>2683</td>
<td>$-1 + 380x - 52013x^2 + 36527x^3 - 68110x^4 + x^5$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_0(x)$</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>71</td>
<td>$-1 + 2x + 4x^3 + 2x^5 - x^6 + x^7$</td>
</tr>
<tr>
<td>151</td>
<td>$-1 - x - x^2 - 3x^4 - x^5 - 3x^6 + x^7$</td>
</tr>
<tr>
<td>223</td>
<td>$-1 - x^2 - 4x^3 + x^4 - 5x^6 + x^7$</td>
</tr>
<tr>
<td>251</td>
<td>$-1 - 5x - 6x^2 + 2x^3 + 4x^4 - 2x^5 - 9x^6 + x^7$</td>
</tr>
<tr>
<td>463</td>
<td>$-1 - 3x - 7x^2 - 7x^3 - 8x^4 - 9x^5 - 11x^6 + x^7$</td>
</tr>
<tr>
<td>467</td>
<td>$-1 - 6x - 7x^2 + 3x^3 - 3x^4 + 23x^5 - 26x^6 + x^7$</td>
</tr>
<tr>
<td>487</td>
<td>$-1 + x - 4x^2 + 7x^3 - 4x^4 + 4x^5 - 13x^6 + x^7$</td>
</tr>
<tr>
<td>587</td>
<td>$-1 - x - 16x^2 + 12x^3 - 20x^4 - 24x^5 - 39x^6 + x^7$</td>
</tr>
<tr>
<td>811</td>
<td>$-1 + 23x - 178x^2 + 434x^3 - 624x^4 + 506x^5 - 177x^6 + x^7$</td>
</tr>
<tr>
<td>827</td>
<td>$-1 + 7x - 38x^2 + 54x^3 - 112x^4 + 146x^5 - 89x^6 + x^7$</td>
</tr>
<tr>
<td>859</td>
<td>$-1 - 5x - 136x^2 - 136x^3 - 268x^4 - 40x^5 - 207x^6 + x^7$</td>
</tr>
<tr>
<td>1163</td>
<td>$-1 - 12x - 71x^2 - 107x^3 - 159x^4 - 3x^5 - 222x^6 + x^7$</td>
</tr>
<tr>
<td>1171</td>
<td>$-1 + 24x - 341x^2 + 541x^3 - 41x^4 + 253x^5 - 580x^6 + x^7$</td>
</tr>
<tr>
<td>1483</td>
<td>$-1 - 40x - 1312x^2 + 3885x^3 - 4641x^4 + 4058x^5 - 2142x^6 + x^7$</td>
</tr>
<tr>
<td>1523</td>
<td>$-1 + 17x - 70x^2 - 60x^3 - 330x^4 - 650x^5 - 523x^6 + x^7$</td>
</tr>
<tr>
<td>1627</td>
<td>$-1 - 52x - 2350x^2 - 679x^3 - 5033x^4 - 662x^5 - 3224x^6 + x^7$</td>
</tr>
<tr>
<td>1787</td>
<td>$-1 - 4x - 146x^2 - 191x^3 - 785x^4 + 2x^5 - 924x^6 + x^7$</td>
</tr>
<tr>
<td>1987</td>
<td>$-1 + 54x - 5686x^2 - 2215x^3 + 8083x^4 - 3408x^5 - 8348x^6 + x^7$</td>
</tr>
<tr>
<td>2011</td>
<td>$-1 + 85x - 2270x^2 + 10816x^3 - 20598x^4 + 17310x^5 - 5367x^6 + x^7$</td>
</tr>
<tr>
<td>2083</td>
<td>$-1 + 105x - 15712x^2 - 6686x^3 + 19694x^4 - 5388x^5 - 17101x^6 + x^7$</td>
</tr>
<tr>
<td>2179</td>
<td>$-1 - 99x - 2490x^2 - 96x^3 - 7906x^4 + 5534x^5 - 7879x^6 + x^7$</td>
</tr>
<tr>
<td>2251</td>
<td>$-1 - 10x - 2872x^2 - 10039x^3 - 16857x^4 - 11152x^5 - 9246x^6 + x^7$</td>
</tr>
<tr>
<td>2467</td>
<td>$-1 - 166x - 15444x^2 - 28543x^3 - 41993x^4 - 31676x^5 - 26178x^6 + x^7$</td>
</tr>
<tr>
<td>2707</td>
<td>$-1 + 214x - 22340x^2 + 29873x^3 - 65105x^4 + 22328x^5 - 44458x^6 + x^7$</td>
</tr>
<tr>
<td>3019</td>
<td>$-1 + 148x - 10313x^2 + 24261x^3 - 77069x^4 + 79601x^5 - 44492x^6 + x^7$</td>
</tr>
<tr>
<td>3067</td>
<td>$-1 + 169x - 153036x^2 - 3218x^3 - 314654x^4 + 14452x^5 - 180021x^6 + x^7$</td>
</tr>
<tr>
<td>3187</td>
<td>$-1 - 787x - 159924x^2 - 64498x^3 + 42926x^4 - 128964x^5 - 206273x^6 + x^7$</td>
</tr>
<tr>
<td>3907</td>
<td>$-1 + 1155x - 580316x^2 + 296724x^3 - 501876x^4 + 863956x^5 - 871043x^6 + x^7$</td>
</tr>
<tr>
<td>4603</td>
<td>$-1 + 3173x - 3044222x^2 + 8737396x^3 - 12888730x^4 + 9529898x^5 - 3660515x^6 + x^7$</td>
</tr>
<tr>
<td>5107</td>
<td>$-1 - 1284x - 9975791x^2 + 13060981x^3 - 7848235x^4 + 12441833x^5 - 11434554x^6 + x^7$</td>
</tr>
<tr>
<td>5923</td>
<td>$-1 + 9980x - 37245663x^2 + 86617409x^3 - 108558395x^4 + 103524961x^5 - 44709246x^6 + x^7$</td>
</tr>
<tr>
<td>( D )</td>
<td>( f_u(x) )</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>167</td>
<td>(-1 - x^2 + 5x^4 - 4x^5 - 10x^4 - 6x^5 - 11x^6 - 7x^7 - 9x^8 - 4x^9 - 2x^{10} + x^{11})</td>
</tr>
<tr>
<td>271</td>
<td>(-1 - x^2 - 3x^4 + 3x^5 + 6x^6 + 3x^7 - 5x^8 - 6x^9 - 5x^{10} + x^{11})</td>
</tr>
<tr>
<td>659</td>
<td>(-1 + 7x^2 - 7x^3 - 19x^4 + 43x^5 + 5x^6 - 91x^7 + 157x^8 - 97x^9 - 49x^{10} + x^{11})</td>
</tr>
<tr>
<td>967</td>
<td>(-1 - 2x + x^2 - 13x^3 - 6x^4 + 18x^5 - 81x^6 + 99x^7 - 122x^8 + 68x^9 - 43x^{10} + x^{11})</td>
</tr>
<tr>
<td>1283</td>
<td>(-1 + 16x - 87x^2 + 141x^3 - 272x^4 + 55x^5 - 139x^6 + 212x^7 - 209x^8 + 135x^9 - 300x^{10} + x^{11})</td>
</tr>
<tr>
<td>1303</td>
<td>(-1 - 8x - 30x^2 - 57x^3 - 67x^4 - 59x^5 - 73x^6 - 68x^7 - 33x^8 - 57x^9 - 79x^{10} + x^{11})</td>
</tr>
<tr>
<td>1307</td>
<td>(-1 + 17x - 87x^2 + 77x^3 + 55x^4 - x^5 - 375x^6 - 281x^7 + 87x^8 + 475x^9 - 319x^{10} + x^{11})</td>
</tr>
<tr>
<td>1459</td>
<td>(-1 - 7x - 581x^2 + 1111x^3 - 2999x^4 + 2555x^5 - 3731x^6 + 1243x^7 - 2047x^8 - 43x^9 - 1333x^{10} + x^{11})</td>
</tr>
<tr>
<td>1531</td>
<td>(-1 - 30x - 758x^2 - 1387x^3 - 939x^4 + 1432x^5 + 66x^6 - 1161x^7 - 2121x^8 - 123x^9 - 1620x^{10} + x^{11})</td>
</tr>
<tr>
<td>1699</td>
<td>(-1 - 27x - 1007x^2 + 105x^3 + 75x^4 - 357x^5 + 4973x^6 - 1617x^7 - 4013x^8 + 1787x^9 - 2511x^{10} + x^{11})</td>
</tr>
<tr>
<td>2027</td>
<td>(-1 - 21x - 215x^2 - 311x^3 - 1079x^4 + 347x^5 - 2067x^6 + 753x^7 - 2741x^8 - 21x^9 - 1493x^{10} + x^{11})</td>
</tr>
<tr>
<td>2267</td>
<td>(-1 + 10x - 199x^2 - 1025x^3 - 1432x^4 - 3025x^5 - 6623x^6 - 6106x^7 - 1124x^8 - 6159x^9 - 2344x^{10} + x^{11})</td>
</tr>
<tr>
<td>2539</td>
<td>(-1 + 119x - 4611x^2 - 579x^3 - 7447x^4 + 52555x^5 - 136587x^6 + 143909x^7 - 123761x^8 + 41047x^9 - 17133x^{10} + x^{11})</td>
</tr>
<tr>
<td>2731</td>
<td>(-1 - 92x - 6949x^2 - 45050x^3 - 138258x^4 - 267561x^5 - 360727x^6 - 342212x^7 - 231523x^8 - 100109x^9 - 25342x^{10} + x^{11})</td>
</tr>
<tr>
<td>2851</td>
<td>(-1 - 7x - 7661x^2 + 29515x^3 - 82871x^4 + 191043x^5 - 308179x^6 + 350459x^7 - 278007x^8 + 137289x^9 - 32157x^{10} + x^{11})</td>
</tr>
<tr>
<td>2971</td>
<td>(-1 + 128x - 9925x^2 + 53157x^3 - 211950x^4 + 430911x^5 - 538615x^6 + 326888x^7 - 17419x^8 + 5107x^9 - 40586x^{10} + x^{11})</td>
</tr>
<tr>
<td>3203</td>
<td>(-1 + 37x - 965x^2 + 6035x^3 - 16339x^4 + 24571x^5 - 38403x^6 + 65823x^7 - 75375x^8 + 44521x^9 - 11257x^{10} + x^{11})</td>
</tr>
<tr>
<td>3347</td>
<td>(-1 + 26x - 845x^2 + 155x^3 - 4898x^4 - 1337x^5 - 35843x^6 - 53002x^7 - 56815x^8 - 35535x^9 - 14014x^{10} + x^{11})</td>
</tr>
<tr>
<td>3499</td>
<td>(-1 - 124x + 20553x^2 - 62467x^3 - 226666x^4 + 114679x^5 - 336183x^6 - 1002868x^7 + 53185x^8 + 328567x^9 - 107382x^{10} + x^{11})</td>
</tr>
<tr>
<td>3739</td>
<td>(-1 + 296x - 28754x^2 + 60949x^3 - 202727x^4 + 37250x^5 - 428774x^6 - 207077x^7 - 411733x^8 - 204754x^9 - 163072x^{10} + x^{11})</td>
</tr>
<tr>
<td>3931</td>
<td>(-1 - 209x - 37413x^2 + 163441x^3 - 608793x^4 - 1311421x^5 - 2067299x^6 - 2185531x^7 - 1670847x^8 - 789323x^9 - 225627x^{10} + x^{11})</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_a(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>4051</td>
<td>$-1 - 31x - 42953x^2 - 219401x^3 - 196703x^4 + 533487x^5 + 201377x^6 - 2215513x^7 - 2106711x^8 + 111033x^9 - 275289x^{10} + x^{11}$</td>
</tr>
<tr>
<td>5179</td>
<td>$-1 - 820x - 169173x^2 + 678705x^3 - 2774074x^4 + 8668303x^5 - 21122499x^6 + 34572536x^7 - 36597275x^8 + 12647275x^9 - 1571682x^{10} + x^{11}$</td>
</tr>
<tr>
<td>5653</td>
<td>$-1 + 8398394x - 14854221x^2 + 21997495x^3 - 6296206x^4 + 29693963x^5 - 3735859x^6 + 11566574x^7 - 7576935x^8 + 2003973x^9 + 2822x^{10} + x^{11}$</td>
</tr>
<tr>
<td>6163</td>
<td>$-1 - 3788x - 3591973x^2 - 4202351x^3 - 25004342x^4 - 1969157x^5 - 3638215x^6 - 19165688x^7 - 30972087x^8 + 3172615x^9 - 16911014x^{10} + x^{11}$</td>
</tr>
<tr>
<td>6547</td>
<td>$-1 + 13149x - 43872478x^2 + 55968668x^3 - 215242299x^4 + 183916761x^5 - 372179181x^6 + 200124087x^7 - 270804488x^8 + 72213558x^9 - 69610673x^{10} + x^{11}$</td>
</tr>
<tr>
<td>7027</td>
<td>$-1 + 833x - 10104117x^2 - 43021433x^3 - 123445359x^4 - 184242077x^5 - 238998931x^6 - 264085669x^7 - 182512527x^8 - 118802531x^9 - 55830189x^{10} + x^{11}$</td>
</tr>
<tr>
<td>7507</td>
<td>$-1 - 4943x - 17264599x^2 + 99169813x^3 - 235007585x^4 + 285076103x^5 - 311387423x^6 + 313361615x^7 - 207501361x^8 + 169891963x^9 - 105021583x^{10} + x^{11}$</td>
</tr>
<tr>
<td>7603</td>
<td>$-1 - 23500x - 185497072x^2 + 889915169x^3 - 103765787x^4 + 160410242x^5 - 107087508x^6 - 93607025x^7 - 182028581x^8 + 430201762x^9 - 310426426x^{10} + x^{11}$</td>
</tr>
<tr>
<td>7867</td>
<td>$-1 - 9219x - 25752304x^2 - 112176072x^3 - 101375577x^4 + 140517573x^5 - 1211612659x^6 + 2232524787x^7 - 2184557146x^8 + 988997500x^9 - 166483305x^{10} + x^{11}$</td>
</tr>
<tr>
<td>8443</td>
<td>$-1 + 29353x - 388177191x^2 + 288927033x^3 - 29175965x^4 - 451014821x^5 - 889226723x^6 - 295120325x^7 - 601639549x^8 - 532811037x^9 - 947958527x^{10} + x^{11}$</td>
</tr>
<tr>
<td>9283</td>
<td>$-1 + 54466x + 1198722371x^2555965759x^3 - 14539942028x^4 + 27870197863x^5 - 36670141327x^6 + 35328991558x^7 - 27218960117x^8 + 13257800465x^9 - 2741854700x^{10} + x^{11}$</td>
</tr>
<tr>
<td>9403</td>
<td>$-1 + 12695x - 212052790x^2 + 1629800354x^3 + 46592443x^4 + 522305919x^5 - 9591292755x^6 + 459970497x^7 - 504759326x^8 + 2810339422x^9 - 4169927531x^{10} + x^{11}$</td>
</tr>
<tr>
<td>9643</td>
<td>$-1 + 70334x - 1487220977x^2 - 41570689x^3 - 6227130658x^4 + 7695089239x^5 - 17670440767x^6 + 17638972982x^7 - 16361522423x^8 + 6590658881x^9 - 4259028310x^{10} + x^{11}$</td>
</tr>
<tr>
<td>9787</td>
<td>$-1 + 27690x - 1737785153x^2 - 677419073x^3 - 1105709722x^4 + 8860133921x^5 - 4941239275x^6 + 266277882x^7 - 8363632655x^8 - 11520522563x^9 - 5067751210x^{10} + x^{11}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>10987</td>
<td>$-1 + 61314405984x + 114364774708x^2 + 95591958621x^3 +$</td>
</tr>
<tr>
<td></td>
<td>$54262052109x^4 + 29904891994x^5 + 36289831148x^6 + 105165742891x^7 +$</td>
</tr>
<tr>
<td></td>
<td>$134827732039x^8 + 63034014574x^9 + 477598x^{10} + x^{11}$</td>
</tr>
<tr>
<td>13267</td>
<td>$-1 + 846990888455x - 1799023588057x^2 + 2744145123395x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$2368121024661x^4 + 1888601286699x^5 - 2541375200547x^6 +$</td>
</tr>
<tr>
<td></td>
<td>$3434423365701x^7 - 2818840264043x^8 + 1023274107337x^9 +$</td>
</tr>
<tr>
<td></td>
<td>$1918897x^{10} + x^{11}$</td>
</tr>
<tr>
<td>14107</td>
<td>$-1 + 2029473072556x - 5319047290345x^2 + 7882967680809x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$8072917885098x^4 + 8987400284963x^5 - 10201119435567x^6 +$</td>
</tr>
<tr>
<td></td>
<td>$9630695008816x^7 - 5602956523931x^8 + 1743400665127x^9 -$</td>
</tr>
<tr>
<td></td>
<td>$2447378x^{10} + x^{11}$</td>
</tr>
<tr>
<td>14683</td>
<td>$-1 + 2586357818926x + 1090050369743x^2 + 89406422411x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$721860349034x^4 - 22726786509x^5 - 83643198619x^6 - 1372974284214x^7 +$</td>
</tr>
<tr>
<td></td>
<td>$1426724418293x^8 + 1550765289497x^9 + 2097906x^{10} + x^{11}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
</tr>
<tr>
<td>191</td>
<td>$-1 + 2x - 4x^3 + 5x^4 - x^5 - 5x^6 + 11x^7 - 19x^8 + 22x^9 - 16x^{10} + 10x^{11} - 6x^{12} + x^{13}$</td>
</tr>
<tr>
<td>263</td>
<td>$-1 + 6x - 15x^2 + 21x^3 - 19x^4 + 13x^5 - 12x^6 + 22x^7 - 36x^8 + 38x^9 - 27x^{10} + 16x^{11} - 8x^{12} + x^{13}$</td>
</tr>
<tr>
<td>607</td>
<td>$-1 + 2x - 3x^2 + x^3 + 7x^4 + 9x^5 - 21x^6 - 21x^7 + 3x^8 + 34x^9 + 16x^{10} - 15x^{11} - 17x^{12} + x^{13}$</td>
</tr>
<tr>
<td>631</td>
<td>$-1 + 2x - 3x^2 + 21x^3 - 25x^4 - 17x^5 + 27x^6 - 71x^7 - 77x^8 - 69x^{10} - 33x^{11} - 17x^{12} + x^{13}$</td>
</tr>
<tr>
<td>727</td>
<td>$-1 + 4x - 8x^2 + 5x^3 - 6x^4 - 4x^5 - 8x^7 - 30x^8 + 15x^9 - 41x^{10} + 23x^{11} - 25x^{12} + x^{13}$</td>
</tr>
<tr>
<td>1019</td>
<td>$-1 - 41x^2 + 111x^3 - 333x^4 + 599x^5 - 835x^6 + 1091x^7 - 947x^8 + 661x^9 - 591x^{10} + 45x^{11} - 152x^{12} + x^{13}$</td>
</tr>
<tr>
<td>1451</td>
<td>$-1 - 10x - 120x^2 - 545x^3 - 1033x^4 - 1072x^5 - 1997x^6 - 4383x^7 - 4436x^8 - 1291x^9 + 737x^{10} + 269x^{11} - 446x^{12} + x^{13}$</td>
</tr>
<tr>
<td>1499</td>
<td>$-1 + 14x - 33x^2 - 263x^3 - 233x^4 - 103x^5 - 891x^6 - 1059x^7 + 501x^8 + 1651x^9 - 1859x^{10} - 365x^{11} - 496x^{12} + x^{13}$</td>
</tr>
<tr>
<td>1667</td>
<td>$-1 - 6x - 126x^2 - 157x^3 - 669x^4 - 1368x^5 - 1815x^6 - 2071x^7 - 2458x^8 - 2151x^9 - 1767x^{10} - 1544x^{11} - 716x^{12} + x^{13}$</td>
</tr>
<tr>
<td>1907</td>
<td>$-1 + 13x - 144x^2 - 196x^3 + 488x^4 + 1408x^5 + 298x^6 - 4814x^7 - 9552x^8 - 8428x^9 - 4776x^{10} - 2336x^{11} - 1177x^{12} + x^{13}$</td>
</tr>
<tr>
<td>2131</td>
<td>$-1 - 51x - 2286x^2 - 42x^3 - 520x^4 - 21014x^5 - 33204x^6 - 45286x^7 - 53178x^8 - 40902x^9 - 41120x^{10} - 19714x^{11} - 7067x^{12} + x^{13}$</td>
</tr>
<tr>
<td>2143</td>
<td>$-1 - 12x^2 - 43x^3 + 14x^4 + 268x^5 + 396x^6 - 155x^7 - 1292x^8 - 2161x^9 - 2058x^{10} - 1147x^{11} - 299x^{12} + x^{13}$</td>
</tr>
<tr>
<td>2371</td>
<td>$-1 + 75x - 3466x^2 - 420x^3 - 18598x^4 - 17646x^5 - 49702x^6 - 68340x^7 - 75358x^8 - 83756x^9 - 47218x^{10} - 12938x^{11} - 1209x^{12} + x^{13}$</td>
</tr>
<tr>
<td>2659</td>
<td>$-1 - 30x - 5701x^2 - 11339x^3 - 46657x^4 - 1979x^5 - 26355x^6 - 29435x^7 - 115779x^8 + 192451x^9 - 192615x^{10} + 98371x^{11} - 21924x^{12} + x^{13}$</td>
</tr>
<tr>
<td>2963</td>
<td>$-1 - 10x - 561x^2 + 441x^3 - 4629x^4 - 1379x^5 - 3895x^6 + 5925x^7 + 6677x^8 + 9507x^9 - 6407x^{10} - 4225x^{11} - 7716x^{12} + x^{13}$</td>
</tr>
<tr>
<td>3083</td>
<td>$-1 - 8x - 661x^2 - 1417x^3 - 5817x^4 - 1781x^5 - 6423x^6 - 13609x^7 - 9115x^8 - 33415x^9 - 45303x^{10} + 3397x^{11} - 9336x^{12} + x^{13}$</td>
</tr>
<tr>
<td>3691</td>
<td>$-1 - 317x - 27133x^2 - 65791x^3 - 282538x^4 - 410040x^5 - 511069x^6 - 540359x^7 - 863218x^8 - 1014180x^9 - 837605x^{10} - 498155x^{11} - 150161x^{12} + x^{13}$</td>
</tr>
<tr>
<td>4003</td>
<td>$-1 - 607x - 187186x^2 - 11358x^3 - 54808x^4 + 438558x^5 + 1033252x^6 - 1304258x^7 - 1056526x^8 + 680750x^9 + 515096x^{10} + 476098x^{11} - 553843x^{12} + x^{13}$</td>
</tr>
<tr>
<td>4507</td>
<td>$-1 - 1283x - 413825x^2 + 950317x^3 - 764859x^4 + 88959x^5 - 649834x^6 + 32306x^7 + 1652761x^8 + 2857339x^9 - 1270653x^{10} - 3006039x^{11} - 1318389x^{12} + x^{13}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_{0}(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
</tr>
<tr>
<td>4643</td>
<td>$-1 + 49x - 2864x^2 + 5112x^3 - 20796x^4 - 61688x^5 - 83202x^6 - 11282x^7 - 69680x^8 - 110856x^9 - 62500x^{10} - 27880x^{11} - 84397x^{12} + x^{13}$</td>
</tr>
<tr>
<td>5347</td>
<td>$-1 + 1924x - 1279956x^2 + 706003x^3 - 4424605x^4 + 10109050x^5 - 2341585x^6 + 1671095x^7 - 2722980x^8 + 756625x^9 - 6555847x^{10} + 6519178x^{11} - 5054802x^{12} + x^{13}$</td>
</tr>
<tr>
<td>5419</td>
<td>$-1 + 708x - 236301x^2 + 2954507x^3 - 14927209x^4 + 40961219x^5 - 72420695x^6 + 88007295x^7 - 76830079x^8 + 48979433x^9 - 23212227x^{10} + 8785697x^{11} - 2219812x^{12} + x^{13}$</td>
</tr>
<tr>
<td>5779</td>
<td>$-1 - 1164x - 347949x^2 - 2291989x^3 - 4269649x^4 - 3547957x^5 - 10837823x^6 - 10006545x^7 - 8642911x^8 - 1234551x^9 - 6529725x^{10} - 5057191x^{11} - 3674092x^{12} + x^{13}$</td>
</tr>
<tr>
<td>6619</td>
<td>$-1 + 1323x - 822869x^2 - 5685215x^3 - 19315334x^4 - 28598664x^5 - 38124205x^6 - 60663567x^7 - 102221486x^8 - 96236292x^9 - 27445181x^{10} - 7831067x^{11} - 11236757x^{12} + x^{13}$</td>
</tr>
<tr>
<td>7243</td>
<td>$-1 - 6908x - 12981396x^2 - 27775005x^3 - 28530953x^4 + 89342378x^5 + 26633415x^6 + 66656595x^7 + 93767452x^8 - 130141507x^9 - 63945855x^{10} - 31946658x^{11} - 7438358x^{12} + x^{13}$</td>
</tr>
<tr>
<td>7963</td>
<td>$-1 + 504503712x + 717509253x^2 - 51289545x^3 - 312413739x^4 + 15206371x^5 + 16270039x^6 - 26566357x^7 + 532120415x^8 - 30470059x^9 - 433583153x^{10} + 205634345x^{11} + 27790x^{12} + x^{13}$</td>
</tr>
<tr>
<td>9547</td>
<td>$-1 + 22583x - 144907308x^2 - 781165162x^3 - 3855206178x^4 - 10292522764x^5 - 22540471528x^6 - 32217460592x^7 - 3806693136x^8 - 27870495470x^9 - 18081019526x^{10} - 5081530548x^{11} - 1258060831x^{12} + x^{13}$</td>
</tr>
<tr>
<td>9739</td>
<td>$-1 + 6385x - 15228383 + 122410651x^3 - 667801611x^4 + 1420059379x^5 - 803375646x^6 - 630619898x^7 - 143263519x^8 + 269241784x^9 - 3486753243x^{10} + 1897953671x^{11} - 423517949x^{12} + x^{13}$</td>
</tr>
<tr>
<td>11467</td>
<td>$-1 - 48052889745x - 28740101544x^2 - 16501071200x^3 + 9969711440x^4 - 15228914916x^5 - 54570570994x^6 + 41927959822x^7 + 5963904848x^8 - 16859497400x^9 - 29325252720x^{10} + 33082793052x^{11} + 312267x^{12} + x^{13}$</td>
</tr>
<tr>
<td>11587</td>
<td>$-1 + 55001161173x + 89503894627x^2 - 148470535055x^3 - 307810857984x^4 + 116362782302x^5 + 406536767631x^6 + 19481221713x^7 - 244664405420x^8 - 63796869354x^9 + 56494299095x^{10} + 2221499689x^{11} - 12567x^{12} + x^{13}$</td>
</tr>
<tr>
<td>11827</td>
<td>$-1 + 52494307348x + 235924136658x^2 + 749108519979x^3 + 1596394155499x^4 + 2049680387234x^5 + 1691384182653x^6 + 1055901802899x^7 + 631789862614x^8 + 354856850309x^9 + 120702182973x^{10} + 17095450374x^{11} - 175180x^{12} + x^{13}$</td>
</tr>
<tr>
<td>11923</td>
<td>$-1 + 58296293506x - 212844694271x^2 + 477580419265x^3 - 726767275135x^4 + 814543726901x^5 - 767676247989x^6 + 668987769657x^7 + 496367978237x^8 + 283614484475x^9 + 101649174397x^{10} + 16813372295x^{11} - 164794x^{12} + x^{13}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>12043</td>
<td>$-1 + 18718509932x + 71827892568x^2 + 172802194339x^3 + 292250130527x^4 + 364940561682x^5 + 35834903571x^6 + 268940238667x^7 + 152478552176x^8 + 63499532589x^9 + 15219793497x^{10} + 1468341862x^{11} + 76590x^{12} + x^{13}$</td>
</tr>
<tr>
<td>14347</td>
<td>$-1 + 1593351568977x - 10212558120106x^2 + 31767420092910x^3 - 63196894066464x^4 + 89153963200294x^5 - 93042810011032x^6 + 72952057472526x^7 - 42878483636694x^8 + 18340547591074x^9 - 5272252188160x^{10} + 800966129754x^{11} + 1169449x^{12} + x^{13}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_n(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>383</td>
<td>$-1 + 22x + 221x^2 + 1089x^3 + 3092x^4 + 6724x^5 + 11369x^6 + 16288x^7 + 19829x^8 + 19579x^9 + 16226x^{10} + 11346x^{11} + 6161x^{12} + 2557x^{13} + 878x^{14} + 219x^{15} + 25x^{16} + x^{17}$</td>
</tr>
<tr>
<td>991</td>
<td>$1 + 324x + 673x^2 + 47776x^3 + 116808x^4 + 66257x^5 - 390710x^6$</td>
</tr>
<tr>
<td>1091</td>
<td>$201636x^7 + 374990x^8 + 220398x^9 - 103806x^{10} - 82734x^{11} + 4587x^{12} + 15447x^{13} + 4869x^{14} + 668x^{15} + 42x^{16} + x^{17}$</td>
</tr>
<tr>
<td>1571</td>
<td>$1 + 644x^2 - 5593x^3 + 26795x^4 - 63918x^5 + 94013x^6 - 101154x^7 + 91408x^8 - 72130x^9 + 47790x^{10} - 22460x^{11} + 5810x^{12} - 1693x^{13} + 2160x^{14} - 1109x^{15} + 103x^{16} + 26x^{17} + x^{18}$</td>
</tr>
<tr>
<td>1663</td>
<td>$1 - 1799x + 5159x^2 - 93537x^3 + 34809x^4 + 13921x^5 - 200270x^6 + 148538x^7 + 44658x^8 + 62430x^9 + 30710x^{10} + 49742x^{11} + 35935x^{12}$</td>
</tr>
<tr>
<td>1783</td>
<td>$8751x^{13} + 2679x^{14} + 625x^{15} - 31x^{16} + x^{17}$</td>
</tr>
<tr>
<td>2531</td>
<td>$1 - 1 + 16881x - 557622x^2 + 6294042x^3 - 23845953x^4 + 46634077x^5 - 5875964x^{11} + 2066772x^{12} + 136215x^{13} - 19227x^{14} + 3749x^{15} - 115x^{16} + x^{17}$</td>
</tr>
<tr>
<td>3323</td>
<td>$1691882x^{11} + 224567x^{12} - 151755x^{13} - 8398x^{14} + 4450x^{15} + 71x^{16} + x^{17}$</td>
</tr>
<tr>
<td>3947</td>
<td>$1 + 501269x + 19699862x^2 + 821331183x^3 - 1974514329x^4 + 5592843597x^5 - 8077995938x^6 + 9618930994x^7 - 9807146560x^8 + 693449704x^9 - 4099127558x^{10} + 207905874x^{11} - 565883685x^{12} + 83199969x^{13} - 6231478x^{14} + 191134x^{15} - 313x^{16} + x^{17}$</td>
</tr>
<tr>
<td>4339</td>
<td>$1 + 438582x - 2499315x^2 + 3735097x^3 + 3827776x^4 - 5826355x^5 - 4339607x^6 + 12629724x^7 - 6215046x^8 - 3490790x^9 + 607184x^{10} + 6818050x^{11} - 7146397x^{12} + 3239230x^{13} - 724663x^{14} + 67085x^{15} - 448x^{16} + x^{17}$</td>
</tr>
<tr>
<td>4447</td>
<td>$1 + 2765955x - 66143066x^2 + 2122601876466x^3 - 51489792551504x^4 + 608523191355758x^5 - 8875688180225392x^6 + 2571388650262763x^7 - 36318487121129892x^8 + 2422818074079732x^9 - 657942992235294x^{10} + 73026311344680x^{11} - 42273982392x^{12} + 63837613820x^{13} + 577415049x^{14} + 4469408x^{15} - 4356x^{16} + x^{17}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_w(x)$</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4547</td>
<td>$-1 + 3311969x + 230560228x^2 + 14575649680x^3 + 74216045594x^4 + 127299857910x^5 + 36054214580x^6 - 108069133448x^7 - 86260254955x^8 + 4313879311x^9 + 50586537588x^{10} + 4600529560x^{11} - 5805504343x^{12} + 1086456502x^{13} - 84387928x^{14} + 2456640x^{15} - 2797x^{16} + x^{17}$</td>
</tr>
<tr>
<td>4651</td>
<td>$-1 + 714031x + 2785953x^2 + 6416779x^3 - 7667993x^4 - 11842599x^5 - 2750262x^6 + 10519842x^7 + 177758x^8 + 12892234x^9 - 13895382x^{10} + 2545462x^{11} - 655641x^{12} + 1439359x^{13} - 637455x^{14} + 91515x^{15} + 31x^{16} + x^{17}$</td>
</tr>
<tr>
<td>5483</td>
<td>$-1 + 20350006x + 3253094887x^2 + 214777796269x^3 - 752354950902x^4 + 626351989957x^5 - 246785103362x^6 + 1828736935572x^7 - 371532145826x^8 + 3281949571890x^9 - 1741382905716x^{10} + 599915756058x^{11} - 100703254597x^{12} + 9760854710x^{13} - 548893093x^{14} + 16230145x^{15} - 3222x^{16} + x^{17}$</td>
</tr>
<tr>
<td>6203</td>
<td>$-1 + 41686139x + 2420829799x^2 + 1022493998289x^3 + 4144674497593x^4 + 13313097215161x^5 + 29808858365706x^6 + 42070876151698x^7 + 36992195430106x^8 + 20155027662214x^9 + 6597458572854x^{10} + 1185886311830x^{11} + 110759926247x^{12} + 10994611363x^{13} + 444539567x^{14} + 26746361x^{15} + 225x^{16} + x^{17}$</td>
</tr>
<tr>
<td>6379</td>
<td>$-1 + 8226985x + 12029768x^2 - 1632676x^3 - 75364613x^4 - 38676181x^5 + 38023366x^6 + 164283560x^7 + 79028146x^8 + 32118420x^9 - 68928876x^{10} + 1491492x^{11} - 2231013x^{12} + 13378047x^{13} + 2200662x^{14} + 653680x^{15} + 1601x^{16} + x^{17}$</td>
</tr>
<tr>
<td>6451</td>
<td>$-1 + 9039086x - 3130097x^2 + 61024849x^3 - 71518118x^4 + 81397661x^5 - 81204266x^6 + 98767804x^7 - 96713890x^8 + 85696218x^9 - 53638332x^{10} + 5076947x^{11} - 37225077x^{12} + 2258837x^{13} - 4851153x^{14} + 698357x^{15} + 98x^{16} + x^{17}$</td>
</tr>
<tr>
<td>6827</td>
<td>$-1 + 104626859x + 3338452274x^2 + 451351599757x^3 - 25539558680331x^4 + 39776020539775x^5 - 15654253069748x^6 + 31101946277510x^7 + 24912762792086x^8 + 24040576215390x^9 + 4642346573706x^{10} + 7910663643752x^{11} + 699855645085x^{12} + 9032413439x^{13} + 359735312x^{14} + 51206662x^{15} + 14257x^{16} + x^{17}$</td>
</tr>
<tr>
<td>6907</td>
<td>$-1 + 47513193x - 14550610x^2 + 123039464x^3 - 286578689x^4 + 346532709x^5 + 226449006x^6 - 11309266x^7 - 354113528x^8 - 316837424x^9 + 95623842x^{10} + 131750170x^{11} + 125781907x^{12} + 8787887x^{13} + 19466426x^{14} + 8699298x^{15} + 4847x^{16} + x^{17}$</td>
</tr>
<tr>
<td>7883</td>
<td>$-1 + 453331542x - 291698387667x^2 + 52381212730101x^3 + 31480435313700x^4 + 410216143617737x^5 - 398669609479474x^6 - 399841228929288x^7 + 248919932040246x^8 + 198169852078490x^9 - 183861449828852x^{10} + 49941480305542x^{11} - 5265188386669x^{12} + 333024042946x^{13} - 11543854515x^{14} + 219183121x^{15} - 28864x^{16} + x^{17}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8539</td>
<td>$-1 + 113679903x - 1545089419x^2 + 6884741359x^3 - 4267420061x^4 -$</td>
</tr>
<tr>
<td></td>
<td>$3192718543x^5 + 11464851818x^6 - 819413590x^7 - 13312179674x^8 +$</td>
</tr>
<tr>
<td></td>
<td>$1856409962x^9 - 10629151598x^{10} + 2279857182x^{11} + 107633447x^{12} -$</td>
</tr>
<tr>
<td></td>
<td>$73443161x^{13} - 15182475x^{14} + 5309799x^{15} - 4037x^{16} + x^{17}$</td>
</tr>
<tr>
<td>8731</td>
<td>$-1 + 141141186x - 838136204x^2 + 3159558247x^3 - 7185611583x^4 +$</td>
</tr>
<tr>
<td></td>
<td>$11038623536x^5 - 1221774671x^6 + 10321778211x^7 - 6630087229x^8 +$</td>
</tr>
<tr>
<td></td>
<td>$3260401329x^9 - 1290875967x^{10} + 266674167x^{11} + 15196788x^{12} -$</td>
</tr>
<tr>
<td></td>
<td>$22564029x^{13} + 27061713x^{14} + 6311120x^{15} + 2694x^{16} + x^{17}$</td>
</tr>
<tr>
<td>9883</td>
<td>$-1 + 1844238918x + 3245664159x^2 + 13992493269x^3 + 15980661258x^4 +$</td>
</tr>
<tr>
<td></td>
<td>$2067736149x^5 + 10975074502x^6 + 3047953634x^7 - 11769490666x^8 +$</td>
</tr>
<tr>
<td></td>
<td>$2656615918x^9 - 11323246148x^{10} + 4184314058x^{11} - 2064519493x^{12} +$</td>
</tr>
<tr>
<td></td>
<td>$2482421078x^{13} - 217222349x^{14} + 200899481x^{15} + 19738x^{16} + x^{17}$</td>
</tr>
<tr>
<td>11251</td>
<td>$-1 + 1988572771x + 8249720601x^2 + 14996482171x^3 + 13798186975x^4 -$</td>
</tr>
<tr>
<td></td>
<td>$588778383x^5 + 19764780774x^6 - 27610905654x^7 - 18329676346x^8 +$</td>
</tr>
<tr>
<td></td>
<td>$837718282x^9 + 13744715418x^{10} + 15591363454x^{11} + 9333404151x^{12} +$</td>
</tr>
<tr>
<td></td>
<td>$3534435523x^{13} + 570815025x^{14} + 52300395x^{15} + 919x^{16} + x^{17}$</td>
</tr>
<tr>
<td>11443</td>
<td>$-1 + 10056614148x + 16427085216x^2 + 97827220291x^3 +$</td>
</tr>
<tr>
<td></td>
<td>$111117936978x^4 + 211330899500x^5 + 190486148529x^6 + 21866895814x^7 +$</td>
</tr>
<tr>
<td></td>
<td>$83304015887x^8 - 1213310145x^9 - 12890770374x^{10} + 39736486871x^{11} -$</td>
</tr>
<tr>
<td></td>
<td>$8107210884x^{12} + 15306849766x^{13} + 3191271525x^{14} + 863687024x^{15} -$</td>
</tr>
<tr>
<td></td>
<td>$28876x^{16} + x^{17}$</td>
</tr>
<tr>
<td>12907</td>
<td>$-1 + 44592882119x - 134126978650x^2 + 224143225924x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$281486828459x^4 + 315820890151x^5 - 86217243724x^6 + 35287530074x^7 +$</td>
</tr>
<tr>
<td></td>
<td>$157789120178x^8 - 153921235750x^9 + 107614527614x^{10} - 8464404976x^{11} -$</td>
</tr>
<tr>
<td></td>
<td>$1075717755x^{12} + 47411121375x^{13} - 11330823312x^{14} + 3093677482x^{15} -$</td>
</tr>
<tr>
<td></td>
<td>$14291x^{16} + x^{17}$</td>
</tr>
<tr>
<td>13627</td>
<td>$-1 + 89926614866x - 199912392010x^2 + 783479129571x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$2049042731134x^4 + 1779964033264x^5 - 461781294725x^6 -$</td>
</tr>
<tr>
<td></td>
<td>$53704544688x^7 + 856714080233x^8 - 457231356385x^9 -$</td>
</tr>
<tr>
<td></td>
<td>$412074883432x^{10} - 430526437x^{11} + 36737508272x^{12} + 98050475758x^{13} +$</td>
</tr>
<tr>
<td></td>
<td>$41873588997x^{14} + 5642387042x^{15} + 9558x^{16} + x^{17}$</td>
</tr>
<tr>
<td>14083</td>
<td>$-1 + 138888632811x - 828114961969x^2 + 232174400501x^3 -$</td>
</tr>
<tr>
<td></td>
<td>$2463095976582x^4 + 339009518136x^5 + 259539983101x^6 -$</td>
</tr>
<tr>
<td></td>
<td>$4439540870277x^7 + 366252421890x^8 - 419073899552x^9 -$</td>
</tr>
<tr>
<td></td>
<td>$1551244148391x^{10} + 1907788843051x^{11} - 1110431691358x^{12} +$</td>
</tr>
<tr>
<td></td>
<td>$416808017628x^{13} - 84756271861x^{14} + 819032701x^{15} - 23229x^{16} + x^{17}$</td>
</tr>
<tr>
<td>14779</td>
<td>$-1 + 51077714262x + 482019050121x^2 + 1345367507713x^3 +$</td>
</tr>
<tr>
<td></td>
<td>$578516741140x^4 + 108407835677x^5 + 2243394840214x^6 +$</td>
</tr>
<tr>
<td></td>
<td>$1389286399548x^7 - 156679389486x^8 + 1013417820202x^9 +$</td>
</tr>
<tr>
<td></td>
<td>$78423848008x^{10} + 125590976770x^{11} + 81705949451x^{12} +$</td>
</tr>
<tr>
<td></td>
<td>$61420234222x^{13} + 12076320893x^{14} + 702639413x^{15} + 52580x^{16} + x^{17}$</td>
</tr>
<tr>
<td>( D )</td>
<td>( f_u(x) )</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>14947</td>
<td>(-1 + 1575451x - 621406306975x^2 - 2582043455253x^3 - 4405371179613x^4 + 107415863425x^5 + 10814147462458x^6 + 13662177722626x^7 - 3916328002626x^8 - 22964432871406x^9 - 16003605223646x^{10} + 8280305942910x^{11} + 14938511615687x^{12} - 215784003933x^{13} - 11288214079903x^{14} - 7968009086077x^{15} - 1880378597637x^{16} + x^{17})</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>311</td>
<td>$-1 + 16x + 53x^2 + 123x^3 + 182x^4 - 29x^5 - 585x^6 - 758x^7 + 32x^8 + 1012x^9 + 963x^{10} - 29x^{11} + 766x^{12} - 570x^{13} + 3x^{14} + 227x^{15} + 121x^{16} + 22x^{17} + 2x^{18} + x^{19}$</td>
</tr>
<tr>
<td>359</td>
<td>$-1 + 24x - 20x^2 + 284x^3 - 110x^4 + 461x^5 - 296x^6 + 1778x^7 - 1913x^8 + 3116x^9 - 2405x^{10} + 2571x^{11} - 1668x^{12} + 1145x^{13} - 589x^{14} + 294x^{15} - 100x^{16} + 28x^{17} - 3x^{18} + x^{19}$</td>
</tr>
<tr>
<td>919</td>
<td>$-1 + 259x - 934x^2 + 3066x^3 - 92583x^4 + 115292x^5 + 133308x^6 - 289301x^7 + 152248x^8 + 176839x^9 - 283346x^{10} + 37344x^{11} + 116154x^{12} - 56559x^{13} - 4827x^{14} + 10522x^{15} - 3301x^{16} + 469x^{17} - 32x^{18} + x^{19}$</td>
</tr>
<tr>
<td>1063</td>
<td>$-1 + 593x - 14131x^2 + 167461x^3 - 481216x^4 + 423161x^5 - 250290x^6 + 912877x^7 + 195450x^8 + 56728x^9 + 15706x^{10} - 240531x^{11} + 173000x^{12} + 76368x^{13} - 30818x^{14} + 9238x^{15} - 1609x^{16} + 301x^{17} + 25x^{18} + x^{19}$</td>
</tr>
<tr>
<td>1543</td>
<td>$-1 + 2594x - 127171x^2 + 3105236x^3 - 14777043x^4 + 20237372x^5 + 8687141x^6 + 3230778x^7 + 28674905x^8 + 40363732x^9 + 22635074x^{10} + 28498519x^{11} + 4943736x^{12} + 7920911x^{13} + 1794519x^{14} + 348725x^{15} + 36299x^{16} + 503x^{17} - 63x^{18} + x^{19}$</td>
</tr>
<tr>
<td>1831</td>
<td>$-1 + 3495x - 24143x^2 + 5531936x^3 - 35315147x^4 + 123938054x^5 - 128407068x^6 + 289484864x^7 - 355963237x^8 + 363952028x^9 - 230130187x^{10} + 114511489x^{11} - 42939772x^{12} + 11837091x^{13} - 2378334x^{14} + 316145x^{15} - 2358x^{16} + 625x^{17} + 13x^{18} + x^{19}$</td>
</tr>
<tr>
<td>2099</td>
<td>$-1 + 6599x - 171400x^2 + 1621252x^3 - 6379052x^4 + 14402464x^5 - 20553269x^6 + 19241978x^7 - 10917088x^8 + 3514200x^9 + 110504x^{10} + 444896x^{11} - 436275x^{12} + 445941x^{13} - 13096x^{14} + 39396x^{15} + 3524x^{16} + 2240x^{17} + 41x^{18} + x^{19}$</td>
</tr>
<tr>
<td>2339</td>
<td>$-1 + 11189x + 220939x^2 + 1873283x^3 - 110865x^4 + 4226321x^5 - 2298813x^6 + 6041549x^7 - 6985578x^8 + 9108592x^9 - 10331724x^{10} + 8514330x^{11} - 6359321x^{12} + 3471109x^{13} - 1208801x^{14} + 295237x^{15} - 49435x^{16} + 4629x^{17} - 113x^{18} + x^{19}$</td>
</tr>
<tr>
<td>2459</td>
<td>$-1 + 14507x - 284660x^2 + 483800x^3 + 13150252x^4 + 50207576x^5 + 93254063x^6 + 101181379x^7 + 68776624x^8 + 30778208x^9 + 10285072x^{10} + 3545352x^{11} + 912949x^{12} - 479503x^{13} - 430108x^{14} - 43064x^{15} + 21028x^{16} + 4160x^{17} + 29x^{18} + x^{19}$</td>
</tr>
<tr>
<td>3343</td>
<td>$-1 + 285063x + 11399872x^2 + 22774854253x^3 - 369226170934x^4 + 1403970972145x^5 + 2495992149904x^6 + 7336850588376x^7 + 3216092861664x^8 + 10199735131115x^9 + 315621778365x^{10} + 4195310552614x^{11} + 196427547817x^{12} + 365480566433x^{13} + 32692205960x^{14} + 1460970933x^{15} + 18689086x^{16} + 429313x^{17} + 470x^{18} + x^{19}$</td>
</tr>
<tr>
<td>3463</td>
<td>$-1 + 205738x - 85314321x^2 + 17675700672x^3 - 348934943665x^4 + 2434773874389x^5 - 508831101645x^6 + 780059103802x^7 - 2731177190703x^8 + 3563885529035x^9 - 1931682361506x^{10} + 521719979166x^{11} - 66852698344x^{12} + 3286590506x^{13} + 57345633x^{14} + 12190607x^{15} - 411029x^{16} + 77832x^{17} + 208x^{18} + x^{19}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_D(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>3467</td>
<td>$-1 + 367595x + 2258897x^2 + 366142681x^3 - 2046232798x^4 + 5514595458x^5 - 9502266774x^6 + 12448181910x^7 - 1328285979x^8 + 11463782805x^9 - 792490573x^{10} + 4472967519x^{11} - 1995847954x^{12} + 643590162x^{13} - 112316370x^{14} + 24444326x^{15} - 1820077x^{16} + 274995x^{17} + 557x^{18} + x^{19}$</td>
</tr>
<tr>
<td>3607</td>
<td>$-1 + 486985x - 258959730x^2 + 68884714646x^3 + 649618675133x^4 + 9309104861926x^5 + 11287975529117x^6 + 3854080680559x^7 + 64415700217189x^8 + 63006816631982x^9 + 33985132648442x^{10} + 10684027198596x^{11} + 2021806941967x^{12} + 232073510912x^{13} + 16284006247x^{14} + 761202185x^{15} + 23466120x^{16} + 398064x^{17} + 1171x^{18} + x^{19}$</td>
</tr>
<tr>
<td>4019</td>
<td>$-1 + 261127x + 4010608x^2 + 373472016x^3 + 87576998x^4 + 730901132x^5 - 27875221x^6 + 1251606651x^7 + 128666648x^8 + 1054462944x^9 - 106023312x^{10} + 291046960x^{11} - 139624563x^{12} + 75273469x^{13} - 25255048x^{14} + 5400016x^{15} - 676596x^{16} + 45764x^{17} - 311x^{18} + x^{19}$</td>
</tr>
<tr>
<td>4139</td>
<td>$-1 + 317875x + 17297028x^2 + 381519768x^3 - 3040335456x^4 + 961394454x^5 - 1809724309x^6 + 23409656075x^7 - 21275137416x^8 + 1368713896x^9 - 5950565616x^{10} + 1664388912x^{11} - 352113595x^{12} + 126635649x^{13} - 33443840x^{14} + 6235136x^{15} - 771312x^{16} + 53908x^{17} - 399x^{18} + x^{19}$</td>
</tr>
<tr>
<td>4327</td>
<td>$-1 + 2655437x - 4188435567x^2 + 1595635406271x^3 + 44544236206598x^4 + 311208822444962x^5 + 189909827193218x^6 + 799956695297692x^7 + 1034431453184x^8 + 102890174928562x^9 - 76728653644204x^{10} + 21855873115361x^{11} - 5562001145507x^{12} + 1331591898124x^{13} + 137133482407x^{14} + 5976878089x^{15} + 162031785x^{16} + 2167917x^{17} - 1115x^{18} + x^{19}$</td>
</tr>
<tr>
<td>5059</td>
<td>$-1 + 1318511x - 4074490x^2 + 24642070x^3 - 35903584x^4 + 60330214x^5 - 105227063x^6 + 21540797x^7 - 318587708x^8 + 347802868x^9 - 279511584x^{10} + 179550244x^{11} - 97088527x^{12} + 47460589x^{13} - 18444298x^{14} + 6344246x^{15} - 1493184x^{16} + 148406x^{17} + 135x^{18} + x^{19}$</td>
</tr>
<tr>
<td>5147</td>
<td>$-1 + 7848021x - 1343213058x^2 + 67065884136x^3 - 21888297442x^4 + 453043000530x^5 - 401335937029x^6 + 295289870263x^7 - 80353307820x^8 + 66127350672x^9 - 9747650164x^{10} + 121624766604x^{11} - 23402064467x^{12} + 106966300019x^{13} - 11184781010x^{14} + 1559452936x^{15} - 94961910x^{16} + 4414498x^{17} + 2521x^{18} + x^{19}$</td>
</tr>
<tr>
<td>5527</td>
<td>$-1 + 21897208x - 9932319613x^2 + 111797329811033x^3 + 509297781841320x^4 + 46562480280599340x^5 - 201845911975447551x^6 + 806294615459894402x^7 - 1569860871290754608x^8 + 130181688151491078x^9 - 240823386433620675x^{10} - 149427591618150445x^{11} + 3397685156363486x^{12} + 10153892219635526x^{13} + 188330452118393x^{14} + 1894960712487x^{15} - 13723831105x^{16} + 55964405x^{17} - 6210x^{18} + x^{19}$</td>
</tr>
<tr>
<td>$D$</td>
<td>$f_u(x)$</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
</tr>
<tr>
<td>5659</td>
<td>$-1 + 3111592x + 6740396x^2 + 24118945x^3 - 90471837x^4 + 257636294x^5 - 299958084x^6 + 152644345x^7 + 175455376x^8 - 269292530x^9 + 179756578x^{10} + 25683996x^{11} - 54793413x^{12} + 48755550x^{13} - 17604732x^{14} + 6457105x^{15} - 730885x^{16} + 297310x^{17} + 202x^{18} + x^{19}$</td>
</tr>
<tr>
<td>6803</td>
<td>$-1 + 41267131x + 7212449729x^2 + 1303567003181x^3 - 7795247319149x^4 + 21197108330701x^5 - 19374002217377x^6 + 457479626131x^7 + 19450994595952x^8 + 1707577125388x^9 - 1251621013730x^{10} - 73752962768x^{11} - 121466101585x^{12} + 294212294849x^{13} + 57290822599x^{14} + 5905040639x^{15} + 293526143x^{16} + 7537339x^{17} - 5173x^{18} + x^{19}$</td>
</tr>
<tr>
<td>8419</td>
<td>$-1 + 99177937x - 344740278x^2 + 5149851804x^3 - 2486098326x^4 + 11206388178x^5 - 494903809x^6 + 1766430913x^7 - 14618062692x^8 + 29493914648x^9 - 18224473700x^{10} + 12352247148x^{11} - 1931603979x^{12} - 259332033x^{13} + 172747674x^{14} + 81926092x^{15} - 44531590x^{16} + 4780098x^{17} - 3187x^{18} + x^{19}$</td>
</tr>
<tr>
<td>8923</td>
<td>$-1 + 60708883x - 4750977367x^2 + 15289085437x^3 - 25968762975x^4 + 25150374033x^5 - 11869995489x^6 + 2277597453x^7 - 10826058220x^8 + 35613489970x^9 - 60147173200x^{10} + 67800312100x^{11} - 54406486059x^{12} + 3167845897x^{13} - 13216672965x^{14} + 3864496161x^{15} - 73034209x^{16} + 77905315x^{17} + 1085x^{18} + x^{19}$</td>
</tr>
<tr>
<td>8971</td>
<td>$-1 + 184363559x + 222382635x^2 + 12392040203x^3 + 4226272882x^4 + 97913244834x^5 + 161039768028x^6 + 193168195512x^7 + 172268252877x^8 + 115121508131x^9 + 58277202791x^{10} + 23982693801x^{11} + 9456524430x^{12} + 3881944956x^{13} + 1296217284x^{14} + 256378670x^{15} + 27791525x^{16} + 7787793x^{17} - 3557x^{18} + x^{19}$</td>
</tr>
<tr>
<td>9619</td>
<td>$-1 + 372733905x - 566134762x^2 + 1304137292x^3 - 2017882642x^4 - 971003482x^5 + 5975139379x^6 - 5280943129x^7 - 2601868052x^8 + 7111017096x^9 - 2790101492x^{10} - 2588689524x^{11} + 2647596957x^{12} + 25483143x^{13} - 688803330x^{14} + 110949100x^{15} + 72354630x^{16} + 13671118x^{17} - 5391x^{18} + x^{19}$</td>
</tr>
<tr>
<td>10891</td>
<td>$-1 + 1389734708x - 174920200392x^2 + 17348550289x^3 + 489493021049x^4 + 1567299956853x^5 + 2095801963080x^6 + 2007558592569x^7 + 1212665485326x^8 + 841997541086x^9 + 422943258062x^{10} + 160936169270x^{11} + 28900544531x^{12} + 13795723602x^{13} - 301130759x^{14} + 559226961x^{15} - 143074951x^{16} + 39214357x^{17} + 12134x^{18} + x^{19}$</td>
</tr>
<tr>
<td>11299</td>
<td>$-1 + 2084971938x - 1651579998x^2 + 55736492333x^3 - 81055656533x^4 + 37061013528x^5 + 8658455476x^6 - 132973215963x^7 + 49163215944x^8 + 56674540702x^9 - 61934352174x^{10} + 8957576624x^{11} + 8561256659x^{12} - 8110928008x^{13} + 3153709676x^{14} + 1169537781x^{15} - 516697405x^{16} + 54249016x^{17} + 6266x^{18} + x^{19}$</td>
</tr>
</tbody>
</table>
Bibliography


