National Library of Canada
Acquisitions and Bibliographic Services Branch
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale du Canada
Direction des acquisitions et des services bibliographiques
395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

The Euclidean Algorithm for Galois Extensions of the Rational Numbers

David Alan Clark

Department of Mathematics and Statistics
McGill University
Montréal, Québec

August 1992

A thesis submitted to the Faculty of Graduate Studies
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

ISBN 0-315-80359-2

ABSTRACT

Let K be a totally real, quartic, Galois extension of $\mathbb{Q}$ whose ring of integers R is a principal ideal domain. If there is a prime ideal $\mathfrak{p}$ of R such that the unit group maps onto $(R/\mathfrak{p}^2)^*$, then R is a Euclidean domain. This criterion is generalized to arbitrary Galois extensions.

Let E be an elliptic curve over a number field F. Suppose $[F : \mathbb{Q}] \leq 4$ and $F(E[q]) \not\subseteq F$ for all primes q such that F contains a primitive q^{th} root of unity, then the reduced elliptic curve $\tilde{E}(F_\mathfrak{p})$ is cyclic infinitely often. In general, if Γ a subgroup of $E(F)$ with the rank of Γ sufficiently large, there are infinitely many prime ideals $\mathfrak{p}$ of F such that the reduced curve $\tilde{E}(F_\mathfrak{p}) = \Gamma_\mathfrak{p}$, where $\Gamma_\mathfrak{p}$ is the reduction modulo $\mathfrak{p}$ of Γ.

RÉSUMÉ

Soit K un extension galoisienne totalement réelle de degré quatre du corps $\mathbb{Q}$, dont l'anneau des entiers R est un anneau à idéaux principaux. S'il existe un idéal premier $\mathfrak{p}$ de R tel que le groupe des unités de R s'applique surjectivement sur $(R/\mathfrak{p}^2)^*$, alors R est un anneau euclidien. Nous généralisons ce critère aux extensions galoisiennes quelconques de $\mathbb{Q}$.

Soit E une courbe elliptique définie sur un corps de nombres F. Si $[F:\mathbb{Q}] \leq 4$ et si $F(E[q]) \not\subseteq F$ pour chaque nombre premier q pour lequel F contient une racine q-ième de l'unité, alors le groupe $\tilde{E}(F_\mathfrak{p})$ est cyclique pour une infinité d'idéaux premiers de F. En général, si $E(F)$ admet un sous-groupe Γ de rang suffisamment grand, alors il existe une infinité d'idéaux premiers $\mathfrak{p}$ de F tels que l'homomorphisme de réduction de $E(F)$ dans $\tilde{E}(F_\mathfrak{p})$ soit surjectif sur $\Gamma(\mathrm{mod}\ \mathfrak{p})$.

PREFACE

I would like to thank my thesis supervisor, Professor Ram Murty, for his helpful discussions during the preparation of this thesis and for his enjoyable courses. I also want to thank the KANT group (in particular Max Jüntgen) at the Universität Düsseldorf for providing the data used for the computations in chapter 4. The KANT computer package for computational algebraic number theory and the MAPLE symbolic computation system were used for the computations summarized in this thesis.

The Generalized Čebotarev Density Theorem proved in chapter 1 does not appear in the literature; however, the proof is a direct translation of the proof of Lagarias and Odlyzko [21] to the generalized setting. The Average Density Theorem proved in chapter 2 is a slight improvement in the level of distribution of the theorem of K. Murty and R. Murty [29] (from $x^{1/\eta-\epsilon}$ to $x^{1/\eta}/(\log x)^B$, for some positive number B), but again my proof is only a slight modification of the one they give. The results in chapter 3 are specializations of the arguments of R. Gupta, K. Murty, and R. Murty [15] to the case of totally real quartic fields. The material in chapters 4 and 5 are new and constitute the main contribution of this thesis. Chapter 6 is a straightforward extension of R. Gupta and R. Murty [14] to algebraic number fields using of the results of chapters 1, 2, and 3.

TABLE OF CONTENTS

INTRODUCTION

In Book VII, Proposition 2 of his *Elements*, Euclid describes the following procedure for determining the greatest common denominator of two natural numbers $b_1 \geq b_2$. Subtract a multiple of b_2 from b_1 to yield a natural number b_3 which is smaller than b_2. Repeat this step using b_2 and b_3 in place of b_1 and b_2. The procedure terminates when $b_{n+1} = 0$ and yields $\gcd(b_1, b_2) = b_n$.

In modern terminology, Euclid's algorithm determines a generator for the ideal (b_1, b_2) of the ring of rational integers. More generally, let R be an integral domain. A Euclidean algorithm for R is a map

$$\phi : R \setminus \{0\} \to \mathbb{N}_0,$$

the set of nonnegative integers, such that for all $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ with $a = qb + r$ and either $\phi(r) < \phi(b)$ or $r = 0$. An integral domain equipped with a Euclidean algorithm is called a Euclidean domain.

As might be expected from the example of the rational integers, Euclidean domains have the property that every ideal is principal. Indeed, if $\mathfrak{A}$ is an ideal of R, b a nonzero element of $\mathfrak{A}$ such that $\phi(b)$ is minimal, and a an arbitrary element of $\mathfrak{A}$, then there are $q, r \in R$ with $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$. Since $r \in \mathfrak{A}$ and $\phi(b)$ is minimal, it follows that $r = 0$ so that $\mathfrak{A}$ is generated by b.

In the special case $\mathfrak{A} = R$, this argument shows that a nonzero element u of R with $\phi(u)$ minimal is a unit of R. An example of Samuel [33] shows that the converse need not be true; namely, that if u is a unit of R, then $\phi(u)$ need not be the smallest element of $\phi(R \setminus \{0\})$. Consider $R = \mathbb{Z}$ with $\phi(n) = |n|$, for $n \neq -1$, and $\phi(-1)$ chosen arbitrarily. However, another algorithm can be constructed from ϕ,

$$\tilde{\phi}(r) = \min_{a \in Rr \setminus (0)} \phi(a),$$

which does satisfy the converse. To see that this function is a Euclidean algorithm, choose $a, b \in R$, $b \neq 0$. There is $b' \in R$ with $b' = bc'$ such that $\tilde{\phi}(b) = \phi(b')$. Since ϕ is Euclidean, there is $r \in R$ such that $\phi(r) < \phi(b')$ and $a = q'b' + r$. Choose $q = q'c'$ so that $a = qb + r$ and $\tilde{\phi}(r) \leq \phi(r) < \phi(b') = \tilde{\phi}(b)$.

The Fastest Algorithm

Motzkin [26] constructed a special kind of Euclidean algorithm. Given a nonempty collection of Euclidean algorithms ϕ_α on R, the map defined by

$$\phi(r) = \min_{\alpha} \phi_\alpha(r)$$

is also a Euclidean algorithm on R. To check this, let $a, b \in R$, $b \neq 0$. Choose an α_1 such that $\phi(b) = \phi_{\alpha_1}(b)$. Since

$$\phi(r) \leq \phi_{\alpha_1}(r) < \phi_{\alpha_1}(b) = \phi(b),$$

ϕ is Euclidean. If the minimum is taken over all the Euclidean algorithms of the ring R, the resulting algorithm E is called the fastest algorithm.

Let $E_n = \{0\} \cup \{r \in R : \ E(r) \leq n\}$. Since $\tilde{E} = E$, E_0 is the set of units of R. If $b \in E_{n+1}$ and $a + Rb$ is any residue class mod Rb, then there exist $q, r \in R$ with $a = qb + r$ and $r = 0$ or $E(r) < E(b)$ so that $r \in E_n$. Thus, $E_n \to R/Rb$ is surjective. Conversely, consider $b \in R$ such that $E_n \to R/Rb$ is surjective. If $E(b) > n + 1$ then a new map E' could be defined by $E'(r) = E(r)$, for $r \neq b$ and $E'(b) = n + 1$. To see that E' is an algorithm it suffices to consider the cases when b occurs as either a divisor or a remainder. Since $E_n \to R/Rb$ is surjective, every residue class $a + Rb$ has a representative such that $a = qb + r$, $r \in E_n$ which implies $E'(r) < n + 1 = E'(b)$. If $a = qc + b$ with $E(b) < E(c)$, then trivially $E'(b) < E(b) < E(c) = E'(c)$. Thus, the sets E_n may be defined inductively as $E_0 = \{0\} \cup \{\text{units}\}$, $E_1 = \{r \in R : \ E_0 \to R/(r)$ is onto, and in general $E_{n+1} = \{0\} \cup \{r \in R : \ E_n \to R/(r)$ is onto$\}$.

The importance of the sets E_n is that they can be constructed in any ring. If

$$\bigcup_{n \geq 0} E_n = R, \tag{1}$$

then R is Euclidean with algorithm defined by

$$\phi(r) = \min\{n : r \in E_n\}.$$

On the other hand, if R is Euclidean then every element of R is in some E_n. So the condition (1) is necessary and sufficient for R to be a Euclidean domain.

The fastest algorithm has several nice properties.

Property 1. *If a and b are nonzero elements of R, then $E(ab) \geq E(a)$.*

Proof. If E_n maps onto R/Rab, then composing with the surjection

$$R/Rab \to R/Ra$$

shows that E_n maps onto R/Ra.

Property 2. *If a, b, c are nonzero elements of R, then $E(ac) \leq E(bc)$ if and only if $E(a) \leq E(b)$.*

Proof. Suppose $E(a) \leq E(b)$ but there exists some c with $E(ac) > E(bc)$. Consider the set of such elements c with $E(ac) - E(bc)$ as small as possible. From this set choose one with $E(bc)$ minimal. There is $x \in R$ such that $E(bx) \leq E(bc) - 1$ and $E(bx') \geq E(bx)$ for all bx' in the coset $bx + Rbc$. The coset $ax + Rac$ contains an element ay with $E(ay) < E(ac)$. Since $by \in bx + Rbc$, $E(by) \geq E(bc) - 1$. If $E(by) = E(bc) - 1$, then

$$E(ay) - E(by) \leq E(ac) - 1 - E(bc) + 1 = E(ac) - E(bc),$$

which contradicts the choice of c with $E(bc)$ minimal. If $E(by) \geq E(bc)$, then

$$E(ay) - E(by) < E(ac) - E(bc),$$

which contradicts the choice of c with $E(ac) - E(bc)$ minimal. Thus, $E(ac) \leq E(bc)$. For the converse, suppose $E(ac) \leq E(bc)$. If $E(a) > E(b)$ then the first part shows that $E(ac) > E(bc)$, which immediately yields a contradiction, so $E(a) \leq E(b)$.

Property 3. *If a, b are nonzero elements of R, then $E(ab) \geq E(a) + E(b)$.*

Proof. Suppose that for some element b there exist elements a' such that $E(a'b) < E(a') + E(b)$. Consider the set of such a' with $E(a'b) - E(a')$ minimal. From this set choose an element a with $E(a)$ minimal. By property 1, a is not a unit. There is a coset $c + Ra$ containing an element x with $E(x) = E(a) - 1$, and $E(x') \geq E(x)$ for all $x' \in c + Ra$. The coset $cb + Rab$ contains an element yb such that $E(yb) < E(ab)$ and $y \in c + Ra$. If $E(y) = E(a) - 1$, then

$$E(yb) - E(y) \leq E(ab) - 1 - (E(a) - 1) = E(ab) - E(a).$$

Since $E(y) < E(a)$, this contradicts the choice of a. If $E(x) \geq E(a)$, then

$$E(xb) - E(x) < E(ab) - E(a),$$

which again contradicts the choice of a. This proves the claim.

Property 4. *If $x \in R$ is nonzero, then*

$$E(x) \geq \sum v_p(x),$$

where the sum is over all normalized valuations of R.

Proof. If x is a unit, $E(x) = 0$ and $\sum v_p(x) = 0$. Suppose that $E(x) \geq \sum v_p(x)$ for x such that $\sum v_p(x) \leq n$. If $\sum v_p(x') = n + 1$, $x' = y'p'$, for some prime element p'. By Property 2, $E(x') > E(y') \geq \sum v_p(y') = n$, so that $E(x') \geq \sum v_p(x')$.

The Euclidean Algorithm in Algebraic Number Fields

The Euclidean algorithm on the ring of rational integers which was studied by Euclid is defined by

$$N(x) = |x| = |\mathbb{Z}/\mathbb{Z}x|.$$

More generally the function $N(b) = |R/Rb|$ is called the norm of R. For subrings of algebraic number fields the only known examples of Euclidean rings have been Euclidean with the norm as algorithm, though the possibility of constructing rings of S-integers which are not Euclidean for the norm is implicit in Gupta and R. Murty [15].

For imaginary quadratic fields, $\mathbb{Q}(\sqrt{-d})$ whose rings of integers are Euclidean, the norm is always a Euclidean algorithm. To see this consider the construction of the fastest algorithm. If $d \neq 1,\ 3$, the only units in the ring of integers are 1 and -1. So in this case the construction terminates with the units unless there are elements x with $N(x) \leq 3$. If $-d \equiv 1 (\mathrm{mod}\ 4)$, then the ring of integers of $\mathbb{Q}(\sqrt{-d})$ is generated by 1 and $(1+\sqrt{-d})/2$ over $\mathbb{Z}$. Since $N(a + b(1 + \sqrt{-d})/2) = (a + b/2)^2 + d(b/2)^2 \leq 3$ implies $d \leq 12$, the choices are $d = 7,\ 11$. If $-d \equiv 2, 3 (\mathrm{mod}\ 4)$, then the ring of integers is generated by 1 and $\sqrt{-d}$. The inequality $N(a + b\sqrt{-d}) = a^2 + db^2 \leq 3$ implies $d \leq 3$ or $d = 2$.

It can be verified that in each of these cases, $d = 1,\ 2,\ 3,\ 7,\ 11$, the ring of integers is Euclidean for the norm. For $d = 1,\ 2$, the ring of integers consists of elements $a_1 + a_2\sqrt{-d}$ with a_1, a_2 rational integers. If $a_1 + a_2\sqrt{-d}$

and $b_1 + b_2\sqrt{-d}$ are in the ring of integers, then look at

$$\frac{a_1 + a_2\sqrt{-d}}{b_1 + b_2\sqrt{-d}} = \frac{a_1b_1 + a_2b_2d + \sqrt{-d}\,(a_2b_1 - a_1b_2)}{b_1^2 + db_2^2}.$$

Pick an element $q_1 + q_2\sqrt{-d}$ of the ring of integers such that

$$\left|\frac{a_1b_1 + da_2b_2}{b_1^2 + db_2^2} - q_1\right| < \frac{1}{2}$$
$$\left|\frac{a_2b_1 - a_1b_2}{b_1^2 + db_2^2} - q_2\right| < \frac{1}{2},$$

then

$$\begin{aligned} &N\left(a_1 + a_2\sqrt{-d} - \left(b_1 + b_2\sqrt{-d}\right)\left(q_1 + q_2\sqrt{-d}\right)\right) \\ &\quad \leq \left(\frac{1}{4} + \frac{d}{4}\right)(b_1^2 + db_2^2) \\ &\quad < N(b_1 + b + 2\sqrt{-d}). \end{aligned}$$

For $d = 3,\ 7,\ 11$, the ring of integers consists of elements $(a_1 + a_2\sqrt{-d})/2$ with a_1, a_2 rational integers either both even or both odd. If the elements $(a_1 + a_2\sqrt{-d})/2$ and $(b_1 + b_2\sqrt{-d})/2$ are in the ring of integers, look at

$$\frac{a_1 + a_2\sqrt{-d}}{b_1 + b_2\sqrt{-d}} = \frac{a_1b_1 + a_2b_2d + \sqrt{-d}\,(a_2b_1 - a_1b_2)}{b_1^2 + db_2^2}.$$

Choose q_2 such that

$$\left|\frac{a_2b_1 - a_1b_2}{b_1^2 + db_2^2} - \frac{q_2}{2}\right| < \frac{1}{4},$$

then q_1 may be chosen with the same parity of q_2 satisfying

$$\left|\frac{a_1b_1 + da_2b_2}{b_1^2 + db_2^2} - \frac{q_1}{2}\right| < \frac{1}{2}.$$

Hence,

$$\begin{aligned} & N\left(\frac{a_1+a_2\sqrt{-d}}{2}-\left(\frac{b_1+b_2\sqrt{-d}}{2}\right)\left(\frac{q_1+q_2\sqrt{-d}}{2}\right)\right) \\ & \leq \left(\frac{1}{4}+\frac{d}{16}\right) N\left(\frac{b_1+b_2\sqrt{-d}}{2}\right) \\ & < N\left(\frac{b_1+b_2\sqrt{-d}}{2}\right). \end{aligned}$$

So the ring of integers of $\mathbb{Q}(\sqrt{-d})$ is a Euclidean domain for

$$d = 1,\ 2,\ 3,\ 7,\ 11.$$

Since it is known that the ring of integers is a principal ideal domain for $d = 19,\ 43,\ 67,$ and 163, these rings give examples of principal ideal domains which are not Euclidean for any algorithm.

Heilbronn [17] showed that there are only finitely many real quadratic fields which are Euclidean for the norm. Chatland and Davenport [4] showed that the norm is a Euclidean algorithm for the ring of integers of $\mathbb{Q}(\sqrt{d})$ precisely for

$$d = 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.$$

Davenport [7],[8] showed that there are only finitely many fields of degree three or four with unit groups of rank one which are Euclidean for the norm.

If the ring contains a unit of infinite order which generates $R/R\mathfrak{p}$ for infinitely many primes $\mathfrak{p}$ of R, then by analogy to Artin's Primitive Root Conjecture, the set E_1 in the construction of the fastest algorithm would

contain these prime ideals. Weinberger [42] made this connection more precise. He modified the conditional proof of Artin's conjecture, due to Hooley [18], to show that for algebraic number fields containing infinitely many units, the ring of integers is Euclidean if and only if it is a principal ideal domain, assuming the Generalized Riemann Hypothesis for Dedekind zeta functions. The main ideas of his proof are as follows. First, it is enough to show that all primes $\mathfrak{p}$ are in E_2. That is, in every nonzero residue class modulo $\mathfrak{p}$ there is a unit or a prime from E_1. If a unit ϵ is not a primitive root modulc $\mathfrak{q}$, then ϵ is a q^{th} power mod $\mathfrak{q}$ for some $q|(N\mathfrak{q}-1)$. This is equivalent to $\mathfrak{q}$ splitting completely in $K(\zeta_q, \epsilon^{1/q})$. So, it is enough to find a prime ideal $\mathfrak{q}$, which does not split completely in any $K(\zeta_q, \epsilon^{1/q})$, in each residue class mod $\mathfrak{p}$ which does not contain zero or a unit. Now, the argument of Hooley can be applied using the Prime Ideal Theorem for prime ideals in ideal classes with the error term implied by the Generalized Riemann Hypothesis.

The Euclidean algorithm has been studied for more general types of subrings of algebraic number fields. Let S be a set of valuations of the ring of integers of an algebraic number field containing the archimedean valuations. The ring of S-integers of an algebraic number field is the intersection of the valuation rings for valuations not in S. Euclidean algorithms on rings of S-integers have also been studied. O'Meara [31] showed that for every field there is a set S of valuations such that the ring of S-integers is Euclidean for the norm. Lenstra [24] extended the result of Weinberger described

above to rings of S-integers with $|S| \geq 2$. Utilizing the methods of R. Gupta and R. Murty [12] on Artin's primitive root conjecture, R. Gupta, K. Murty, and R. Murty [15] showed that the assumption of the Generalized Riemann Hypothesis could be removed from Lenstra's result if the number of elements of S is large enough. More precisely, they proved:

Theorem. *Let K be a Galois extension of $\mathbb{Q}$ and let S be a collection of primes containing the infinite primes such that*

(1) $|S| \geq \max(5, 2[K:\mathbb{Q}] - 3)$,

(2) *K has a real embedding or $\zeta_g \in K$, where*

$$g = gcd(N\mathfrak{p} - 1 : \ \mathfrak{p} \in S \setminus S_\infty),$$

then $R_S$the ring of S-integers is Euclidean if and only if R_S is a principal ideal domain.

In the proof of the theorem, the use of the Generalized Riemann Hypothesis is avoided by applying sieve methods and a generalization of the Bombieri-Vinogradov theorem on rational on primes in arithmetic progressions to algebraic number fields due to K. Murty and R. Murty [29].

Introduction to This Thesis

For technical reasons the most promising point to try to improve the Theorem stated aboveis for totally real Galois extensions of $\mathbb{Q}$ of degree four. In chapter 3, the proof in [15] is studied in detail for these fields. It appeared that by improving the arguments in [15] and, more especially in

[29], it might be possible to prove that the ring of integers of such a field is Euclidean if, and only if, it is a principal ideal domain. To this end, the Bombieri-Vinogradov type theorem of [29] is studied in chapter 2. The proof of this theorem required the use of a generalized form of the Čebotarev Density Theorem, which is proved in chapter 1. This approach was not successful and appears to require a much more precise understanding of the distribution of prime ideals.

In chapter 4, the desired result is proved assuming the existence of a prime $\mathfrak{p}$ of the field such that the unit group maps onto the coprime residue classes modulo $\mathfrak{p}^2$, such primes will be called special primes. Special note should be taken that since the ring of integers is always assumed to be a principal ideal domain, there will be a certain ambiguity between prime ideals and prime elements.

Theorem. *Let K be a totally real quartic Galois extension of $\mathbb{Q}$. If the ring of integers R of K contains a prime ideal $\mathfrak{p}$ such that the unit group maps onto $(R/\mathfrak{p}^2)^*$, then R is a Euclidean domain if and only if it is a principal ideal domain*

A probabilistic argument suggests that special primes occur frequently. Let

$$S(x) = \left\{\mathfrak{p} : N\mathfrak{p} \leq x,\ U \text{ maps onto } (R/\mathfrak{p}^2)^*\right\}.$$

Let q^n be the exact power of an odd prime q dividing

$$|(R/\mathfrak{p}^2)^*| = N\mathfrak{p}(N\mathfrak{p} - 1).$$

Consider the cyclic factor of $(R/p^2)^*$ of order q^n. In order for a unit ϵ not to be a generator of this group, it must land in the q^{n-1} part of the group. The probability of this occurring is $1/q$. For the prime 2, the units ± 1 always generate a subgroup of order 2; otherwise, the same heuristics work. Since totally real quartic fields have a rank three unit group, one would expect that $S(x)$ is asymptotic to

$$\sum_{N\mathfrak{p}\leq x} \prod_{\substack{q \mid \frac{N\mathfrak{p}(N\mathfrak{p}-1)}{2} \\ q \text{ prime}}} \left(1 - \frac{1}{q^3}\right).$$

Buchmann, Ford, Pohst, and von Schmettow [2] [3] computed the integral bases, discriminants, unit groups, and class numbers of all totally real fields of degree 4 with discriminant less than one million. From their tables, 165 of these fields satisfy the first requirement of the theorem, namely that the class number is one and the field is Galois over $\mathbb{Q}$. A special prime is found for each of these fields. Some of these fields are shown not to have the norm as Euclidean algorithm, providing the first such examples in the case of algebraic number fields.

In chapter 5 the result of the previous chapter is extended to all finite Galois extensions K of $\mathbb{Q}$. Since these extensions are Galois, they are either totally real or totally complex, that is these extensions have either r_1 real embeddings or $2r_2$ complex embeddings, and the unit group has rank $r = r_1 - 1$ or $r = r_2 - 1$, in the respective cases. In the first step, search for r primes $\mathfrak{p}_{11}, \ldots, \mathfrak{p}_{1r}$ such that the unit group maps onto

$$(R/\mathfrak{p}_{11}^2 \cdots \mathfrak{p}_{1r}^2)^*.$$

In the second step, take these primes and the units and find $2r$ new primes $\mathfrak{p}_{21},\ldots,\mathfrak{p}_{2(2r)}$ such that the group generated by the units and $\mathfrak{p}_{11},\ldots,\mathfrak{p}_{1r}$ map onto

$$\left(R/\mathfrak{p}_{21}^2\cdots\mathfrak{p}_{2(2r)}^2\right)^*.$$

Continue this constuction until $s=\max(4-r,2[K:\mathbb{Q}]-r-4)$ primes $\mathfrak{p}_{i1},\ldots,\mathfrak{p}_{is}$ are found such that the group generated by the units and the primes produced in the previous step map onto

$$\left(R/\mathfrak{p}_{i1}^2\cdots\mathfrak{p}_{is}^2\right)^*.$$

Theorem. *Let K be a Galois extension of $\mathbb{Q}$ whose ring of integers is a principal ideal domain. If the procedure described above produces*

$$s=\max(4-r,2[K:\mathbb{Q}]-r-4)$$

primes, then the ring of integers of K is a Euclidean domain.

Examples are given of the determination of these special primes for quadratic fields, real cubic fields, and totally complex quartic fields.

In the final chapter, the results of chapters 1, 2 and 3 are used to extend the results of Gupta and R. Murty [14] on cyclicity and generation of elliptic curves modulo p, p a rational prime, to algebraic number fields. Let E be an elliptic curve over a number field F. For every prime ideal $\mathfrak{p}$ of F, there is a reduction map $E(F)\rightarrow\tilde{E}(F_{\mathfrak{p}})$ modulo $\mathfrak{p}$.

Theorem. *Suppose that $[F:\mathbb{Q}]\leq 4$. The group $\tilde{E}(F_{\mathfrak{p}})$ is cyclic for infinitely many primes $\mathfrak{p}$ of F if and only if $K_q=F(E[q])\not\subseteq F$ for all $q|d$,*

where d is the largest integer such that $\mathbb{Q}(d) \subseteq F$. Furthermore, the number of primes $N\mathfrak{p} \leq x$ for which $\tilde{E}(F_\mathfrak{p})$ is cyclic is greater than $\delta_2 x/(\log x)^{2+1/4}$, for some positive constant δ_2.

Theorem. *Let Γ be a free subgroup of $E(F)$ and*

$$N_\Gamma(x) = \{\mathfrak{p} : \ N\mathfrak{p} \leq x, \Gamma \to E(F_\mathfrak{p}) \text{ is onto}\}.$$

Let E be an elliptic curve defined over a number field F. If the rank r of Γ satisfies $r > 2(2\eta - 1)$, then

$$N_\Gamma(x) \gg \frac{x}{(\log x)^{2+1/4}},$$

where $\eta = \max(2, d-2)$ and d is the order of the maximal abelian subgroup of $\mathrm{Gal}(F/\mathbb{Q})$.

CHAPTER 1
GENERALIZED ČEBOTAREV DENSITY THEOREM

Lagarias and Odlyzko [21] proved an effective version of the Čebotarev Density Theorem. A generalization of their result is required in the next chapter. Let K be an algebraic number field and define $n_K = [K : \mathbb{Q}]$ and d_K equal to the absolute value of the discriminant of K. Suppose that L is a Galois extension of K with Galois group $G = \mathrm{Gal}(L/K)$. If $\mathfrak{p}$ is a prime ideal of K which is unramified in L and $\mathfrak{P}$ is a prime of L lying above $\mathfrak{p}$, then the Frobenius symbol, $\sigma_{\mathfrak{P}} \in G$, is defined by $\sigma_{\mathfrak{P}} x \equiv x^{N\mathfrak{p}} (\mathrm{mod}\ \mathfrak{P})$. Here N is the absolute norm. Let $\sigma_{\mathfrak{p}}$ be the conjugacy class of G containing the $\sigma_{\mathfrak{P}}$ with $\mathfrak{P}|\mathfrak{p}$. If the dependence of the Artin symbol on the fields is important, then the notation $(\mathfrak{p}, L/K)$ will be used. If ξ is a class function of G, $I_{\mathfrak{P}}$ the inertia group of $\mathfrak{P}$, and $D_{\mathfrak{P}}$ the decomposition group of $\mathfrak{P}$, then let

$$\tilde{\xi}(\mathfrak{P}^m) = \frac{1}{|I_{\mathfrak{P}}|} \sum_{\alpha \in I_{\mathfrak{P}}} \xi(\tau^m \alpha),$$

where τ is a generator of the cyclic group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. Define

$$\psi_k(x, \xi, L/K) = \frac{1}{k!} \sum_{N\mathfrak{p}^j \leq x} \left(x - N\mathfrak{p}^j\right)^k \tilde{\xi}(\mathfrak{P}^j)(\log N\mathfrak{p}).$$

Let ρ be an irreducible representation and η its character. Let V be the representation space of ρ. For each prime ideal $\mathfrak{p}$ of K, chose $\mathfrak{P}|\mathfrak{p}$ and let

$V^{I_\mathfrak{P}}$ be the vector subspace of V of elements fixed by the image of $I_\mathfrak{P}$ under ρ. Then the Artin L-function is defined as

$$L(s,\eta) = \prod_{\mathfrak{p}} \det\left(1 - \rho(\sigma_\mathfrak{P}) N\mathfrak{p}^{-s} | V^{I_\mathfrak{P}}\right)^{-1}$$

and is absolutely convergent for $\mathrm{Re}(s) > 1$. Brauer proved that it extends to a meromorphic function. If $\rho \neq 1$, Artin conjectured that it extends to an entire function. Artin did prove a functional equation for $L(s,\eta)$ of the form

$$L(s,\eta) = W(\eta) G(s,\eta) L(1-s,\overline{\eta}),$$

where

$$G(s,\eta) = A(\eta)^{2s-1} \left(\frac{2}{(2\pi)^s}\right)^n (\cos\frac{s\pi}{2})^{a(\eta)} (\sin\frac{s\pi}{2})^{b(\eta)} \Gamma^n(s),$$

and $n = n_K = a(\omega \otimes \chi) + b(\omega \otimes \chi)$.

Suppose $\xi = \sum_\eta a_\eta \eta$, where the summation is over irreducible characters of G, $a_\eta \in \mathbb{C}$, then the formula

$$\psi_k(x, \xi, L/K) = -\frac{1}{2\pi i} \sum_\eta a_\eta \int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} \frac{L'}{L}(s,\eta) \frac{x^{s+k}}{s(s+1)\cdots(s+k)}\, ds,$$

where $\sigma_0 > 1$ is a consequence of the following lemma.

Lemma 1. *Let k be a positive integer, then*

$$\left| \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{y^{s+k}}{s(s+1)\cdots(s+k)}\, ds \right| < \frac{y^{\sigma_0+k}}{\pi k T^k}, \quad \text{for } 0 < y \leq 1,$$

$$\left| \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{y^{s+k}}{s(s+1)\cdots(s+k)}\, ds - \frac{1}{k!}(y-1)^k \right| < \frac{y^{\sigma_0+k}}{\pi k T^k}, \quad \text{for } 1 \leq y.$$

Proof. For $0 < y \leq 1$,

$$\frac{y^{s+k}}{s(s+1)\cdots(s+k)},$$

goes to zero as σ goes to $+\infty$, so that

$$\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{y^{s+k}}{s(s+1)\cdots(s+k)}ds$$
$$=\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\infty-iT}\frac{y^{s+k}}{s(s+1)\cdots(s+k)}ds-\frac{1}{2\pi i}\int_{\sigma_0+iT}^{\infty+iT}\frac{y^{s+k}}{s(s+1)\cdots(s+k)}ds,$$

since the integrand has no poles for $\mathrm{Re}(s) > 1$. The absolute value of both of these integrals is

$$\leq \frac{1}{2\pi k}\frac{y^{\sigma_0+k}}{T^k}.$$

This proves the first inequality.

For $y \geq 1$,

$$\frac{y^{s+k}}{s(s+1)\cdots(s+k)},$$

goes to zero as σ goes to $-\infty$, so that

$$\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{y^{s+k}\,ds}{s(s+1)\cdots(s+k)}$$
$$=\Sigma+\frac{1}{2\pi i}\int_{c-iT}^{-\infty-iT}\frac{y^{s+k}\,ds}{s(s+1)\cdots(s+k)}-\frac{1}{2\pi i}\int_{c+iT}^{-\infty+iT}\frac{y^{s+k}\,ds}{s(s+1)\cdots(s+k)},$$

where Σ is the sum of the residues of the integrand at $0, -1, \cdots, -k$. The two integrals are estimated as above, and

$$\Sigma=\sum_{j=0}^{k}(-1)^j\frac{y^{-j+k}}{j!(k-j)!}=\frac{1}{k!}(y-1)^k,$$

giving the second inequality.

Now let $\xi_C = \sum_\eta a_\eta \eta$ be the characteristic function of a conjugacy class C of G, and let

$$I_k(x, C, T) = -\frac{1}{2\pi i} \sum_\eta a_\eta \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{L'}{L}(s, \eta) \frac{x^{s+k}}{s(s+1)\cdots(s+k)}\, ds,$$

where $\sigma_0 > 1$, and $x \geq 2$. By Lemma 1,

$$\begin{aligned} |I_k(x, C, T) - \psi_k(x, \xi_C, L/K)| &\leq \frac{1}{\pi k T^k} \left\{ \sum_{\mathfrak{p}^j} \left(\frac{x}{N\mathfrak{p}^j} \right)^{\sigma_0 + k} \log N\mathfrak{p} \right\} \\ &\leq \frac{1}{\pi k T^k} \left\{ \sum_{\mathfrak{p}^j} \left(\frac{x}{N\mathfrak{p}^j} \right)^{\sigma_0 + k} \log N\mathfrak{p} \right\}, \end{aligned}$$

where the sum is over the prime power ideals. Choose $\sigma_0 = 1 + (\log x)^{-1}$, then the estimate

$$\begin{aligned} \sum_{\mathfrak{p}^j} \left(\frac{x}{N\mathfrak{p}^j} \right)^{\sigma_0 + k} \log N\mathfrak{p} &\ll x^{k+1} \sum_{p^j} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{j(\sigma_0 + k)}} \\ &\ll x^{k+1} \frac{\zeta_K'}{\zeta_K}(\sigma_0 + k) \ll \frac{n_K x^{k+1}}{k+1}, \end{aligned}$$

follows from

$$-\frac{\zeta_K'}{\zeta_K}(\sigma) \ll n_K (\sigma - 1)^{-1}.$$

Therefore,

$$\psi_k(x, \xi_C, L/K) = I_k(x, T, C) + O\left(\frac{n_K x^{k+1}}{(k+1)^2 T^k}\right), \tag{2}$$

for all $x \geq 2$ and $T \geq 1$.

Choose $g \in C$, let H be the cyclic group generated by g, and E the fixed field of H. Since the L-series is invariant under induction,

(3)

$$I_k(x, C, T) = -\frac{|C|}{|G|} \sum_\chi \bar{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^{s+k}}{s(s+1)\cdots(s+k)} \frac{L'}{L}(s, \chi) ds,$$

where the sum runs over the characters of the abelian group $H = \mathrm{Gal}(L/E)$.

Next, the integral

$$(4) \qquad I_k(x,T,\chi) = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} \frac{x^{s+k}}{s(s+1)\cdots(s+k)}\frac{L'}{L}(s,\chi)\,ds,$$

will be evaluated, where χ is a character of H, $U = j + \frac{1}{2}$, and j is an integer greater than k. Define

$$I_k(x,T,U,\chi) = \frac{1}{2\pi i}\int_{R_{T,U}} \frac{x^{s+k}}{s(s+1)\cdots(s+k)}\frac{L'}{L}(s,\chi)\,ds,$$

where $R_{T,U}$ is the rectangle with vertices at $\sigma_0 \pm iT$, and $-U \pm iT$.

The difference between these two integrals

$$R_k(x,T,U,\chi) = I_k(x,T,U,\chi) - I_k(x,T,\chi)$$

may be divided into three parts

$$V_k(x,T,U,\chi) = \frac{1}{2\pi}\int_{T}^{-T} \frac{x^{-U+k+it}}{(-U+it)(-U+1+it)\cdots(-U+k+it)} \times \frac{L'}{L}(-U+it,\chi)\,dt,$$

$$H_k(x,T,U,\chi) = \frac{1}{2\pi i}\int_{-U}^{-\frac{1}{4}} \left\{ \frac{x^{\sigma+k-iT}}{(\sigma-iT)(\sigma+1-iT)\cdots(\sigma+k-iT)} \times \frac{L'}{L}(\sigma-iT,\chi) - \frac{x^{\sigma+k+iT}}{(\sigma+iT)(\sigma+1+iT)\cdots(\sigma+k+iT)} \times \frac{L'}{L}(\sigma+iT,\chi) \right\} d\sigma,$$

$$H_k^*(x,T,\chi) = \frac{1}{2\pi i}\int_{-\frac{1}{4}}^{\sigma_0}\Bigg\{\frac{x^{\sigma+k-iT}}{(\sigma-iT)(\sigma+1-iT)\cdots(\sigma+k-iT)} \times \frac{L'}{L}(\sigma-iT,\chi) - \frac{x^{\sigma+k+iT}}{(\sigma+iT)(\sigma+1+iT)\cdots(\sigma+k+iT)} \times \frac{L'}{L}(\sigma+iT,\chi)\Bigg\}\,d\sigma.$$

Since $U = j+\frac{1}{2}$ and $|-U+m+it| \geq \frac{1}{4}$ for every integer m,

$$\begin{aligned} V_k(x,T,U,\chi) &\ll \frac{x^{-U+k}}{U(U-1)\cdots(U-k)}\int_{-T}^{T}\left|\frac{L'}{L}(-U+it,\chi)\right|dt, \\ &\ll \frac{x^{-U+k}}{U^k}T(\log A(\chi)+n_E\log(T+U)), \\ H_k(x,T,U,\chi) &\ll \int_{-\infty}^{-\frac{1}{4}}\frac{x^{\sigma+k}}{T^k}(\log A(\chi)+n_E\log(|\sigma|+2)+n_E\log T)\,d\sigma, \\ &\ll \frac{x^{-\frac{1}{4}+k}}{T^k}(\log A(\chi)+n_E\log T), \end{aligned}$$

using Lemma 6.2 of Lagarias and Odlyzko [21]. By Lemma 5.6 of [21],

$$\begin{aligned} &H_k^*(x,T,\chi) \\ &\quad - \frac{1}{2\pi i}\int_{-\frac{1}{4}}^{\sigma_0}\Bigg\{\frac{x^{\sigma+k-iT}}{(\sigma-iT)(\sigma+1-iT)\cdots(\sigma+k-iT)}\sum_{\substack{\rho \\ |\gamma+T|\leq 1}}\frac{1}{\sigma-iT-\rho} \\ &\quad - \frac{x^{\sigma+k+iT}}{(\sigma+iT)(\sigma+1+iT)\cdots(\sigma+k+iT)}\sum_{\substack{\rho \\ |\gamma+T|\leq 1}}\frac{1}{\sigma+iT-\rho}\Bigg\}\,d\sigma \\ &\quad \ll \int_{-\frac{1}{4}}^{\sigma_0}\frac{x^{\sigma+k}}{T^{k+1}}(\log A(\chi)+n_E\log T)\,d\sigma, \\ (5)\qquad &\quad \ll \frac{x^{k+1}}{T^{k+1}}(\log A(\chi)+n_E\log T). \end{aligned}$$

Lemma 2. *Let $\rho = \beta + i\gamma$, with $\gamma \neq T$, then*

$$\int_{-\frac{1}{4}}^{\sigma_1} \frac{x^{\sigma+k+iT}}{(\sigma+iT)(\sigma+1+iT)\cdots(\sigma+k+iT)(\sigma+iT-\rho)}\,d\sigma \ll \frac{x^{\sigma_1+k}(\sigma_1-\beta)}{|T|^{k+1}},$$

where $|T| \geq 2$, $x \geq 2$, and $1 < \sigma_1 \leq 3$.

Proof. Suppose $\gamma > T$. Let B be the rectangle with vertices

$$\sigma_1 + iT, \quad -\tfrac{1}{4} + iT, \quad -\tfrac{1}{4} + i(T-1), \quad \sigma_1 + i(T-1).$$

Cauchy's Residue Theorem gives

$$\int_B \frac{x^{s+k}}{s(s+1)\cdots(s+k)(s-\rho)}\,ds = 0.$$

On the sides of the rectangle other than $[-\frac{1}{4}+iT, \sigma_1+iT]$ the integrand is

$$\ll \frac{x^{\sigma_1+k}}{(|T|-1)^{k+1}(\sigma_1-\beta)},$$

which proves the lemma for $\gamma > T$. For $\gamma < T$, use the rectangle with vertices

$$-\tfrac{1}{4} + iT, \quad \sigma_1 + iT, \quad \sigma_1 + i(T+1), \quad -\tfrac{1}{4} + i(T+1).$$

The lemma implies that

$$\frac{1}{2\pi i}\int_{-\frac{1}{4}}^{\sigma_0} \frac{x^{\sigma+k-iT}}{(\sigma-iT)(\sigma+1-iT)\cdots(\sigma+k-iT)} \left(\sum_{\substack{\rho \\ |\gamma+T|\leq 1}} \frac{1}{\sigma-iT-\rho}\right) d\sigma \ll \frac{x^{k+1}}{T^{k+1}}(\log A(\chi) + n_E \log T),$$

for $x \geq 2$ and $T \geq 2$. The same estimate holds for the other integral in (5) so that

$$H_k^*(x,T,\chi) \ll \frac{x^{k+1}}{T^{k+1}}(\log A(\chi) + n_E \log T).$$

Therefore,

$$I_k(x,T,U,\chi) - I_k(x,T,\chi) \ll \frac{x^{k+1}}{T^{k+1}}(\log A(\chi) + n_E \log T) + \frac{Tx^{-U+k}}{U^{k+1}}(\log A(\chi) + n_E \log(T+U)).$$

The next goal will be to evaluate $I_k(x,T,U,\chi)$ using Cauchy's Residue Theorem, for $T \neq \gamma$ for any zero $\rho = \beta + i\gamma$ of the Artin L-function L. If $\chi = \chi_1$, the principal character, then L'/L has a simple pole at $s = 1$ with residue -1. The residue of the integrand is

$$-\delta(\chi)\frac{x^{k+1}}{(k+1)!}$$

At the nontrivial zeros ρ of $L(s,\chi)$, L'/L has a simple pole with residue equal to the multiplicity of the zero. (Note that since L/E is cyclic, the Artin L-functions $L(s,\chi)$ are entire by the reciprocity law.) This contributes a term

$$\frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)}.$$

for each zero $\rho = \beta + i\gamma$ with $|\gamma| < T$, counted according to multiplicity. At nonpositive integers, L'/L also has simple poles coming from the trivial zeros of $L(s,\chi)$. At odd integers $-(2j-1) < -k$, L'/L has residue $b(\chi)$ and at even integers $-2j < -k$, L'/L has residue $a(\chi)$. These contribute

the term

$$b(\chi)\sum_{j=[\frac{k+1}{2}]}^{[\frac{U+1}{2}]}\frac{(-1)^{k+1}x^{-2j+1+k}}{(2j-1)(2j-2)\cdots(2j-(k+1))}$$
$$+a(\chi)\sum_{j=[\frac{k+2}{2}]}^{[\frac{U}{2}]}\frac{(-1)^{k+1}x^{-2j+k}}{2j(2j-1)\cdots(2j-k)}.$$

Note that if $i \le k$,

$$\frac{x^{s+k}}{s(s+1)\cdots(s+k)} = \frac{x^{-i+k}}{(s+i)(-i)(-i+1)\cdots(-1)(1)\cdots(-i+\overline{k})}$$
$$+\frac{x^{-i+k}\log x}{(-i)(-i+1)\cdots(-1)(1)\cdots(-i+k)}+(s+i)h_1(s),$$

where $h_1(s)$ is analytic at $s=-i$, $0 \le i \le k$. Also,

$$\frac{\Gamma'}{\Gamma}(s) = -\frac{1}{s}-\gamma-\sum_{k=1}^{\infty}(\frac{1}{s+k}-\frac{1}{k})$$
$$=-\frac{1}{s+i}+\frac{2}{i}-\gamma-\sum_{t=1}^{i-1}\frac{1}{t}+(s+i)h_2(s),$$

where $h_2(s)$ is analytic at $s=j$. So for odd integers $-k \le -(2j+1) < 0$,

$$\frac{L'}{L}(s,\chi) = \frac{b(\chi)}{s+2j+1}+r_{1,j}(\chi)+(s+2j+1)h_{3,j}(s)$$

where

$$r_{1,j}(\chi) = B(\chi)-\frac{1}{2}\log A(\chi)+\delta(\chi)\left(\frac{1}{2j+2}+\frac{1}{2j+1}\right)$$
$$-\sum_{\rho}\left(\frac{1}{2j+1+\rho}-\frac{1}{\rho}\right)+\frac{1}{2}n_E\log\pi$$
$$+\frac{b(\chi)}{2}\left(\frac{2}{j}-\gamma-\sum_{t=1}^{j-1}\frac{1}{t}\right)+\frac{a(\chi)}{2}\left(\frac{\Gamma'}{\Gamma}(-j-\frac{1}{2})\right)$$

For even integers $-k \le -2j < 0$,

$$\frac{L'}{L}(s,\chi) = \frac{a(\chi)}{s+2j} + r_{2,j}(\chi) + (s+2j)h_{4,j}(s)$$

where

$$r_{2,j}(\chi) = B(\chi) - \frac{1}{2}\log A(\chi) + \delta(\chi)\left(\frac{1}{2j}+\frac{1}{2j+1}\right) - \sum_{\rho}\left(\frac{1}{2j-\rho}-\frac{1}{\rho}\right)$$
$$+ \frac{1}{2}n_E\log\pi + \frac{b(\chi)}{2}\left(\frac{\Gamma'}{\Gamma}(-j+\frac{1}{2})\right) + \frac{a(\chi)}{2}\left(\frac{2}{j} - \gamma - \sum_{t=1}^{j-1}\frac{1}{t}\right)$$

Finally at $s=0$,

$$\frac{L'}{L}(s,\chi) = \frac{a(\chi)-\delta(\chi)}{s} + r_0(\chi) + sh_5(s),$$

where

$$r_0(\chi) = B(\chi) - \frac{1}{2}\log A(\chi) + \delta(\chi) + \frac{1}{2}n_E\log\pi - \frac{b(\chi)}{2}\frac{\Gamma'}{\Gamma}(\frac{1}{2}) - \frac{a(\chi)}{2}\frac{\Gamma'}{\Gamma}(1)$$

Therefore, Cauchy's theorem gives

$$\begin{aligned}
I_k(x,T,U,\chi) = {} & \\
& -\delta(\chi)\frac{x^{k+1}}{(k+1)!} + \sum_{\substack{\rho \\ |\gamma|<T}}\frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)} \\
& + x^k(r_0(\chi) + (a(\chi)-\delta(\chi))\log x) \\
& + (-1)^{k+1}\Big\{b(\chi)\sum_{j=[\frac{k+1}{2}]}^{[\frac{U+1}{2}]}\frac{x^{-2j-1+k}}{(2j-1)(2j-2)\cdots(2j-(k+1))} \\
& + a(\chi)\sum_{j=[\frac{k+2}{2}]}^{[\frac{U}{2}]}\frac{x^{-2j+k}}{2j(2j-1)\cdots(2j-k)}\Big\} \\
& - \sum_{j=1}^{[\frac{k+1}{2}]}\frac{x^{-2j+1+k}}{(2j-1)!(-2j+1+k)!}(r_{1,j}(\chi)+b(\chi)\log x) \\
& + \sum_{j=1}^{[\frac{k}{2}]}\frac{x^{-2j+k}}{(2j)!(-2j+k)!}(r_{2,j}(\chi)+a(\chi)\log x).
\end{aligned}$$

Letting U tend to infinity gives

$$
\begin{aligned}
I_k(x,T,\chi) + \delta(\chi)\frac{x^{k+1}}{(k+1)!} &- \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)} \\
&- x^k(r_0(\chi) - (a(\chi)-\delta(\chi))\log x) \\
&- (-1)^{k+1}\Big\{b(\chi)\sum_{j=[\frac{k+1}{2}]}^{\infty} \frac{x^{-2j-1+k}}{(2j-1)(2j-2)\cdots(2j-(k+1))} \\
&- a(\chi)\sum_{[\frac{k+2}{2}]}^{\infty} \frac{x^{-2j+k}}{2j(2j-1)\cdots(2j-k)}\Big\} \\
&+ \sum_{j=1}^{[\frac{k+1}{2}]} \frac{x^{-2j+1+k}}{(2j-1)!(-2j+1+k)!}(r_{1,i}(\chi) + b(\chi)\log x) \\
&- \sum_{j=1}^{[\frac{k}{2}]} \frac{x^{-2j+k}}{(2j)!(-2j+k)!}(r_{2,i}(\chi) - a(\chi)\log x) \\
&\ll \frac{x^{k+1}\log x}{T^{k+1}}(\log A(\chi) + n_E \log T)
\end{aligned}
$$

Clearly, $r(\chi) \ll B(\chi) + \log A(\chi) + n_E \log k$, where $r(\chi)$ is any of the subscipted $r(\chi)$'s appearing above. By Lemma 5.5 of [21],

$$B(\chi) + \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho} \ll \log A(\chi) + n_E.$$

Hence,

$$
\begin{aligned}
I_k(x,T,\chi) + \delta(\chi)\frac{x^{k+1}}{(k+1)!} &- \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{x^k \log x}{\rho} \\
&\ll \log A(\chi) + n_E \log(kx) + \frac{x^{k+1}\log x}{T^{k+1}}(\log A(\chi) + n_E \log T) \\
&\quad + x^k \log x(\log A(\chi) + n_E \log k), \\
&\ll \frac{x^{k+1}\log x}{T^{k+1}}(\log A(\chi) + n_E \log T) + x^k \log x(\log A(\chi) + n_E \log k).
\end{aligned}
$$

Therefore by (3) and (4) with T not equal to the imaginary part of any zero of $L(s,\chi)$,

$$I_k(x,C,T) - \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\left\{\delta(\chi)\frac{x^{k+1}}{(k+1)!} - \sum_{\substack{\rho \\ |\gamma|<T}}\frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)} - \sum_{\substack{\rho \\ |\rho|<1/2}}\frac{x^k\log x}{\rho}\right\}$$

$$\ll \frac{|C|}{|G|}\sum_{\chi}\left(\frac{x^{k+1}\log x}{T^{k+1}}(\log A(\chi)+n_E\log T)+x^k\log x(\log A(\chi)+n_E\log k)\right)$$

$$\ll \frac{|C|}{|G|}\left(\frac{x^{k+1}\log x}{T^{k+1}}(\log d_L+n_L\log T)+x^k\log x((\log d_L)^2+n_L\log k)\right),$$

using the conductor-discriminant formula and the estimate

$$\sum_{\chi}\sum_{\substack{\rho \\ |\rho|<\frac{1}{2}}}\left|\frac{1}{\rho}\right| \ll (\log d_L)^2.$$

Therefore by (2),

$$\psi_k(x,\xi_C) - \frac{|C|}{|G|}\frac{x^{k+1}}{(k+1)!} + \frac{|C|}{|G|}\sum_{\chi}\bar{\chi}(g)\sum_{\substack{\rho \\ |\gamma|<T}}\frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)}$$

$$\ll \frac{|C|}{|G|}\left(\frac{x^{k+1}\log x}{T^{k+1}}(\log d_L+n_L\log T)+x^k\log x((\log d_L)^2+n_L\log k)\right)$$

$$+\frac{n_E x^{k+1}}{k^2T^k}.$$

Theorem 1. *There is an effectively computable constant c_1 such that if*

$$x \geq \exp((\log d_L)^2/n_L + \log 2\log d_L + n_L(\log 2)^2),$$

then

$$\psi_k(x,\xi_C) = \frac{|C|}{|G|}\frac{x^{k+1}}{(k+1)!} + O(\frac{|C|}{|G|}\frac{x^{\beta_0}}{\beta_0(\beta_0+1)\cdots(\beta_0+k)})$$

$$+O(x^{k+1}\exp(-c_1 n_L^{-1/2}(\log x)^{1/2}),$$

where the second term occurs only if $\zeta_L(s)$ has an exceptional zero β_0.

Proof. If $\rho = \beta + i\gamma \neq \beta_0$ is a nontrivial zero of some $L(s, \chi)$ with $|\gamma| \leq T$, then Lemma 8.1 of [21] shows that

$$\left|x^{\rho+k}\right| \leq x^{k+1} \exp\left(-c\frac{\log x}{\log d_L T^{n_L}}\right),$$

for some effectively computable constant c and for $x, T \geq 2$. The estimate

$$N_\chi(T) \ll \log A(\chi) + n_E \log(T+2)$$

implies that

$$\sum_\chi \sum_{\substack{\rho \\ |\rho| \geq 1/2 \\ |\gamma| \leq T}} \left|\frac{1}{\rho(\rho+1)\cdots(\rho+k)}\right| \ll \frac{\log d_L + n_L}{k!},$$

for $k \geq 1$ by the conductor-discriminant formula. In addition,

$$\begin{aligned}\sum_\chi \sum_{\substack{\rho \neq 1-\beta_0 \\ |\rho|<1/2}} &\left|\frac{x^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)}\right| \\ &\ll x^{1/2+k} \sum_\chi \sum_{\substack{\rho \neq 1-\beta_0 \\ |\rho|<1/2}} \left|\frac{1}{\rho(\rho+1)\cdots(\rho+k)}\right| \\ &\ll \frac{x^{1/2+k}}{k!}(\log d_L)^2 \qquad (6)\end{aligned}$$

and

$$\sum_\chi \sum_{\substack{\rho \neq 1-\beta_0 \\ |\rho|<1/2}} \left|\frac{x^k \log x}{\rho}\right| \ll x^k \log x (\log d_L)^2$$

using Lemmas 8.1 and 8.2 of [21]. Lemma 8.2 of [21] implies that

$$\begin{aligned}&\left|\frac{x^{k+1-\beta_0}}{(1-\beta_0)(2-\beta_0)\cdots(k+1-\beta_0)}\right| \\ &\qquad \leq \frac{1}{k!} \max\left[c(n_L)\log d_L, c_3 d_L^{1/n_L}\right] x^{k+\min\left[\frac{1}{c(n_L)\log d_L}, \frac{1}{d_L^{1/n_L}}\right]}\end{aligned}$$

and

$$\left|\frac{x^k \log x}{1-\beta_0}\right| \le x^k \log x \max\left[c(n_L)\log d_L, c_3 d_L^{1/n_L}\right].$$

Hence, by (6),

$$\begin{aligned}\psi_k(x,\xi_C) &- \frac{|C|}{|G|}\frac{x^{k+1}}{(k+1)!} \\ &\ll \frac{|C|}{|G|}\frac{x^{\beta_0+k}}{\beta_0(\beta_0+1)\cdots(\beta_0+k)} + \frac{|C|}{|G|}\frac{x^{k+1}\log x}{T^{k+1}}(\log d_L + n_L \log T) \\ &+ \frac{|C|}{|G|}x^k \log x((\log d_L)^2 + n_L \log k) + n_E \frac{x^{k+1}}{T^k}\log x.\end{aligned}$$

Choose

$$T = \exp(n_L^{-1/2}(\log x)^{1/2} - (\log d_L)/n_L)$$

to obtain the theorem.

A result of Stark [39, p. 148] gives an effective bound for the exceptional zero.

Lemma 3. *The Dedekind zeta function $\zeta_L(s)$ has no real zeros for*

$$\max\left[1-(c(n_L)\log d_L)^{-1}, 1-(c_3 d_L^{1/n_L})^{-1}\right] \le \beta < 1,$$

where $c(n_L) = 4$ if L is Galois over $\mathbb{Q}$, $c(n_L) = 16$ if there is a sequence of fields $\mathbb{Q} = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = L$ with each F_j normal over F_{j+1}.

Theorem 2. *There exists effectively computable constants c_1, c_2 such that for $x \ge \exp((\log d_L)^2/n_L + \log 2 \log d_L + n_L(\log 2)^2)$,*

$$\begin{aligned}\psi_k(x,\xi_C) &= \frac{|C|}{|G|}\frac{x^{k+1}}{(k+1)!} + O\left(x^{k+1}\exp(-c_1 n_L^{1/2}(\log x)^{1/2})\right) \\ &+ O\left(x^{k+1}\exp(-\frac{\log x}{c(n_L)\log d_L})\right) + O\left(x^{k+1}\exp(-\frac{\log x}{c_2 (d_L)^{1/n_L}}\right)\end{aligned}$$

Proof. Apply Lemma 3 to estimate the term depending on the exceptional zero in the previous theorem.

CHAPTER 2
AVERAGE DENSITY OF PRIME IDEALS IN ALGEBRAIC NUMBER FIELDS

Bombieri [1] and Vinogradov [40] proved an average prime number theorem for primes in arithmetic progressions.

Bombieri-Vinogradov Theorem. *For every $A > 0$ there exists $B > 0$ such that*

$$\sum_{q \le x^{1/2}/(\log x)^B} \max_{y \le x} \max_{(a,q)=1} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll \frac{x}{\log^A x}.$$

K. Murty and R. Murty [29] proved a similar result for algebraic number fields. For the application to Euclidean domains in the next chapter, a more precise estimate is needed which requires only a slight modification of their proof.

The notation in this chapter is the same as before. For a conjugacy class C of $G = \mathrm{Gal}(L/K)$, define

$$\pi_C(x, L/K) = \sum_{\substack{N\mathfrak{p} \le x \\ \mathfrak{p} \text{ unramified in } L \\ \sigma_\mathfrak{p} = C}} 1$$

$$\psi_C(x, L/K) = \sum_{\substack{N\mathfrak{p}^m \le x \\ \mathfrak{p} \text{ unramified in } L \\ \sigma_\mathfrak{p}^m = C}} (\log N\mathfrak{p}).$$

If ξ is a class function of G, define

$$\psi(x, \xi, L/K) = \sum_{N\mathfrak{p}^m \le x} (\log N\mathfrak{p}) \tilde{\xi}(\mathfrak{p}^m).$$

If $\xi = \sum_\eta a_\eta \eta$, where the summation is over irreducible characters of G, $a_\eta \in \mathbb{C}$, and $L(s,\eta)$ is the Artin L-function then

$$\psi(x,\xi,L/K) = \frac{1}{2\pi i}\sum_\eta \int_{\sigma-i\infty}^{\sigma+i\infty} \frac{L'}{L}(s,\eta)\frac{x^s}{s}\,ds,$$

for $\mathrm{Re}(\sigma) > 1$.

If $L = K(\zeta_q)$ and $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$, then

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}).$$

Let $\xi(C,q,a)$ be the characteristic function of $C \times \{a\}$, where $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is regarded as $(\mathbb{Z}/q\mathbb{Z})^*$ so that a is a residue class modulo q, then

$$\psi(x,\xi(C,q,a),K(\zeta_q)/\mathbb{Q}) = \sum_{\substack{p^m \le x \\ p^m \equiv a \pmod q \\ \sigma_{\mathfrak{p}}{}^m = C}} \epsilon(p)(\log p),$$

where $\epsilon(p) = 1$ for unramified p and $\epsilon(p) \le 1$ for ramified p.

The average density result which will be proved is

Theorem. *Given $A > 0$, there is $B > 0$ such that for*

$$Q = x^{\frac{1}{\eta}}(\log x)^{-B},$$

then

$$\sum_{q\le Q}{}' \max_{(a,q)=1} \max_{y\le x} |\psi(y,\xi(C,q,a),K(\zeta_q)/\mathbb{Q}) - \delta(C,a,q)y| \ll \frac{x}{\log^A x},$$

where $\eta = \max(d-2,2)$, with

$$d = \min_M \max_\omega [G : H]\omega(1),$$

and where the' indicates summation over q *such that* $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$, *which implies* $\delta(C, a, q) = |C|/(\phi(q)|G|)$. *The* min *is taken over subfields* M *of* K *such that* $L(s, \omega \otimes \chi, K(\zeta_q)/M)$ *are holomorphic for all characters* χ *and the* max *is over characters of* $H = \mathrm{Gal}(K/M)$.

If K/M is abelian then each $L(s, \omega \otimes \chi)$ is holomorphic, so d is less than the degree of the largest subfield over which K is abelian. K. Murty and R. Murty [29] proved this result with $x^{1/\eta - \epsilon}$ instead of $x^{1/\eta}/(\log x)^B$.

Reduction to Holomorphic L-functions

Let δ_D denote the characteristic function of a conjugacy class D in some group H, then

$$\delta_D = \frac{|D|}{|H|} \sum_{\eta} \overline{\eta(g_D)} \eta, \tag{7}$$

where g_D is an element of D and the summation is over all irreducible characters of H. In particular, this relation implies

$$\psi(x, \xi(C, q, a), K(\zeta_q)/\mathbb{Q}) = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \psi(x, \delta_C \otimes \chi, K(\zeta_q)/\mathbb{Q}),$$

where the χ range over characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. From the previous chapter,

$$\psi_n(x, \omega \otimes \chi) \ll \frac{x^{n+1} \log x}{T^{n+1}} \log A(\omega \otimes \chi) + n \log T.$$

Choose $T = \exp(n^{1/2}(\log x)^{1/2} - \frac{1}{n} \log A(\omega \otimes \chi))$. Use Lemma 3.7 to estimate the possible exceptional zero. Since $A(\omega \otimes \chi) \ll q^n$ where the implied constant depends only on the field,

$$\psi_n(x, \omega \otimes \chi) \ll n \log q x^{n+1} \exp(-c(\log x)^{1/2}).$$

Hence,

$$\psi(x,\delta_C\otimes 1,K(\zeta_q)/\mathbb{Q})=\frac{|C|}{\phi(q)|G|}x+O(x\exp(-cn_K^{-\frac{1}{2}}(\log x)^{\frac{1}{2}})),$$

where c is some absolute constant and the O constant depends on the field K. Therefore,

$$\sum_{q\le Q_1}{}'\max_{(a,q)=1}\max_{y\le x}|\psi(y,\xi(C,q,a),K(\zeta_q)/\mathbb{Q})-\delta(C,a,q)y|$$
$$=\sum_{q\le Q_1}{}'\frac{1}{\phi(q)}\max_{y\le x}\sum_{\chi\neq 1}|\psi(y,\delta_C\otimes\chi,K(\zeta_q)/\mathbb{Q})|+O(x\exp(-c(\frac{\log x}{n_K})^{1/2})),$$

for any real number Q_1.

To reduce to a sum involving only primitive characters, observe that if $\chi(\mathrm{mod}\ q)$ is induced by $\chi_1(\mathrm{mod}\ q_1)$, then

$$|\psi(x,\delta_C\otimes\chi,K(\zeta_q)/\mathbb{Q})-\psi(x,\delta_C\otimes\chi_1,K(\zeta_q)/\mathbb{Q})|\le\sum_{p^m|q/q_1}\log p\ll\log\frac{q}{q_1}.$$

This implies,

$$\sum_{q\le Q_1}{}'\frac{1}{\phi(q)}\max_{y\le x}\sum_{\chi\neq 1}|\psi(y,\delta_C\otimes\chi,K(\zeta_q)/\mathbb{Q})|$$
$$\ll(\log x)\sum_{1<q\le Q_1}{}'\frac{1}{\phi(q)}\max_{y\le x}\sum_{\chi}{}^{*}|\psi(y,\delta_C\otimes\chi,K(\zeta_q)/\mathbb{Q})|+O(\log^2 x).$$

Let M be a subfield of K such that $L(s,\omega\otimes\chi,K(\zeta_q)/M)$ are holomorphic for all characters χ and all characters ω of $H=\mathrm{Gal}(K/M)$. If $S=H\times\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, then M is also the fixed field of S. If $g_C\in H\cap C$ then the conjugacy class of H containing g_C is denoted by C_H. By the invariance of L-series under induction

$$\psi(y,\delta_C\otimes\chi,K(\zeta_q)/\mathbb{Q})=\frac{|H||C|}{|C_H||G|}\psi(y,(\delta_{C_H}\otimes\chi)|_S,K(\zeta_q)/M).$$

The character relation (7) implies

$$\psi(y,(\delta_{C_H}\oslash\chi)|s,K(\zeta_q)/M)$$
$$G=\frac{|C_H|}{|H|}\sum_{\omega}\bar{\omega}(g_C)\psi(y,\omega\oslash\chi,K(\zeta_q)/M),$$

where the ω range over irreducible characters of H. Therefore,

$$\sum_{q\le Q_1}{}' \max_{(a,q)=1}\max_{y\le x}|\psi(y,\xi(C,q,a),K(\zeta_q)/\mathbb{Q})-\delta(C,a,q)y|$$
$$\ll(\log x)\frac{|C||H|}{|G|}\max_{\omega}\left\{\sum_{1<q\le Q_1}{}'\frac{1}{\phi(q)}\max_{y\le x}\sum_{\chi}{}^{*}|\psi(y,\omega\otimes\chi,K(\zeta_q)/M)|\right\}$$
$$\ll(\log x)(\log Q_1)\frac{|C||H|}{|G|}\max_{\omega}\max_{Q\le Q_1}\sum_{Q/2<q\le Q}{}'\frac{1}{\phi(q)}\max_{y\le z}\sum_{\chi}{}^{*}|\psi(y,\omega\otimes\chi)|$$
$$\ll(\log x)^2\frac{|C||H|}{|G|}\max_{\omega}\max_{Q\le Q_1}\sum_{1<q\le Q}{}'\frac{\log\log Q}{Q}\max_{y\le x}\sum_{\chi}{}^{*}|\psi(y,\omega\otimes\chi)|$$
$$\ll(\log\log x)(\log x)^2\frac{|C||H|}{|G|}\max_{\omega}\max_{Q\le Q_1}\sum_{1<q\le Q}{}'\frac{1}{Q}\max_{y\le x}\sum_{\chi}{}^{*}|\psi(y,\omega\otimes\chi)|,$$

since $\phi(q)\gg q/\log\log q$. This reduces the theorem stated above to an estimate involving holomorphic Artin L-series.

The L-series in the Critical Strip

The following theorem is useful for estimating functions in a strip.

Phragmen-Lindelöf Theorem. *Let $f(s)$ be regular and analytic in the strip*

$$S=\{s\in\mathbb{C}:\ a\le Re(s)\le b\}$$

such that

$$|f(a+it)| \leq A|Q+a+it)|^{\alpha}$$

$$|f(b+it)| \leq B|Q+b+it|^{\beta},$$

with $Q+a>0$ *and* $\alpha \geq \beta$, *then for* s *in the strip* S,

$$|f(s)| \leq (A|Q+s|^{\alpha})^{\frac{b-\sigma}{b-a}} \left(B|Q+s|^{\beta}\right)^{\frac{\sigma-a}{b-a}}.$$

This form of the theorem is due to Rademacher [32].

Since the coefficients of the Dirichlet series $L(s,\omega\otimes\chi)$ satisfy $A_m \leq n$ with $n = n(\omega\otimes\chi) = n_M(\omega\otimes\chi)(1)$, it follows that for $\epsilon>0$,

$$|L(1+\epsilon+it,\omega\otimes\chi)| \leq \zeta^n(1+\epsilon).$$

Artin L-series have the functional equation

$$L(s,\omega\otimes\chi) = W(\omega\otimes\chi)G(s,\omega\otimes\chi)L(1-s,\overline{\omega\otimes\chi}), \tag{8}$$

where

$$G(s,\omega\otimes\chi) = A(\omega\otimes\chi)^{2s-1}\left(\frac{2}{(2\pi)^s}\right)^n (\cos\frac{s\pi}{2})^{a(\omega\otimes\chi)}(\sin\frac{s\pi}{2})^{b(\omega\otimes\chi)}\Gamma^n(s),$$

and $a(\omega\otimes\chi)+b(\omega\otimes\chi)=n$. Stirling's formula in the form

$$|\Gamma(z)| = e^{-\pi/2y}|z|^{x-1/2}(2\pi)^{1/2}(1+O(|z|^{-1/2})),$$

with $z=x+iy$, shows that

$$|G(z,\omega\otimes\chi)| \leq A(\omega\otimes\chi)^{2x-1}2^n(2\pi)^{-nx+1/2}|z|^{n(x-1/2)}(1+O(|z|^{-1/2})).$$

Therefore,

$$|L(-\epsilon+it,\omega\oslash\chi)|\leq A(\omega\oslash\chi)^{\frac{1}{2}+\epsilon}(|t|+2)^{n(\frac{1}{2}+\epsilon)}\zeta(1+\epsilon)^n$$

With these two estimates in hand the Phragmen-Lindelöf theorem gives the estimate

$$|L(s,\omega\oslash\chi)|\leq\zeta^n(1+\epsilon)(A(\omega\otimes\chi)(|t|+2)^n)^{\frac{1-\sigma+\epsilon}{2}}, \tag{9}$$

for $-\epsilon\leq \mathrm{Re}(s)\leq 1+\epsilon$. Now choose $\epsilon=(\log(A(\omega\otimes\chi)(|t|+2)^n))^{-1}$, which gives

$$|L(\sigma+it,\omega\oslash\chi)|\leq(A(\omega\otimes\chi)(|t|+2)^n)^{\frac{1-\sigma}{2}}(\log(A(\omega\otimes\chi)(|t|+2)^n))^n,$$

since $\zeta(1+\epsilon)\ll\epsilon^{-1}$.

To obtain a similar estimate for $L'(s,\omega\otimes\chi)$, differentiate the functional equation (8),

$$L'(1-s,\omega\otimes\chi)=-G'(s,\omega\otimes\chi)L(s,\overline{\omega\otimes\chi})-G(s,\omega\otimes\chi)L'(s,\overline{\omega\otimes\chi}).$$

Since

$$\left|\frac{\Gamma'}{\Gamma}(z)\right|\ll\log(|z|+2),$$

then

$$\frac{G'}{G}(s,\omega\otimes\chi)\ll n\log(|t|+2),$$

which implies

$$G'(s,\omega\otimes\chi)\ll n(A(\omega\otimes\chi)(|t|+2)^n)^{\frac{1}{2}-\sigma}\log(|t|+2).$$

The same argument as above shows

$$|L'(s,\omega\otimes\chi)|\ll(A(\omega\otimes\chi)(|t|+2)^n)^{\frac{1-\sigma}{2}}(\log A(|t|+2)^n)^n. \tag{10}$$

Proof of the Theorem

Suppose that

$$\frac{1}{L(s,\omega\otimes\chi)}=\prod_{\mathfrak{p}}(1-(\omega\otimes\chi)(\mathfrak{p})N\mathfrak{p}^{-s})=\sum_{j=1}^{\infty}\frac{b_j\chi(j)}{j^s}$$

$$-\frac{L'}{L}(s,\omega\otimes\chi)=\sum_{j=1}^{\infty}\frac{\Lambda(j)c_j\chi(j)}{j^s}$$

and define

$$F_z=F_z(s,\omega\otimes\chi)=\sum_{j\le z}\frac{\Lambda(j)c_j\chi(j)}{j^s}$$

$$G_z=G_z(s,\omega\otimes\chi)=\sum_{j>z}\frac{\Lambda(j)c_j\chi(j)}{j^s}$$

$$M_z=M_z(s,\omega\otimes\chi)=\sum_{j\le z}\frac{b_j\chi(j)}{j^s},$$

for $\sigma>1$ where Λ denotes von Mangoldt's function and $z>0$. Since $|(\omega\otimes\chi)(\mathfrak{p})|\le 1$, $b_{p^m}=0$ for $m>n$, $|b_{p^m}|\le\binom{n}{m}$, and $|b_j|\le 2^{np(j)}$, where $p(j)$ is the number of distinct prime divisors of j.

The identity

$$-\frac{L'}{L}(s,\omega\otimes\chi)=G_z(1-LM_z)+F_z(1-LM_z)-L'M_z.$$

together with the formula

$$\psi_k(x,\omega\otimes\chi)=\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}-\frac{L'}{L}(s,\omega\otimes\chi)\frac{x^{s+k}}{s(s+1)\cdots(s+k)}\,ds,$$

valid for $c > 1$, yields

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}|\psi_k(x,\chi)|$$
$$\ll x\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}\int_{1+(\log x)^{-1}-i\infty}^{1+(\log x)^{-1}+i\infty}(|G_z|^2+|1-LM_z|^2)\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$+x^{1/2}\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}\int_{1/2-i\infty}^{1/2+i\infty}(1+|F_z|^2+|M_z|^2+|F_zM_z|^2+|L|^2+|L'|^2)$$
$$\times\frac{|ds|}{|s||s+1|\cdots|s+k|},$$

where the line of integration of the second integral has been moved to 1/2.

The Large Sieve inequality in a form due to Gallagher [9] gives good estimates of most of these terms.

Large Sieve Inequality. *If* $\sum_n |A_n|^2 < +\infty$, *then*

$$\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}\int_{-T}^{T}\left|\sum_{m=1}^{\infty}A_m\chi(m)m^{it}\right|^2 dt \ll \sum_{m=1}^{\infty}|A_m|^2(m+Q^2T).$$

Since $|c_j| \le n$, the Large Sieve Inequality implies

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{c-i}^{c+i}|G_z|^2\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll\sum_{j>z}\frac{\Lambda^2(j)|c_j|^2}{j^{2c}}(j+Q^2)$$
$$\ll(\log x)^3(1+\frac{Q^2}{z})$$

and

$$\sum_{Q_1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{c-(j+1)i}^{c-ji}+\int_{c+ji}^{c+(j+1)i}|G_z|^2\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll\frac{1}{j^{k+1}}\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{c-(j+1)i}^{c+(j+1)i}|G_z|^2\,|ds|$$
$$\ll\frac{1}{j^k}(\log x)^3(1+\frac{Q^2}{z}).$$

For $k\ge 2$ summing this inequality over j gives the estimate

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{c-i\infty}^{c+i\infty}|G_z|^2\frac{|ds|}{|s||s+1|\cdots|s+k|}\ll(\log x)^3(1+\frac{Q^2}{z}).$$

Observe that

$$1-LM_z=-\sum_{j>z}\sum_{\substack{e|j\\e>z}}b_e a_{j/e}\frac{\chi(j)}{j^s}.$$

Since $|a_j|\le\tau_n(j)$ and $b_j\le 2^{np(j)}$,

$$|\sum_{\substack{e|j\\e>z}}b_e a_{j/e}|\le\tau_{n+1}(j)2^{np(j)},$$

where $\tau_{n+1}(j)$ is the number of distinct ways of writing j as the product of $n+1$ integers. The Large Sieve Inequality gives

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{1+(\log x)^{-1}-i\infty}^{1+(\log x)^{-1}+i\infty}|1-LM_z|^2\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll\frac{\tau_{n+1}^2(j)4^{np(j)}}{j^{2c}}(j+Q^2)$$
$$\ll(\log x)^{(n+1)^2 4^n}(1+\frac{Q^2}{z}).$$

Since $|c_j| \le n$,

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}(1+|F_z|^2+|M_z|^2+|F_zM_z|^2)\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll \sum_{j\le z^2}\frac{4^{np(j)}}{j}(j+Q^2)$$
$$\ll (Q^2+z^2)(\log z)^{4^n}.$$

The direct estimate of

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}(|L|^2+|L'|^2)\frac{|ds|}{|s||s+1|\cdots|s+k|}$$

using the Large Sieve inequality is unsatisfactory. However, the Mellin transform

$$e^{-j/U}=\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\Gamma(w)U^w j^{-w}\,dw,$$

provides the relation

$$\sum_{j=1}^{\infty}a_j\chi(j)e^{-j/U}j^{-s}=\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}L(s+w,\omega\otimes\chi)\Gamma(w)U^w\,dw.$$

Moving the line of integration to $c_1=-1/2-1/\log V$ yields

(11)
$$L(s,\omega\otimes\chi)=\sum_{j=1}^{\infty}a_je^{-j/U}j^{-s}-\frac{1}{2\pi i}\int_{c_1-i\infty}^{c_1+i\infty}L(s+w,\omega\otimes\chi)U^w\Gamma(w)\,dw,$$

where the $L(s,\omega\otimes\chi)$ comes from the pole of $\Gamma(w)$ at $w=0$. By the functional equation,

$$L(s+w,\omega\otimes\chi)=G(s+w,\omega\otimes\chi)L(s+w-1,\omega\otimes\chi)$$
$$=G(s+w,\omega\otimes\chi)\sum_{j=1}^{\infty}\tilde{a}_j\bar{\chi}(j)j^{s+w-1},$$

for $\mathrm{Re}(s+w)<0$. Substituting this relation into the integral gives

$$\begin{aligned} L(s,\omega\otimes\chi) &= \sum_{j=1}^{\infty} a_j\chi(j)e^{-j/U}j^{-s} \\ &\quad - \frac{1}{2\pi i}\int_{c_1-i\infty}^{c_1+i\infty} G(s+w,\omega\otimes\chi)\sum_{j>U}\bar{a}_j\bar{\chi}(j)j^{s+w-1}U^w\Gamma(w)\,dw \\ &\quad - \frac{1}{2\pi i}\int_{c_1-i\infty}^{c_1+i\infty} G(s+w,\omega\otimes\chi)\sum_{j\le U}a_j\chi(j)j^{s+w-1}U^w\Gamma(w)\,dw. \end{aligned} \tag{12}$$

Stirling's inequality implies that

$$G(s,\omega\otimes\chi)\ll(A(\omega\otimes\chi)(|t|+2)^d)^{\frac{1}{2}-\sigma}.$$

If the line of integration of the second integral is moved to $-1/\log V$, then by Cauchy's inequality

$$\begin{aligned} \int_{-T}^{T}|L(\tfrac{1}{2}+it,\omega\otimes\chi)|^2\,dt &\ll \int_{-T}^{T}\Big|\sum_{j=1}^{\infty}a_j\chi(j)e^{-j/U}j^{-\frac{1}{2}+it}\Big|^2\,dt \\ &+\left(\frac{A(\omega\otimes\chi)T^n}{U}\right)^{-2c_1}\int_{-\infty}^{+\infty}\int_{-T}^{T}\left|\sum_{j>U}\bar{a}_j\bar{\chi}(j)j^{-1-1/\log V+i(y+t)}\right|^2 \\ &\qquad\qquad \times\Gamma^2(c_1+iy)\,dt\,dy \\ &+\left(\frac{A(\omega\otimes\chi)T^n}{U}\right)^{2c_2}\int_{-\infty}^{+\infty}\int_{-T}^{T}\left|\sum_{j\le U}\bar{a}_j\bar{\chi}(j)j^{-1/2-1/\log V+i(y+t)}\right|^2 \\ &\qquad\qquad \times\Gamma^2(c_2+iy)\,dt\,dy. \end{aligned}$$

Using this formula, write

$$\sum_{1<q\le Q}\sideset{}{^*}\sum_{\chi}\int_{-T}^{T}|L(\tfrac{1}{2}+it,\chi)|^2\,dt=\Sigma_1+\Sigma_2+\Sigma_3.$$

The Large Sieve Inequality with $U = V = (Q^n T^n)^{\frac{1}{2}}$ implies

$$\begin{aligned}
\Sigma_1 &\ll \sum_{j=1}^{\infty} |a_j|^2 e^{-2j/U} j^{-1} (j + Q^2 T) \\
&\ll (U + Q^2 T)(\log U)^{n^2}. \\
\Sigma_2 &\ll (Q^n T^n)^{\frac{1}{2}} (\sum_{j>U} \frac{|a_j|^2}{j^{2+2/\log V}} (j + Q^2 T)) \\
&\ll U(1 + \frac{Q^2 T}{U})(\log U)^{n^2} = (U + Q^2 T)(\log U)^{n^2}, \\
\Sigma_3 &\ll \sum_{j \le U} |a_j|^2 j^{-1-2/\log V} (j + Q^2 T) \\
&\ll (U + Q^2 T)(\log U)^{n^2}.
\end{aligned}$$

These estimates together show

$$\sum_{q \le Q} \sideset{}{^*}\sum_{\chi} \int_{-T}^{T} |L(\tfrac{1}{2} + it, \chi)|^2 \, dt \ll (A^{1/2} Q^{n/2} T^{n/2} + Q^2 T)(\log AQT)^{n^2},$$

so that

$$\begin{aligned}
&\sum_{q \le Q} \sideset{}{^*}\sum_{\chi} \int_{-T}^{T} |L(\tfrac{1}{2} + it, \chi)|^2 \, dt \\
&\quad \ll \sum_{\tau=1}^{T} \sum_{q \le Q} \sideset{}{^*}\sum_{\chi} \int_{-\tau}^{\tau} |L(\tfrac{1}{2} + it, \chi)|^2 \frac{dt}{|\frac{1}{2} + it|^{k+1}} \\
&\quad \ll (A^{1/2} Q^{n/2} + Q^2)(\log AQ)^{n^2},
\end{aligned}$$

for $k \ge n/2 + 2$. By the Large Sieve Inequality,

$$\begin{aligned}
\int_T^{\infty} \left|L(\tfrac{1}{2} + it, \omega \otimes \chi)\right|^2 \, dt &\ll \int_T^{\infty} (q^n t^n)^{\frac{1}{2}} (\log qt)^{2n} \frac{dt}{t^{k+1}} \\
&\ll \frac{q^{n/2} \log^{2n}(qT)}{T^{k-n/2}}.
\end{aligned}$$

Therefore,

$$\sum_{1<q\le Q}\sum_{\chi}^{*}\int_{T}^{\infty}+\int_{-T}^{-\infty}\left|L(\tfrac{1}{2}+it)\right|^{2}\frac{dt}{|t|^{k+1}}$$
$$\ll \frac{1}{T^{k-n/2}}\sum_{q\le Q}\phi(q)q^{n/2}\log^{2n}(qT)$$
$$\ll \frac{Q^{n/2+2}\log^{2n}(QT)}{T^{k-n/2}}.$$

Hence,

$$\sum_{1<q\le Q}\sum_{\chi}^{*}\int_{c_1-i\infty}^{c_1+i\infty}|L(s,\omega\otimes\chi)|^{2}\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll (A^{1/2}Q^{n/2}+Q^{2})(\log Q)^{n^2}+\frac{Q^{n/2+2}\log^{2n}(QT)}{T^{k-n/2}}$$
$$\ll (A^{1/2}Q^{n/2}+Q^{2})(\log Q)^{n^2}, \tag{13}$$

choosing $T=Q$ and $k=n$.

A similar approach can be used to estimate the term involving L'. Differentiate (12) to obtain

$$L'(s,\omega\otimes\chi)=-\sum_{j=1}^{\infty}a_j\chi(j)\log j e^{-j/U}j^{-s}$$
$$+\frac{1}{2\pi i}\int_{c_1-i\infty}^{c_1+i\infty}G(s+w,\omega\oslash\chi)L'(1-s-w,\overline{\omega\oslash\chi})U^{w}\Gamma(w)\,dw$$
$$-\frac{1}{2\pi i}\int_{c_1-i\infty}^{c_1+i\infty}G'(s+w,\chi)L(1-s-w,\bar{\chi})U^{w}\Gamma(w)\,dw \tag{14}$$

The same argument as above except that (14) is used instead of (11) and (10) instead of (9) shows that

$$\sum_{1<q\le Q}\sum_{\chi}^{*}\int_{c_1-i\infty}^{c_1+i\infty}|L'(s,\omega\oslash\chi)|^{2}\frac{|ds|}{|s||s+1|\cdots|s+k|}$$
$$\ll (A^{1/2}Q^{n/2}+Q^{2})\log^{n(n+2)}Q, \tag{15}$$

Combining the results of (13) and (15) yields

$$\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}|\psi_k(x,\omega\oslash\chi)| \ll x(\log x)^{(n+1)^2 2^{2n}}(1+\frac{Q^2}{z})$$
$$+x^{1/2}(Q^2+z^2)(\log z)^{17}+x^{1/2}(\log Q)^{n(n+2)}(Q^2+Q^{n/2}),$$

where the implied constant depends on the field K. Choose $z=Q(\log x)^M$ with $M>(n+1)^2 2^{2n}+D$, then for

$$(\log x)^M \le Q \le \min(x^{1/2}(\log x)^{-(2M+17+D)}, x^{1/2-\epsilon}, x^{\frac{1}{d-2}-\epsilon}),$$

comes the estimate

$$\frac{1}{Q}\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}|\psi_n(x,\omega\otimes\chi)| \ll x^{n+1}(\log x)^{-D}.$$

From the previous chapter,

$$\psi_n(x,\omega\otimes\chi) \ll \frac{x^{\beta_0+n}}{\beta_0(\beta_0+1)\cdots(\beta_0+n)}$$
$$+\frac{x^{n+1}\log x}{T^{n+1}}(\log A(\omega\otimes\chi)+n_K\log T)$$
$$+x^n\log x(\log A(\omega\otimes\chi)+n_K\log T).$$

Choose

$$T=\exp(n^{-1/2}(\log x)^{1/2}-n^{-1}\log A(\omega\otimes\chi)).$$

Lemma 3.8 of [29] estimates the term coming from the possible exceptional zero β_0 of $L(s,\omega\otimes\chi)$. Since $A(\omega\otimes\chi)\ll q^n$, where the implied constant depends only on the field K,

$$\psi_n(x,\omega\otimes\chi) \ll n(\log q)x^{n+1}\exp(-c(\log x)^{1/2})),$$

for some absolute constant c. Hence, for $Q \le (\log x)^M$,

$$\frac{1}{Q}\sum_{q\le Q}\sideset{}{^*}\sum_{\chi}|\psi_n(x,\omega\otimes\chi)| \ll x^{n+1}(\log x)^M \exp(-c(\log x)^{1/2})$$
$$\ll x^{n+1}(\log x)^{-D},$$

for any positive real number D. The final observation is that

$$\sum_{q\le Q}{}' \max_{(a,q)=1}\max_{y\le x}|\psi_m(y,\xi(C,q,a)) - \delta(C,a,q)\frac{y^{m+1}}{(m+1)!}| \ll \frac{x^{m+1}}{\log^A x}$$

implies

$$\sum_{q\le Q}{}' \max_{(a,q)=1}\max_{y\le x}|\psi_{m-1}(y,\xi(C,q,a)) - \delta(C,a,q)\frac{y^{m}}{m!}| \ll \frac{x^{m}}{\log^A x}.$$

To see this, let

$$\psi_m(x,\xi(C,q,a)) = \delta(C,a,q)\frac{y^{m+1}}{(m+1)!} + r_m(x,\xi(C,q,a)).$$

From the relations

$$\psi_m(x,\xi(C,q,a)) = \int_2^x \psi_{m-1}(y,\xi(C,q,a))\,dy,$$

$$\frac{1}{\lambda}\int_{x-\lambda}^{x}\psi_{m-1}(y,\xi(C,q,a))\,dy \le \psi_{m-1}(x,\xi(C,q,a))$$
$$\le \frac{1}{\lambda}\int_{x}^{x+\lambda}\psi_{m-1}(y,\xi(C,q,a))\,dy$$

it follows that,

$$\psi_{m-1}(x,\xi(C,q,a)) = \delta(C,a,q)\frac{x^m}{m!} + r_{m-1}(x,\xi(C,q,a))$$
$$= \frac{1}{\lambda}\left(\delta(C,a,q)\frac{\lambda x^m}{m!} + O(\lambda^2 x^{m-1}) + O(\max_{y\le x+\lambda}(r_m(y,\xi(C,q,a))))\right).$$

This implies

$$\max_{y\le x}\left(r_{m-1}(y,\xi(C,q,a))\right) \ll \delta(C,a,q)\lambda x^{m-1} + \frac{1}{\lambda}\max_{y\le x+\lambda}\left(r_m(y,\xi(C,q,a))\right).$$

Now choosing $\lambda = x(\log x)^{-\frac{1}{2}(A+1)}$, with Q as above, yields

$$\begin{aligned}
&\sum_{q\le Q}{}' \max_{y\le x}\max_{(a,q)=1}|r_{m-1}(y,\xi(C,q,a))| \\
&\qquad \ll \lambda x^{m-1}\log x + \frac{1}{\lambda}\sum_{q\le Q}\max_{y\le x+\lambda}\max_{(a,q)=1}|r_m(y,\xi(C,q,a))| \\
&\qquad \ll x^m(\log x)^{-\frac{1}{2}(A-1)}.
\end{aligned}$$

Using a decreasing induction on j starting with $j = n$ completes the proof of the theorem.

CHAPTER 3
THE EUCLIDEAN ALGORITHM IN TOTALLY REAL QUARTIC FIELDS

Sieve Lemmas

Let $\mathcal{A}$ be a finite sequence of integers, $\mathcal{P}$ a sequence of rational primes, z a real number greater than 2, and

$$P(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} p.$$

then

$$S(\mathcal{A},\mathcal{P},z) = |\{a \in \mathcal{A} :\ (a, P(z)) = 1\}|$$

is the number of elements of $\mathcal{A}$ whose prime factors which belong to $\mathcal{P}$ are all greater than z. The goal of sieve theory is to find upper and lower estimates for $S(\mathcal{A},\mathcal{P},z)$.

A simple example of a sieve is $\mathcal{B} = \{1 < n \leq x\}$, $\mathcal{P}$ the sequence of primes less than $\sqrt{x}$, and $z = \sqrt{x}$, then $S(\mathcal{B},\mathcal{P},z)$ is the number of primes between $\sqrt{x}$ and x. For the application to Euclidean domains the sequence

$$\mathcal{C} = \{p-1 :\ (p, E/\mathbb{Q}) \subset C\},$$

needs to be investigated with $\mathcal{P}_d = \{p \nmid d(E/\mathbb{Q}, C)\}$, where $(p, E/\mathbb{Q})$ is the Frobenius symbol and $d(E/\mathbb{Q}, C)$ is the largest integer such that $\mathbb{Q}(\zeta_d) \subset E$ and $\sigma|_{\mathbb{Q}(\zeta_d)} = 1$, for all $\sigma \in C$.

For d a square-free integer define

$$\mathcal{A}_d = \{a \in \mathcal{A} : \ a \equiv 0 (\text{mod } d)\}.$$

Let X be an approximation to $|\mathcal{A}|$, the number of elements in $\mathcal{A}$. For each prime $p \in \mathcal{P}$ choose $\omega(p)$ such that $(\omega(p)/p)X$ is a good approximation to $\mathcal{A}_p$, and set $\omega(1) = 1$. For square-free integers composed only of primes in $\mathcal{P}$, define

$$\omega(d) = \prod_{p|d} \omega(p),$$

and for other square-free integers set $\omega(d) = 0$. The numbers

$$R_d = |\mathcal{A}_d| - \frac{\omega(d)}{d} X,$$

give the error of the approximation. Let

$$W(z) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right).$$

For $\mathcal{B}$, the obvious choices are $X = x$ and $\omega(p) = 1$. The Čebotarev density theorem suggests that good choices for $\mathcal{C}$ are

$$X = \frac{|C|}{|G|} \ell i(x)$$

and $\omega(p) = p/(p-1)$ for $p \in \mathcal{P}_d$. With these choices,

$$|R_d| \leq R_C(x,d) = \max_{y \leq x} \max_{(a,d)=1} |\pi_C(y,d,a) - \frac{|C|}{|G|\phi(d)} \ell i(y)|.$$

The reason for proving the theorem in Chapter 2 was to provide estimates for the remainder terms $R_C(x,d)$. The appropriate form of that theorem for estimating this sequence is stated below. Let $\nu(n)$ be the number of distinct prime divisors of n.

Lemma 1. *Given any positive constant B there exists a positive number A such that*

$$\sum_{q \le x^{1/\eta}/(\log x)^A} \mu^2(q) 3^{\nu(q)} R_C(x,q) \ll \frac{x}{(\log x)^B},$$

where η is defined as in the theorem in chapter 2, and where the implied constant depends on the field K and on the constant B.

Proof. Since $R_C(x,d) \ll x/d$, for $x \ge d$, Cauchy's inequality implies

$$\begin{aligned}
&\sum_{d \le x^{1/\eta}/\log^A x} \mu^2(d) 3^{\nu(d)} R_C(x,d) \\
&\qquad \ll x^{1/2} \left(\sum_{d \le x^{1/\eta}/\log^A x} \frac{\mu^2(d) 3^{\nu(d)}}{d^{1/2}} R_C^{1/2}(x,d) \right) \\
&\qquad \ll x^{1/2} \left(\sum_{d < x^{1/2}} \frac{\mu^2(d) 9^{\nu(d)}}{d} \right)^{1/2} \left(\sum_{d < x^{1/\eta}/\log^A x} R_C(x,d) \right)^{1/2}.
\end{aligned}$$

The estimate

$$\begin{aligned}
\sum_{d<x} \frac{\mu^2(d) 9^{\nu(d)}}{d} &= \sum_{d_1 \cdots d_9 < x} \frac{\mu^2(d_1 \cdots d_9)}{d_1 \cdots d_9} \\
&\le \left(\sum_{n<x} \frac{1}{n} \right)^9 \le (\log x + 1)^9,
\end{aligned}$$

and the theorem of the previous chapter imply the result.

In the next section, the proof of the theorem will require the existence of many primes p such that if $\ell | p-1$, ℓ a prime not equal to 2, then ℓ is large. The linear sieve shows that many such primes exist.

Lemma 2. *Assume that*

$$0 \le \frac{\omega(p)}{p} \le 1 - \frac{1}{A_1}$$
$$-L \le \sum_{w \le p < z} \frac{\omega(p)\log p}{p} - \kappa \log \frac{z}{w} \le A_2$$

then for $\xi \ge z$ there is the lower bound

$$S(\mathcal{A}, \mathcal{P}, z) \ge XW(z)\left\{ f\left(\frac{\log \xi^2}{\log z}\right) - B\frac{L}{(\log \xi)^{1/3}}\right\} - \sum_{\substack{n < \xi^2 \\ n | P(z)}} 3^{\nu(n)}|R_n|.$$

$$S(\mathcal{A}, \mathcal{P}, z) \le XW(z)\left\{ F\left(\frac{\log \xi^2}{\log z}\right) + B\frac{L}{(\log \xi)^{1/3}}\right\} + \sum_{\substack{n < \xi^2 \\ n | P(z)}} 3^{\nu(n)}|R_n|.$$

This lemma is proved in Iwaniec [19]. The function f is defined by

$$f(u) = \frac{2e^{\gamma}}{u}\log(u-1),$$

for $2 \le u \le 4$. The function F is defined by

$$F(u) = \frac{2e^{\gamma}}{u},$$

for $0 \le u \le 3$.

Lemma 3. *There are more than*

$$\delta_1 x/(\log x)^{2+1/4}$$

rational primes p such that

(1) $p \le x$,

(2) $(p, E/\mathbb{Q}) \subseteq C$,

(3) *If $\ell \mid (p-1)$, then $\ell \mid d(E/\mathbb{Q})$ or $\ell > x^{1/2\eta}\exp\left(-(\log x)^{1/4}\right)$,*

where $\delta_1 > 0$, $d = d(E/\mathbb{Q})$ *is the largest integer such that* $\mathbb{Q}(d) \subseteq E$ *and* $\eta = \max(d' - 2, 2)$, *with*

$$d' = \min_{M} \max_{\omega} [G : H]\omega(1),$$

and the min *is taken over subfields* M *of* K *such that* $L(s, \omega \otimes \chi, K(\zeta)/M)$ *are holomorphic for all characters* χ *and the* max *is over characters of* $H = \mathrm{Gal}(K/M)$.

Proof. Consider the sequence $\mathcal{C}$ with $\mathcal{P} = \mathcal{P}_d$. To apply Lemma 2, the two conditions must be checked. The first condition is trivial since $2 \mid d(E/\mathbb{Q}, C)$ and $0 \leq 1/(p-1) \leq 1/2$ for $p \geq 3$. Since $\psi(x) \sim x$, partial summation implies that

$$\sum_{w \leq p < z} \frac{\log p}{p-1} = \log \frac{z}{w} + O(1),$$

which implies the second condition for $\kappa = 1$ since only finitely many primes divide $d(E/\mathbb{Q}, C)$. By Lemma 1,

$$\sum_{\substack{n < x^{1/\eta}/(\log x)^B \\ n \mid P(z)}} 3^{\nu(n)} |R_n| \ll x/(\log x)^4,$$

for some constant $B \geq 1$. Choose $z = x^{1/2\eta} \exp(-(\log x)^{3/4})$ and $\xi^2 = x^{1/\eta}/(\log x)^B$. Apply Lemma 2 to obtain

$$S(\mathcal{A}^3, \mathcal{P}_d, z) \geq XW(z) \left\{ f\left(\frac{\log \xi^2}{\log z}\right) - B_1 \frac{L}{(\log \xi)^{1/3}} \right\} - O\left(\frac{x}{(\log x)^4}\right).$$

Recall the construction of the fastest algorithm in the Introduction. Suppose that every prime of R is contained in E_2. Consider a residue class $a + Rb = a'(a'' + b''R)$, where $a'' + b''R$ is a coprime residue class of R/Rb''. If b'' is not in E_2, then $a'' + Rb''$ contains an element of E_2 by an extension to algebraic number fields of Dirichlet's Theorem on primes in arithmetic progressions and if b'' is in E_2, then $a'' + Rb''$ contains an element of E_1. So by induction on $n_1 + n_2$ the construction of the fastest algorithm will reach all elements of R, where n_1 is the number of prime divisors of b in E_1 and n_2 is the number in E_2.

The key fact to be proved is that every prime ideal $\mathfrak{p}$ of K is contained in E_2. Consider the ray class field of K with modulus $\mathfrak{p}$. The ray class field F is the maximal abelian extension of K with the conductor of F/K dividing $R\mathfrak{p}$, with the infinite primes remaining unramified, and with

$$\text{Gal}(F/K) \cong (R/R\mathfrak{p})^* / \psi_{\mathfrak{p}}(U), \tag{16}$$

where U is the unit group of R and $\psi_{\mathfrak{p}}$ is reduction modulo $\mathfrak{p}$. This reduces the proof of the claim to showing that for every residue class $a + R\mathfrak{p}$ there is a prime $\mathfrak{q}$ of R such that the Frobenius symbol $(\mathfrak{q}, F/K)$ is mapped onto $(a + R\mathfrak{p})\psi_{\mathfrak{p}}(U)$ under the isomorphism (16) and such that $\psi_{\mathfrak{q}}$ maps U onto $(R/R\mathfrak{q})^*$.

Intended Theorem. *Let K be a totally real Galois extension of $\mathbb{Q}$ of degree four whose ring of integers R is a principal ideal domain, then R is*

Euclidean.

Let $\mathfrak{p}$ be a prime of K and F the ray class field of modulus $\mathfrak{p}$. F is also totally real since the infinite primes of K do not ramify in F. Let ω_1, ω_2, ω_3 be a system of positive fundamental units of K. Consider

$$L = K(\sqrt{\omega_1}, \sqrt{\omega_2}, \sqrt{\omega_3}),$$

$L_1 = F \cdot L$, and L_2 the smallest field containing L_1 which is Galois over $\mathbb{Q}$. Now, L, L_1, and L_2 are not necessarily totally real because ω_1, ω_2, ω_3 need not be totally positive. $\mathrm{Gal}(L_1/K)$ is abelian since it is a subgroup of $\mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$. L_2 is the compositum of all the embeddings, $\sigma_1 L_1, \ldots, \sigma_m L_1$, of L_1 into the real numbers. Let τ be an element of $\mathrm{Gal}(L_2/K)$. Since L_1 is Galois over K, τ maps L_1 to L_1 and since K is Galois over $\mathbb{Q}$, τ maps each $\sigma_i L_1$ to itself. Since each $\sigma_i L_1$ is abelian over K, the compositum is also abelian over K.

Let $C = \{\sigma\}$ be the conjugacy class of $\mathrm{Gal}(F/K)$ corresponding to $(a + R\mathfrak{p})\psi_{\mathfrak{p}}(U)$ and

$$C_1 = \{\tau \in \mathrm{Gal}(L_1/K) : \ \tau|_F = C, \ \tau|_L \neq 1\}.$$

It is not obvious that C_1 is nonempty. If C_1 were empty, then

$$L \subseteq F^\sigma = \{x \in F : \ \sigma(x) = x\}.$$

L/K ramifies only at the primes dividing 2, so only these primes need to be considered. In this case the characteristic of $R/R\mathfrak{p}$ is 2 so

$$|(R/R\mathfrak{p})^*| = 2^m - 1.$$

Since $[L : K]$ divides $[F : K]$, $[F : K]$ divides $|(R/R\mathfrak{p})^*|$, and 2 is the only prime dividing $[L : K]$, a contradiction results. Therefore, C_1 is nonempty and $L \cap F = K$.

Let C_2 be the inverse image of C_1 in $\mathrm{Gal}(L_2/K)$, and C_3 the smallest subset of $\mathrm{Gal}(L_2/\mathbb{Q})$ closed under conjugation. Since L_2 need not be totally real, there might be additional roots of unity in L_2. However, the only roots of unity ζ_d in L_2 such that

$$\sigma'|_{\mathbb{Q}(\zeta_d)} = 1 \tag{17}$$

for all $\sigma' \in C_3$ are ± 1. The first claim is that the only roots of unity in L_1 satisfying (17) are ± 1. Let $H = \mathrm{Gal}(L_1/F)$ and $H_2 = \mathrm{Gal}(L_1/L)$. Suppose there is an integer d greater than 2 such that $\zeta_d \in L_1$ and such that the condition (17) is satisfied for all $\sigma' \in C_1$. Let $J = \mathrm{Gal}(L_1/K(\zeta_d))$. For any $\tau \in C_1$,

$$\tau H \setminus (\tau H \cap H_2) \subseteq C_1 \subseteq J \cap \tau H.$$

Therefore,

$$|H| - |H \cap H_2| \leq |J \cap \tau H| \leq \frac{1}{2}|H|,$$

since $[K(\zeta_d) : K] \geq 2$. This implies $H \cap H_2| \geq \frac{1}{2}|H|$. Note that

$$H \cap H_2 = H/\mathrm{Gal}(L/L \cap F) = H/\mathrm{Gal}(L/K).$$

This yields a contradiction since $|H \cap H_2| = 1$ and $|H| = 8$. Therefore, the first claim is proved. Suppose there is some integer d greater than two satisfying (17) for all $\sigma' \in C_2$. Then a prime $\mathfrak{q}$ of K can be found which does

not split completely in $K(\zeta_d)$ such that $(\mathfrak{q}, L_1/K) \in C_1$. But this condition is equivalent to $(\mathfrak{q}, L_2/K) \in C_2$, which contradicts the assumption that d satisfies (17) for all $\sigma' \in C_2$. Clearly, from the definition, the only roots of unity in L_2 satisfying (17) for all $\sigma' \in C_3$ are ± 1.

Lemma 4. *There are more than $\delta_2 x/(\log x)^{2+1/4}$ primes $\mathfrak{p}$ of K such that*

(1) $N_{K/\mathbb{Q}}\mathfrak{p} = p \leq x$, *$p$ a rational prime,*

(2) $(\mathfrak{p}, F/K) = C$,

(3) $(\mathfrak{p}, L/K) \neq 1$,

(4) *If $q|p-1$, q a rational prime, then $q = 2$ or*

$$q > x^{1/4} \exp\left(-(\log x)^{1/3}\right),$$

for some positive constant δ_2.

Proof. Let p be a rational prime which is unramified in L_2 with $(p, L_2/\mathbb{Q}) \subseteq C_3$. If $\mathfrak{P}|p$ be a prime in L_2, then for some η in $\mathrm{Gal}(L_2/\mathbb{Q})$, $(\eta\mathfrak{P}\eta^{-1}, L_2/\mathbb{Q})$ is in C_2. Let $\mathfrak{p}$ be the prime of K lying below $\eta\mathfrak{P}\eta^{-1}$, then $N_{K/\mathbb{Q}}\mathfrak{p} = p$ and $(\mathfrak{p}, L/K) \subseteq C_1$. By Lemma 2 there are more than $\delta_2 x/(\log x)^{2+1/4}$ primes $p \leq x$ with $(p, L_2/\mathbb{Q}) \subseteq C_3$ such that if $q|(p-1)$ and $q \neq 2$ then $q > x^{1/4} \exp\left(-(\log x)^{1/3}\right)$.

Lemma 5. *The number of primes $\mathfrak{p}$ of K with $|\psi_{\mathfrak{p}}(U)| < y$ is $O(y^{4/3})$.*

Proof. The number of integer triples (a_1, a_2, a_3) with

$$|a_1| + |a_2| + |a_3| \leq y^{1/3} \tag{18}$$

is less than $\frac{4}{3}y$. If $|\psi_{\mathfrak{p}}(U)| \leq y$, then

$$\omega_1^{a_1}\omega_2^{a_2}\omega_3^{a_3} \equiv \omega_1^{b_1}\omega_2^{b_2}\omega_3^{b_3} (\mathrm{mod}\ \mathfrak{p}),$$

for some pair of triples satisfying (18), implying that $\mathfrak{p}$ divides

$$\omega_1^{a_1-b_1}\omega_2^{a_2-b_2}\omega_3^{a_3-b_3} - 1.$$

The number of primes dividing this element is $O(y^{1/3})$. Thus the total number of primes $\mathfrak{p}$ such that $|\psi_{\mathfrak{p}}(U)| \leq y$ is $O(y^{4/3})$.

Consider the primes $\mathfrak{p}$ of K found in Lemma 3. For these primes either $|\psi_{\mathfrak{p}}(U)| < x^{3/4}/(\log x)^2$ or 2 is the only possible divisor of

$$|(R/R\mathfrak{p})^*/\psi_{\mathfrak{p}}(U)|.$$

By Lemma 4 the number of primes satisfying the first condition is

$$\ll \left(x^{3/4}\exp\left((\log x)^{1/3}\right)\right)^{4/3} = x\exp\left(4/3(\log x)^{1/3}\right).$$

This estimate is clearly worse than the trivial estimate. However, if Lemma 4 could be slightly improved, then the Intended Theorem could be proved.

Conjecture. *For some $\epsilon > 0$ and some $\delta_2 > 0$, there are more than $\delta_2 x/(\log x)^{8/3-\epsilon}$ primes $\mathfrak{p}$ of K such that*

(1) $N_{K/\mathbb{Q}}\mathfrak{p} = p \leq x$, *$p$ a rational prime,*

(2) $(\mathfrak{p}, F/K) = C$,

(3) $(\mathfrak{p}, L/K) \neq 1$,

(4) *If $q|(p-1)$, q a rational prime, then $q = 2$ or $q > x^{1/4}(\log x)^2$.*

Using the Conjecture, the number of primes satisfying the first condition is

$$\ll \left(x^{3/4}/(\log x)^2\right)^{4/3} = x/(\log x)^{8/3},$$

so that these primes can be disregarded. In the other case, 2 divides

$$|(R/R\mathfrak{p})^*/\psi_{\mathfrak{p}}(U)|.$$

This would imply that 2 splits completely in L, contradicting the fact that

$$(\mathfrak{p}, L/K) \neq 1.$$

This completes the conjectural argument for a proof of the Intended Theorem.

Remarks on the Hooley-Weinberger Conditional Proof

It may be possible to adapt the conditional proof of Hooley [18] and Weinberger [42] to give unconditional proofs of Artin's Primitive Root Conjecture and the extension of the Intended Theorem proved in this chapter to any algebraic number field.

The heuristics are simpler for Artin's conjecture. Let a be a square-free integer and p, q primes. Let $R(q,p)$ denote the condition that $q|(p-1)$ and a is a q^{th} power residue modulo p. Hooley defines

$$N_a(x) = |\{p \leq x : \ a \text{ is a primitive root mod } p\}|$$

$$N_a(x,\eta_1) = |\{p \leq x : \ R(q,p) \text{ does not hold for any } q \leq \eta_1\}|$$

$$M_a(x,\eta_1,\eta_2) = |\{p \leq x : \ R(q,p) \text{ holds for some } \eta_1 < q \leq \eta_2\}|$$

$$P_a(x,k) = |\{p \leq x : \ R(q,p) \text{ holds for every } q|k\}|,$$

where k is a square-free integer. Note that

$$N_a(x) \le N_a(x, \eta_1)$$

$$N_a(x) \ge N_a(x, \eta_1) - M_a(x, \eta_1, x-1)$$

$$M_a(x, \eta_1, x-1) \le M_a(x, \eta_1, \eta_2) + M_a(x, \eta_2, \eta_3) + M_a(x, \eta_3, x-1).$$

Choose $\eta_1 = \frac{1}{2}\log\log x$, $\eta_2 = x^{1/2}/\log^2 x$, $\eta_3 = x^{1/2}\log x$. Hooley shows that

$$M_a(x, \eta_2, \eta_3) = O\left(\frac{x\log\log x}{\log x}\right)$$

$$M_a(x, \eta_3, x-1) = O\left(\frac{x}{\log^2 x}\right).$$

Note that

$$N_a(x, \eta_1) = \sum_{\ell'} \mu(\ell') P_a(x, \ell'),$$

where the sum is over positive square-free integers with prime factors not exceeding η_1 and

$$M_a(x, \eta_1, \eta_2) \le \sum_{\eta_1 < q \le \eta_2} P_a(x, q).$$

Hooley also shows

$$n_{G_k} P_a(x, k) = \pi(x, G_k) + O(n_{G_k}\omega(k)) + O(n_{G_k} x^{1/2}),$$

where $\pi(x, G_k)$ is the number of prime ideals $\mathfrak{p}$ of $G_k = \mathbb{Q}(\sqrt[k]{a}, \sqrt[k]{-1})$ with $N\mathfrak{p} \le x$. By the Čebotarev Density Theorem for $k \le \log x$,

$$\pi(x, G_k) \gg \frac{x}{\log x}.$$

Thus,

$$N_a(x,\eta_1) \gg \frac{x}{\log x}\left(\sum_{\ell'}\frac{\mu(\ell')}{n_{G_{\ell'}}}\right) \gg \frac{x}{\log x}.$$

Let $Z_q = \mathbb{Q}(\sqrt[q]{-1})$, $F_q = (\sqrt[q]{a})$. Trivially,

$$\pi(x,F_q) \ll q\frac{x}{\log x}.$$

Lagarias, Montgomery, and Odlyzko [20] show that

$$\pi(x,F_q) \ll \frac{x}{\log x}$$

for $x > \exp(A(\log d_{F_q})(\log\log d_{F_q})(\log\log\log d_{F_q}))$. Assume the hypothesis

$$\pi(x,F_q) \ll \frac{q}{(\log\log q)^{1+\epsilon}}\frac{x}{\log x}, \tag{17}$$

for $x \geq q^2(\log q)^4$, then the Brun-Titchmarsh Theorem implies that

$$\pi(x,G_q) \ll \frac{q}{(\log\log q)^{1+\epsilon}}\frac{x}{\log x}.$$

Hence,

$$M_a(x,\eta_1,\eta_2) \leq \frac{x}{\log x}\sum_{\eta_1<q\leq\eta_2}\frac{1}{(q-1)(\log\log q)^{1+\epsilon}}.$$

By partial summation,

$$\sum_{\eta_1<q\leq\eta_2}\frac{1}{(q-1)(\log\log q)^{1+\epsilon}} \ll \frac{1}{(\log\log\log\log x)^{\epsilon}}.$$

Under the hypothesis (17), this implies that $N_a(x) \gg x/\log x$.

CHAPTER 4
TOTALLY REAL QUARTIC FIELDS WITH CLASS NUMBER ONE AND DISCRIMINANT LESS THAN ONE MILLION

A proof of the conjecture in the last chapter appears to be difficult. Reconsider the result of R. Gupta, K. Murty, and R. Murty [15]. They proved the following theorem.

Theorem. *Let K be a Galois extension of $\mathbb{Q}$ and let S be a collection of primes containing the infinite primes such that*

(1) $|S| \geq \max(5, 2[K:\mathbb{Q}] - 3)$,

(2) *K has a real embedding or $\zeta_g \in K$, where $g = gcd(N\mathfrak{p} - 1 : \mathfrak{p} \in S \setminus S_\infty)$,*

then R_S, the ring of S-integers is a Euclidean domain if and only if it is a principal ideal domain.

In this chapter, the theorem stated above will be used to show that a totally real quartic Galois extension K of the rational numbers whose ring of integer is a principal ideal domain is Euclidean, assuming the existence of a special prime in the field.

Recall the construction of the fastest algorithm. Previously we tried to show that all primes were in E_2. Actually much less is required.

Lemma 1. *Let R be a principal ideal domain, assume that for every prime $\mathfrak{p}$ there is an integer m such that $\mathfrak{p} \in E_m$, then R is a Euclidean domain.*

Proof. For any element b of R define

$$\mathrm{ht}^*(b) = \max_{(a,b)=1} \min_{\mathfrak{p} \equiv a (\mathrm{mod}\ b)} (m : \mathfrak{p} \in E_m) + 1.$$

For primes $\mathfrak{p}$ define

$$\mathrm{ht}(\mathfrak{p}) = \begin{cases} 1, & \text{if } \mathfrak{p} \in E_1, \\ \mathrm{ht}^*(\mathfrak{p}), & \text{otherwise.} \end{cases}$$

By induction on the number of prime divisors of b define

$$\mathrm{ht}(b) = \max \left(\mathrm{ht}^*(b), \max_{\substack{q_1 q_2 = b \\ (q_1),\ (q_2) \neq R}} \mathrm{ht}(q_1) + \mathrm{ht}(q_2) \right) + 1.$$

Every residue class of R/bR contains an element r with $\mathrm{ht}(r) < \mathrm{ht}(b)$ and elements with $\mathrm{ht}(b) = 1$ are in E_1 so that $b \in E_{\mathrm{ht}(b)}$. This proves that $\cup_{n \geq 0} E_n = R$. So R is Euclidean.

Lemma 2. *Let ϵ be a primitive root modulo $\mathfrak{p}^2$, with $N\mathfrak{p} = p$, a rational prime, then ϵ is a primitive root modulo $\mathfrak{p}^n$ for every n.*

Proof. Suppose that ϵ is a primitive root mod $\mathfrak{p}^n$. Suppose that

$$\epsilon^t \equiv 1 (\mathrm{mod}\ \mathfrak{p}^{n+1})$$

with t the smallest such positive exponent. Since

$$\epsilon^t \equiv 1 (\mathrm{mod}\ \mathfrak{p}),$$

$p-1$ divides t. Also t divides $p^n(p-1)$, so that $t = p^u(p-1)$ for some positive integer u. By assumption, ϵ is a primitive root modulo $\mathfrak{p}^n$ and $\mathfrak{p}^{n-1}$ so that

$$\epsilon^{p^{n-2}(p-1)} \equiv 1 (\mathrm{mod}\ \mathfrak{p}^{n-1}),$$

$$\epsilon^{p^{n-2}(p-1)} \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}^{n}),$$

so that

$$\epsilon^{p^{n-2}(p-1)} = 1 + b\mathfrak{p}^{n-1},$$

where $\mathfrak{p} \nmid b$. Hence,

$$\epsilon^{p^{n-1}(p-1)} = \left(1 + b\mathfrak{p}^{n-1}\right)^p \equiv 1 + b\mathfrak{p}^n (\mathrm{mod}\ \mathfrak{p}^{n+1}).$$

Thus ϵ is a primitive root mod $\mathfrak{p}^{n+1}$ and by induction ϵ is a primitive root mod $\mathfrak{p}^m$ for all positive integers m.

Suppose that a special prime $\mathfrak{p}$ can be found such that the unit group generates the coprime residue classes modulo $\mathfrak{p}^2$, then by Lemma 2 the unit group generates the coprime residue classes modulo $\mathfrak{p}^n$ for every positive integer n. Taking into account the residue classes are not coprime, then by induction $\mathfrak{p}^n$ is in E_n. The theorem of R. Gupta, K. Murty, and R. Murty quoted above can be applied with $S = \{\mathfrak{p}\} \cup S_\infty$. Since

$$R_S/\mathfrak{q}R_S = R/\mathfrak{q}R$$

for $\mathfrak{q} \notin S$, Lemma 1 implies that for any prime $\mathfrak{q}$ of the ring of integers R the residue classes modulo $\mathfrak{q}$ contain either 0, a unit, a power of $\mathfrak{p}$, or

a prime such that each of its residue classes contains either 0, a unit, or a power of $\mathfrak{p}$. Therefore, $\mathfrak{q}$ is in some E_m which implies that R is a Euclidean domain. This proves the following theorem.

Theorem. *Let K be a totally real quartic Galois extension of $\mathbb{Q}$. If the ring of integers R of K contains a prime ideal $\mathfrak{p}$ such that the unit group maps onto $(R/\mathfrak{p}^2)^*$, then R is a Euclidean domain if and only if it is a principal ideal domain*

Note that the argument given above could have been used in conjunction with a much worse average density estimate than the one given in chapter 2.

Buchmann, Ford, Pohst, and von Schmettow [2] [3] computed integral basis, discriminant, fundamental units, and class groups for all totally real quartic fields with discriminant less than one million. The following table contains a list of those fields with class number one which are Galois over the rationals. In each case, a prime $\mathfrak{p}$ can be found such that the unit group generates the coprime residue classes modulo $\mathfrak{p}^2$. In the following table the rational prime occuring under $\mathfrak{p}$ indicates that any linear prime of the field, lying above the rational prime, is a special prime.

A superscript g means that Godwin [11] showed that the field is Euclidean for the norm. A superscript c means that Cohn and Deutsch showed that the field is Euclidean for the norm. A superscript n means that the field is not Euclidean for the norm. For the Galois groups, $C4$ denotes the cyclic group of order 4, and $V4$ denotes the *Viergruppe*, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Some examples of the verification that a field is not Euclidean for the norm are given at the end of the chapter.

Table of Totally Real Quartic Fields

Discriminant	Generating Polynomial	Prime	Galois Group
1125^g	$x^4 - x^3 - 4x^2 + 4x + 1$	29	C4
1600^g	$x^4 - 6x^2 + 4$	31	V4
2000	$x^4 - 2x^3 - 6x^2 + 2x + 1$	19	C4
2048^c	$x^4 - 4x^2 + 2$	17	C4
2304^g	$x^4 - 4x^2 + 1$	23	V4
3600	$x^4 - 2x^3 - 7x^2 + 8x + 1$	11	V4
4225	$x^4 - 9x^2 + 4$	29	V4
4913	$x^4 - x^3 - 6x^2 + 1x + 1$	13	C4
6125	$x^4 - x^3 - 14x^2 - 6x + 1$	19	C4
7056	$x^4 - 5x^2 + 1$	37	V4
7225	$x^4 - 11x^2 + 9$	19	V4
8000	$x^4 - 2x^3 - 11x^2 + 2x + 11$	29	C4
10816	$x^4 - 2x^3 - 9x^2 + 10x - 1$	17	V4
11025	$x^4 - 13x^2 + 16$	41	V4
12544	$x^4 - 8x^2 + 9$	31	V4
14400	$x^4 - 22x^2 + 1$	19	V4
15125	$x^4 - x^3 - 19x^2 - 11x + 11$	19	C4
17424	$x^4 - 7x^2 + 4$	37	V4
18432	$x^4 - 12x^2 + 18$	7	C4
18496	$x^4 - 2x^3 - 11x^2 + 12x + 2$	47	V4
19600	$x^4 - 24x^2 + 4$	19	V4
19773	$x^4 - x^3 - 11x^2 - 9x + 3$	17	C4
24336	$x^4 - 2x^3 - 11x^2 + 12x - 3$	163	V4
27225	$x^4 - 2x^3 - 25x^2 + 26x + 4$	29	V4
28224	$x^4 - 10x^2 + 4$	5	V4
28224	$x^4 - 2x^3 - 13x^2 + 14x + 7$	17	V4
30976	$x^4 - 20x^2 + 1$	7	V4
34225	$x^4 - 21x^2 + 64$	11	V4
35152^n	$x^4 - 13x^2 + 13$	23	C4
41616	$x^4 - 2x^3 - 13x^2 + 14x - 2$	13	V4
42025	$x^4 - 23x^2 + 81$	31	V4
45125	$x^4 - x^3 - 29x^2 - 21x + 61$	11	C4
48400	$x^4 - 32x^2 + 36$	19	V4
48841	$x^4 - 15x^2 + 1$	43	V4
51984	$x^4 - 11x^2 + 16$	59	V4
53361	$x^4 - 27x^2 + 9$	17	V4
53824	$x^4 - 2x^3 - 17x^2 + 18x + 23$	23	V4
66125	$x^4 - x^3 - 34x^2 - 26x + 101$	19	C4
68921	$x^4 - x^3 - 15x^2 - 18x - 4$	23	C4
69696	$x^4 - 14x^2 + 16$	29	V4
69696	$x^4 - 2x^3 - 19x^2 + 20x + 34$	149	V4
70225	$x^4 - x^3 - 45x^2 + 122x + 44$	29	V4
74529	$x^4 - 17x^2 + 4$	17	V4
76176	$x^4 - 25x^2 + 1$	11	V4
78400	$x^4 - 38x^2 + 81$	11	V4
81225	$x^4 - 31x^2 + 169$	29	V4
87616	$x^4 - 2x^3 - 21x^2 + 22x + 47$	7	V4

Discriminant	Generating Polynomial	Prime	Galois Group
92416	$x^4 - 28x^2 + 25$	17	V4
93025	$x^4 - 33x^2 + 196$	19	V4
94864	$x^4 - 9x^2 + 1$	19	V4
97344	$x^4 - 2x^3 - 17x^2 + 18x + 3$	23	V4
100352	$x^4 - 32x^2 - 56x + 46$	23	C4
107653"	$x^4 - x^3 - 24x^2 - 22x + 29$	29	C4
119025	$x^4 - x^3 - 57x^2 + 158x + 124$	11	V4
120125	$x^4 - x^3 - 44x^2 - 36x + 211$	29	C4
121104	$x^4 - 2x^3 - 19x^2 + 20x + 13$	13	V4
127449	$x^4 - 19x^2 + 1$	43	V4
132496	$x^4 - 2x^3 - 19x^2 + 20x + 9$	29	V4
133225	$x^4 - x^3 - 60x^2 + 167x + 149$	19	V4
135424	$x^4 - 32x^2 + 49$	41	V4
138384	$x^4 - 29x^2 + 1$	11	V4
140608	$x^4 - 2x^3 - 31x^2 - 46x + 9$	23	C4
142129	$x^4 - 21x^2 + 16$	23	V4
144400	$x^4 - 48x^2 + 196$	31	V4
148225	$x^4 - 41x^2 + 324$	19	V4
159201	$x^4 - x^3 - 26x^2 + 63x - 21$	41	V4
166464	$x^4 - 2x^3 - 19x^2 + 20x - 2$	19	V4
179776	$x^4 - 2x^3 - 29x^2 + 30x + 119$	7	V4
184041	$x^4 - 23x^2 + 25$	17	V4
193600	$x^4 - 54x^2 + 289$	29	V4
197136	$x^4 - 2x^3 - 23x^2 24x 33$	11	V4
207936	$x^4 - 46x^2 + 16$	29	V4
207936	$x^4 - 2x^3 - 31x^2 + 32x + 142$	41	V4
211600	$x^4 - 56x^2 + 324$	11	V4
216225	$x^4 - x^3 - 75x^2 + 212x + 304$	11	V4
219501"	$x^4 - x^3 - 25x^2 + 67x - 35$	7	C4
226576	$x^4 - 2x^3 - 21x^2 + 22x + 2$	19	V4
231125	$x^4 - x^3 - 59x^2 - 51x + 451$	11	C4
231361	$x^4 - 25x^2 + 36$	53	V4
233289	$x^4 - x^3 - 31x^2 + 76x - 20$	17	V4
235225	$x^4 - 51x^2 + 529$	11	V4
238144	$x^4 - 2x^3 - 33x^2 + 34x + 167$	41	V4
242064	$x^4 - 2x^3 - 25x^2 + 26x + 46$	23	V4
243049	$x^4 - 23x^2 + 9$	13	V4
246016	$x^4 - 40x^2 + 121$	23	V4
247808	$x^4 - 48x^2 - 88x + 158$	23	C4
265837	$x^4 - x^3 - 37x^2 - 35x + 81$	43	C4
266256	$x^4 - 35x^2 + 16$	13	V4
276125	$x^4 - x^3 - 64x^2 - 56x + 551$	19	C4
283024	$x^4 - 13x^2 + 9$	31	V4
284089	$x^4 - 27x^2 + 49$	23	V4
297025	$x^4 - 57x^2 + 676$	29	V4
304704	$x^4 - 50x^2 + 4$	5	V4
304704	$x^4 - 2x^3 - 37x^2 + 38x + 223$	17	V4
314721	$x^4 - 25x^2 + 16$	67	V4
318096	$x^4 - 37x^2 + 25$	11	V4

Discriminant	Generating Polynomial	Prime	Galois Group
319225	$x^4 - 59x^2 + 729$	11	V4
327184	$x^4 - 48x^2 + 4$	43	V4
341056	$x^4 - 2x^3 - 39x^2 + 40x + 254$	23	V4
370881	$x^4 - 25x^2 + 4$	5	V4
379456	$x^4 - 18x^2 + 4$	13	V4
379456	$x^4 - 2x^3 - 41x^2 + 42x + 287$	17	V4
384400	$x^4 - 72x^2 + 676$	11	V4
389017	$x^4 - x^3 - 27x^2 + 41x + 2$	37	C4
390224"	$x^4 - 29x^2 + 29$	53	C4
393129	$x^4 - 45x^2 + 36$	29	V4
395641	$x^4 - 27x^2 + 25$	47	V4
404496	$x^4 - 2x^3 - 49x^2 + 50x - 11$	11	V4
414736	$x^4 - 15x^2 + 16$	19	V4
416025	$x^4 - 67x^2 + 961$	29	V4
423801	$x^4 - x^3 - 41x^2 + 102x - 12$	17	V4
435125	$x^4 - x^3 - 79x^2 - 71x + 911$	41	C4
442225	$x^4 - 69x^2 + 1024$	11	V4
455877"	$x^4 - x^3 - 69x^2 - 7x + 49$	11	C4
469225	$x^4 - 71x^2 + 1089$	19	V4
473344	$x^4 - 52x^2 + 289$	7	V4
484416	$x^4 - 2x^3 - 25x^2 + 26x - 5$	23	V4
497025	$x^4 - 73x^2 + 1156$	11	V4
501264	$x^4 - 31x^2 + 196$	11	V4
506944	$x^4 - 2x^3 - 47x^2 + 48x + 398$	17	V4
529984	$x^4 - 54x^2 + 1$	43	V4
535824	$x^4 - 2x^3 - 35x^2 + 36x + 141$	13	V4
549081	$x^4 - 2x^3 - 53x^2 + 54x - 12$	29	V4
553536	$x^4 - 34x^2 + 196$	19	V4
553536	$x^4 - 2x^3 - 49x^2 + 50x + 439$	7	V4
555025	$x^4 - 77x^2 + 1296$	19	V4
559504	$x^4 - 2x^3 - 29x^2 + 30x + 38$	19	V4
561125	$x^4 - x^3 - 89x^2 - 81x + 1201$	79	C4
565504	$x^4 - 48x^2 + 529$	17	V4
576081	$x^4 - x^3 - 44x^2 + 117x + 27$	17	V4
577600	$x^4 - 2x^3 - 77x^2 + 78x + 1331$	11	V4
602176	$x^4 - 2x^3 - 51x^2 + 52x + 482$	31	V4
630125	$x^4 - x^3 - 94x^2 - 86x + 1361$	131	C4
646416	$x^4 - 35x^2 + 256$	11	V4
648025	$x^4 - 83x^2 + 1521$	19	V4
652864	$x^4 - 2x^3 - 53x^2 + 54x + 527$	17	V4
659344	$x^4 - 2x^3 - 27x^2 + 28x - 7$	53	V4
698896	$x^4 - 15x^2 + 4$	5	V4
704969	$x^4 - x^3 - 33x^2 - 39x + 8$	11	C4
725904	$x^4 - 37x^2 + 289$	11	V4
739328	$x^4 - 80x^2 - 152x + 574$	17	C4
739600	$x^4 - 2x^3 - 87x^2 + 88x + 1721$	19	V4
741321	$x^4 - 31x^2 + 25$	37	V4
748225	$x^4 - 89x^2 + 1764$	29	V4
753424	$x^4 - 19x^2 + 36$	83	V4

Discriminant	Generating Polynomial	Prime	Galois Group
760384	$x^4 - 2x^3 - 57x^2 + 58x + 623$	7	V4
780125	$x^4 - x^3 - 104x^2 - 96x + 1711$	11	C4
783225	$x^4 - 91x^2 + 1849$	11	V4
788544	$x^4 - 2x^3 - 29x^2 + 30x + 3$	47	V4
793117"	$x^4 - x^3 - 76x^2 + 316x - 179$	103	C4
810448"	$x^4 - 37x^2 + 333$	11	C4
815409	$x^4 - x^3 - 77x^2 - 300x - 300$	67	V4
846400	$x^4 - 2x^3 - 93x^2 + 94x + 1979$	41	V4
861125	$x^4 - x^3 - 109x^2 - 101x + 1901$	19	C4
891136	$x^4 - 60x^2 + 841$	17	V4
900061	$x^4 - 43x^2 + 225$	23	V4
906304	$x^4 - 2x^3 - 35x^2 + 36x + 86$	43	V4
912673	$x^4 - x^3 - 36x^2 - 91x - 61$	43	C4
915849	$x^4 - 31x^2 + 1$	67	V4
931225	$x^4 - 99x^2 + 2209$	31	V4
938961	$x^4 - 37x^2 + 100$	43	V4
968256	$x^4 - 2x^3 - 31x^2 + 32x + 10$	5	V4
974169	$x^4 - x^3 - 82x^2 - 329x - 329$	37	V4
976144	$x^4 - 2x^3 - 43x^2 + 44x + 237$	17	V4
992016	$x^4 - 43x^2 + 400$	37	V4

The following two examples of totally real quartic Galois extensions K of $\mathbb{Q}$ with class number one are not Euclidean for the norm.

The first example is K, the splitting field of $x^4 - 18x^2 + 4$. K has an integral basis $\{1, \alpha, \alpha^2/2, \alpha^3/2\}$, where α is a root of the polynomial. The unit group of K is generated by

$$-9 + \alpha^2/2,\ 1 - 2\alpha - \alpha^2/2,\ 30 + 63\alpha - 3/2\alpha^2 - 7/2\alpha^3.$$

To determine the prime ideals of K, look at the factorizations of $x^4 - 18x^2 + 4$ modulo p for $p \leq 7$.

$$\begin{aligned} x^4 - 18x^2 + 4 &\equiv x^4 (\text{mod } 2) \\ &\equiv (x^2 + x + 2)(x^2 + 2x + 2)(\text{mod } 3) \\ &\equiv (x^2 + 3x + 3)(x^2 + 2x + 3)(\text{mod } 5) \\ &\equiv (x + 3)^2(x + 4)^2(\text{mod } 7) \end{aligned}$$

Using these factorizations, determine the image of the unit group modulo the prime ideal $(7, \alpha + 3)$.

$$-9 + \alpha^2/2 \equiv -2 + \alpha^2/2 + 7/2\alpha^2 \equiv -2 + 4\alpha^2 \equiv -2 + 2\alpha \equiv -1\ (7, \alpha + 3)$$

$$1 - 2\alpha - \alpha^2/2 \equiv 1 - 2\alpha + 3\alpha^2 \equiv 1 - 11\alpha \equiv 1 - 4\alpha \equiv -1\ (7, \alpha + 3)$$

$$30 + 63\alpha - 3/2\alpha^2 - 7/2\alpha^3 \equiv 2 - 3/2\alpha^2 \equiv 2 + 2\alpha^2 \equiv 2 + \alpha \equiv -1\ (7, \alpha + 3)$$

Therefore, the image of the unit group is $\{\pm 1\}$. There is only one nontrivial ideal of norm less than 7, namely $(2, \alpha) = (\alpha)$ of norm 4. Only the classes ± 1, ± 3 modulo $(7, \alpha + 3)$ contain elements of norm less than 7. Hence, the

norm is not a Euclidean algorithm for the ring of integers of K. But, since $-9 + \alpha^2/2 \equiv 102 (\text{mod } (13, \alpha + 12)^2)$, and 102 is a primitive root modulo 13^2, the theorem implies that K is indeed Euclidean.

The second example is K the splitting field of $x^4 - x^3 - 24x^2 - 22x + 29$. K has an integral basis $\{1, \beta, \beta^2, (-1 + 6\beta - 6\beta^2 + \beta^3)/17\}$, where β is a root of the polynomial. A basis for the unit group is given by

$$4 - \beta + \gamma/17,\ 6 + 5\beta - \beta^2 - 3\gamma/17,\ 1 - 2\beta + \gamma/17,$$

where $\gamma = -1 + 6\beta - 6\beta^2 + \beta^3$. Look at the factorizations of the polynomial of $x^4 - x^3 - 24x^2 - 22x + 29$, modulo p for $p \leq 13$.

$$\begin{aligned} x^4 - x^3 - 24x^2 - 22x + 29 &\equiv x^4 + x^3 + 1 (\text{mod } 2) \\ &\equiv (x^2 + 2x + 2)(x^2 + 1) (\text{mod } 3) \\ &\equiv x^4 + 4x^2 + x^2 + 3x + \cdot (\text{mod } 5) \\ &\equiv (x^2 + 3x + 1)^2 (\text{mod } 7) \\ &\equiv x^4 + 10x^3 + 9x^2 + 7 (\text{mod } 11) \\ &\equiv (x + 3)^4 (\text{mod } 13) \end{aligned}$$

Determine the image of the unit group modulo the prime ideal $(13, \beta + 3)$.

$$4 - \beta + \gamma/17 \equiv -6 - 6\beta + 5\beta^2 - 3\beta^3 \equiv -5\ (13, \beta + 3)$$

$$6 + 5\beta - \beta^2 - 3\gamma/17 \equiv -3 - 6\beta - 3\beta^2 - 4\beta^3 \equiv 5\ (13, \beta + 3)$$

$$1 - 2\beta + \gamma/17 \equiv 4 + 6\beta + 5\beta^2 - 3\beta^3 \equiv -5\ (13, \beta + 3)$$

Therefore, the image of the unit group is $\{\pm 1, \pm 5\}$. There are only two nontrivial ideals of norm less than 13, namely $(3, \beta^2 + 2\beta + 2) = (-\beta + \gamma/17)$

and $(3, \beta^2 + 1) = (1 - 2\beta + 2\gamma/17)$ which both have norm 9. Check the images of these elements modulo $(13, \beta + 3)$.

$$-\beta + \gamma/17 \equiv 3 - 6\beta + 5\beta^2 - 3\beta^3 \equiv 4 \ (13, \beta + 3)$$

$$1 - 2\beta + 2\gamma/17 \equiv 5 - 2\beta^2 - 2\beta^3 \equiv 6 \ (13, \beta + 3)$$

Hence, only the classes $\pm 1, \pm 5, \pm 4, \pm 6$ modulo $(13, \beta + 3)$ contain elements of norm less than 13. Therefore, the ring of integers of K is not Euclidean for the norm. However, $4 - \beta + \gamma/17 \equiv 804 (\text{mod } (29, \alpha + 1)^2$ and 804 is a primitive root mod 29^2, so the theorem implies that K is Euclidean.

CHAPTER 5
MORE EXAMPLES

The idea introduced in the last chapter can be extended to any fields which satisfy the assumptions of the theorem of R. Gupta, K. Murty, and R. Murty. Let K be an algebraic number field which is Galois over $\mathbb{Q}$, whose ring of integers R is a principal ideal domain. These extensions have either r_1 real embeddings or $2r_2$ complex embeddings. The unit group of K has rank $r = r_1 - 1$ or $r = r_2 - 1$, respectively. Suppose that r unramified linear primes $\mathfrak{p}_i$, $i = 1, \ldots, r$ can be found such that the unit group of K maps onto the coprime residue classes modulo $\mathfrak{p}_1^2 \cdots \mathfrak{p}_r^2$. An argument by induction shows that the unit group maps onto the coprime residue classes modulo $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$. Suppose this claim has been proved for all products $\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$, such that $m_i \leq n_i$ for $i = 1, \ldots, s$ and at least one of the inequalities strict. Use the inductive assumption to find a unit ϵ_1 such that $\epsilon_1 \equiv 1 (\mathrm{mod}\ \mathfrak{p}_i^{n_i})$ for $i = 2, \ldots, s$ and ϵ_1 has order $p_1^{n_1-2}(p_1 - 1)$ modulo $\mathfrak{p}_1^{n_1-1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_s^{n_s}$, where $N\mathfrak{p}_1 = p_1$. Then,

$$\epsilon_1^{p_1^{n-3}(p_1-1)} = 1 + k\mathfrak{p}_1^{n-2}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_s^{n_s},$$

$$\epsilon_1^{p_1^{n_1-2}(p_1-1)} \equiv 1 + k'\mathfrak{p}_1^{n_1-1} (\mathrm{mod}\ \mathfrak{p}_1^{n_1-1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_s^{n_s})$$

where $\mathfrak{p}_1 \nmid k, k'$ which implies that ϵ_1 has order $p_1^{n_1-1}(p_1 - 1)$ modulo $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_s^{n_s}$. Similarly, units ϵ_i can be found such that $\epsilon_i \equiv 1 (\mathrm{mod}\ \mathfrak{p}_j^{n_j})$

for $j \neq i$ and ϵ_i has order $p_i^{n_i-1}(p_i-1)$ modulo $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots\mathfrak{p}_s^{n_s}$. Then the multiplicative group generated by $\epsilon_1, \ldots, \epsilon_r$ maps onto the coprime residue classes modulo $\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r}$. If $r \geq s = \max(4-r, 2[K:\mathbb{Q}]-r-4)$, then apply the same argument of the previous chapter with

$$S = S_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\},$$

to see that R is Euclidean. Otherwise, find $2r$ primes $\mathfrak{p}_i'$ such that the multiplicative subgroup generated by the units and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ maps onto the coprime residue classes modulo ${p_1'}^2 \cdots {p_{2r}'}^2$. If $2r \geq s$, then apply the the argument above. Repeat this step until at least s primes have been found.

Theorem. *Let K be a Galois extension of $\mathbb{Q}$ whose ring of integers is a principal ideal domain. If the procedure described above produces*

$$s = \max(4-r, 2[K:\mathbb{Q}]-r-4)$$

primes, then the ring of integers of K is a Euclidean domain.

Special note should be taken that it is not sufficient to take any three primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ such that the unit group maps onto $(R/\mathfrak{p}_i^2)^*$ for each i. The reason is that it need not be true that all residue classes, say mod $\mathfrak{p}_1\mathfrak{p}_2$ contain units.

Examples

Next, the requirements of the theorem are verified for several real quadratic fields, real cubic fields, and totally complex quartic fields.

Real Quadratic Fields. If $K = \mathbb{Q}(\sqrt{14})$, then $R = \mathbb{Z}[\sqrt{14}]$. The fundamental unit of K is $15 + 4\sqrt{14}$.

$$15 + 4\sqrt{14} \equiv -3 (\text{mod } (5, \sqrt{14} + 2)^2)$$

Since -3 is a primitive root modulo 25, the unit group maps onto $(R/\mathfrak{p}^2)^*$. The generator of $(5, \sqrt{14}+2)$ is $3-\sqrt{14}$. The multiplicative group generated by the units and $3 - \sqrt{14}$ maps onto $(R/\mathfrak{p}_{11}^2\mathfrak{p}_{12}^2)^*$ with

$$\mathfrak{p}_{11} = (11, \sqrt{14} + 6) \quad \mathfrak{p}_{12} = (47, \sqrt{14} + 22).$$

The generator of $(11, \sqrt{14}+6)$ is $5-\sqrt{14}$ and the generator of $(47, \sqrt{14}+22)$ is $3 - 2\sqrt{14}$. The multiplicative subgroup generated by the units $5 - \sqrt{14}$ and $3 - 2\sqrt{14}$ maps onto $R/\mathfrak{p}_{21}^2\mathfrak{p}_{22}^2\mathfrak{p}_{23}^2$ with

$$\mathfrak{p}_{21} = (67, \sqrt{14} + 9) \quad \mathfrak{p}_{22} = (311, \sqrt{14} + 90) \quad \mathfrak{p}_{23} = (479, \sqrt{14} + 79).$$

The theorem implies that $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain.

The following table summarizes similar computations for other real quadratic fields $\mathbb{Q}(\sqrt{D})$. In the table, $\alpha = \sqrt{D}$ if $D \equiv 2$ or $3 (\text{mod } 4)$, and $\alpha = (1 + \sqrt{D})/2$ if $D \equiv 1 (\text{mod } 4)$. The problem of determining if $\mathbb{Z}[\sqrt{14}]$ is Euclidean was first raised by Samuel [33].

Table of Real Quadratic Fields

D	Fundamental Unit	Primes
14	$15+4\alpha$	$(5,\alpha+2)$
		$(11,\alpha+6),(47,\alpha+22)$
		$(67,\alpha+9),(311,\alpha+90),(479,\alpha+79)$
22	$197+42\alpha$	$(13,\alpha+3)$
		$(29,\alpha+15),(167,\alpha+32)$
		$(173,\alpha+117),(239,\alpha+71),(263,\alpha+223)$
23	$24+5\alpha$	$(11,\alpha+1)$
		$(13,\alpha+7),(23,\alpha)$
		$(29,\alpha+20),(179,\alpha+24),(191,\alpha+65)$
31	$1520+273\alpha$	$(5,\alpha+4)$
		$(11,\alpha+8),(167,\alpha+96)$
		$(173,\alpha+107),(199,\alpha+164),(239,\alpha+105)$
38	$37+6\alpha$	$(11,\alpha+4)$
		$(13,\alpha+8),(71,\alpha+40)$
		$(79,\alpha+14),(83,\alpha+72),(347,\alpha+205)$
43	$3482+531\alpha$	$(7,\alpha+6)$
		$(13,\alpha+11),(71,\alpha+16)$
		$(109,\alpha+32),(151,\alpha+88),(263,\alpha+147)$
47	$48+7\alpha$	$(11,\alpha+5)$
		$(23,\alpha+1),(31,\alpha+27)$
		$(43,\alpha+2),(167,\alpha+61),(311,\alpha+228)$
53	$3+\alpha$	$(11,\alpha+1)$
		$(29,\alpha+22),(47,\alpha+18)$
		$(59,\alpha+8),(199,\alpha+37),(347,\alpha+183)$
59	$530+69\alpha$	$(5,\alpha+2)$
		$(11,\alpha+9),(47,\alpha+23)$
		$(67,\alpha+40),(191,\alpha+21),(367,\alpha+303)$
61	$39+5\alpha$	$(5,\alpha+4)$
		$(19,\alpha+8),(41,\alpha+33)$
		$(47,\alpha+12),(107,\alpha+37),(131,\alpha+86)$
67	$48842+5967\alpha$	$(7,\alpha+5)$
		$(29,\alpha+3),(31,\alpha+25)$
		$(37,\alpha+17),(191,\alpha+81),(983,\alpha+800)$
69	$25+3\alpha$	$(11,\alpha+8)$
		$(31,\alpha+20),(83,\alpha+30)$
		$(107,\alpha+23),(137,\alpha+26),(211,\alpha+185)$
71	$3480+413\alpha$	$(5,\alpha+4)$
		$(11,\alpha+7),(47,\alpha+27)$
		$(109,\alpha+92),(479,\alpha+103),(599,\alpha+168)$
73	$943+250\alpha$	$(19,\alpha+11)$
		$(23,\alpha+12),(71,\alpha+29)$
		$(97,\alpha+24),(251,\alpha+134),(359,\alpha+278)$
77	$4+\alpha$	$(13,\alpha+2)$
		$(17,\alpha+15),(23,\alpha+6)$
		$(41,\alpha+17),(163,\alpha+149),(179,\alpha+81)$

D	Fundamental Unit	Primes
83	$82+9\alpha$	$(19,\alpha+8)$
		$(29,\alpha+24),(79,\alpha+77)$
		$(103,\alpha+17),(107,\alpha+46),(179,\alpha+21)$
86	$10405+1122\alpha$	$(5,\alpha+1)$
		$(7,\alpha+3),(59,\alpha+33)$
		$(67,\alpha+32),(71,\alpha+50),(263,\alpha+136)$
89	$447+106\alpha$	$(11,\alpha+10)$
		$(17,\alpha+9),(67,\alpha+54)$
		$(71,\alpha+53),(73,\alpha+38),(179,\alpha+159)$
93	$13+3\alpha$	$(7,\alpha+5)$
		$(11,\alpha+3),(103,\alpha+58)$
		$(137,\alpha+48),(727,\alpha+655),(907,\alpha+876)$
94	$2143295+221064\alpha$	$(5,\alpha+2)$
		$(13,\alpha+4),(311,\alpha+191)$
		$(317,\alpha+98),(367,\alpha+185),(401,\alpha+351)$
97	$5035+1138\alpha$	$(11,\alpha+1)$
		$(43,\alpha+32),(47,\alpha+29)$
		$(53,\alpha+18),(103,\alpha+35),(167,\alpha+63)$
101	$9+2\alpha$	$(17,\alpha+6)$
		$(19,\alpha+2),(23,\alpha+1)$
		$(37,\alpha+14),(107,\alpha+11),(131,\alpha+12)$
103	$227528+22419\alpha$	$(11,\alpha+9)$
		$(29,\alpha+25),(47,\alpha+3)$
		$(61,\alpha+46),(263,\alpha+222),(383,\alpha+334)$
107	$962+93\alpha$	$(7,\alpha+3)$
		$(29,\alpha+22),(31,\alpha+13)$
		$(43,\alpha+8),(89,\alpha+75),(191,\alpha+38)$
109	$118+25\alpha$	$(7,\alpha+2)$
		$(31,\alpha+17),(83,\alpha+72)$
		$(89,\alpha+25),(347,\alpha+130),(439,\alpha+243)$
113	$703+146\alpha$	$(7,\alpha)$
		$(11,\alpha+8),(127,\alpha+84)$
		$(131,\alpha+107),(149,\alpha+91),(227,\alpha+60)$
118	$306917+28254\alpha$	$(23,\alpha+7)$
		$(31,\alpha+26),(47,\alpha+20)$
		$(101,\alpha+44),(719,\alpha+223),(823,\alpha+781)$

Real Cubic Fields.

For real cubic fields, the theorem requires the existence of two primes $\mathfrak{p}, \mathfrak{q}$ such that the unit group maps onto $R/\mathfrak{p}^2\mathfrak{q}^2R$. Davenport [6], Godwin [10], and J.R. Smith [37] have studied the norm as a Euclidean algorithm in these fields. In the following table, superscripts d, g, s denotes that Davenport, Godwin, or Smith, respectively, showed that this field is Euclidean for the norm. Smith also showed that at most four additional real cubic fields with discriminant less than 10^8 could be Euclidean for the norm. These fields are denoted by superscript p.

Table of Real Cubic Fields

Discriminant	Generating Polynomial	Primes
49^d	$x^3 - x^2 - 2x + 1$	$(13, \alpha + 8), (83, \alpha + 57)$
81^d	$x^3 - 3x + 1$	$(17, \alpha + 4), (19, \alpha + 16)$
169^g	$x^3 - x^2 - 4x - 1$	$(5, \alpha + 4), (83, \alpha + 75)$
361^g	$x^3 - x^2 - 6x + 7$	$(7, \alpha), (11, \alpha + 6)$
961^s	$x^3 - x^2 - 10x + 8$	$(23, \alpha + 6), (263, \alpha + 159)$
1369^s	$x^3 - x^2 - 12x - 11$	$(11, \alpha + 7), (43, \alpha + 4)$
1849^s	$x^3 - x^2 - 14x - 8$	$(11, \alpha + 5), (47, \alpha + 16)$
3721^s	$x^3 - x^2 - 20x + 9$	$(11, \alpha + 8), (53, \alpha + 36)$
4489^s	$x^3 - x^2 - 22x - 5$	$(5, \alpha + 3), (43, \alpha + 21)$
5329^s	$x^3 - x^2 - 24x + 27$	$(7, \alpha + 2), (83, \alpha + 59)$
6241	$x^3 - x^2 - 26x - 41$	$(41, \alpha + 16), (179, \alpha + 140)$
9409	$x^3 - x^2 - 32x + 79$	$(19, \alpha + 17), (47, \alpha + 19)$
10609^p	$x^3 - x^2 - 34x + 61$	$(23, \alpha + 12), (79, \alpha + 65)$
11881^p	$x^3 - x^2 - 36x + 4$	$(17, \alpha + 5), (19, \alpha + 1)$
13689	$x^3 - 39x + 26$	$(11, \alpha + 9), (59, \alpha + 24)$
16129^p	$x^3 - x^2 - 42x - 80$	$(19, \alpha + 14), (47, \alpha + 16)$
19321	$x^3 - x^2 - 46x - 103$	$(23, \alpha + 15), (59, \alpha + 23)$
22801	$x^3 - x^2 - 50x + 123$	$(19, \alpha + 11), (29, \alpha + 25)$
24649^p	$x^3 - x^2 - 52x - 64$	$(23, \alpha + 10), (59, \alpha + 23)$
32761	$x^3 - x^2 - 60x + 67$	$(19, \alpha + 7), (59, \alpha + 36)$
37249	$x^3 - x^2 - 64x - 143$	$(11, \alpha), (179, \alpha + 10)$
39601	$x^3 - x^2 - 66x - 59$	$(11, \alpha + 5), (179, \alpha + 109)$
44521	$x^3 - x^2 - 70x + 125$	$(11, \alpha + 9), (107, \alpha + 82)$

Totally Complex Quartic Fields.

Uchida [39] found all totally complex biquadratic fields with class number one with the possibility of one exception. Montgomery and Weinberger [25] showed that the exceptional field does not exist. Setzer [35] found all totally complex cyclic quartic fields with class number one. In the table below each of these fields is listed together with two rational primes which split completely into linear primes in the given field.

Lakein [22] showed that eight of these fields are Euclidean for the norm. This is denoted by superscript l. Lenstra [23] showed that one additional field is Euclidean for the norm. This is denoted by superscript e.

Table of Totally Complex Quartic Fields

Discriminant	Generating Polynomial	Primes
125^r	x^4+5x^2+5	$(31,\alpha+17)$
		$(61,\alpha+25),(431,\alpha+281)$
		$(1181,\alpha+810),(2111,\alpha+1129),(181,\alpha+98)$
144^l	x^4+8x^2+4	$(73,\alpha+29),(157,\alpha+3),(277,\alpha+261)$
		$(997,\alpha+770),(4549,\alpha+2229),(3541,\alpha+2570)$
225^l	x^4-x^2+4	$(19,\alpha+7)$
		$(31,\alpha+7),(229,\alpha+53)$
		$(619,\alpha+609),(1279,\alpha+175),(31,\alpha+13)$
256	x^4+6x^2+1	$(97,\alpha+5)$
		$(401,\alpha+278),(1049,\alpha+188)$
		$(137,\alpha+49),(1553,\alpha+1494),(3049,\alpha+2341)$
400^l	x^4-8x^2+36	$(41,\alpha+22)$
		$(269,\alpha+61),(29,\alpha+1)$
		$(149,\alpha+125),(509,\alpha+474),(709,\alpha+437)$
441^l	x^4+5x^2+1	$(37,\alpha+18)$
		$(211,\alpha+176),(823,\alpha+404)$
		$(67,\alpha+41),(1303,\alpha+765),(193,\alpha+158)$
576^l	x^4+10x^2+1	$(19,\alpha+9)$
		$(907,\alpha+35),(37483,\alpha+9403)$
		$(19,\alpha+9),1051,\alpha+762),(1747,\alpha+487)$
576^l	x^4+2x^2+25	$(70,\alpha+23)$
		$(7,\alpha),(313,\alpha+236)$
		$(223,\alpha+159),(727,\alpha+13),(193,\alpha+117)$
784^l	x^4+16x^2+36	$(113,\alpha+43)$
		$(29,\alpha+26),(53,\alpha+47)$
		$(389,\alpha+70),(653,\alpha+190),(757,\alpha+305)$
1089^l	x^4+7x^2+4	$(223,\alpha+213)$
		$(31,\alpha+4),(727,\alpha+515)$
		$(223,\alpha+89),(1543,\alpha+1125),(1153,\alpha+371)$
1225	x^4+x^2+9	$(71,\alpha+48)$
		$(179,\alpha+51),(29,\alpha+2)$
		$(239,\alpha+88),(11,\alpha+1),(109,\alpha+69)$
1600	x^4-6x^2+49	$(59,\alpha+31)$
		$(179,\alpha+71),(211,\alpha+158)$
		$(59,\alpha+44),(409,\alpha+185),(131,\alpha+51)$
1936	x^4+24x^2+100	$(401,\alpha+317)$
		$(37,\alpha+33),(229,\alpha+148)$
		$(773,\alpha+690),(829+\alpha+23),(617,\alpha+572)$
2048	x^4+4x^2+2	$(7,\alpha+6)$
		$(151,\alpha+42),(103,\alpha+28)$
		$(23,\alpha+16),(359,\alpha+112),(113,\alpha+7)$
2197	x^4+13x^2+13	$(157,\alpha+133)$
		$(191,\alpha+92),(53,\alpha+17)$
		$(107,\alpha+47),(113,\alpha+106),(61,\alpha+17)$
2601	x^4-7x^2+25	$(421,\alpha+106)$
		$(13,\alpha+2),(151,\alpha+50)$
		$(859,\alpha+302),(409,\alpha+13),(1087,\alpha+869)$

Discriminant	Generating Polynomial	Primes
2704	$x^4 - 24x^2 + 196$	$(29, \alpha + 22)$
		$(269, \alpha + 115), (53, \alpha + 45)$
		$(29, \alpha + 27), (173, \alpha + 159), (1193, \alpha + 926)$
3136	$x^4 + 18x^2 + 25$	$(43, \alpha + 21)$
		$(163, \alpha + 130), (137, \alpha + 53)$
		$(11, \alpha + 6), (107, \alpha + 66), (193, \alpha + 113)$
3249	$x^4 + 11x^2 + 16$	$(163, \alpha + 134)$
		$(283, \alpha + 228), (463, \alpha + 169)$
		$(727, \alpha + 441), (1987, \alpha + 1797), (61, \alpha + 6)$
5776	$x^4 + 40x^2 + 324$	$(593, \alpha + 372)$
		$(5, \alpha + 3), (149, \alpha + 73)$
		$(809, \alpha + 118), (1013, \alpha + 191), (701, \alpha + 498)$
5929	$x^4 + 9x^2 + 1$	$(37, \alpha + 15)$
		$(163, \alpha + 109), (71, \alpha + 17)$
		$(23, \alpha + 5), (191, \alpha + 118), (37, \alpha + 32)$
7744	$x^4 + 26x^2 + 81$	$(59, \alpha + 38)$
		$(137, \alpha + 71), (179, \alpha + 38)$
		$(59, \alpha + 38), (419, \alpha + 266), (97, \alpha + 55)$
7744	$x^4 + 18x^2 + 169$	$(23, \alpha + 4)$
		$(191, \alpha + 50), (103, \alpha + 30)$
		$(23, \alpha + 14), (71, \alpha + 17), (31, \alpha + 11)$
8281	$x^4 - 3x^2 + 25$	$(23, \alpha + 1)$
		$(127, \alpha + 24), (179, \alpha + 139)$
		$(23, \alpha + 18), (263, \alpha + 81), (211, \alpha + 55)$
15129	$x^4 - 19x^2 + 121$	$(37, \alpha + 9)$
		$(103, \alpha + 102), (139, \alpha + 76)$
		$(349, \alpha + 85), (1579, \alpha + 197), (31, \alpha + 28)$
16641	$x^4 + 23x^2 + 100$	$(127, \alpha + 106)$
		$(103, \alpha + 23), (13, \alpha + 8)$
		$(643, \alpha + 570), (1303, \alpha + 852), (1777, \alpha + 41)$
17689	$x^4 + 13x^2 + 9$	$(11, \alpha + 7)$
		$(197, \alpha + 191), (263, 253)$
		$(23, \alpha + 22), (137, \alpha + 132), (163, \alpha + 113)$
21904	$x^4 - 72x^2 + 1444$	$(41, \alpha + 32)$
		$(293, \alpha + 274), (173, \alpha + 53)$
		$(53, \alpha + 274), (317, \alpha + 9), (317, \alpha + 221), (197, \alpha + 134)$
23104	$x^4 + 42x^2 + 289$	$(11, \alpha + 2)$
		$(283, \alpha + 211), (347, \alpha + 277)$
		$(239, \alpha + 38), (11, \alpha + 2), (163, \alpha + 101)$
24389	$x^4 + 29x^2 + 29$	$(23, \alpha + 17)$
		$(107, \alpha + 13), (103, \alpha + 6)$
		$(23, \alpha + 6), (83, \alpha + 38), (181, \alpha + 23)$
29584	$x^4 + 88x^2 + 1764$	$(41, \alpha + 39)$
		$(13, \alpha + 5), (101, \alpha + 72)$
		$(53, \alpha + 43), (197, \alpha + 87), (397, \alpha + 269)$
34969	$x^4 - 3x^2 + 49$	$(47, \alpha + 40)$
		$(223, \alpha + 134), (353, \alpha + 185)$
		$(47, \alpha + 40), (103, \alpha + 100), (53, \alpha + 30)$

Discriminant	Generating Polynomial	Primes
40401	$x^4 + 35x^2 + 256$	$(181, \alpha + 74)$
		$(103, \alpha + 101), (37, \alpha + 31)$
		$(823, \alpha + 178), (223, \alpha + 111), (151, \alpha + 83)$
43681	$x^4 + 15x^2 + 4$	$(163, \alpha + 47)$
		$(229, \alpha + 217), (251, \alpha + 100)$
		$(47, \alpha + 27), (137, \alpha + 47), (5, \alpha + 4)$
53653	$x^4 - 2x^3 + 20x^2 - 19x + 7$	$(83, \alpha + 12)$
		$(71, \alpha + 20), (137, \alpha + 55)$
		$(83, \alpha + 12), (53, \alpha + 20), (127, \alpha + 115)$
53824	$x^4 - 54x^2 + 961$	$(59, \alpha + 41)$
		$(107, \alpha + 24), (139, \alpha + 136)$
		$(59, \alpha + 54), (179, \alpha + 149), (227, \alpha + 226)$
71289	$x^4 - 43x^2 + 529$	$(67, \alpha + 42)$
		$(223, \alpha + 3), (607, \alpha + 446)$
		$(367, \alpha + 311), (643, \alpha + 352), (673, \alpha + 234)$
71824	$x^4 + 136x^2 + 4356$	$(241, \alpha + 231)$
		$(37, \alpha + 3), (269, \alpha + 217)$
		$(149, \alpha + 21), (157, \alpha + 131), (557, \alpha + 169)$
90601	$x^4 + 25x^2 + 81$	$(11, \alpha + 4)$
		$(197, \alpha + 2), (67, \alpha + 19)$
		$(107, \alpha + 9), (239, \alpha + 199), (317, \alpha + 66)$
118336	$x^4 + 90x^2 + 1681$	$(107, \alpha + 68)$
		$(251, \alpha + 191), (97, \alpha + 49)$
		$(83, \alpha + 26), (307, \alpha + 4), (11, \alpha + 7)$
148877	$x^4 + 53x^2 + 53$	$(47, \alpha + 19)$
		$(307, \alpha + 252), (311, \alpha + 238)$
		$(47, \alpha + 28), (227, \alpha + 38), (281, \alpha + 96)$
182329	$x^4 - 27x^2 + 289$	$(197, \alpha + 90)$
		$(239, \alpha + 5), (109, \alpha + 61)$
		$(107, \alpha + 96), (113, \alpha + 24), (163, \alpha + 13)$
226981	$x^4 + 305x^2 + 61$	$(73, \alpha + 43)$
		$(137, \alpha + 26), (269, \alpha + 50)$
		$(47, \alpha + 26), (179, \alpha + 30), (73, \alpha + 6)$
239121	$x^4 + 83x^2 + 1600$	$(307, \alpha + 142)$
		$(367, \alpha + 161), (547, \alpha + 484)$
		$(499, \alpha + 476), (2179, \alpha + 501), (733, \alpha + 240)$
287296	$x^4 + 138x^2 + 4225$	$(17, \alpha + 11)$
		$(89, \alpha + 32), (163, \alpha + 34)$
		$(59, \alpha + 49), (19, \alpha + 10), (17, \alpha + 9)$
425104	$x^4 + 328x^2 + 26244$	$(1049, \alpha + 638)$
		$(173, \alpha + 57), (97, \alpha + 7)$
		$(1109, \alpha + 136), (113, \alpha + 2), (53, \alpha + 37)$
543169	$x^4 + 39x^2 + 196$	$(23, \alpha + 16)$
		$(157, \alpha + 100), (71, \alpha + 51)$
		$(23, \alpha + 16), (269, \alpha + 138), (37, \alpha + 28)$
1301881	$x^4 + 85x^2 + 1521$	$(71, \alpha + 37)$
		$(263, \alpha + 13), (53, \alpha + 18)$
		$(179, \alpha + 145), (347, \alpha + 92), (71, \alpha + 37)$

Discriminant	Generating Polynomial	Primes
1620529	$x^4 + 43x^2 + 144$	$(23, \alpha + 13)$
		$(163, \alpha + 131), (17, \alpha + 14)$
		$(23, \alpha + 8), (83, \alpha + 81), (73, \alpha + 30)$
3214849	$x^4 + 87x^2 + 1444$	$(53, \alpha + 16)$
		$(199, \alpha + 65), (383, \alpha + 345)$
		$(179, \alpha + 157), (71, \alpha + 62), (97, \alpha + 37)$
8300161	$x^4 + 55x^2 + 36$	$(719, \alpha + 399)$
		$(269, 40), (797, \alpha + 399)$
		$(23, \alpha + 17), (83, \alpha + 52), (17, \alpha + 15)$
9591409	$x^4 + 91x^2 + 1296$	$(347, \alpha + 311)$
		$(419, \alpha + 2), (2099, \alpha + 179)$
		$(47, \alpha + 9), (43, \alpha + 30), 199, \alpha + 173)$
49126081	$x^4 + 103x^2 + 900$	$(47, \alpha + 20)$
		$(787, \alpha + 390), (1091, \alpha + 984)$
		$(47, \alpha + 22), (367, \alpha + 70), (173, \alpha + 118)$
119268241	$x^4 + 115x^2 + 576$	$(1567, \alpha + 1480)$
		$(743, \alpha + 332), (1399, \alpha + 213)$
		$(47, \alpha + 3), (71, \alpha + 40), (223, \alpha + 85)$

Conclusion.

In all the examples which were tested it was possible to show that the ring of integers contained the desired prime ideals. It would be nice if a general proof could be given for the existence of these prime ideals. Nevertheless, it should be possible to find these ideals in any particular case. It would certainly be of interest to do this for other classes of fields, in particular for cyclotomic fields.

CHAPTER 6
CYCLICITY AND GENERATION MOD p OF ELLIPTIC CURVES OVER ALGEBRAIC NUMBER FIELDS

Let

$$E:\ y^2 = x^3 + ax + b$$

be an elliptic curve defined over a number field F. If $\mathfrak{p}$ is a prime ideal of F, then

$$\tilde{E}:\ y^2 = x^3 + \tilde{a}x + \tilde{b}$$

is called the reduction of E modulo the prime ideal $\mathfrak{p}$, where $\tilde{a}$ is the image of a in $F_{\mathfrak{p}}$. In analogy to Artin's Primitive Root Conjecture, Serre [34] asked how often $\tilde{E}(F_{\mathfrak{p}})$ is cyclic. He showed that for the case $F = \mathbb{Q}$ the method of Hooley [18] implied the existence of $\gg x/\log x$ primes $p \leq x$ such that $\tilde{E}(\mathbb{F}_p)$ is cyclic, assuming the Generalized Riemann Hypothesis where $\mathbb{F}_p$ is the finite field with p elements. R. Murty [27], [28] gave an unconditional proof of the existence of infinitely many such p for elliptic curves with CM and in a few other cases. Gupta and R. Murty [14] showed that $\tilde{E}(\mathbb{F}_p)$ is cyclic if and only if E has a non-rational 2-division point and that the density of such primes is $\gg x/(\log x)^2$.

Another question related to Artin's conjecture is how often the reduction of a free subgroup Γ of the F-rational points of E generates $\tilde{E}(F_{\mathfrak{p}})$. Gupta and R. Murty considered the case of elliptic curves with CM over $F = \mathbb{Q}$

and showed that if Γ has rank at least six, then there are $\gg x/(\log x)^2$ primes such that $\tilde{E}(\mathbb{F}_p) = \Gamma_p$, where Γ_p is the reduction of Γ modulo p.

Cyclicity of Elliptic Curves

Let $K_n = F(E[n])$ for each positive integer n, where $E[n]$ is the set of n-division points of E.

Lemma 1. *If $\mathfrak{p}$ is a prime of good reduction in F, then $\tilde{E}(F_\mathfrak{p})$ is cyclic if and only if $\mathfrak{p}$ does not split completely in K_q for any prime q.*

Proof. Consider the Frobenius automorphism of $F_\mathfrak{p}$ defined by $\pi_\mathfrak{p}(x) = x^{N\mathfrak{p}}$. This map induces an endomorphism $\pi_\mathfrak{p} : \tilde{E} \to \tilde{E}$ such that

$$\ker(\pi_\mathfrak{p} - \mathrm{id}) = \tilde{E}(F_\mathfrak{p}).$$

$\tilde{E}(F_\mathfrak{p})[q]$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^2$ if q is coprime to $N\mathfrak{p}$; otherwise, it is isomorphic to either $\mathbb{Z}/q\mathbb{Z}$ or $\{O\}$, see Silverman [36, p. 89]. Therefore, $\tilde{E}(F_\mathfrak{p})$ is noncyclic if $\pi_\mathfrak{p}$ acts trivially on some $\tilde{E}(F_\mathfrak{p})[q]$; that is, $\mathfrak{p}$ splits completely in some K_q.

Lemma 2. *The field $F(\zeta_n)$ is contained in K_n for every positive integer n.*

Proof. This is Corollary 8.1.1 of Silverman [36]. The Weil pairing on n-torsion points of E is bilinear and non-degenerate so that all the n^{th} roots of unity are in its image. The Galois invariance of the pairing implies that the n^{th} roots of unity are in K_q.

Lemma 3. *There are more than $\delta_1 x/(\log x)^{2+1/4}$ primes $\mathfrak{p}$ of F with the properties*

(1) $N_{F/\mathbb{Q}}\mathfrak{p} = p \leq x$, *$p$ a rational prime,*

(2) *If $\ell|(p-1)$, then either $\ell|d$ or $\ell > x^{1/2\eta}\exp\left(-(\log x)^{1/3}\right)$, where d is the largest integer such that $\mathbb{Q}(\zeta_d) \subseteq F$,*

(3) *$\mathfrak{p}$ does not split completely in any K_q for $q|d$.*

Proof. Choose nontrivial abelian extensions $A_q \subseteq K_q$ of F for $q|d$. Let A be the compositum of all the A_q for $q|d$. The condition that $\mathfrak{p}$ not split completely in any K_q is satisfied for $\mathfrak{p}$ such that $\sigma_\mathfrak{p} = \tau$ for some element τ of $\mathrm{Gal}(A/F)$. Now apply Lemma 3 of the previous chapter.

Suppose that F is a field of degree less than or equal to four.

Theorem. *The group $\tilde{E}(F_\mathfrak{p})$ is cyclic for infinitely many primes $\mathfrak{p}$ of F if and only if $K_q \not\subseteq F$ for all $q|d$, furthermore, the number of primes $N\mathfrak{p} \leq x$ for which $\tilde{E}(F_\mathfrak{p})$ is cyclic is greater than $\delta_2 x/(\log x)^{2+1/4}$.*

Proof. Let $S(a,x)$ be the set of primes $\mathfrak{p}$ of F satisfying the conditions of the previous lemma with the additional property that $a_\mathfrak{p} = a$, where $|a| \leq 2x^{1/2}$. If $\tilde{E}(F_\mathfrak{p})$ is not cyclic then

$$(\mathbb{Z}/q\mathbb{Z})^2 \subseteq \tilde{E}(F_\mathfrak{p})$$

for some rational prime q. The prime $p = N\mathfrak{p}$ splits completely in K_q so p splits completely in $\mathbb{Q}(\zeta_q)$; that is, q divides $p-1$. Since

$$\left|\tilde{E}(F_\mathfrak{p})\right| = p + 1 - a,$$

it follows that $q^2|p+1-a$ and also $q|a-2$. Since $q \geq x^{1/4}(\log x)^2$ and $|a-2| \leq 2x^{1/2}$, a determines q for $x \geq 4$. The number of p such that

$$p \equiv a-1 (\mathrm{mod}\ q^2)$$

is less than $x/q^2 + O(1) \ll x^{1/2}/(\log x)^4$. Counting these p for all a gives

$$\ll x^{1/2}/(\log x)^4 x^{1/2} = x/(\log x)^4$$

primes $\mathfrak{p}$ such that $\tilde{E}(F_\mathfrak{p})$ is not cyclic. These primes may be disregarded to give $\gg x/(\log x)^{2+1/15}$ primes $\mathfrak{p}$ such that $\tilde{E}(F_\mathfrak{p})$ is cyclic.

Generation of Reduced Elliptic Curves

Let E be an elliptic curve defined over an arbitrary field F with complex multiplication by an order in an imaginary quadratic field k. Suppose that Γ is a free subgroup of $F-$rational points of E.

Lemma 4. *There are more than $\delta_3 x/(\log x)^{2+1/15}$ primes $\mathfrak{p}$ of F with the properties*

(1) $N_{F/\mathbb{Q}}\mathfrak{p} = p \leq x$, *for p a rational prime,*

(2) $\mathfrak{p}$ *is supersingular and does not split in K_2,*

(3) *If $\ell|(p+1)$, then either $\ell = 2$ or $\ell > x^{1/2\eta}\exp\left(-(\log x)^{1/3}\right)$,*

where $\eta = \max(2, d-2)$ and d is the order of the maximal abelian subgroup of $\mathrm{Gal}(F/\mathbb{Q})$.

Proof. Consider the sequence

$$\mathcal{D} = \{p+1 : \ p \text{ a supersingular prime of } E,\ (p, K/\mathbb{Q}) \subseteq C\}.$$

By Lemma 3 of the previous chapter,

$$S(\mathcal{D}, \mathcal{P}_d, z) \geq \delta_4 \frac{x}{(\log x)^{2+1/4}},$$

with $z = x^{1/2\eta} \exp\left(-(\log x)^{1/3}\right)$

Let $N_\Gamma(x)$ denote the number of primes $\mathfrak{p}$ of F with $N_{F/\mathbb{Q}}\mathfrak{p} \leq x$ such that $\tilde{E}(F_\mathfrak{p}) = \Gamma_\mathfrak{p}$, where $\Gamma_\mathfrak{p}$ is the reduction of Γ modulo $\mathfrak{p}$.

Lemma 5. *The number of primes $\mathfrak{p}$ such that $|\Gamma_\mathfrak{p}| < y$ is $\ll y^{1+2/r}$.*

Proof. Let $H(P) = \langle P, P \rangle$, where $\langle , \rangle$ is the Weil pairing. Denote the generators of Γ by $P_1, P_2, \ldots, P_r$. First note that the number of integer solutions to

$$H(n_1 P_1 + \cdots + n_r P_r) \leq x$$

is

$$\frac{(\pi x)^{r/2}}{\sqrt{R}\Gamma\left(\frac{r}{2}+1\right)} + O(x^{(r-1)/2+\epsilon}),$$

where $R = \det(\langle P_i, P_j \rangle)$, see Walfisz [41]. Choose a constant C such that

$$\frac{(C\pi)^{r/2}}{\sqrt{R}\Gamma\left(\frac{r}{2}\right)} > 1.$$

Consider the set of all r-tuples of integers $(n_1, \ldots, n_r)$ such that

$$H(n_1 P_1 + \cdots n_r P_r) \leq C y^{2/r}.$$

The previous remark implies that the number of r-tuples is greater than y. In addition, since $\Gamma_\mathfrak{p} < y$, there are two distinct r-tuples $n_1, \ldots, n_r$ and $m_1, \ldots, m_r$ with

$$n_1 P_1 + \cdots + n_r P_r \equiv m_1 P_1 + \cdots + m_r P_r (\mathrm{mod}\ \mathfrak{p}),$$

so that $\mathfrak{p}$ divides the denominator of the non-zero point

$$Q = (n_1 - m_1)P_1 + \cdots + (n_r - m_r)P_r.$$

Let $h(P)$ be the usual logarithmic height on $E(F)$. The number of $\mathfrak{p}$ dividing the denominator of Q is bounded by $h(Q)$. Since Q is not a torsion point,

$$h(Q) \ll H(Q) \leq 2Cy^{2/r},$$

which implies that the number of such points Q is $O(y)$. Each Q gives rise to $O(y^{2/r})$ prime factors, which implies the desired result.

Theorem. *Let E be an elliptic curve defined over a number field F. If the rank r of Γ satisfies $r > 2(2\eta - 1)$, then*

$$N_\Gamma(x) \gg \frac{x}{(\log x)^{2+1/15}}.$$

Proof. Consider the primes estimated in Lemma 4. Since these are supersingular primes of E, $a_\mathfrak{p} = 0$. If

$$\ell | [\tilde{E}(F_\mathfrak{p}) : \Gamma_\mathfrak{p}],$$

then $\ell > x^{1/2\eta} \exp(-(\log x)^{1/3})$. This implies that

$$|\Gamma_\mathfrak{p}| < x^{1-1/2\eta} \exp((\log x)^{1/3}).$$

Lemma 5 shows that the number of such $\mathfrak{p}$ is

$$\begin{aligned} &\ll \left(x^{1-1/2\eta} \exp((\log x)^{1/3})\right)^{1+2/r} \\ &= x^{1+2/r-1/2\eta-1/\eta r} \exp((1+2/r)(\log x)^{1/3}, \end{aligned}$$

so that these primes may be disregarded.

References

1. E. Bombieri, *On the Large Sieve*, Mathematika **12** (1965), 201–225.
2. J. Buchmann and D. Ford, *On the Computation of Totally Real Quartic Fields of Small Discriminant*, Math. Comp. **52** (1989), 161–174.
3. J. Buchmann, M. Pohst, and J. v. Schmettow, *On the Computation of Unit Groups and Class Groups of Totally Real Quartic Fields*, Math. Comp. **53** (1989), 387–397.
4. H. Chatland and H. Davenport, *Euclid's Algorithm in Real Quadratic Fields*, Canad. Jour. Math. **2** (1950), 13–15.
5. H. Cohn and J. Deutsch, *Use of a Computer Scan to Prove* $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ *and* $\mathbb{Q}(\sqrt{3+\sqrt{2}})$ *are Euclidean*, Math. Comp. **46** (1986), 295–299.
6. H. Davenport, *On the Product of Three Non-Homogeneous Linear Forms*, Proc. Camb. Phil. Soc. **43** (1947), 137–152.
7. H. Davenport, *Euclid's Algorithm in Cubic Fields of Negative Discriminant*, Acta Math. **84** (1950), 159–179.
8. H. Davenport, *Euclid's Algorithm in Certain Quartic Fields*, Trans. Amer. Math. Soc. **68** (1950), 508–532.
9. P.X. Gallagher, *A Large Sieve Density Estimate near* $\sigma = 1$, Invent. Math. **11** (1970), 329–339.
10. H.J. Godwin, *On the Inhomogeneous Minima of Totally Real Cubic Norm-forms*, Journal London Math. Soc. **40** (1965), 623–627.
11. H.J. Godwin, *On Euclid's Algorithm in some Quartic and Quintic Fields*, Journal London Math. Soc. **40** (1965), 699–704.
12. R. Gupta and M.R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), 127–130.
13. R. Gupta and M.R. Murty, *Primitive Points on Elliptic Curves*, Compos. Math. **58** (1986), 13–44.
14. R. Gupta and M.R. Murty, *Cyclicity and Generation of Points mod p on Elliptic Curves*, Invent. Math. **101** (1990), 225–235.
15. R. Gupta, M.R. Murty, and V.K. Murty, *The Euclidean Algorithm for S-integers* in Conference Proceedings of the CMS Vol. 7, 1987, pp. 189–201.
16. H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
17. H. Heilbronn, *On Euclid's Algorithm in Real Quadratic Fields*, Proc. Camb. Phil. Soc. **34** (1938), 521–526.
18. C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
19. H. Iwaniec, *Rosser's Sieve*, Acta Arithmetica **36** (1980), 171–202.

20. J. Lagarias, H. Montgomery, and A. Odlyzko, *A Bound for the Least Prime Ideal in the Chebotarev Density Theorem*, Invent. Math. **54** (1979), 271–296.
21. J. Lagarias and A. Odlyzko, *Effective Versions of the Chebotarev Density Theorem;* in Algebraic Number Fields (A. Fröhlich, ed.), Academic Press, London, 1977, pp. 409–464.
22. R.B. Lakein, *Euclid's Algorithm in Complex Quartic Fields*, Acta Arithmetica **20** (1972), 393–400.
23. H.W. Lenstra, Jr., *Euclidean Number Fields of Large Degree*, Invent. Math. **38** (1977), 237–254.
24. H.W. Lenstra, Jr., *On Artin's Conjecture and Euclid's Algorithm in Global Fields*, Invent. Math. **42** (1977), 201–224.
25. H. Montgomery and P. Weinberger, *Notes on Small Class Numbers*, Acta Arithmetica **24** (1979), 529–542.
26. Th. Motzkin, *The Euclidean Algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.
27. M.R. Murty, *On Artin's Conjecture*, J. Number Theory **16** (1983), 147 168.
28. M.R. Murty, *On the Supersingular Reduction of Elliptic Curves*, Proc. Indian Acad. Sci., Math. Sci. **97** (1987), 247–250.
29. M.R. Murty and V.K. Murty, *A Variant of the Bombieri-Vinogradov Theorem* in Conference Proceedings of the CMS Vol. 7, 1987, pp. 243 271.
30. M.R. Murty, V.K. Murty, and N. Saradha, *Modular Forms and the Chebotarev Density Theorem*, Am. J. Math. **110** (1988), 253–281.
31. O.T. O'Meara, *On the Finite Generation of Linear Groups over Hasse Domains*, J. Reine Angew. Math. **217** (1965), 79–108.
32. H. Rademacher, *On the Phragmén-Lindelöf Theorem and Some Applications*, Math. Zeit. **72** (1959), 192–204.
33. P. Samuel, *About Euclidean Rings*, J. Algebra **19** (1971), 282–301.
34. J.-P. Serre, *Resumé de cours (1977);* Oeuvres, Springer Verlag, Berlin-Heidelberg-New York, 1986.
35. B. Setzer, *The Determination of all Imaginary, Quartic, Abelian Number Fields with Class Number One*, Math. Comp. **no. 152** (1980), 1383–1386.
36. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag, New York, 1986.
37. J.R. Smith, *On Euclid's Algorithm in some Cyclic Cubic Fields*, Journal London Math. Soc. **44** (1969), 577–582.
38. H. Stark, *Some Effective Cases of the Brauer-Siegel Theorem*, Invent. Math. **23** (1974), 135–152.

39. K. Uchida, *Imaginary Abelian Number Fields with Class Number One*, Tôhoku Math. Jour. **24** (1972), 487–499.
40. A.I. Vinogradov, *On the Density Hypothesis for Dirichlet L-functions*, Izv. Akad. Nauk. SSSR, ser. mat. **29** (1965), 903–934.
41. A. Walfisz, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden* III, Math. Zeit. **27** (1927), 245–268.
42. P. Weinberger, *On Euclidean Rings of Algebraic Integers*, Proc. Symp. Pure Math. **24** (1973), 321–332.