Euclidean algorithm for certain algebraic number fields

Thesis submitted to the

Chennai Mathematical Institute, Chennai

for the degree of

Doctor of Philosophy in Mathematics
(Under the faculty of Science)

by

Subramani Muttukrishnan
Chennai Mathematical Institute, Chennai

Under the guidance of

Dr. K. Srinivas
Professor
The Institute of Mathematical Sciences, Chennai

June, 2017

Chennai Mathematical Institute

Recommendations of the Viva Voce Board

As members of the Viva Voce Board, we certify that we have read the dissertation prepared by Subramani Muttukrishnan entitled Euclidean algorithm for certain algebraic number fields and recommend that it may be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

____ Date:
Chair -

____ Date:
Guide/Convener -

Prof. K. Srinivas__________________________ Date:
Member 1 -

____ Date:
Member 2 -

____ Date:

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to CMI.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it may be accepted as fulfilling the dissertation requirement.

Date:

Place: Guide

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Chennai Mathematical Institute (CMI) and is deposited in the Library to be made available to borrowers under rules of the CMI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of CMI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

M. Subramani

DECLARATION

I hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree/diploma at this or any other Institution/University.

M. Subramani

Dedicated to Prof. K. Srinivas, Prof. T.R. Ramadas, Prof. M. Ram Murty
and to my teachers

ACKNOWLEDGEMENTS

I express my sincere gratitude to Prof. K. Srinivas, Prof. T.R. Ramadas and Prof. M. Ram Murty. It would not have been possible to write this doctoral thesis without their immense support and help. Once again it is a pleasure to convey my gratitude to them all in my humble acknowledgment.

First of all, I wish to express my heartfelt gratitude to my supervisor Prof. K. Srinivas for accepting me as his PhD student and for giving me an opportunity to pursue research in mathematics. I am thankful to him for his inspiring guidance, strong motivation, important discussions, valuable advice and encouragement from the very early stage of this research and through out the research work. I am grateful to him for his patience to rectify my repeated mistakes during our discussions, sometimes I repeated the same mistake again and again. This thesis would not have been materialized without his guidance and encouragement. I also pay my sincere gratitude to his careful reading of our papers and meticulously going through the thesis.

I am grateful to Prof. T.R. Ramadas for being my faculty advisor throughout my PhD programme. I am humbled for his inspiring guidance and important advise at the right time. In particular, I am and I will remain obliged to him for strongly motivating me to discuss (anything I am working) with him even in his busy schedule and allowed me to do that. I thank him for allowing me to knock on his office door whenever I needed his help without prior appointment. I thank Prof. T.R. Ramadas for offering me to be his teaching assistant for two semesters. I acknowledge him with gratitude for supporting me financially through his J.C. Bose fellowship during the last one year of my PhD tenure. I sincerely acknowledge his help in careful reading of my PhD thesis and for making many useful comments.

I have no words to thank Prof. M. Ram Murty enough. I always wanted to be close to him. It was during a discussion with him when he suggested me to pursue this area of research which not only earned me my thesis but in fact, opened up new areas of research, which I will be pursuing in near future. His encouragement and guidance enabled me to complete this thesis . I learned quite a lot discussing with him during his several trips to India and also through e-mail correspondences. I am deeply grateful to Prof. M. Ram Murty for all these sustained supports. I feel blessed to be in his good-books.

I thank Prof. V. Kumar Murty for patiently listening to my presentations during our visit to Bhubaneswar. His encouraging words helped me in gaining confidence.

I thank Prof. Franz Lemmermayer and Prof. Stéphane Louboutin for their useful comments and suggestions. I thank Prof. B.V. Rao, Prof. Sridharan, Prof. Pramathanath Sastry , Prof. Shiva Shankar, Prof. V. Balaji, Prof. Senthamarai Kannan , Prof. Upendra Kulkarni, Prof. M. Sundari, Prof. Purusottam Rath, Prof. V. Indumathi and Prof. A. M. S. Ramasamy for their helpful guidance throughout my PhD programme.

I would like to thank Mr. Sripathy and CMI administrative staffs for their help and friendly atmosphere. I am especially thankful to Mr. Sripathy who helped me at all the times. I thank our librarian Ms. Rajeshwari Nair for her help all these years.

I thank my colleagues especially Sudhir Pujahari, Shivaji Das, Praveen Kumar, Sachin Pathak and Paramjit Singh who shared their valuable thoughts with healthy discussions on and off the subject matters. I am grateful to my friends Abhishek T Bharadwaj, Anbu Arjunan, Sarjick Bakshi, Navnath Daundkar, Mitra Koley, Naveen Kumar, S. P. Murugan Paramasivam, Pinakinath Saha, Praveen Kumar Roy, Shraddha Srivastava who provided me unconditional support at a time when I needed it most.

I sincerely thank the Institute of Mathematical Sciences, Chennai for allowing me to use their infrastructure and computer facilities. This has facilitated me in smoothly

carrying out my work.

I thank Department of Science and Technology, India and Infosys foundation for their financial support.

Last but far from the least I would like to thank my family members K. Muthukrishnan. M. Dhanalakshmi, P. Varalakshmi and M. Raju for their constant support and affection.

Contents

Chapter 1

Introduction

Euclid's algorithm plays central role in mathematics. For the ring of integers $\mathbb{Z}$, it says that given integers a and $b > 0$, we can always find integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

In other words, there exists a unique q such that $0 \leq a - bq < b$ holds. The important point is such a representation is unique. As a consequence of this algorithm, we have one of the most poetic statement in mathematics, namely the *fundamental theorem of arithmetic* which says that every positive integer $n > 1$ can be uniquely written as a product of primes. For a number field K with the ring of integers O_K, define the Euclidean function $\phi : O_K \to \mathbb{N} \cup \{0\}$ as follows:

1. $\phi(\alpha) = 0$ if and only if $\alpha = 0$, and
2. for all $\alpha, \beta \neq 0 \in O_K$ there exists a $\gamma \in O_K$ such that $\phi(\alpha - \beta\gamma) < \phi(\beta)$.

We say that K is Euclidean if such a function exists in O_K. In particular, if ϕ is the absolute value norm, then O_K is called norm-Euclidean. The immediate consequences of having a Euclidean function in an integral domain D , i.e., in a Euclidean domain, is that D is automatically a principal ideal domain, it is possible to compute the greatest common divisor of any two elements of D and so on. Thus, the study of classification of integral domains which are Euclidean is extremely important. It is a simple exercise to show that $\mathbb{Z}$ is Euclidean, so is $F[x]$, where F is a field.

If m is a negative squarefree integer, then the integral domain $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is norm-Euclidean if and only if $m = -1, -2$ and if in addition $m \equiv 1 \pmod 4$, then the integral domain $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{m})/2$ is norm-Euclidean if and only if $m = -3, -7, -11$. On the other hand to determine the positive squrefree integers m for which the integral domains $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ ($m \equiv 2, 3 \pmod 4$) and $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{m})/2$ ($m \equiv 1 \pmod 4$) is norm-Euclidean took considerable efforts of numerous mathematicians (see Ch 2, [1]). The complete classification was provided by Chatland and Davenport (see [3]). Their result is as follows: Let m be a positive squarefree integer with $m \equiv 2, 3 \pmod 4$, then $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is norm-Euclidean if and only if $m = 2, 3, 6, 7, 11, 19$ and if $m \equiv 1 \pmod 4$, then the integral domain $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{m})/2$ is norm-Euclidean if and only if $m = 5, 13, 17, 21, 29, 33, 37, 41, 57, 73$. Thus, for $K = \mathbb{Q}(\sqrt{m})$ the question whether O_K is Euclidean or not with respect to the norm function has been satisfactorily answered.

Suppose we know that an integral domain D is not norm-Euclidean, could it be Euclidean with respect to a different Euclidean function ϕ? In this direction D. A. Clark [5] showed that the integral domain $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{69})/2$ which is known to be *not* norm-Euclidean is in fact Euclidean with respect to infinitely many ϕ's! On the other hand one may ask whether there is a criteria to ensure that an integral domain D is not Euclidean with respect to any function ϕ. One of the ways of establishing this is to show if D is not a field and certain special elements called *universal side divisors* (see page 44, [1]) do not exist in D, then D is not Euclidean. Using this criteria, it can be proved that if m is negative squarefree integer with $m \equiv 2, 3 \pmod 4$ and $m < -2$, then $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is *not* Euclidean. Similarly if m is squarefree negative integer with $m \equiv 1 \pmod 4$ and

$m < -11$, then the integral domain $\mathbb{Z}+\mathbb{Z}(1+\sqrt{m})/2$ is *not* Euclidean with respect to any function ϕ. Thus for $K = \mathbb{Q}(\sqrt{m})$, d squarefree negative integer, the integral domain O_K is Euclidean if and only if $m = -1, -2, -3, -7, -11$.

On the other hand when m is a positive integer, very little is known regarding the Euclidean property in O_K with respect to ϕ different from norm function.

In 1949 Motzkin discovered an elegant criteria to determine when an integral domain is Euclidean. The next big step was taken by Weinberger, who in 1973 showed that assuming the truth of generalized Riemann Hypothesis (GRH) all algebraic number fields with infinitely many units and whose ring of integers are PIDs are in fact Euclidean! Thus, removing GRH was the next big challenge! This challenge was undertaken by Ram Murty and his school who made substantial contributions to this area of research. They showed that GRH can be removed provided the unit rank is at least three (see Theorem 3.1.3). They introduced the concept of *admissible* primes, which now proves to be an indispensable ingredient in the determination of Euclidean algorithm in algebraic number fields. It is interesting to note that the existence of non-Wieferich primes plays crucial role in the construction of *admissible* primes (see Chapter 3).

We make an extensive study of the concept of admissible primes and apply it to study the Euclidean algorithm in real quadratic fields and cyclic cubic fields. Basically, the thesis addresses the following questions:

Question 1. *Are there infinitely many non-Wieferich primes in O_K?*

Question 2. *What is the criteria to determine if a given number ring is Euclidean or not?*

Question 3. *Are there infinitely many real quadratic fields which are Euclidean?*

Question 4. *What is the criteria to show if a given cyclic cubic field with class number one is Euclidean or not?*

1.1 Main results

The thesis is organized as follows: Chapter 1 gives a brief introduction of the problems contained in the thesis and some preliminary results to understand the subsequent chapters. In Chapter 2, we address **Question 1** and prove the following theorems:

Theorem 1.1.1. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one and assume that the* abc *conjecture holds true in K. Then there are infinitely many non-Wieferich primes in O_K with respect to the unit ε satisfying $|\varepsilon| > 1$.*

Theorem 1.1.2. *Let K be any algebraic number field of class number one and assume that the* abc *conjecture holds true in K. Let η be a unit in O_K satisfying $|\eta| > 1$ and $|\eta^{(j)}| < 1$ for all $j \neq 1$, where $\eta^{(j)}$ is the jth conjugate of η. Then there exist infinitely many non-Wieferich primes in K with respect to the base η.*

Chapter 3 addresses **Question 3 &4**. In particular, the study the existence of admissible primes in any real quadratic field and explicit construction of admissible primes for a certain infinite family of real quadratic fields is discussed. The results contained in Chapter 3 are as follows:

Theorem 1.1.3. *Let L be a number field, and O_L be its ring of integers. If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are distinct, unramified prime ideals with odd prime norms q_1 and q_2 and if*

1. *ε has order $q_1(q_1 - 1)/2$ modulo $\mathfrak{q}_1^2$;*
2. *$q_1 \equiv 3 \ (mod\ 4)$;*
3. *$gcd(q_1(q_1 - 1)/2,\ q_2(q_2 - 1)) = 1$; and*
4. *ε has order $q_2(q_2 - 1)$ modulo $\mathfrak{q}_2^2$;*

then $O_L^\times$ maps onto $(O_L/\mathfrak{q}_1^2\mathfrak{q}_2^2)^\times$.

Theorem 1.1.4. *Assume the Hardy-Littlewood and the Wieferich primes conjectures. If K is a real quadratic field such that $\mathcal{O}_K$ has class number one, then $\mathcal{O}_K$ is Euclidean.*

Theorem 1.1.5. *Let $K = \mathbb{Q}(\sqrt{d})$ be as defined in* (3.2) *. Then there exists a set $\{\mathfrak{p}_g, \mathfrak{p}_y\}$ of two unramified prime ideals with odd prime norms p_1 and p_2 respectively such that the canonical map $\mathcal{O}_K^\times \to (\mathcal{O}_K/{\mathfrak{p}_g}^2{\mathfrak{p}_y}^2)^\times$ is surjective.*

Theorem 1.1.6. *There exists a family $C := \left\{\mathbb{Q}(\sqrt{d}) \ : \ d \text{ is prime}\right\}$ of real quadratic fields such that $\mathcal{O}_K$ is Euclidean if and only if it has class number one.*

The final Chapter 4 deals with **Question 4**. The main result of this chapter is the following:

Theorem 1.1.7. *Let K be a cyclic cubic field with conductor f, satisfying $73 \leq f \leq 11971$ and let $\mathcal{O}_K$ be its ring of integers. Then $\mathcal{O}_K$ is Euclidean if and only if it has class number one.*

1.2 Preliminaries

In this section we state some preliminary results (without proof) which are required to understand the technical details contained in this thesis. The interested reader may refer to any standard book in algebraic number theory e.g., [9], [**?**], [17].

Algebraic Number Fields

- Every Euclidean domain is a principal ideal domain. However, the converse is not true!
- The ring $\mathbb{Z}$ is Euclidean with respect to $\varphi(n) =\mid n \mid$.
- The polynomial ring $k[x]$ over a field k is Euclidean with respect to the function $\varphi(f(x)) = deg(f(x)) + 1$.

- Every ideal in a number ring O_K is uniquely representable as a product of prime ideals.

- For a rational prime p, consider the principal ideal pO_K in O_K. Then, we can write $pO_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ uniquely. Let f_i be the dimension of $O_K/\mathfrak{p}_i$ over $\mathbb{Z}/p\mathbb{Z}$. The numbers e_i and f_i are the ramification index and inertial degree respectively. For any number field K of degree n over $\mathbb{Q}$, the numbers e_i, f_i and n are related by the equation $\sum_{i=1}^{r} e_i f_i = n$.

- For a Galois extension K over $\mathbb{Q}$ we have $e := e_1 = e_2 = \cdots = e_r$ and $f := f_1 = f_2 = \cdots = f_r$ and hence $ref = n$.

- Let K be a quadratic number field , then the ring of integers O_K can be written as $O_K = \mathbb{Z} + \mathbb{Z}[\delta]$ for some algebraic integer δ. Denote by t and n the *trace* and *norm* of δ respectively. Let $p \in N$ be a prime, and let $v = 0, 1$ or 2 be the number of distinct solutions in $\mathbb{Z}/p\mathbb{Z}$ to the equation $x^2 - tx + n = 0$. Then the type of prime factorization of pO_K is determined by v and is given by :

  1. $v = 0$ *if and only if p is inert.*
  2. $v = 1$ *if and only if p is ramified.*
  3. $v = 2$ *if and only if p splits.*

Cyclotomic Fields

Let $\omega = e^{2\pi i/m}$. The m^{th} cyclotomic field is a number field of the form $\mathbb{Q}(\omega)$. It has degree $\phi(m)$ over $\mathbb{Q}$. The cyclotomic field is a Galois extension. The following fundamental facts are well known.

- The Galois group of the m^{th} cyclotomic field $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is $(\mathbb{Z}/m\mathbb{Z})^{\times}$. The ring of algebraic integers is equal to $\mathbb{Z}[\omega]$.

- (Prime Factorization in a cyclotomic field) Let K be a m^{th} cyclotomic field and p be a rational prime. Let $m = p^k n$ with $(p, n) = 1$. Then ramification index $e = \phi(p^k)$ and the intertial degree f is the multiplicative order of p modulo n.

- A rational prime $p \nmid m$ splits completely in K if and only if $p \equiv 1 \pmod{m}$. In general, p splits into $\phi(m)/f$ distinct primes.

Class Number

Let K be an algebraic number field and $\mathcal{O}_K$ be its ring of integers. Recall that a fractional ideal is a finitely generated $\mathcal{O}_K$ submodule of K. Let $\mathfrak{M}, \mathfrak{N}$ be two fractional ideals. Their product $\mathfrak{M}\mathfrak{N}$ is the collection of all finite sums of the form $\mathfrak{m}\mathfrak{n}$ where $\mathfrak{m} \in \mathfrak{M}, \mathfrak{n} \in \mathfrak{N}$. The inverse of a fractional ideals $\mathfrak{M}$ is defined as the set $\{\alpha \in K : \alpha\mathfrak{M} \subset \mathcal{O}_K\}$. It is a well known fact that the set of all fractional ideals is a group with respect to this product.

Let $\mathcal{F}(K)$ be the group of all fractional ideals and $\mathcal{P}(K)$ be the subgroup of all principal fractional ideals. Then the quotient group

$$Cl(K) := \mathcal{F}(K)/\mathcal{P}(K)$$

is called the *class group* of K. The class group is a finite abelian group. The cardinality of the class group is called the *class number* and it is denoted by $h(K)$. It is an easy exercise to show that K has class number one iff it is a principal ideal domain (PID).

Valuations of a number field

A function $v : K - \{0\} \to \mathbb{R}$ is called an *absolute value* on K, if the following conditions holds true.

- $v(x) \geq 0$,

- $v(xy) = v(x)v(y)$,

- there exists a constant C such that $v(x + y) \leq C\ max\{v(x), v(y)\}$,

for all $x, y \in K$.

Two absolute values v and v' defined on K are said to be equivalent if $v(x) < 1$ holds if and only if $v'(x) < 1$ for all $x \in K$.

A *valuation* v on K is an absolute value and it satisfies triangle inequality. i.e., $v(x + y) \leq v(x) + v(y)$. In addition, if $C = 1$ in the above definition it is called *nonarchimedean* valuation. Otherwise it is called *archimedean*.

Let $\mathfrak{p}$ be a prime ideal in O_K and $v_\mathfrak{p}(x)$ be the exponent of $\mathfrak{p}$ in the ideal factorization of (x). For $c \in (0, 1)$, define the map $|\ .\ |_\mathfrak{p}$: $K \longrightarrow \mathbb{R}$ as $|\ 0\ |_\mathfrak{p} = 0$ and $|\ x\ |_\mathfrak{p} = c^{-v_\mathfrak{p}(x)}$ for all $x \in K$.

An equivalence class of valuations on a field K is called a *prime* of K. An equivalence class of archimedean valuations is called an *infinite* prime and an equivalence class of non-archimedean valuations is called a *finite* prime. A finite prime is equal to $|\ .\ |_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$.

Dirichlet Unit Theorem

Let us label the embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n$ of K into $\mathbb{C}$ in such a way that $\sigma_1, \sigma_2, \ldots, \sigma_r$ are real embeddings and $\sigma_{r+1}, \sigma_2, \ldots, \sigma_{r+2s}$ are complex embeddings and $\sigma_{r+i} = \bar{\sigma}_{r+i+1}$ for all $1 \leq i \leq r + 2s - 1$. Then the *Dirichlet unit theorem* is the following statement:

Let K be an algebraic number field of degree n. Let r be the number of real conjugate fields of K and $2s$ the number of complex conjugate fields of K so that r and s satisfy $r + 2s = n$. Then O_K contains $r + s - 1$ units $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ such that each unit of O_K can be expressed uniquely in the form $\rho\varepsilon_1^{n_1} \ldots \varepsilon_{r+s-1}^{n_{r+s-1}}$ where ρ is a root of unity in O_K and $n_1, ..., n_{r+s-1}$ are integers.

Chapter 2

Non-Wieferich primes and abc conjecture

2.1 Introduction

An odd rational prime p is called a Wieferich prime if

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{2.1}$$

A. Wieferich [**?**] proved that if an odd prime p is a non-Wieferich prime, i.e., p satisfies

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

then there are no integer solutions to the Fermat equation $x^p + y^p = z^p$, with $p \nmid xyz$. The known Wieferich primes are 1093 and 3511 and according to the PrimeGrid project [**?**], these are the only Wieferich primes less than 17×10^{15}. One of the unsolved problems in this area of research is to determine whether the number of Wieferich or non-Wieferich primes is finite or infinite. Instead of the base 2 if we take any base a, then p is said to be a Wieferich prime with respect to the base a if

$$a^{p-1} \equiv 1 \pmod{p^2}, \tag{2.2}$$

and if the congruence (2.2) does not hold then we shall say that p is non-Wieferich prime to the base a. Assuming the truth of famous *abc* conjecture (defined below), J. H. Silverman [**?**] proved that given any integer a, there are infinitely many non-Wieferich primes to the base a. He established this result by showing that for any fixed $\alpha \in \mathbb{Q}^{\times}, \alpha \neq \pm 1$, and provided the *abc* conjecture holds,

$$\operatorname{card}\left\{p \leq x : \alpha^{p-1} \not\equiv 1 \pmod{p^2}\right\} \gg_{\alpha} \log x \quad \text{as} \quad x \to \infty.$$

In [10] Hester Graves and M. Ram Murty extended this result to primes in arithmetical progression by showing that for any $a \geq 2$ and any fixed $k \geq 2$, there are $\gg \log x / \log\log x$ primes $p \leq x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of *abc* conjecture.

In this chapter, we study non-Wieferich primes in algebraic number fields of class number one. This chapter is based on the paper [**?**]. More precisely, we prove the following

Theorem 2.1.1. *Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one and assume that the* abc *conjecture holds true in K. Then there are infinitely many non-Wieferich primes in O_K with respect to the unit ε satisfying $|\varepsilon| > 1$.*

Theorem 2.1.2. *Let K be any algebraic number field of class number one and assume that the* abc *conjecture holds true in K. Let η be a unit in O_K satisfying $|\eta| > 1$ and $|\eta^{(j)}| < 1$ for all $j \neq 1$, where $\eta^{(j)}$ is the jth conjugate of η. Then there exist infinitely many non-Wieferich primes in K with respect to the base η.*

2.2 The *abc*-conjecture

The *abc*-conjecture propounded by Oesterlé and Masser (1985) states that given any $\delta > 0$ and positive integers a, b, c such that $a + b = c$ with $(a, b) = 1$, we have

$$c \ll_\delta (\mathrm{rad}(abc))^{1+\delta},$$

where $\mathrm{rad}(abc) := \prod_{p|abc} p$.

The *abc* conjecture has several applications, the reader may refer to [**?**], [13], [**?**], [**?**] for details.

To state the analogue of *abc*-conjecture for number fields, we need some preparations, which we do below. ([**?**], [13] for more details.)

Let K be an algebraic number field and let V_K denote the set of primes on K, that is, any v in V_K is an equivalence class of norm on K (finite or infinite). Let $\|x\|_v := N_{K/\mathbb{Q}}(\mathfrak{p})^{-v_\mathfrak{p}(x)}$, if v is a prime defined by the prime ideal $\mathfrak{p}$ of the ring of integers O_K in K and $v_\mathfrak{p}$ is the corresponding valuation, where $N_{K/\mathbb{Q}}$ is the absolute value norm. Let $\|x\|_v := |g(x)|^e$ for all non-conjugate embeddings $g : K \to \mathbb{C}$ with $e = 1$ if g is real and $e = 2$ if g is complex. Define the height of any triple $a, b, c \in K^\times$ as

$$H_K(a, b, c) := \prod_{v \in V_K} max(\|a\|_v, \|b\|_v, \|c\|_v),$$

and the radical of (a, b, c) by

$$\mathrm{rad}_K(a, b, c) := \prod_{\mathfrak{p} \,\in\, I_K(a,b,c)} N_{K/\mathbb{Q}}(\mathfrak{p})^{v_\mathfrak{p}(p)},$$

where p is a rational prime with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ and $I_K(a, b, c)$ is the set of all primes $\mathfrak{p}$ of O_K for which $\|a\|_v, \|b\|_v, \|c\|_v$ are not equal.

The abc conjecture for algebraic number fields is stated as follows: For any $\delta > 0$, we have

$$H_K(a, b, c) \ll_{\delta,K} (\mathrm{rad}_K(a, b, c))^{1+\delta}, \tag{2.3}$$

for all $a, b, c, \in K^\times$ satisfying $a + b + c = 0$, the implied constant depends on K and δ.

2.3 Wieferich/non-Wieferich primes in number fields

Let K be an algebraic number field and O_K be its ring of integers. A prime $\pi \in O_K$ is called Wieferich prime with respect to the base $\varepsilon \in O_K^*$ if

$$\varepsilon^{N(\pi)-1} \equiv 1 \pmod{\pi^2}, \tag{2.4}$$

where $N(.)$ is the absolute value norm. If the congruence (2.4) does not hold for a prime $\pi \in O_K$, then it is called non-Wieferich prime to the base ε.

Notation: In this chapter, ε will denote a unit in O_K and we shall write $\varepsilon^n - 1 = u_n v_n$, where u_n is the square free part and v_n is the squarefull part, i.e., if $\pi | v_n$ then $\pi^2 | v_n$. We shall denote absolute value norm on K by N.

2.4 Proof of theorem (2.1.1)

Let $K = \mathbf{Q}(\sqrt{m}), m > 0$ be a real quadratic field and O_K be its ring of integers. Let $\varepsilon \in O_K^\times$ be a unit with $|\varepsilon| > 1$. The results of Silverman [**?**], Ram Murty and Hester [10] quoted in the introduction use a key lemma of Silverman (Lemma 3, [**?**]). We first derive an analogue of Silverman's lemma for number fields which will play a fundamental role in the proof of the main theorems.

Lemma 2.4.1. *Let $K = \mathbf{Q}(\sqrt{m})$ be a real quadratic field of class number one. Let*

$\varepsilon \in O_K^\times$ be a unit. If $\varepsilon^n - 1 = u_n v_n$, then every prime divisor π of u_n is a non-Wieferich prime with respect to the base ε.

Proof. The assumption that K has class number one allows us to write the element $\varepsilon^n - 1 \in O_K$ as a product of primes uniquely. Accordingly, we shall write

$$\varepsilon^n - 1 = u_n v_n$$

for $n \in \mathbb{N}$. Then

$$\varepsilon^n = 1 + \pi w, \tag{2.5}$$

with $\pi | u_n$ and π and w are coprime. As π is a prime, we have $N(\pi) = p$ or p^2, p is a rational prime.

Case (1): Suppose $N(\pi) = p$.

From equation (2.5), we get

$$\varepsilon^{n(p-1)} \equiv 1 + (p-1)\pi w \not\equiv 1 \pmod{\pi^2}.$$

Case (2): Suppose $N(\pi) = p^2$.

Again from equation (2.5), we obtain

$$\varepsilon^{n(p^2-1)} = \varepsilon^{n(N(\pi)-1)} = (1+\pi w)^{(p^2-1)} \equiv 1 + \pi w(p^2-1) \not\equiv 1 \pmod{\pi^2}.$$

Thus in either case,

$$\varepsilon^{(N(\pi)-1)} \not\equiv 1 \pmod{\pi^2},$$

and hence π is a non-Wieferich prime to the base ε.

The above lemma shows that whenever a prime π divides u_n for some positive integer n, then π is a non-Wieferich prime with respect to the base ε. Thus, if we can show that the set $\{N(u_n) : n \in \mathbb{N}\}$ is unbounded, then this will imply that the set $\{\pi : \pi | u_n, n \in \mathbb{N}\}$ is an infinite set. Consequently, this establishes the fact that there are infinitely many non-Wieferich primes in every real quadratic field of class number one with respect to the unit ε, with $|\varepsilon| > 1$. Therefore, we need only to show the following

Lemma 2.4.2. *Let $\mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one. Let $\varepsilon \in O_K^\times$ be a unit with $|\varepsilon| > 1$. Then under abc-conjecture for number fields, the set $\{N(u_n) : n \in \mathbb{N}\}$ is unbounded.*

Proof. Invoking the *abc*-conjecture (2.3) to the equation

$$\varepsilon^n = 1 + u_n v_n \tag{2.6}$$

yields

$$|\varepsilon^n| \ll \Big(\prod_{\mathfrak{p}|u_n v_n} N(\mathfrak{p})^{v_\mathfrak{p}(p)}\Big)^{1+\delta} = \left(\prod_{\mathfrak{p}|u_n} N(\mathfrak{p})^{v_\mathfrak{p}(p)} \prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{v_\mathfrak{p}(p)} \right)^{1+\delta} \tag{2.7}$$

for some $\delta > 0$. Here the implied constant depends on K and δ.

As $v_\mathfrak{p}(p) \leq 2$ for any prime ideal $\mathfrak{p}$ lying above the rational prime p, we have

$$\prod_{\mathfrak{p}|u_n} N(\mathfrak{p})^{v_\mathfrak{p}(p)} \leq N(u_n)^2. \tag{2.8}$$

For a prime ideal $\mathfrak{p}|v_n$, let $e_\mathfrak{p}$ be the largest exponent of $\mathfrak{p}$ dividing v_n, i.e., $\mathfrak{p}^{e_\mathfrak{p}} || v_n$. As v_n is the square-full part of $\varepsilon^n - 1$, we have $e_\mathfrak{p} \geq 2$. Hence,

1. $N(\mathfrak{p})^{2v_\mathfrak{p}(p)} \leq N(\mathfrak{p})^{2+e_\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ with $v_\mathfrak{p}(p) = 2$.

2. $N(\mathfrak{p})^{2v_\mathfrak{p}(p)} \leq N(\mathfrak{p})^{e_\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ with $v_\mathfrak{p}(p) = 1$.

Thus

$$\begin{aligned}\prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{2v_{\mathfrak{p}}(p)} &\leq \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{2+e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \\ &\leq \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{2} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \\ &\leq {\prod_{\mathfrak{p}}}' N(\mathfrak{p})^{2} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=2}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p}|v_n \\ v_{\mathfrak{p}}(p)=1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)},\end{aligned}$$

where $'$ indicates that the product is over all primes $\mathfrak{p}$ in O_K such that $v_{\mathfrak{p}}(p) = 2$. As it is well known that there are only finitely many ramified primes in a number field, it follows that the product is bounded by a constant A (say). Thus, we have

$$\prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leq \sqrt{AN(v_n)}. \tag{2.9}$$

Combining equations (2.7), (2.8) and (2.9), we get

$$|\varepsilon^n| \ll \left(N(u_n)^2 \sqrt{N(v_n)}\right)^{1+\delta}. \tag{2.10}$$

Now, as $|\varepsilon| > 1$,

$$N(u_n)N(v_n) = N(\varepsilon^n - 1) \leq 2|\varepsilon^n - 1| < 2|\varepsilon|^n,$$

i.e.,

$$N(v_n) < 2|\varepsilon|^n / N(u_n).$$

Substituting the above expression in (2.10), we obtain

$$|\varepsilon^n| \ll \left(N(u_n)^2 \frac{|\varepsilon|^{n/2}}{\sqrt{N(u_n)}}\right)^{(1+\delta)}.$$

Thus,

$$(N(u_n))^{\frac{3(1+\delta)}{2}} \gg |\varepsilon|^{\frac{n(1-\delta)}{2}}.$$

Thus, for a fixed δ, $N(u_n) \to \infty$ as $n \to \infty$. This proves the lemma and completes the proof of the theorem.

2.5 Non-Wieferich primes in algebraic number fields

In this section, we generalize the arguments of previous section to arbitrary number fields. In this section, K will always denote an algebraic number field of degree $[K : \mathbb{Q}] = l$ over $\mathbb{Q}$ of class number one. Let r_1 and r_2 be the number of real and non-conjugate complex embeddings of K into $\mathbb{C}$ respectively, so that $l = r_1 + 2r_2$. We begin with an analogue of Lemma (2.4.1).

Lemma 2.5.1. *Let ε be a unit in O_K. If $\varepsilon^n - 1 = u_n v_n$, then every prime divisor π of u_n is a non-Wieferich prime with respect to the base ε.*

Proof. Let $N(\pi) = p^k$, where p is a rational prime and k is a positive integer. Then

$$\varepsilon^{n(N(\pi)-1)} = \varepsilon^{n(p^k-1)} = (1 + w\pi)^{(p^k-1)} \equiv 1 + (p^k - 1)w\pi \not\equiv 1 \pmod{\pi^2}.$$

This implies $\varepsilon^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}$.

Thus, the lemma shows that π is a non-Wieferich prime to the base ε whenever the hypothesis of the lemma is met. Now, under the *abc* conjecture for number fields, we show below the existence of infinitely many non-Wieferich primes.

Lemma 2.5.2. *The set $\{N(u_n) : n \in \mathbb{N}\}$ is unbounded, where u_n's are as defined in Lemma* (2.5.1).

Proof. By the hypothesis of the lemma, we have $\varepsilon^n = 1 + u_n v_n$, where $\varepsilon^n, 1, u_n v_n \in K^* := K - \{0\}$. Applying the *abc* conjecture for number fields to the above equation, we obtain

$$\prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v) \ll (\prod_{\mathfrak{p} | u_n v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)})^{1+\delta}, \tag{2.11}$$

for some $\delta > 0$.

Note that for the absolute value $|.|$ in V_K, we have

$$|\varepsilon^n| \leq \prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v). \tag{2.12}$$

As $v_{\mathfrak{p}}(p) \leq l$ for any prime ideal $\mathfrak{p}$ lying above the rational prime p, we have

$$\prod_{\mathfrak{p} | u_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leq N(u_n)^l. \tag{2.13}$$

As before, we denote by $e_{\mathfrak{p}}$ the largest exponent of $\mathfrak{p}$ which divides v_n, i.e., $\mathfrak{p}^{e_{\mathfrak{p}}} \| v_n$. Clearly $e_{\mathfrak{p}} \geq 2$. Then

$$\begin{aligned}
\prod_{\mathfrak{p} | v_n} N(\mathfrak{p})^{2 v_{\mathfrak{p}}(p)} &\leq \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) \geq 2}} N(\mathfrak{p})^{2l + e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \\
&\leq \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) \geq 2}} N(\mathfrak{p})^{2l} \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) \geq 2}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \\
&\leq {\prod_{\mathfrak{p}}}' N(\mathfrak{p})^{2l} \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) \geq 2}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)} \prod_{\substack{\mathfrak{p} | v_n \\ v_{\mathfrak{p}}(p) = 1}} N(\mathfrak{p})^{e_{\mathfrak{p}}(p)},
\end{aligned}$$

where $'$ indicates that the product is over all primes $\mathfrak{p}$ in O_K such that $v_{\mathfrak{p}}(p) \geq 2$. As there are only finitely many ramified primes in a number field, it is bounded by a constant B (say). Thus, we have

$$\prod_{\mathfrak{p}|v_n} N(\mathfrak{p})^{v_{\mathfrak{p}}(p)} \leq \sqrt{BN(v_n)}. \tag{2.14}$$

Therefore, the equations (2.11) - (2.14) yield

$$|\varepsilon^n| \ll \left(N(u_n)^l \sqrt{N(v_n)}\right)^{1+\delta}. \tag{2.15}$$

Note that in the case of real quadratic fields, the unit ε satisfies $|\varepsilon| > 1$ and this information was crucial in proving Theorem 2.1.1. However, in the case of general number fields, the following result (see Lemma 8.1.5, [9]) comes to our rescue. We state this result as

Lemma 2.5.3. *Let $E = \{k \in \mathbb{Z} : 1 \leq k \leq r_1 + r_2\}$. Let $E = A \cup B$ be a proper partition of E. There exists a unit $\eta \in \mathcal{O}_K$ with $|\eta^{(k)}| < 1$, for $k \in A$ and $|\eta^{(k)}| > 1$, for $k \in B$.*

Taking $A = \{k : 1 < k \leq r_1 + r_2\}$ and $B = \{1\}$, Lemma 2.5.3 produces a unit $\eta \in \mathcal{O}_K^\times$ such that $|\eta| > 1$ and $|\eta^{(k)}| < 1$, where $\eta^{(k)}$ denotes the k^{th} conjugate of $\eta, k \neq 1$. Since, every unit satisfies (2.15), replacing ε with η in (2.15), we obtain

$$|\eta^n| \ll \left(N(u_n)^l \sqrt{N(v_n)}\right)^{1+\delta}, \tag{2.16}$$

where, by abuse of notation, we shall denote $\eta^n - 1 = u_n v_n$, with u_n and v_n denoting the same quantities as defined earlier.

Now,

$$N(u_n)N(v_n) = N(\eta^n - 1) = (\eta^n - 1)(\eta^{(2)n} - 1)(\eta^{(3)n} - 1)\cdots(\eta^{(l)n} - 1).$$

By Lemma 2.5.3, $|\eta^{(j)n} - 1| < 2$ for all $j, 2 \leq j \leq l$.

Thus,

$$N(u_n)N(v_n) < C|\eta^n| \qquad \text{or} \qquad N(v_n) < C|\eta^n|/N(u_n).$$

Now, (2.16) can be written as

$$(N(u_n))^{\frac{(2l-1)(1+\delta)}{2}} \gg |\eta|^{n\frac{1-\delta}{2}}. \tag{2.17}$$

For a fixed δ, the right hand side of (2.17) tends to ∞ as $n \to \infty$. Therefore the set $\{N(u_n) : n \in \mathbb{N}\}$ is unbounded. This shows that there are infinitely many non-Wieferich primes in K with respect to the base η.

Chapter 3

Admissible primes and Euclidean quadratic fields

3.1 Introduction

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. Recall that a number ring $\mathcal{O}_K$ is called Euclidean with respect to a given function $\phi : \mathcal{O}_K \to \mathbb{N} \cup \{0\}$ if ϕ has the following properties

1. $\phi(\alpha) = 0$ if and only if $\alpha = 0$, and
2. for all $\alpha, \beta \neq 0 \in \mathcal{O}_K$ there exists a $\gamma \in \mathcal{O}_K$ such that $\phi(\alpha - \beta\gamma) < \phi(\beta)$.

In particular, if ϕ is the absolute value norm, then $\mathcal{O}_K$ is called norm-Euclidean.

It is easy to show that if $\mathcal{O}_K$ is Euclidean then $\mathcal{O}_K$ is a principal ideal domain so that its class number is one. The converse, however, is not true. Indeed, in 1949, Motzkin [**?**] derived a useful criterion for any ring to be Euclidean and using it, he showed that the ring of integers of $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67$ and 163 are not Euclidean, though they all have class number one. As there are only nine imaginary quadratic fields with class number one, Motzkin's paper shows that only five of these are Euclidean (and in fact, they are all norm-Euclidean). Are there any other examples of rings O_K with class number one which are **not** Euclidean? In 1973, Weinberger [**?**] showed that if we assume the generalized Riemann hypothesis (GRH), there are no more counterexamples. In other words, apart from the five imaginary quadratic fields found by Motzkin, there are no further examples of O_K having class number one and not being Euclidean, if we believe in the GRH! This surprising result makes one wonder how an analytic hypothesis can lead to such an algebraic result and if the use of the GRH in such questions is necessary. Such a program of research was initiated by M. Ram Murty and his school. We will describe their results below.

Determining all norm-Euclidean quadratic number fields is a classical problem that has received a lot of attention. The situation for imaginary quadratic fields has been described above. It is known that $\mathbb{Q}(\sqrt{d})$, $d > 0$ is norm-Euclidean if and only if $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Thus, we have a complete list of quadratic number fields which are Euclidean with respect to the absolute value norm. We refer the reader to [19] for a survey of these classical results.

Thus, it is an interesting question to ask whether or not a given real quadratic field is Euclidean with respect to a function different from the absolute value norm. As indicated earlier, in 1949, Motzkin [**?**] proved a fundamental result which gives a criterion for an integral domain to be Euclidean. His result is the following:

Let R be an integral domain. Define the sets E_k, $k \geq 0$, as follows:
Let $E_0 := \{0\}$, $E_k := \{0\} \cup \{\alpha \in R$: *each residue class mod* α *contains* $\beta \in E_{k-1}\}$, *for* $k \geq 1$. *Then, R is Euclidean if and only if* $\cup_{k\geq 0} E_k = R$.

As an application of Motzkin's contruction, one obtains that if $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, then O_K is Euclidean if and only if $d = -1, -2, -3, -7, -11$, which is the classical result mentioned in the beginning. But, it seems difficult to use Motzkin's construction directly for real quadratic fields due to the presence of infinitely many units! However, with the additional assumption of the generalized Riemann hypothesis (GRH), Weinberger proved that O_K is Euclidean if and only if it has class number one [**?**] by adapting an argument of Hooley [16] used in his solution of the Artin primitive root conjecture. On the other hand, for a certain class of integers, called S-integers (defined below) R. Gupta, M. Ram Murty and V. Kumar Murty [12] established that the ring of S-integers is Euclidean if and only if O_S is a PID without the use of the GRH. Here is a precise statement of their result.

Let S be a finite set of places of K containing the infinite places S_∞. An element x of K is called an S-integer if $ord_{\mathfrak{p}}(x) \geq 0$ for all primes $\mathfrak{p}$ of K not in S. Let O_S denote the ring of S-integers. Let $g := gcd\,\{N_{K/\mathbb{Q}}(\mathfrak{p}) - 1 : \mathfrak{p} \in S - S_\infty\}$. Then

Theorem 3.1.1. *(R. Gupta, M. Ram Murty, V. Kumar Murty) [12]*

Let K be Galois over $\mathbb{Q}$ and that

1. $|S| \geq max\,\{5, 2[K : \mathbb{Q}] - 3\}$;
2. *K has a real embedding or $\zeta_g \in K$.*

If O_S is a PID, then it is Euclidean.

Though their work initiated a method of removing GRH from these questions, it could not be applied to study the rings O_K.

In 1995, M. Ram Murty and David A. Clark [4] developed a new criteria for the existence of a Euclidean algorithm to hold in a general number ring. In order to state their result (see Theorem 3.1.2), we need the concept of an *admissible* set of primes in O_K which we define in what follows.

Assume that O_K has class number one. Let $\pi_1, \ldots, \pi_s \in O_K$ be distinct non-associate primes. A set of primes $\{\pi_1, \ldots, \pi_s\}$ is called an *admissible* set of primes if, for all

$\beta = \pi_1^{a_1} \ldots \pi_s^{a_s}$ with a_i non-negative integers, every co-prime residue class $\pmod{\beta}$ can be represented by a unit $\varepsilon \in O_K^{\times}$. In other words, the set $\{\pi_1, \ldots, \pi_s\}$ is *admissible* if the canonical map $O_K^{\times} \to (O_K/(\pi_1^{a_1} \ldots \pi_s^{a_s}))^{\times}$ is surjective.

In [4], D.A. Clark and M. Ram Murty showed that it is enough to take $a_1 = a_2 = \cdots = a_s = 2$ in the above definition, (i.e,. the set $\{\pi_1, \ldots, \pi_s\}$ is *admissible* if the canonical map $O_K^{\times} \to (O_K/(\pi_1^2 \ldots \pi_s^2))^{\times}$ is a surjective).

Using this concept, Clark and Murty proved:

Theorem 3.1.2. *(M. Ram Murty, David A. Clark) [4] Let K be a totally real Galois extension with degree n_K such that O_K has class number one. Suppose that O_K has a set S of admissible primes with $m = |n_K - 4| + 1$ elements, then O_K is Euclidean.*

When $K/\mathbb{Q}$ is abelian, M. Ram Murty and M. Harper obtained a more precise and useful criteria which we state below.

Theorem 3.1.3. *(M. Ram Murty, M. Harper) [**?**] Let $K/\mathbb{Q}$ be abelian of degree n with O_K having class number one, that contains a set of admissible primes with s elements. Let r be the rank of the unit group. If $r + s \geq 3$, then O_K is Euclidean.*

There are other notable results in [**?**]. Specifically, Harper and Murty show that if $K/\mathbb{Q}$ is a finite Galois extension with unit rank > 3, then O_K is Euclidean if and only if O_K is a PID. This still leaves open the discussion for fields of small degree, in particular, real quadratic fields. This will be the focus of this paper.

For real quadratic fields, $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, it is therefore enough to exhibit the existence of an *admissible* set having two elements, as in this case the rank of the unit group is one. Harper [14] proved that $\mathbb{Z}[\sqrt{14}]$ is Euclidean, by exhibiting the set $\{5 - \sqrt{14}, 3 - 2\sqrt{14}\}$ as an *admissible* set of primes. Additionally, in his thesis M. Harper also established that all the real quadratic fields with discriminant ≤ 500 and having class number one are Euclidean. Thus, the explicit construction of admissible primes is of independent interest in its own right and it is the purpose of this paper to construct a set of admissible primes for an infinite family of real quadratic fields. It is possible that this family contains infinitely many with class number one and we give some reasons at the end of the chapter for this belief.

In this context, two famous conjectures have some bearing on our goals. The first concerns the Hardy-Littlewood conjecture. Fix a natural number r and b coprime to r. Hardy and Littlewood conjectured that the number of primes $p \leq x$ with $p \equiv b \pmod r$ such that $2p + 1$ is also prime is

$$\frac{x}{\log^2 x}.$$

The second conjecture we need is an estimate for the number of Wieferich primes. We call this the Wieferich primes conjecture. Though this is generally believed, we have not found a precise formulation of it in the literature so we give one here. Let ε be an element of $O_K^\times$ of infinite order. The number of primes $p \leq x$ such that

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

is $o(x/\log^2 x)$. Both of these conjectures are unproven though sieve theory has made some progress towards the Hardy-Littlewood conjecture. They will be relevant to our discussion below.

The content of this chapter are taken from our paper [**?**].

3.2 Statement of the theorems

The following result is inspired from the work in [**?**], which we state as

Theorem 3.2.1. *Let L be a number field, and O_L be its ring of integers. If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are distinct, unramified prime ideals with odd prime norms q_1 and q_2 and if*

1. *ε has order $q_1(q_1-1)/2$ modulo $\mathfrak{q}_1^2$;*

2. *$q_1 \equiv 3$ (mod 4);*

3. *$gcd(q_1(q_1-1)/2,\ q_2(q_2-1)) = 1$; and*

4. *ε has order $q_2(q_2-1)$ modulo $\mathfrak{q}_2^2$;*

then $O_L^\times$ maps onto $(O_L/\mathfrak{q}_1^2\mathfrak{q}_2^2)^\times$.

Proof: We shall use the notation $G = \langle g \rangle$ to mean that g generates the group G.

Let

$$\beta := \varepsilon^{q_1(q_1-1)/2}.$$

By (3) and (4), it follows that

$$\langle \beta \rangle = (O_L/\mathfrak{q}_2^2)^\times.$$

On the other hand by (1), we have

$$\beta \equiv 1 \pmod{\mathfrak{q}_1^2}.$$

Since β generates the group $(O_L/\mathfrak{q}_2^2)^\times$ and the image of ε lies in $(O_L/\mathfrak{q}_2^2)^\times$, there exists a positive integer k such that

$$(\beta^k)(-\varepsilon) \equiv 1 \pmod{\mathfrak{q}_2^2}.$$

i.e., β^k is the inverse of $-\varepsilon$ modulo $\mathfrak{q}_2^2$.

Now, let

$$\alpha := -\beta^k \varepsilon.$$

Then by the above congruence, we have

$$\alpha \equiv 1 \pmod{\mathfrak{q}_2^2}.$$

Also,

$$\alpha \equiv -\varepsilon \pmod{\mathfrak{q}_1^2},$$

thus by (1), α generates the group $(\mathcal{O}_L/\mathfrak{q}_1^2)$. By the Chinese remainder theorem

$$(\mathcal{O}_L/\mathfrak{q}_1^2\mathfrak{q}_2^2)^\times \simeq (\mathcal{O}_L/\mathfrak{q}_1^2)^\times \times (\mathcal{O}_L/\mathfrak{q}_2^2)^\times.$$

Let $(x, y) \in (\mathcal{O}_L/\mathfrak{q}_1^2)^\times \times (\mathcal{O}_L/\mathfrak{q}_2^2)^\times$. Then there exist positive integers e, f such that

$$\alpha^e \equiv x \pmod{\mathfrak{q}_1^2} \quad \text{and} \quad \beta^f \equiv y \pmod{\mathfrak{q}_2^2}.$$

Now the element $z := \alpha^e\beta^f$ maps onto the element (x, y). Since (x, y) was arbitrary, the canonical map takes $\mathcal{O}_L^\times$ onto $(\mathcal{O}_L/\mathfrak{q}_1^2\mathfrak{q}_2^2)^\times$.

In particular, we can use the previous theorem to produce admissible primes for any real quadratic field.

Theorem 3.2.2. *Assume the Hardy-Littlewood and the Wieferich primes conjectures. If K is a real quadratic field such that $\mathcal{O}_K$ has class number one, then $\mathcal{O}_K$ is Euclidean.*

Proof. The strategy is as follows. We want to select two primes q_1, q_2 satisfying the conditions of our previous theorem and then apply Theorem 3.1.3. The Hardy-Littlewood conjecture predicts that there are

$$\gg \frac{x}{\log^2 x}$$

primes such that $2q_1 + 1$ is also a prime p (say). Let ε be a fundamental unit of $\mathcal{O}_K$. If we want ε to be a square mod p, we want

$$\varepsilon^{(p-1)/2} \equiv 1(\bmod p). \tag{3.1}$$

But this means that p splits in the quadratic field $K(\sqrt{\varepsilon})$ which is an abelian extension of $\mathbb{Q}$. By the Kronecker-Weber theorem, it is contained in a cyclotomic extension $\mathbb{Q}(\zeta_r)$ for some primitive r-th root of unity ζ_r. The condition 3.1 above is equivalent to saying that p lies in a certain arithmetic progression (mod r). By the Hardy-Littlewood conjecture, the number of primes $p \leq x$ such that $2p + 1$ is prime and p splits in $K(\sqrt{\epsilon})$ is

$$\gg \frac{x}{\log^2 x}.$$

Let us call this set T_x. A similar estimate holds for the number of such primes for which ϵ is not a quadratic residue (mod p). Let us call this set S_x. By the Wieferich primes conjecture, the number of primes $p \leq x$ such that

$$\varepsilon^{p-1} \equiv 1(\bmod p^2),$$

is $o(x/\log^2 x)$ and so, after removing these primes from T_x and S_x (if necessary), we deduce that the number of primes in each of these sets is $\gg x/\log^2 x$. These are also disjoint sets on account of the splitting and non-splitting conditions. Let $p_1 \in T_x$ and $p_2 \in S_x$ and write $q_1 = 2p_1+1, q_2 = 2p_2+1$. Then, clearly, $\gcd(q_1(q_1-1)/2, q_2(q_2-1)) = \gcd(q_1p_1, 2q_2p_2)$=1 and it is easily checked that all the conditions of the theorem are satisfied. Finally, we need only apply the theorem of Harper and Murty to deduce the final conclusion. □

3.3 Explicit constructions

Now we give an explicit construction of admissible primes for a certain infinite family of real quadratic fields.

Fix two primes $p_1 := 11$ and $p_2 := 13$. Let

$$d := (a+1)^2 b^2 n^2 + 2(a+1)^2 n + 23 \tag{3.2}$$

where a, b, n are integers such that

$$a \equiv 24 \pmod{p_1^3 p_2^3},\ b \equiv 5 \pmod{p_1^3 p_2^3}, \tag{3.3}$$

and

$$n \equiv 0 \ (\mathrm{mod}\ p_1 p_2).$$

We define

$$K := \mathbb{Q}(\sqrt{d}) = \mathbb{Q}\Big(\sqrt{((a+1)^2 b^2 n^2 + 2(a+1)^2 n + 23)}\Big). \tag{3.4}$$

With the above notations, we state the main theorems of this chapter as follows.

Theorem 3.3.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be as defined above. Then there exists a set $\{\mathfrak{p}_g, \mathfrak{p}_y\}$ of two unramified prime ideals with odd prime norms p_1 and p_2 respectively such that the canonical map $O_K^\times \to (O_K/{\mathfrak{p}_g}^2{\mathfrak{p}_y}^2)^\times$ is surjective.*

As a consequence of Theorem (3.3.1) we deduce:

Theorem 3.3.2. *There exists a family $C := \Big\{\mathbb{Q}(\sqrt{d}) \ : \ d \text{ is prime}\Big\}$ of real quadratic fields such that O_K is Euclidean if and only if it has class number one.*

Remark 1. The reason for the above choice of d is governed by the fact that in $\mathbb{Q}(\sqrt{d})$, units can be found by solving the Brahmagupta-Pell equation

$$u^2 - dv^2 = 1$$

with

$$u := u(n) = b^4(a+1)n^2 + 2b^2(a+1)n + a$$

and

$$v := v(n) = b^3 n + b.$$

where a, b have to satisfy the Brahmagupta-Pell equation $x^2 - 23y^2 = 1$.

The family is motivated by the following construction of Zapponi [**?**].

3.4 Proof of the theorems

In our case, $K = \mathbb{Q}(\sqrt{d})$ with d as defined in the equation (3.2), we only need to find a unit ε and primes such that all hypotheses of Lemma 3.2.1 are satisfied for K. As $p_1 = 11$ and $p_2 = 13$, we see that (2) and (3) are satisfied. It is enough to check conditions (1) and (4) of Lemma 3.2.1.

Therefore, it remains to find a unit $\varepsilon \in \mathcal{O}_K^\times$ and show that p_1, p_2 are unramified primes in $\mathcal{O}_K$, (i.e., the primes p_1, p_2 split in $\mathcal{O}_K$). Then Lemma 3.4.1 (below) allows us to find an *admissible* set of primes $\{\mathfrak{p}_1, \mathfrak{p}_2\}$.

Let us set $\varepsilon := u + v\sqrt{d}$ where u and v are as defined before (see Remark 1). Since u and v satisfies the Brahmagupta-Pell equation

$$u^2 - dv^2 = 1,$$

we explicitly get a unit $\varepsilon \in \mathcal{O}_K^\times$.

We now show that the two rational primes p_1 and p_2 split in O_K. By construction of integers d, we see that $d \equiv 23 \pmod{p_1}$. The discriminant, d_K, of the field K is congruent to 1 *or* 4 $\pmod{p_1}$. In either case d_K is a square modulo p_1. Therefore, by a standard result about splitting of primes in quadratic fields (see Theorem 25, [**?**]), the rational prime p_1 splits in O_K. Similarly, d_K is congruent to 10 or 40 $\pmod{p_2}$. Thus, p_2 also splits in O_K.

For a given unit $\rho \in O_K^\times$ and an unramified prime ideal $\mathfrak{q}$, the following lemma tells us when the set $\{\mathfrak{q}\}$ is an *admissible* set.

Lemma 3.4.1. *Let $\rho \in O_K^\times$ be a unit and $\mathfrak{q}$ be an unramified prime ideal with odd prime norm q. If ρ is a primitive root modulo $\mathfrak{q}$, and $\mathfrak{q}$ is a non-Wieferich prime to the base ρ, i.e., $\rho^{q-1} \not\equiv 1$ (mod $\mathfrak{q}^2$), then ρ generates the group $(O_K/\mathfrak{q}^2)^\times$.*

Proof: We only need to show that ρ has order $q(q-1)$ modulo $\mathfrak{q}^2$. We proceed by contradiction: suppose $\rho^l \equiv 1 \pmod{\mathfrak{q}^2}$ for some divisor l of $q-1$, then $\rho^{q-1} \equiv 1 \pmod{\mathfrak{q}^2}$, this contradicts our assumption that $\rho^{q-1} \not\equiv 1 \pmod{\mathfrak{q}^2}$.
Now, if $\rho^{ql} \equiv 1 \pmod{\mathfrak{q}^2}$ for some $l|q-1$. Then $\rho^{ql} \equiv 1 \pmod{\mathfrak{q}}$. Since ρ is a primitive root modulo $\mathfrak{q}$, we have $q-1|ql$. This forces $l = q-1$. Hence ρ generates $(O_K/\mathfrak{q}^2)^\times$.

In order to use Lemma 3.4.1 in our case, we need to show that (i) ε is a primitive root modulo $\mathfrak{p}_1$, a prime ideal lying above p_1 in O_K, and (ii) $\mathfrak{p}_1$ is a non-Wieferich prime to the base ε.

Note that

$$N(\varepsilon^2 - 1) = \varepsilon^2\bar{\varepsilon}^2 - (\varepsilon^2 + \bar{\varepsilon}^2) + 1 \equiv 2 - 2(a^2 + 23b^2) \equiv 10 \pmod{p_1}, \tag{3.5}$$

and

$$\begin{aligned} N(\varepsilon^5 - 1) = \varepsilon^5\bar{\varepsilon}^5 - (\varepsilon^5 + \bar{\varepsilon}^5) + 1 &= 2 - 2\left(u^5 + 10u^3v^2d + 5uv^4d^2\right) \\ &\equiv 2 - 2(-1) \equiv 4 \pmod{p_1}. \end{aligned} \tag{3.6}$$

The equation (3.5) and (3.6) shows that ε does not have order 2 and 5 modulo any prime ideal in O_K lying above p_1. Since $p_1 - 1 = 2 \times 5$, the unit ε is a primitive root modulo any prime ideal lying above p_1.

Next, to establish (ii), note that

$$N(\varepsilon^5 - 1) = (\varepsilon^5 - 1)(\bar{\varepsilon}^5 - 1) = 2 - (\varepsilon^5 + \bar{\varepsilon}^5) \equiv 367 \pmod{p_1^3},$$

and

$$N(\varepsilon^5 + 1) = (\varepsilon^5 + 1)(\bar{\varepsilon}^5 + 1) = 2 + (\varepsilon^5 + \varepsilon^{\bar{5}}) = 4 - N(\varepsilon^5 - 1) \equiv 968 \pmod{p_1^3}.$$

Thus,

$$N(\varepsilon^{10} - 1) = N(\varepsilon^5 + 1)N(\varepsilon^5 - 1) \equiv 1210 \not\equiv 0 \pmod{p_1^3}. \tag{3.7}$$

From (3.7), we conclude that there exists a prime ideal in O_K lying above p_1, say $\mathfrak{p}_1$, such that

$$\varepsilon^{10} \not\equiv 1 \pmod{\mathfrak{p}_1^2}.$$

As $p_1 - 1 = 10$, the prime ideal $\mathfrak{p}_1$ is a non-Wieferich prime with respect to the base ε. Therefore, by applying Lemma 3.4.1, ε has order $p_1(p_1 - 1)$ modulo $\mathfrak{p}_1^2$.

Now we shall show that ε has order $p_2(p_2 - 1)$ modulo $\mathfrak{p}_2^2$, where $\mathfrak{p}_2$ is a prime ideal lying above p_2 in O_K. Observe that

$$N(\varepsilon^4 - 1) \equiv 2 - 2(a^4 + 138a^2b^2 + 23^2b^4) \equiv 3 \not\equiv 0 \pmod{p_2},$$

and

$$N(\varepsilon^3 - 1) \equiv 2 - 2(a^3 + 69ab^2) \equiv 2 - 2(0) \equiv 2 \not\equiv 0 \pmod{p_2}.$$

From this, we obtain

$$N(\varepsilon^3+1) = 4 - N(\varepsilon^3-1) \equiv 4-2 \equiv 2 \pmod{p_2}.$$

Therefore,

$$N(\varepsilon^6-1) = N(\varepsilon^3-1)N(\varepsilon^3+1) \equiv 4 \not\equiv 0 \pmod{p_2}.$$

This shows that ε does not have order 4 and 6 modulo any prime ideal in O_K lying above p_2, which means ε is a primitive root modulo any prime lying above p_2.

Again, by routine computation, we see that

$$N(\varepsilon^6-1) \equiv 511 \pmod{p_2^3},$$

and

$$N(\varepsilon^6+1) = 4 - N(\varepsilon^6-1) \equiv 4-511 \equiv 1690 \pmod{p_2^3}.$$

This gives,

$$N(\varepsilon^{12}-1) = N(\varepsilon^6-1)N(\varepsilon^6+1) \equiv 169 \pmod{p_2^3},$$

we conclude that there exists a prime ideal, say $\mathfrak{p}_2$, lying above p_2 in O_K which is a non-Wieferich prime with respect to the base ε. Thus, ε has order $p_2(p_2-1)$ modulo $\mathfrak{p}_2^2$.

Now, we set

$$\tau := -\varepsilon,$$

and observe that

$$\tau^{\frac{p_1(p_1-1)}{2}} \equiv -1 \times \varepsilon^{\frac{p_1(p_1-1)}{2}} \equiv -1 \times -1 \equiv 1 \pmod{\mathfrak{p}_1^2}, \tag{3.8}$$

which shows that τ has order $\frac{p_1(p_1-1)}{2}$ modulo $\mathfrak{p}_1^2$.

Since $p_2 \equiv 1 \pmod 4$, the units ε and $-\varepsilon$ have the same order modulo $\mathfrak{p}_2^2$. Hence τ has order $p_2(p_2-1)$ modulo $\mathfrak{p}_2^2$. Therefore, conditions (1) and (4) are satisfied for the unit τ and primes $\mathfrak{p}_1, \mathfrak{p}_2$. This leads us to conclude that O_K contains a set of two *admissible* primes $\{\mathfrak{p}_1, \mathfrak{p}_2\}$. Thus, if O_K has class number one, then by Lemma 3.2.1, O_K is Euclidean.

Proof of Theorem 3.5: In order to prove the theorem, we first show the following. Let (a, b) be a solution for the Brahmagupta-Pell equation

$$x^2 - 23y^2 = 1 \tag{3.9}$$

satisfying

$$a \equiv 24 \pmod{p_1^3 p_2^3} \text{ and } b \equiv 5 \pmod{p_1^3 p_2^3}. \tag{3.10}$$

Then there are infinitely many square free integers d of the form

$$d = (a+1)^2 b^2 n^2 + 2(a+1)^2 n + 23,$$

where $n \equiv 0 \pmod{p_1 p_2}$. Our main ingredient is the classical result of Ricci [**?**] who showed that if $f(x) \in \mathbb{Z}[X]$ is a separable quadratic polynomial with $gcd\{f(n) : n \in \mathbb{Z}\}$ a square-free integer, then there are infinitely many square-free values taken by $f(n)$ (in fact, he had shown that a positive proportion of the values are square-free). Now consider the quadratic polynomial $f(n) := (a+1)^2 b^2 n^2 + 2(a+1)^2 n + 23, n \in \mathbb{Z}$. The discriminant of this polynomial is $8(a+1)^3$, which is not zero. Therefore, $f(n)$ is a separable polynomial and the $gcd\{f(m) : m \in \mathbb{Z}\}$ is square-free. Thus, the result of Ricci implies that there are infinitely many square-free values taken by $f(n)$. We remark that if the square-free values taken by $f(n)$ has t distinct prime factors, then 2^{t-1} divides the class number of $\mathbb{Q}(\sqrt{d})$ (see Problem 8.3.1, [9]). Thus, we need only consider the prime values of $f(n)$ if we want that the class number of $\mathbb{Q}(\sqrt{d})$ is one. It may be noted that a famous conjecture of Buniakovsky [2] says that if $g(x) \in \mathbb{Z}[x]$ is irreducible and $N = \gcd\{g(m) : m \in \mathbb{N}\}$ then there are infinitely many $m \in \mathbb{N}$ such that $(1/N)|g(m)|$ is a prime. In our case, if we take $a = 24$ and $b = 5$, for example, then $N = 1$. Thus our polynomial $f(n)$ assumes infinitely many prime values under Buniakovsky's conjecture.

We shall now prove that there are infinitely many solutions a, b to the Brahmagupta-Pell equation (3.9) satisfying the conditions (3.10).

Note that $24 + 5\sqrt{23}$ is the fundamental unit in the ring of integers for the field $\mathbb{Q}(\sqrt{23})$, therefore $a = 24, b = 5$ is a pair satisfying (3.9) and (3.10).

Let us set

$$\mu := 24 + 5\sqrt{23},$$

and define

$$\mu^k := a_k + b_k\sqrt{23}, \quad a_k, b_k \in \mathbb{N}.$$

Observe that each pair (a_k, b_k) is a solution for the equation (3.9). A simple computation carried out in Python gives us the following:

$$a_{1210s+1} \equiv 24 \pmod{p_1^3} \text{ and } b_{1210s+1} \equiv 5 \pmod{p_1^3} \text{ for all } s \in \mathbb{N},$$

and

$$a_{2028s'+1} \equiv 24 \pmod{p_2^3} \text{ and } b_{2028s'+1} \equiv 5 \pmod{p_2^3} \text{ for all } s' \in \mathbb{N}.$$

Thus, $a_{k+1} \equiv 24 \pmod{p_1^3 p_2^3}$ and $b_{k+1} \equiv 5 \pmod{p_1^3 p_2^3}$, for $k = 1210s = 2028s'$, for all $s, s' \in \mathbb{Z}$. This shows that there are infinitely many integer pairs (a, b) satisfying (3.9) and (3.10).

As we vary a, b and n, we get an infinite family of infinitely many real quadratic fields of the form $\mathbb{Q}(\sqrt{d})$.

3.5 Remarks

The set of quadratic fields with class number one in the family C is non-empty since $\mathbb{Q}(\sqrt{23}) \in C$. We expect there are more examples and this may be useful to investigate further numerically. For ease of exposition, we fixed the primes $p_1 = 11$ and $p_2 = 13$. In fact, the main theorem holds true for any real quadratic field K provided there exists two unramified rational primes $p_1 \equiv 3 \pmod 4$ and $p_2 \equiv 1 \pmod 4$ satisfying the following conditions:

1. $N(\varepsilon^{p_1(p_1-1)}) \not\equiv 0 \pmod{p_1}$;
2. $N(\varepsilon^{p_2(p_2-1)}) \not\equiv 0 \pmod{p_2}$; and
3. $gcd(p_1(p_1 - 1)/2,\ p_2(p_2 - 1)) = 1$;

for any fixed unit $\varepsilon \in O_K^\times$.

It should be possible to go further. For example, the results of this chapter can be easily extended to study cubic fields which are Euclidean, which we do in the next chapter. In these cases, the unit rank is either 1 or 2 and so a similar dichotomy emerges. Also, the results of [?] were confined to the case that K is Galois over the rationals. This was due to a similar restriction in the work of Murty and Murty [?]. But this restriction was recently removed in a work of Murty and Peterson [?] and consequently, there is a wide scope for further progress.

The two hypotheses we assumed, namely the Hardy-Littlewood conjecture and the Wieferich primes hypothesis are both reasonable from a heuristic perspective. Indeed, the former is encouraging given the recent progress on the twin prime problem. As for the second, it is unclear at the moment. Heuristic reasoning suggests that the number of such primes less than x should not be more than O($loglogx$). Our hypothesis is much weaker from this viewpoint in that we postulate the number is $o(x/log^2x)$. Certainly these hypotheses are far less imposing than the elusive and fugitive generalized Riemann hypothesis.

Chapter 4

Euclidean cyclic cubic fields

4.1 Introduction

Let K be a cyclic cubic field with discriminant f^2, where f is the conductor of K. In 1969, J. R. Smith [**?**] proved that the cyclic cubic fields with conductors $7, 9, ..., 67$ are norm-Euclidean. Further, in the same paper he showed that the fields with conductors $73, 79, 97, 139, 151$ and $163 < f < 10^4$ are *not* norm-Euclidean. The object of this note is to show that all cyclic cubic fields with conductors $f \in [73, 11971]$ are in fact Euclidean provided they have class number one.

It is well known that if the conductor f of the cyclic cubic field K has t distinct prime factors, then the class number of K is divisible by 3^{t-1} (see appendix of Heilbronn's paper [15] for a proof). Thus a cyclic cubic field with class number one must have prime conductor f. Moreover, a necessary condition for a cyclic cubic field to have class number one is that its conductor is either 9 or a prime in the residue class 1 (mod 6) (see [15], [11]). Accordingly, from now onwards, we shall be dealing with only those cyclic cubic fields K with prime conductor f satisfying $f \equiv 1 \pmod 6$.The contents of this chapter are taken from [**?**]. Our main aim is to prove the following

Theorem 4.1.1. *Let K be a cyclic cubic field with conductor f, satisfying $73 \leq f \leq 11971$ and let O_K be its ring of integers. Then O_K is Euclidean if and only if it has class number one.*

Proof. It is easy to show that if a number ring O_K is Euclidean, then it has class number one. To prove the converse, we use a result of Harper and Ram Murty (Theorem 4.1.2 below) which gives a useful criteria to establish the Euclidean algorithm for certain number fields.

We again recall the statement of Harper and Ram Murty as follows:

Theorem 4.1.2. *(M. Ram Murty, M. Harper) [**?**] Let $K/\mathbb{Q}$ be abelian of degree n with O_K having class number one, that contains a set of admissible primes with s elements. Let r be the rank of the unit group. If $r + s \geq 3$, then O_K is Euclidean.*

The well known Dirichlet's unit theorem states that the rank r of the group of units in O_K is given by $r = r_1 + r_2 - 1$, where r_1 is the number of real embeddings and r_2 is the number of conjugate pairs of complex embeddings of K. In our case, K is cyclic cubic field which means the Galois group over $\mathbb{Q}$ is cyclic of order three. This can only happen if K is totally real. Thus, $r = 3 - 1 = 2$. All we need to do now is to exhibit an *admissible* set of primes with one element (i.e. $s = 1$). For this we recall a special case of lemma 3.2.1 from Chapter 3

Lemma 4.1.3. *Let $\rho \in O_K^\times$ be a unit and $\mathfrak{q}$ be an unramified prime ideal with odd prime norm q. If ρ is a primitive root modulo $\mathfrak{q}$, and $\mathfrak{q}$ is a non-Wieferich prime to the base ρ, i.e., $\rho^{q-1} \not\equiv 1$ (mod $\mathfrak{q}^2$), then ρ generates the group $(O_K/\mathfrak{q}^2)^\times$.*

Thus, we need to find an unramified prime π with odd prime norm such that the group $(O_K/\pi)^\times$ has a primitive root $\varepsilon \in O_K^\times$ and π is a non-Wieferich prime with respect to ε. As the field K is Galois of degree 3 over $\mathbb{Q}$, this means that an unramified rational prime

p either splits completely or remains as a prime in O_K. It is well-known that a rational prime p ($\neq f$) splits completely in K if and only if p is a cube modulo f. By Euler's criterion, it follows that p is a cube modulo f if and only if $p^{\frac{f-1}{3}} \equiv 1 \pmod{f}$.

In what follows, we shall exhibit a set of *admissible* primes with one element for the cyclic cubic field K with conductor $f = 73$. By Theorem 4.1.2 and Lemma 4.1.3 it will then follow that this field is Euclidean as it has class number one. For all other fields in the range $73 < f \leq 11971$ with class number one, we shall give an algorithm which produces an *admissible* set of primes with one element. The database [18] gives all such fields. In the end, we shall list in a table the defining polynomial of all the class number one cyclic cubic fields with conductors in the above range and the corresponding set of *admissible* primes. This will complete the proof of our main theorem.

Thus, we start with the cyclic cubic field K with conductor 73. It is known that K has class number one. The fundamental units $\varepsilon_1, \varepsilon_2$ for K are

$$\begin{aligned}\varepsilon_1 &:= \frac{2}{3}a^2 - \frac{14}{3}a + 7,\\ \varepsilon_2 &:= \frac{4}{3}a^2 + \frac{14}{3}a - 7,\end{aligned}$$

where a is a root of the defining polynomial $x^3 - x^2 - 24x + 27$ for K. This is obtained by using Sage programme.

Let us take the rational prime $p = 3$. It is unramified in K since $p \nmid 73$.
Also, as $3^{\frac{73-1}{3}} \equiv 1 \pmod{73}$ implies that p splits completely in O_K. The prime ideal decomposition of 3 in O_K is given by:

$$(3) = \left(\tfrac{1}{3}a^2 + \tfrac{2}{3}a - 11\right)\left(-\tfrac{1}{3}a^2 + \tfrac{1}{3}a + 6\right)\left(\tfrac{2}{3}a^2 + \tfrac{1}{3}a - 17\right).$$

Let π be the prime element such that $(\pi) := \left(\frac{1}{3}a^2 + \frac{2}{3}a - 11\right)$. A simple calculation gives

$$\varepsilon_1 \equiv -1 \pmod{\pi}, \tag{4.1}$$

and

$$\varepsilon_1^2 \equiv 16 \not\equiv 1 \pmod{\pi^2}. \tag{4.2}$$

As $(O_K/\pi)^\times$ has order 2, it follows from (4.1) that ε_1 is a primitive root modulo π. The equation (4.2) says that π is a non-Wieferich prime with respect to ε. Thus, by Lemma 4.1.3 the set $\{\pi\}$ is *admissible*. Thus K is Euclidean.

In section 4.2, we present an algorithm to determine a set of *admissible* primes with one element.

Appendix will contain table of admissible primes and Sage Code to compute a *admissible* prime for cyclic cubic fields.

4.2 Algorithm to find an admissible prime

```
data ← list of [defining polynomials, conductor]
flat ← false
foo ← false
print ("Conductor|Defining Polynomial|Admissible prime")
for $u$ in data:
    prime ← int(math.sqrt(u[1]))
    $K$ ← Number field with defining polynomial u[0]
    if (class number of $K$ is not 1):
        break
    u ← unit group associated with $K$
    eps ← one of the fundamental units of u
    list p ← [all cubic residues mod p]
    for q set of primes
        if q==2:
            continue
        if q>100000:
            break
        ((q modulo prime) in list p):
            f ← prime decomposition of q in $K$
            for term in f:
                frc ← fractional ideal in term
                for $d \in \{1, \ldots q-1\}$
                    if (q-1 mod d is 0 and (eps$^{d}$) modulo frc ==1):
                        flat ← true
                        break
            if (flat is true):
                flat ← false
                continue
            frcs ← (frc)$^{2}$
            if (eps$^{q-1}$ mod frcs is not 1)
                print(prime, polynomial, fractional ideal)
                    foo ← true
                    break
foo is true:
    foo ← false
    break
```

```
if(prime > 100000):
    break.
```

4.3 Remarks

As and when new fields with class number one are added to the database [18], it is possible to check with the algorithm given in this paper to determine whether it is Euclidean or not.

Chapter 5

Appendix

5.1 Sage code to compute an admissible prime

```
Sage Code for generating an Admissible Prime in Cyclic Cubic Fields


J = JonesDatabase()

P = Primes()


import math

flag = false

foo = false

print(’{:<10} | {:<30} | {:<200} | {:<100}’.format("Regulator", "\Defining pol

for ll in data:

prime = int(math.sqrt(ll[1]))

if (prime%6==1 and prime<7000):

#and prime>8000
```

```
#print("\nWorking for prime "+str(prime))
#output = J.ramified_at(prime,3)
#print("Number fields are "+str(output))
#for K in output:
#print("Class number s " + str(K.class_number()))
K = NumberField(ll[0],'a')
if (K.class_number() != 1):
#print("Class number for "+str(prime)+" is not one")
break
U = UnitGroup(K)
#print("Fundamental units are "+str(U.fundamental_units()))
eps = U.fundamental_units()[0]
listp = []
for i in range(prime):
if ((i^((prime-1)/3))%prime==1):
listp.append(i)
#print("The list for prime "+str(prime)+" is "+str(listp))
for q in P:
if (q==2):
continue
if (q>10000000):
break
if ((q%prime) in listp):
#print("The prime I am working with is "+str(q))
f=K.factor(q)
for pair in f:
```

```
frc = pair[0]
#print(frc)
for d in range(1,q-1):
if ((q-1)%d==0):
#print("The divisor I got is "+str(d))
#print("The remainder I got is "+str(frc.small_residue(eps^d)))
if (frc.small_residue(eps^d) == 1):
flag = true
break
if (flag):
flag = false
continue
frcs = frc^2
if (frcs.small_residue(eps^(q-1)) != 1):
#print("eps^(q-1) module ideal squared "+str(frcs)+" is not one.")
print('{:<10} | {:<30} | {:<100}'.format(prime, K.absolute_polynomial(), (str(
#print("For prime "+str(prime)+": Unit is "+str(eps)+", ideal is "+str(frc)+",
foo = true
break
#                        print(frc.small_residue(eps))
if (foo):
foo = false
break
if (prime > 100000):
break
```

5.2 Table of admissible primes

Here we list an *admissible* prime for cyclic cubic fields with $f < 11971$.

Table of admissible primes.

f	*polynomial*	*admissible prime*
79	$x^3 - x^2 - 26x - 41$	$a + 1$
97	$x^3 - x^2 - 32x + 79$	$a^2 + 3a - 21$
103	$x^3 - x^2 - 34x + 61$	$\frac{2}{3}a^2 - 3a - \frac{8}{3}$
109	$x^3 - x^2 - 36x + 4$	$\frac{35}{2}a^2 + \frac{191}{2}a - 12$
127	$x^3 - x^2 - 42x - 80$	$9a^2 + 5a - 153$
139	$x^3 - x^2 - 46x - 103$	$a + 4$
151	$x^3 - x^2 - 50x + 123$	$a^2 + 3a - 53$
157	$x^3 - x^2 - 52x - 64$	$\frac{135}{2}a^2 + \frac{977}{2}a + 523$
181	$x^3 - x^2 - 60x + 67$	$\frac{2}{5}a^2 + \frac{21}{5}a - \frac{26}{5}$
193	$x^3 - x^2 - 64x - 143$	$\frac{29}{3}a^2 - 65a - \frac{734}{3}$
199	$x^3 - x^2 - 66x - 59$	$2a^2 + 16a + 13$
211	$x^3 - x^2 - 70x + 125$	$a^2 - 62$
223	$x^3 - x^2 - 74x + 256$	$5313a^2 + 28133a - 216059$
229	$x^3 - x^2 - 76x + 212$	$266a^2 + 1704a - 7627$
271	$x^3 - x^2 - 90x - 261$	$3a^2 - 3a - 152$
283	$x^3 - x^2 - 94x - 304$	$448a^2 + 4698a + 11855$
331	$x^3 - x^2 - 110x + 49$	$\frac{3}{7}a^2 + \frac{30}{7}a - 1$
337	$x^3 - x^2 - 112x - 25$	$4a^2 - 3a - 428$
367	$x^3 - x^2 - 112x - 435$	$\frac{1633}{3}a^2 - \frac{13919}{3}a - 3149$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
373	$x^3 - x^2 - 124x + 221$	$\frac{38}{7}a^2 - \frac{475}{7} + \frac{733}{7}$
379	$x^3 - x^2 - 126x - 365$	$\frac{13}{5}a^2 + \frac{156}{5}a + 74$
409	$x^3 - x^2 - 136x + 515$	$\frac{19}{5}a^2 - \frac{252}{5}a + 134$
421	$x^3 - x^2 - 140x + 343$	$\frac{13}{7}a^2 + \frac{134}{7}a - 60$
433	$x^3 - x^2 - 144x + 16$	$\frac{4257}{4}a^2 - \frac{53501}{4}a + 1472$
439	$x^3 - x^2 - 146x + 504$	$(3, \frac{1}{6}a^2 + \frac{1}{6}a - 16)$
457	$x^3 - x^2 - 152x + 220$	$(5, a - 2)$
463	$x^3 - x^2 - 154x - 343$	$(7, \frac{2}{7}a^2 - 23/7a - 30)$
487	$x^3 - x^2 - 162x + 505$	$(5, a)$
499	$x^3 - x^2 - 166x - 536$	$(13, a + 6)$
523	$x^3 - x^2 - 174x + 891$	$(11, a)$
541	$x^3 - x^2 - 180x - 521$	$(7, -\frac{2}{7}a^2 - \frac{3}{7}a + \frac{251}{7})$
571	$x^3 - x^2 - 190x + 719$	$(7, -\frac{3}{7}a^2 + \frac{4}{7}a + \frac{354}{7})$
577	$x^3 - x^2 - 192x - 171$	$(3, \frac{1}{9}a^2 + \frac{11}{9}a - \frac{44}{3})$
601	$x^3 - x^2 - 200x - 512$	$(13, a + 3)$
613	$x^3 - x^2 - 204x - 999$	$(3, \frac{1}{3}a^2 - \frac{13}{3}a - 44)$
619	$x^3 - x^2 - 206x - 321$	$(3, a)$
631	$x^3 - x^2 - 210x + 1075$	$(43, a + 14)$
643	$x^3 - x^2 - 214x + 1024$	$(3, \frac{1}{6}a^2 + \frac{1}{2}a - \frac{68}{3})$
661	$x^3 - x^2 - 220x + 1273$	$(3, a + 1)$
673	$x^3 - x^2 - 224x + 997$	$(23, a + 3)$
691	$x^3 - x^2 - 230x - 128$	$(5, -\frac{1}{10}a^2 - \frac{23}{10}a + 74$
727	$x^3 - x^2 - 242x - 1104$	$(3, \frac{1}{6}a^2 + \frac{1}{6}a - 27)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
733	$x^3 - x^2 - 244x - 1276$	$(5, a - 1)$
739	$x^3 - x^2 - 246x + 520$	$(5, a)$
751	$x^3 - x^2 - 250x - 1057$	$(7, -\frac{1}{7}a^2 + \frac{11}{7}a + 23)$
757	$x^3 - x^2 - 252x - 729$	$(3, -\frac{1}{9}a^2 + \frac{10}{9}a + 19)$
769	$x^3 - x^2 - 256x + 1481$	$(5, \frac{1}{5}a^2 + a - \frac{166}{5})$
787	$x^3 - x^2 - 262x + 991$	$(31, a + 8)$
811	$x^3 - x^2 - 270x - 1592$	$(7, a - 2)$
823	$x^3 - x^2 - 274x - 61$	$(5, a + 2)$
829	$x^3 - x^2 - 276x + 307$	$(7, a + 2)$
859	$x^3 - x^2 - 286x + 509$	$(59, a + 28)$
883	$x^3 - x^2 - 294x - 1439$	$(17, a - 4)$
907	$x^3 - x^2 - 302x + 739$	$(11, -\frac{5}{11}a^2 - \frac{40}{11}a + \frac{1007}{11})$
919	$x^3 - x^2 - 306x + 1872$	$(29, a - 4)$
967	$x^3 - x^2 - 322x - 1361$	$(3, \frac{1}{9}a^2 - \frac{1}{3}a - \frac{226}{9})$
991	$x^3 - x^2 - 330x + 2349$	$(3, \frac{1}{3}a^2 + \frac{11}{3}a - 74)$
997	$x^3 - x^2 - 332x + 480$	$(5, a + 1)$
1021	$x^3 - x^2 - 340x - 416$	$(7, a - 2)$
1033	$x^3 - x^2 - 344x - 1913$	$(37, a - 1)$
1039	$x^3 - x^2 - 346x - 2155$	$(5, a)$
1051	$x^3 - x^2 - 350x + 2608$	$(53, a + 24)$
1069	$x^3 - x^2 - 356x - 2336$	$(29, a - 6)$
1087	$x^3 - x^2 - 362x + 2335$	$(5, a - 2)$
1093	$x^3 - x^2 - 364x + 1012$	$(3, \frac{1}{12}a^2 - \frac{1}{4}a - \frac{113}{6})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
1117	$x^3 - x^2 - 372x - 2565$	$(3, \frac{1}{3}a^2 - \frac{13}{3}a - 82)$
1123	$x^3 - x^2 - 374x - 1331$	$(5, a + 2)$
1153	$x^3 - x^2 - 384x + 427$	$(7, a)$
1171	$x^3 - x^2 - 390x - 347$	$(13, \frac{1}{13}a^2 + \frac{4}{13}a - \frac{214}{13})$
1201	$x^3 - x^2 - 400x - 2491$	$(13, a - 4)$
1213	$x^3 - x^2 - 404x - 629$	$(13, a - 6)$
1231	$x^3 - x^2 - 410x + 1003$	$(11, a + 4)$
1237	$x^3 - x^2 - 412x - 1741$	$(11, \frac{1}{11}a^2 - \frac{2}{11}a - \frac{245}{11})$
1249	$x^3 - x^2 - 416x - 2313$	$(3, a)$
1279	$x^3 - x^2 - 426x + 2179$	$(11, a + 3)$
1291	$x^3 - x^2 - 430x + 3347$	$(5, \frac{1}{5}a^2 + \frac{8}{5}a - \frac{278}{5})$
1297	$x^3 - x^2 - 432x + 1345$	$(5, a)$
1303	$x^3 - x^2 - 434x + 2799$	$(3, \frac{1}{9}a^2 + \frac{4}{9}a - 32)$
1321	$x^3 - x^2 - 440x - 3327$	$(59, a + 9)$
1327	$x^3 - x^2 - 442x + 344$	$(7, \frac{1}{14}a^2 - \frac{1}{2}a - \frac{137}{7})$
1381	$x^3 - x^2 - 460x + 1739$	$(13, -\frac{1}{13}a^2 + \frac{54}{13}a + \frac{341}{13})$
1423	$x^3 - x^2 - 474x - 896$	$(5, a - 2)$
1429	$x^3 - x^2 - 476x - 3599$	$(37, a + 5)$
1447	$x^3 - x^2 - 482x - 1715$	$(13, a + 1)$
1453	$x^3 - x^2 - 484x + 3767$	$(7, -\frac{1}{7}a^2 - 3a + \frac{344}{7})$
1471	$x^3 - x^2 - 490x + 4304$	$(13, a - 4)$
1483	$x^3 - x^2 - 494x + 2197$	$(13, \frac{1}{13}a^2 - \frac{1}{13}a - 26)$
1531	$x^3 - x^2 - 510x + 567$	$(5, -\frac{2}{15}a^2 - \frac{16}{15}a + \frac{227}{5})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
1543	$x^3 - x^2 - 514x - 4229$	$(3, a + 1)$
1549	$x^3 - x^2 - 516x - 459$	$(3, -\frac{1}{15}a^2 + \frac{2}{3}a + \frac{117}{5})$
1579	$x^3 - x^2 - 526x - 1696$	$(11, a - 1)$
1597	$x^3 - x^2 - 532x - 2780$	$(3, a + 1)$
1609	$x^3 - x^2 - 536x + 1311$	$(3, a)$
1621	$x^3 - x^2 - 540x + 4923$	$(23, a + 10)$
1627	$x^3 - x^2 - 542x - 4640$	$(13, a + 5)$
1657	$x^3 - x^2 - 552x + 4480$	$(7, a + 2)$
1663	$x^3 - x^2 - 554x + 4681$	$(7, a + 3)$
1669	$x^3 - x^2 - 556x + 4327$	$(3, a + 1)$
1693	$x^3 - x^2 - 564x - 2759$	$(11, a - 3)$
1723	$x^3 - x^2 - 574x + 2744$	$(7, \frac{1}{14}a^2 - \frac{1}{14}a - 28)$
1741	$x^3 - x^2 - 580x + 3353$	$(13, -\frac{1}{13}a^2 - \frac{40}{13}a + \frac{318}{13})$
1747	$x^3 - x^2 - 582x + 4141$	$(19, a + 9)$
1753	$x^3 - x^2 - 584x + 844$	$(5, a + 2)$
1759	$x^3 - x^2 - 586x + 2215$	$(3, -\frac{1}{15}a^2 - \frac{4}{5}a + \frac{74}{3})$
1783	$x^3 - x^2 - 594x - 5283$	$(3, -\frac{1}{3}a^2 + \frac{10}{3}a + 131)$
1801	$x^3 - x^2 - 600x - 4736$	$(29, a - 7)$
1861	$x^3 - x^2 - 620x + 2757$	$(3, a)$
1867	$x^3 - x^2 - 622x + 6085$	$(3, a + 1)$
1873	$x^3 - x^2 - 624x - 4301$	$(11, \frac{1}{11}a^2 - \frac{6}{11}a - 38)$
1933	$x^3 - x^2 - 644x - 4224$	$(11, a)$
1993	$x^3 - x^2 - 664x + 1181$	$(11, a - 1)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
1999	$x^3 - x^2 - 666x + 4072$	$(7, -\frac{1}{7}a^2 - \frac{8}{7}a + \frac{433}{7})$
2011	$x^3 - x^2 - 670x - 4171$	$(13, a + 6)$
2017	$x^3 - x^2 - 672x + 2764$	$(29, a + 5)$
2029	$x^3 - x^2 - 676x - 5561$	$(3, -\frac{1}{9}a^2 + \frac{451}{9})$
2053	$x^3 - x^2 - 684x - 6083$	$(11, a)$
2083	$x^3 - x^2 - 694x - 1543$	$(17, \frac{4}{17}a^2 - \frac{86}{17}a - \frac{1897}{17})$
2089	$x^3 - x^2 - 696x - 2708$	$(19, a + 1)$
2113	$x^3 - x^2 - 704x + 6652$	$(41, a + 15)$
2137	$x^3 - x^2 - 712x + 6965$	$(5, a)$
2143	$x^3 - x^2 - 714x - 7064$	$(23, a - 11)$
2161	$x^3 - x^2 - 720x - 2081$	$(29, a + 8)$
2179	$x^3 - x^2 - 726x + 7344$	$(3, a - 1)$
2203	$x^3 - x^2 - 734x - 408$	$(3, \frac{1}{18}a^2 + \frac{7}{18}a - \frac{83}{3})$
2221	$x^3 - x^2 - 740x - 4113$	$(5, \frac{1}{15}a^2 - \frac{2}{15}a - \frac{176}{5})$
2239	$x^3 - x^2 - 746x + 7795$	$(7, a + 2)$
2251	$x^3 - x^2 - 750x + 1584$	$(19, a - 6)$
2269	$x^3 - x^2 - 756x - 6723$	$(47, a + 11)$
2281	$x^3 - x^2 - 760x - 7012$	$(13, a + 6)$
2287	$x^3 - x^2 - 762x - 1440$	$(3, \frac{1}{18}a^2 + \frac{23}{18}a - \frac{86}{3})$
2293	$x^3 - x^2 - 764x + 3397$	$(17, \frac{7}{17}a^2 + \frac{13}{17}a - \frac{3504}{17})$
2341	$x^3 - x^2 - 780x - 6156$	$(3, -\frac{1}{12}a^2 - \frac{5}{12}a + \frac{87}{2})$
2347	$x^3 - x^2 - 782x + 5824$	$(7, \frac{1}{14}a^2 + \frac{3}{14}a - 37)$
2371	$x^3 - x^2 - 790x - 3337$	$(17, a + 3)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
2377	$x^3 - x^2 - 792x + 7219$	$(41, a + 5)$
2383	$x^3 - x^2 - 794x + 2736$	$(7, a + 1)$
2389	$x^3 - x^2 - 796x - 4955$	$(3, \frac{1}{15}a^2 + \frac{4}{5}a - \frac{107}{3})$
2467	$x^3 - x^2 - 822x - 731$	$(17, a)$
2473	$x^3 - x^2 - 824x + 6961$	$(13, \frac{5}{13}a^2 - \frac{14}{13}a - \frac{2722}{13})$
2503	$x^3 - x^2 - 834x - 4079$	$(17, a + 1)$
2521	$x^3 - x^2 - 840x + 9337$	$(5, \frac{1}{5}a^2 + \frac{13}{5}a - \frac{553}{5})$
2539	$x^3 - x^2 - 846x - 7523$	$(11, -\frac{5}{11}a^2 + \frac{100}{11}a + \frac{2858}{11})$
2551	$x^3 - x^2 - 850x + 4913$	$(23, a + 2)$
2593	$x^3 - x^2 - 864x + 2689$	$(53, a + 10)$
2617	$x^3 - x^2 - 872x + 9111$	$(3, \frac{1}{9}a^2 + \frac{10}{9}a - \frac{194}{3})$
2647	$x^3 - x^2 - 882x - 2549$	$(19, a + 9)$
2671	$x^3 - x^2 - 890x - 4056$	$(3, a)$
2677	$x^3 - x^2 - 892x + 3371$	$(23, a + 7)$
2683	$x^3 - x^2 - 894x + 9937$	$(13, a + 1)$
2707	$x^3 - x^2 - 902x + 5815$	$(5, a)$
2713	$x^3 - x^2 - 904x + 10651$	$(19, a - 1)$
2719	$x^3 - x^2 - 906x - 9869$	$(11, a + 5)$
2731	$x^3 - x^2 - 910x - 10216$	$(13, a - 6)$
2749	$x^3 - x^2 - 916x - 1120$	$(5, a)$
2767	$x^3 - x^2 - 922x + 8096$	$(7, \frac{1}{14}a^2 + \frac{5}{14}a - \frac{327}{7})$
2791	$x^3 - x^2 - 930x - 9200$	$(5, \frac{1}{10}a^2 - \frac{11}{10}a - 61)$
2833	$x^3 - x^2 - 944x - 9968$	$(7, a)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
2851	$x^3 - x^2 - 950x + 8025$	$(3, a)$
2857	$x^3 - x^2 - 952x - 4021$	$(19, a + 5)$
2887	$x^3 - x^2 - 962x + 10051$	$(11, \frac{1}{11}a^2 + \frac{9}{11}a - \frac{674}{11})$
2917	$x^3 - x^2 - 972x + 11776$	$(23, a)$
2953	$x^3 - x^2 - 984x + 7984$	$(5, a - 2)$
2971	$x^3 - x^2 - 990x - 5832$	$(3, \frac{1}{18}a^2 - \frac{1}{18}a - 36)$
3001	$x^3 - x^2 - 1000x - 8225$	$(3, a + 1)$
3019	$x^3 - x^2 - 1006x + 1789$	$(3, -\frac{1}{21}a^2 + \frac{10}{7}a + \frac{661}{21})$
3049	$x^3 - x^2 - 1016x - 1581$	$(3, \frac{1}{21}a^2 + \frac{1}{3}a - \frac{229}{7})$
3061	$x^3 - x^2 - 1020x - 3968$	$(19, a + 6)$
3067	$x^3 - x^2 - 1022x + 2499$	$(3, a)$
3079	$x^3 - x^2 - 1026x + 9351$	$(3, \frac{-1}{15}a^2 + \frac{2}{3}a + \frac{227}{5})$
3109	$x^3 - x^2 - 1036x - 2303$	$(3, a + 1)$
3121	$x^3 - x^2 - 1040x - 9941$	$(23, a - 11)$
3163	$x^3 - x^2 - 1054x + 13472$	$(43, a + 3)$
3169	$x^3 - x^2 - 1056x + 11737$	$(11, a - 1)$
3181	$x^3 - x^2 - 1060x + 11428$	$(41, a - 19)$
3187	$x^3 - x^2 - 1062x - 3069$	$(3, \frac{1}{21}a^2 + \frac{26}{21}a - \frac{239}{7})$
3229	$x^3 - x^2 - 1076x + 5860$	$(23, a + 8)$
3253	$x^3 - x^2 - 1084x - 13253$	$(3, a + 1)$
3259	$x^3 - x^2 - 1086x + 10984$	$(11, a - 5)$
3301	$x^3 - x^2 - 1100x + 13693$	$(7, \frac{1}{7}a^2 + 2a - \frac{729}{7})$
3307	$x^3 - x^2 - 1102x - 6859$	$(19, -\frac{4}{19}a^2 - \frac{91}{19}a + 156)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
3319	$x^3 - x^2 - 1106x + 4917$	$(3, a)$
3331	$x^3 - x^2 - 1110x + 2344$	$(47, a + 18)$
3343	$x^3 - x^2 - 1114x - 8048$	$(3, \frac{1}{18}a^2 + \frac{5}{6}a - \frac{374}{9})$
3361	$x^3 - x^2 - 1120x - 13693$	$(5, \frac{1}{5}a^2 - \frac{17}{5}a - \frac{753}{5})$
3373	$x^3 - x^2 - 1124x - 11868$	$(3, a)$
3391	$x^3 - x^2 - 1130x - 14192$	$(23, a + 4)$
3433	$x^3 - x^2 - 1144x - 9409$	$(11, a + 5)$
3457	$x^3 - x^2 - 1152x - 13700$	$(5, a)$
3463	$x^3 - x^2 - 1154x + 3976$	$(7, a + 2)$
3469	$x^3 - x^2 - 1156x + 13619$	$(11, a + 1)$
3499	$x^3 - x^2 - 1166x - 11145$	$(3, \frac{1}{15}a^2 - \frac{8}{15}a - 52)$
3511	$x^3 - x^2 - 1170x + 10663$	$(11, a + 2)$
3541	$x^3 - x^2 - 1180x + 8000$	$(5, \frac{1}{20}a^2 - \frac{1}{20}a - 40)$
3559	$x^3 - x^2 - 1186x + 9227$	$(17, a - 8)$
3583	$x^3 - x^2 - 1194x + 1327$	$(7, a - 2)$
3607	$x^3 - x^2 - 1202x - 15096$	$(3, \frac{1}{6}a^2 - \frac{17}{6}a - 133)$
3613	$x^3 - x^2 - 1204x + 2141$	$(13, a + 2)$
3631	$x^3 - x^2 - 1210x + 10624$	$(3, a + 1)$
3637	$x^3 - x^2 - 1212x + 15895$	$(5, a)$
3643	$x^3 - x^2 - 1214x - 1889$	$(23, \frac{1}{23}a^2 + \frac{8}{23}a - \frac{682}{23})$
3673	$x^3 - x^2 - 1224x - 10883$	$(17, \frac{1}{17}a^2 - \frac{6}{17}a - \frac{922}{17})$
3691	$x^3 - x^2 - 1230x - 13397$	$(13, -\frac{5}{13}a^2 + \frac{29}{13}a + \frac{4157}{13})$
3697	$x^3 - x^2 - 1232x - 9311$	$(19, \frac{6}{19}a^2 - \frac{151}{19}a - \frac{5095}{19})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
3709	$x^3 - x^2 - 1236x - 15935$	$(5, -\frac{2}{5}a^2 + \frac{41}{5}a + 329)$
3733	$x^3 - x^2 - 1244x + 8019$	$(3, a)$
3739	$x^3 - x^2 - 1246x - 15233$	$(11, a - 3)$
3769	$x^3 - x^2 - 1256x + 10609$	$(29, a + 10)$
3793	$x^3 - x^2 - 1264x + 14891$	$(13, a - 5)$
3823	$x^3 - x^2 - 1274x + 14584$	$(7, \frac{1}{14}a^2 + \frac{9}{14}a - \frac{438}{7})$
3847	$x^3 - x^2 - 1282x - 7979$	$(3, -\frac{1}{21}a^2 + a + \frac{883}{21})$
3853	$x^3 - x^2 - 1284x + 16839$	$(3, -\frac{1}{9}a^2 - \frac{5}{9}a + \frac{286}{3})$
3877	$x^3 - x^2 - 1292x - 4595$	$(5, a)$
3889	$x^3 - x^2 - 1296x + 144$	$(3, a - 1)$
3907	$x^3 - x^2 - 1302x + 9261$	$(7, \frac{1}{7}a^2 + \frac{6}{7}a - 123)$
3919	$x^3 - x^2 - 1306x - 10741$	$(11, a - 5)$
3931	$x^3 - x^2 - 1310x - 12521$	$(17, -\frac{5}{17}a^2 + \frac{86}{17}a + \frac{4334}{17})$
3943	$x^3 - x^2 - 1314x + 8032$	$(11, a - 5)$
3967	$x^3 - x^2 - 1322x - 17925$	$(3, a)$
4003	$x^3 - x^2 - 1334x - 15419$	$(11, a + 5)$
4021	$x^3 - x^2 - 1340x + 13999$	$(7, a + 2)$
4027	$x^3 - x^2 - 1342x - 15064$	$(7, \frac{1}{14}a^2 - \frac{11}{14}a - 64)$
4051	$x^3 - x^2 - 1350x - 7952$	$(11, a + 3)$
4057	$x^3 - x^2 - 1352x - 3456$	$(3, -\frac{1}{24}a^2 + \frac{17}{24}a + 37)$
4093	$x^3 - x^2 - 1364x + 19707$	$(3, a)$
4111	$x^3 - x^2 - 1370x + 17053$	$(13, \frac{1}{13}a^2 + \frac{11}{13}a - \frac{952}{13})$
4129	$x^3 - x^2 - 1376x - 14528$	$(7, a + 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
4153	$x^3 - x^2 - 1384x - 18304$	$(11, a - 5)$
4159	$x^3 - x^2 - 1386x - 12323$	$(19, \frac{1}{19}a^2 - \frac{5}{19}a - \frac{758}{19})$
4177	$x^3 - x^2 - 1392x + 5724$	$(17, a - 8)$
4201	$x^3 - x^2 - 1400x + 20227$	$(5, \frac{1}{5}a^2 + \frac{18}{5}a - \frac{928}{5})$
4231	$x^3 - x^2 - 1410x + 1567$	$(7, a + 1)$
4243	$x^3 - x^2 - 1414x + 13829$	$(13, a + 6)$
4273	$x^3 - x^2 - 1424x - 7913$	$(23, a + 5)$
4327	$x^3 - x^2 - 1442x + 9295$	$(5, a)$
4363	$x^3 - x^2 - 1454x + 21007$	$(7, \frac{3}{7}a^2 + \frac{37}{7}a - 414)$
4423	$x^3 - x^2 - 1474x - 10648$	$(11, a - 1)$
4441	$x^3 - x^2 - 1480x - 9211$	$(11, a + 1)$
4447	$x^3 - x^2 - 1482x + 19435$	$(23, a + 7)$
4483	$x^3 - x^2 - 1494x + 22581$	$(3, a - 1)$
4507	$x^3 - x^2 - 1502x + 15691$	$(13, a + 4)$
4513	$x^3 - x^2 - 1504x - 7856$	$(3, -\frac{1}{24}a^2 - \frac{9}{8}a + \frac{253}{6})$
4519	$x^3 - x^2 - 1506x + 21256$	$(5, a + 1)$
4549	$x^3 - x^2 - 1516x - 13984$	$(5, a + 1)$
4591	$x^3 - x^2 - 1530x + 23125$	$(7, a - 2)$
4597	$x^3 - x^2 - 1532x - 22304$	$(13, a + 1)$
4603	$x^3 - x^2 - 1534x + 18071$	$(23, a + 4)$
4621	$x^3 - x^2 - 1540x - 21907$	$(7, \frac{2}{7}a^2 - \frac{59}{7}a - \frac{2039}{7})$
4651	$x^3 - x^2 - 1550x + 23944$	$(17, a + 8)$
4657	$x^3 - x^2 - 1552x + 22940$	$(13, a + 4)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
4663	$x^3 - x^2 - 1554x - 2936$	$(5, a - 2)$
4723	$x^3 - x^2 - 1574x - 21341$	$(11, a + 2)$
4729	$x^3 - x^2 - 1576x + 10684$	$(3, -\frac{1}{24}a^2 - \frac{7}{8}a + \frac{509}{12})$
4759	$x^3 - x^2 - 1586x + 5464$	$(7, a - 2)$
4813	$x^3 - x^2 - 1604x - 18539$	$(47, a + 16)$
4831	$x^3 - x^2 - 1610x - 12167$	$(23, -\frac{7}{23}a^2 - \frac{16}{23}a + 329)$
4861	$x^3 - x^2 - 1620x - 24125$	$(5, \frac{2}{5}a^2 - \frac{47}{5}a - 428)$
4903	$x^3 - x^2 - 1634x + 13801$	$(11, a + 3)$
4909	$x^3 - x^2 - 1636x + 17636$	$(5, a + 1)$
4933	$x^3 - x^2 - 1644x + 1827$	$(7, a + 2)$
4951	$x^3 - x^2 - 1650x - 1467$	$(11, a - 2)$
4957	$x^3 - x^2 - 1652x - 15789$	$(7, -\frac{1}{7}a^2 + \frac{12}{7}a + \frac{1121}{7})$
4969	$x^3 - x^2 - 1656x + 25029$	$(3, \frac{1}{9}a^2 + \frac{26}{9}a - 123)$
4987	$x^3 - x^2 - 1662x - 18101$	$(19, -\frac{5}{19}a^2 - \frac{55}{19}a + \frac{5560}{19})$
4993	$x^3 - x^2 - 1664x - 2589$	$(101, a - 25)$
4999	$x^3 - x^2 - 1666x + 26291$	$(5, \frac{1}{5}a^2 + 4a - \frac{1111}{5})$
5011	$x^3 - x^2 - 1670x + 4083$	$(3, a)$
5023	$x^3 - x^2 - 1674x - 24929$	$(11, a + 3)$
5059	$x^3 - x^2 - 1686x - 21735$	$(5, \frac{1}{15}a^2 - \frac{13}{15}a - 75)$
5077	$x^3 - x^2 - 1692x + 5265$	$(5, a + 1)$
5101	$x^3 - x^2 - 1700x - 17948$	$(5, a + 2)$
5107	$x^3 - x^2 - 1702x - 24211$	$(11, a)$
5113	$x^3 - x^2 - 1704x + 13824$	$(5, a - 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
5167	$x^3 - x^2 - 1722x + 24304$	$(29, a - 6)$
5179	$x^3 - x^2 - 1726x + 23785$	$(5, a)$
5209	$x^3 - x^2 - 1736x + 23344$	$(73, a - 1)$
5227	$x^3 - x^2 - 1742x - 6195$	$(3, -\frac{1}{27}a^2 - \frac{34}{27}a + \frac{391}{9})$
5233	$x^3 - x^2 - 1744x - 17831$	$(3, \frac{1}{21}a^2 - \frac{2}{7}a - \frac{1189}{21})$
5281	$x^3 - x^2 - 1760x - 27383$	$(5, a + 2)$
5323	$x^3 - x^2 - 1774x + 22672$	$(3, \frac{1}{18}a^2 + \frac{1}{2}a - \frac{581}{9})$
5347	$x^3 - x^2 - 1782x - 10496$	$(7, a - 2)$
5407	$x^3 - x^2 - 1802x + 22429$	$(11, a + 4)$
5413	$x^3 - x^2 - 1804x + 5012$	$(7, a)$
5419	$x^3 - x^2 - 1806x - 25088$	$(17, a - 2)$
5431	$x^3 - x^2 - 1810x - 25747$	$(13, \frac{2}{13}a^2 + \frac{20}{13}a - \frac{2360}{13})$
5437	$x^3 - x^2 - 1812x - 28796$	$(23, a)$
5443	$x^3 - x^2 - 1814x - 28223$	$(7, \frac{1}{7}a^2 - 6a - \frac{1226}{7})$
5449	$x^3 - x^2 - 1816x - 24016$	$(17, a + 7)$
5503	$x^3 - x^2 - 1834x + 30776$	$(29, a - 1)$
5521	$x^3 - x^2 - 1840x + 10633$	$(7, a)$
5527	$x^3 - x^2 - 1842x - 20061$	$(7, \frac{1}{21}a^2 - \frac{1}{3}a - \frac{418}{7})$
5563	$x^3 - x^2 - 1854x + 28021$	$(7, a)$
5569	$x^3 - x^2 - 1856x + 17532$	$(3, \frac{1}{24}a^2 + \frac{1}{24}a - \frac{205}{4})$
5581	$x^3 - x^2 - 1860x + 7648$	$(7, \frac{1}{28} - \frac{9}{28}a - \frac{328}{7})$
5623	$x^3 - x^2 - 1874x - 10413$	$(19, a - 7)$
5641	$x^3 - x^2 - 1880x + 19639$	$(13, a + 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
5647	$x^3 - x^2 - 1882x + 29699$	$(17, a)$
5653	$x^3 - x^2 - 1884x - 7328$	$(19, a + 6)$
5683	$x^3 - x^2 - 1894x - 421$	$(5, a - 2)$
5689	$x^3 - x^2 - 1896x + 2107$	$(29, a + 2)$
5701	$x^3 - x^2 - 1900x - 15625$	$(7, a + 2)$
5737	$x^3 - x^2 - 1912x - 17636$	$(3, a + 1)$
5743	$x^3 - x^2 - 1914x + 25099$	$(19, a)$
5749	$x^3 - x^2 - 1916x - 2981$	$(11, a - 2)$
5791	$x^3 - x^2 - 1930x - 12011$	$(3, a + 1)$
5821	$x^3 - x^2 - 1940x + 10564$	$(7, \frac{1}{14}a^2 + \frac{3}{2}a - \frac{620}{7})$
5839	$x^3 - x^2 - 1946x - 22491$	$(3, a)$
5851	$x^3 - x^2 - 1950x + 13869$	$(23, a + 10)$
5857	$x^3 - x^2 - 1952x - 26465$	$(5, a)$
5869	$x^3 - x^2 - 1956x + 33475$	$(13, a)$
5881	$x^3 - x^2 - 1960x - 31801$	$(7, \frac{2}{7}a^2 - \frac{37}{7}a - 372)$
5923	$x^3 - x^2 - 1974x + 21937$	$(19, a + 9)$
6007	$x^3 - x^2 - 2002x + 17576$	$(13, -\frac{3}{13}a^2 + \frac{42}{13}a + 306)$
6043	$x^3 - x^2 - 2014x + 15667$	$(3, -\frac{1}{27}a^2 - \frac{8}{9}a + \frac{1306}{27})$
6067	$x^3 - x^2 - 2022x - 34155$	$(5, a + 1)$
6073	$x^3 - x^2 - 2024x + 33289$	$(5, a + 2)$
6091	$x^3 - x^2 - 2030x - 1128$	$(3, -\frac{1}{30}a^2 + \frac{17}{30}a + \frac{223}{5})$
6121	$x^3 - x^2 - 2040x - 22217$	$(13, a)$
6133	$x^3 - x^2 - 2044x + 13856$	$(7, -\frac{3}{28}a^2 - \frac{41}{28}a + \frac{1021}{7})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
6151	$x^3 - x^2 - 2050x + 34400$	$(5, -\frac{1}{5}a^2 - \frac{24}{5}a + 274)$
6199	$x^3 - x^2 - 2066x - 19745$	$(5, \frac{1}{25}a^2 - \frac{3}{25}a - \frac{277}{5})$
6211	$x^3 - x^2 - 2070x - 30825$	$(5, \frac{1}{15}a^2 - \frac{16}{15}a - 91)$
6217	$x^3 - x^2 - 2072x - 30164$	$(11, a + 4)$
6229	$x^3 - x^2 - 2076x - 10151$	$(37, a + 10)$
6271	$x^3 - x^2 - 2090x + 7200$	$(3, \frac{1}{30}a^2 - \frac{41}{30}a - 46)$
6277	$x^3 - x^2 - 2092x + 12089$	$(11, a - 2)$
6301	$x^3 - x^2 - 2100x - 33372$	$(3, \frac{1}{12}a^2 - \frac{19}{12}a - \frac{231}{2})$
6337	$x^3 - x^2 - 2112x - 35675$	$(7, -\frac{1}{7}a^2 + \frac{16}{7}a + \frac{1403}{7})$
6343	$x^3 - x^2 - 2114x - 28661$	$(5, a + 2)$
6361	$x^3 - x^2 - 2120x + 36988$	$(7, a - 3)$
6367	$x^3 - x^2 - 2122x - 34429$	$(11, a + 5)$
6373	$x^3 - x^2 - 2124x + 32101$	$(7, a + 3)$
6379	$x^3 - x^2 - 2126x - 11813$	$(29, a + 11)$
6397	$x^3 - x^2 - 2132x + 35065$	$(5, a)$
6421	$x^3 - x^2 - 2140x - 28300$	$(61, a - 10)$
6427	$x^3 - x^2 - 2142x + 38800$	$(5, a + 1)$
6451	$x^3 - x^2 - 2150x - 35600$	$(5, -\frac{1}{10}a^2 + \frac{1}{10}a + 143)$
6469	$x^3 - x^2 - 2156x + 31147$	$(19, \frac{1}{19}a^2 + \frac{11}{19}a - \frac{1359}{19})$
6481	$x^3 - x^2 - 2160x + 19683$	$(11, a - 2)$
6529	$x^3 - x^2 - 2176x + 3869$	$(13, a + 3)$
6547	$x^3 - x^2 - 2182x - 13579$	$(29, \frac{1}{29}a^2 + \frac{4}{29}a - \frac{1727}{29})$
6571	$x^3 - x^2 - 2190x + 24337$	$(31, a - 6)$
		Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
6577	$x^3 - x^2 - 2192x + 5359$	$(11, a + 4)$
6607	$x^3 - x^2 - 2202x + 15661$	$(37, a + 13)$
6619	$x^3 - x^2 - 2206x - 4903$	$(23, a + 3)$
6661	$x^3 - x^2 - 2220x - 17516$	$(7, \frac{3}{28}a^2 - \frac{53}{28}a - \frac{2193}{14})$
6673	$x^3 - x^2 - 2224x - 38308$	$(37, a + 10)$
6679	$x^3 - x^2 - 2226x - 22016$	$(13, \frac{2}{13}a^2 - \frac{45}{13}a - \frac{2997}{13})$
6691	$x^3 - x^2 - 2230x - 36181$	$(19, a + 4)$
6703	$x^3 - x^2 - 2234x + 41211$	$(3, -\frac{1}{3}a^2 - \frac{28}{3}a + 500)$
6733	$x^3 - x^2 - 2244x - 15461$	$(29, \frac{1}{29}a^2 + \frac{90}{29}a - \frac{1739}{29})$
6763	$x^3 - x^2 - 2254x - 27553$	$(41, a + 9)$
6781	$x^3 - x^2 - 2260x + 35663$	$(19, a - 8)$
6793	$x^3 - x^2 - 2264x - 8051$	$(5, a - 2)$
6823	$x^3 - x^2 - 2274x - 38411$	$(11, a + 3)$
6829	$x^3 - x^2 - 2276x + 10117$	$(67, a + 11)$
6841	$x^3 - x^2 - 2280x + 39019$	$(17, a + 7)$
6871	$x^3 - x^2 - 2290x + 26975$	$(13, a - 2)$
6883	$x^3 - x^2 - 2294x - 31101$	$(5, a + 2)$
6907	$x^3 - x^2 - 2302x - 9721$	$(11, a - 1)$
6949	$x^3 - x^2 - 2316x + 11839$	$(17, a + 3)$
6961	$x^3 - x^2 - 2320x - 2836$	$(7, a + 1)$
6967	$x^3 - x^2 - 2322x - 41544$	$(3, -\frac{1}{6}a^2 + \frac{31}{6}a + 257)$
6997	$x^3 - x^2 - 2332x + 43796$	$(29, a + 6)$
7039	$x^3 - x^2 - 2346x - 11471$	$(11, a + 4)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
7057	$x^3 - x^2 - 2352x - 37376$	$(13, a - 1)$
7069	$x^3 - x^2 - 2356x - 38225$	$(3, \frac{1}{15}a^2 - \frac{6}{5}a - \frac{317}{3})$
7129	$x^3 - x^2 - 2376x - 35381$	$(13, a + 2)$
7159	$x^3 - x^2 - 2386x - 19621$	$(7, a - 3)$
7177	$x^3 - x^2 - 2392x - 24455$	$(3, -\frac{1}{27}a^2 - \frac{8}{9}a + \frac{1603}{27})$
7207	$x^3 - x^2 - 2402x + 39505$	$(5, a - 2)$
7213	$x^3 - x^2 - 2404x - 41408$	$(19, a - 9)$
7219	$x^3 - x^2 - 2406x + 41175$	$(53, a - 25)$
7237	$x^3 - x^2 - 2412x + 21979$	$(29, \frac{3}{29}a^2 + \frac{139}{29}a - \frac{4562}{29})$
7243	$x^3 - x^2 - 2414x + 15559$	$(11, a + 4)$
7309	$x^3 - x^2 - 2436x + 46561$	$(5, a + 1)$
7321	$x^3 - x^2 - 2440x + 45824$	$(11, a + 3)$
7333	$x^3 - x^2 - 2444x - 45356$	$(5, a + 2)$
7369	$x^3 - x^2 - 2456x + 33024$	$(3, \frac{1}{24}a^2 + \frac{7}{24}a - 68)$
7393	$x^3 - x^2 - 2464x + 4381$	$(41, a + 10)$
7411	$x^3 - x^2 - 2470x - 30193$	$(19, a + 3)$
7417	$x^3 - x^2 - 2472x + 17581$	$(17, a + 7)$
7459	$x^3 - x^2 - 2486x + 45859$	$(47, a + 5)$
7477	$x^3 - x^2 - 2492x - 33785$	$(5, a + 1)$
7507	$x^3 - x^2 - 2502x + 7785$	$(5, a + 1)$
7537	$x^3 - x^2 - 2512x - 13120$	$(5, a - 2)$
7549	$x^3 - x^2 - 2516x - 39143$	$(13, a)$
7561	$x^3 - x^2 - 2520x - 7281$	$(3, \frac{1}{33}a^2 + \frac{4}{3}a - \frac{565}{11})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
7573	$x^3 - x^2 - 2524x + 29731$	$(3, a + 1)$
7591	$x^3 - x^2 - 2530x + 9559$	$(11, \frac{1}{33}a^2 - \frac{4}{11}a - \frac{155}{3})$
7603	$x^3 - x^2 - 2534x + 36607$	$(13, a + 5)$
7669	$x^3 - x^2 - 2556x - 38061$	$(3, -\frac{1}{21}a^2 - \frac{8}{21}a + \frac{569}{7})$
7681	$x^3 - x^2 - 2560x + 45517$	$(3, a + 1)$
7699	$x^3 - x^2 - 2566x + 32792$	$(7, a - 1)$
7717	$x^3 - x^2 - 2572x + 50875$	$(5, a)$
7723	$x^3 - x^2 - 2574x + 46624$	$(17, a + 8)$
7741	$x^3 - x^2 - 2580x + 41572$	$(5, \frac{1}{20}a^2 - \frac{7}{20}a - \frac{859}{10})$
7759	$x^3 - x^2 - 2586x - 33335$	$(5, a)$
7789	$x^3 - x^2 - 2596x - 47311$	$(11, \frac{1}{11}a^2 - \frac{56}{11}a - 157)$
7873	$x^3 - x^2 - 2624x - 17204$	$(11, a - 3)$
7927	$x^3 - x^2 - 2642x - 33176$	$(11, a)$
7933	$x^3 - x^2 - 2644x - 27031$	$(5, a - 2)$
7951	$x^3 - x^2 - 2650x + 15313$	$(23, a - 11)$
7963	$x^3 - x^2 - 2654x - 43944$	$(3, \frac{1}{18}a^2 - \frac{17}{18}a - \frac{295}{3})$
7993	$x^3 - x^2 - 2664x + 40261$	$(17, a + 2)$
8053	$x^3 - x^2 - 2684x - 14913$	$(3, a)$
8059	$x^3 - x^2 - 2686x - 8656$	$(17, \frac{1}{34}a^2 + \frac{11}{34}a - \frac{1005}{17})$
8089	$x^3 - x^2 - 2696x - 41943$	$(3, a)$
8101	$x^3 - x^2 - 2700x + 32704$	$(7, \frac{1}{28}a^2 + \frac{3}{28}a - 64)$
8161	$x^3 - x^2 - 2720x + 50175$	$(3, a)$
8167	$x^3 - x^2 - 2722x - 41440$	$(5, a - 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
8179	$x^3 - x^2 - 2726x - 53315$	$(5, a)$
8221	$x^3 - x^2 - 2740x - 17051$	$(3, a + 1)$
8233	$x^3 - x^2 - 2744x + 45129$	$(3, -\frac{1}{21}a^2 + \frac{8}{21}a + 87)$
8263	$x^3 - x^2 - 2754x - 41009$	$(17, a + 2)$
8293	$x^3 - x^2 - 2764x + 27029$	$(5, a - 1)$
8311	$x^3 - x^2 - 2770x + 4925$	$(5, \frac{1}{35}a^2 - \frac{16}{35}a - \frac{373}{7})$
8317	$x^3 - x^2 - 2772x - 32960$	$(5, a)$
8329	$x^3 - x^2 - 2776x + 32699$	$(19, a - 2)$
8353	$x^3 - x^2 - 2784x + 55996$	$(89, a - 42)$
8377	$x^3 - x^2 - 2792x - 40644$	$(3, -\frac{1}{24}a^2 + \frac{35}{24}a + \frac{307}{4})$
8389	$x^3 - x^2 - 2796x - 55616$	$(7, a + 2)$
8419	$x^3 - x^2 - 2806x - 53944$	$(5, \frac{1}{5}a^2 - 7a - \frac{1871}{5})$
8431	$x^3 - x^2 - 2810x - 49337$	$(7, a + 1)$
8443	$x^3 - x^2 - 2814x - 47531$	$(19, -\frac{2}{19}a^2 - \frac{80}{19}a + \frac{3621}{19})$
8461	$x^3 - x^2 - 2820x - 36351$	$(11, a + 2)$
8467	$x^3 - x^2 - 2822x - 26969$	$(19, a + 1)$
8521	$x^3 - x^2 - 2840x + 58069$	$(7, \frac{3}{7}a^2 + \frac{85}{7}a - \frac{5721}{7})$
8527	$x^3 - x^2 - 2842x - 46109$	$(3, a + 1)$
8539	$x^3 - x^2 - 2846x - 32891$	$(13, a - 1)$
8581	$x^3 - x^2 - 2860x + 39409$	$(3, \frac{1}{27}a^2 + \frac{2}{9}a - \frac{1873}{27})$
8599	$x^3 - x^2 - 2866x + 50957$	$(19, \frac{5}{19}a^2 + \frac{213}{19}a - \frac{9455}{19})$
8623	$x^3 - x^2 - 2874x - 54293$	$(11, a + 5)$
8641	$x^3 - x^2 - 2880x + 43525$	$(7, a + 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
8677	$x^3 - x^2 - 2892x + 49491$	$(7, a + 1)$
8689	$x^3 - x^2 - 2896x - 12229$	$(5, a + 1)$
8707	$x^3 - x^2 - 2902x + 60304$	$(3, \frac{1}{6}a^2 + \frac{9}{2}a - \frac{968}{3})$
8713	$x^3 - x^2 - 2904x - 57764$	$(7, a)$
8719	$x^3 - x^2 - 2906x + 56512$	$(7, a + 1)$
8737	$x^3 - x^2 - 2912x + 59541$	$(3, \frac{1}{9}a^2 + \frac{25}{9}a - \frac{649}{3})$
8761	$x^3 - x^2 - 2920x - 26932$	$(17, a + 8)$
8779	$x^3 - x^2 - 2926x - 32840$	$(3, a + 1)$
8803	$x^3 - x^2 - 2934x + 61947$	$(3, -\frac{1}{3}a^2 - \frac{32}{3}a + 655)$
8821	$x^3 - x^2 - 2940x - 14375$	$(5, -\frac{1}{35}a^2 - \frac{44}{35}a + \frac{395}{7})$
8839	$x^3 - x^2 - 2946x + 32737$	$(19, a + 4)$
8863	$x^3 - x^2 - 2954x - 60728$	$(17, a + 8)$
8893	$x^3 - x^2 - 2964x + 59616$	$(3, a - 1)$
8923	$x^3 - x^2 - 2974x - 54199$	$(17, \frac{1}{17}a^2 - \frac{20}{17}a - \frac{1897}{17})$
8929	$x^3 - x^2 - 2976x + 47952$	$(29, a - 8)$
8941	$x^3 - x^2 - 2980x - 51328$	$(5, \frac{1}{20}a^2 - \frac{37}{20}a - \frac{507}{5})$
8971	$x^3 - x^2 - 2990x - 16613$	$(5, -\frac{1}{35}a^2 + \frac{27}{35}a + \frac{2078}{35})$
9001	$x^3 - x^2 - 3000x - 56673$	$(5, \frac{1}{15}a^2 - \frac{22}{15}a - \frac{676}{5})$
9007	$x^3 - x^2 - 3002x + 61381$	$(11, \frac{1}{11}a^2 + \frac{35}{11}a - \frac{1951}{11})$
9013	$x^3 - x^2 - 3004x - 39724$	$(7, a + 1)$
9043	$x^3 - x^2 - 3014x - 49904$	$(11, \frac{2}{11}a^2 - \frac{74}{11}a - \frac{4046}{11})$
9049	$x^3 - x^2 - 3016x + 47591$	$(5, \frac{1}{25}a^2 + \frac{2}{5}a - \frac{1981}{25})$
9067	$x^3 - x^2 - 3022x - 58096$	$(7, a - 3)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
9091	$x^3 - x^2 - 3030x + 57913$	$(13, a + 4)$
9103	$x^3 - x^2 - 3034x - 61361$	$(3, -\frac{1}{9}a^2 + 2a + \frac{2017}{9})$
9133	$x^3 - x^2 - 3044x + 65284$	$(5, a + 2)$
9151	$x^3 - x^2 - 3050x - 59651$	$(13, a + 5)$
9157	$x^3 - x^2 - 3052x + 29845$	$(3, a + 1)$
9181	$x^3 - x^2 - 3060x - 63927$	$(3, \frac{1}{3}a^2 - \frac{34}{3}a - 677)$
9187	$x^3 - x^2 - 3062x + 47296$	$(13, -\frac{1}{13}a^2 + \frac{69}{13}a + \frac{2023}{13})$
9199	$x^3 - x^2 - 3066x + 21805$	$(5, \frac{1}{35}a^2 - \frac{8}{35}a - 58)$
9343	$x^3 - x^2 - 3114x + 47061$	$(7, a)$
9349	$x^3 - x^2 - 3116x - 36011$	$(11, a - 5)$
9397	$x^3 - x^2 - 3132x + 9745$	$(5, a - 2)$
9403	$x^3 - x^2 - 3134x - 26816$	$(5, a + 2)$
9433	$x^3 - x^2 - 3144x - 59393$	$(13, a + 1)$
9439	$x^3 - x^2 - 3146x - 39504$	$(3, \frac{1}{30}a^2 - \frac{1}{6}a - \frac{351}{5})$
9463	$x^3 - x^2 - 3154x - 48016$	$(5, a + 2)$
9547	$x^3 - x^2 - 3182x - 11315$	$(5, a)$
9613	$x^3 - x^2 - 3204x - 47709$	$(19, a)$
9619	$x^3 - x^2 - 3206x + 59139$	$(3, \frac{1}{21}a^2 + \frac{16}{21}a - \frac{712}{7})$
9631	$x^3 - x^2 - 3210x + 70984$	$(7, a + 2)$
9643	$x^3 - x^2 - 3214x + 70001$	$(7, \frac{1}{7}a^2 + a - \frac{2136}{7})$
9661	$x^3 - x^2 - 3220x - 13597$	$(19, a + 9)$
9679	$x^3 - x^2 - 3226x - 39433$	$(11, a + 4)$
9733	$x^3 - x^2 - 3244x + 57677$	$(29, a - 5)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
9739	$x^3 - x^2 - 3246x + 32824$	$(11, a)$
9769	$x^3 - x^2 - 3256x - 52825$	$(5, a)$
9781	$x^3 - x^2 - 3260x - 47456$	$(7, \frac{1}{14}a^2 + \frac{33}{14}a - \frac{1083}{7})$
9787	$x^3 - x^2 - 3262x + 67784$	$(7, -\frac{1}{7}a^2 - \frac{44}{7}a + \frac{2185}{7})$
9811	$x^3 - x^2 - 3270x + 6904$	$(23, a - 2)$
9817	$x^3 - x^2 - 3272x + 57084$	$(3, a)$
9829	$x^3 - x^2 - 3276x + 29851$	$(7, -\frac{1}{35}a^2 + \frac{22}{7}a + \frac{2206}{35})$
9859	$x^3 - x^2 - 3286x + 71569$	$(3, a + 1)$
9871	$x^3 - x^2 - 3290x - 70925$	$(5, \frac{1}{5}a^2 - \frac{31}{5}a - 436)$
9883	$x^3 - x^2 - 3294x + 69547$	$(11, a + 4)$
9901	$x^3 - x^2 - 3300x - 35937$	$(11, \frac{1}{33}a^2 - \frac{1}{33}a - 66)$
9931	$x^3 - x^2 - 3310x - 63632$	$(3, a + 1)$
9949	$x^3 - x^2 - 3316x - 60431$	$(3, a + 1)$
9967	$x^3 - x^2 - 3322x - 47251$	$(29, \frac{1}{29}a^2 - \frac{8}{29}a - \frac{2628}{29})$
9973	$x^3 - x^2 - 3324x + 26964$	$(3, -\frac{1}{36}a^2 - \frac{29}{36}a + \frac{367}{6})$
10009	$x^3 - x^2 - 3336x - 66356$	$(7, a + 2)$
10039	$x^3 - x^2 - 3346x + 56144$	$(11, a)$
10093	$x^3 - x^2 - 3364x + 66539$	$(5, a - 1)$
10099	$x^3 - x^2 - 3366x + 50869$	$(7, a - 3)$
10111	$x^3 - x^2 - 3370x - 20971$	$(17, a + 6)$
10141	$x^3 - x^2 - 3380x + 69109$	$(17, a - 8)$
10159	$x^3 - x^2 - 3386x - 69608$	$(11, a + 4)$
10177	$x^3 - x^2 - 3392x + 55785$	$(3, \frac{1}{27}a^2 + \frac{10}{27}a - \frac{752}{9})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
10243	$x^3 - x^2 - 3414x - 74736$	$(5, a+2)$
10273	$x^3 - x^2 - 3424x - 761$	$(3, \frac{1}{39}a^2 + \frac{6}{13}a - \frac{2341}{39})$
10303	$x^3 - x^2 - 3434x + 39304$	$(59, a-16)$
10321	$x^3 - x^2 - 3440x + 42813$	$(11, a+3)$
10333	$x^3 - x^2 - 3444x + 55492$	$(31, a+13)$
10369	$x^3 - x^2 - 3456x - 51461$	$(11, a+2)$
10429	$x^3 - x^2 - 3476x + 32832$	$(3, -\frac{1}{36}a^2 - \frac{31}{36}a + 65)$
10453	$x^3 - x^2 - 3484x + 75881$	$(19, a+1)$
10459	$x^3 - x^2 - 3486x - 65853$	$(7, \frac{1}{21}a^2 - \frac{19}{21}a - \frac{761}{7})$
10477	$x^3 - x^2 - 3492x - 10089$	$(3, \frac{1}{39}a^2 + \frac{14}{39}a - \frac{769}{13})$
10501	$x^3 - x^2 - 3500x - 26447$	$(11, a+2)$
10531	$x^3 - x^2 - 3510x - 20672$	$(7, a+3)$
10567	$x^3 - x^2 - 3522x + 81405$	$(3, -\frac{1}{3}a^2 - \frac{35}{3}a + 786)$
10597	$x^3 - x^2 - 3532x - 32576$	$(3, a+1)$
10627	$x^3 - x^2 - 3542x + 72421$	$(19, a+3)$
10639	$x^3 - x^2 - 3546x - 74079$	$(3, \frac{1}{15}a^2 - \frac{5}{3}a - \frac{782}{5})$
10651	$x^3 - x^2 - 3550x + 73768$	$(3, \frac{1}{18}a^2 + \frac{7}{6}a - \frac{1175}{9})$
10657	$x^3 - x^2 - 3552x + 46575$	$(5, a)$
10663	$x^3 - x^2 - 3554x + 69112$	$(23, a+8)$
10711	$x^3 - x^2 - 3570x + 68233$	$(11, a+2)$
10723	$x^3 - x^2 - 3574x - 29389$	$(7, a+2)$
10729	$x^3 - x^2 - 3576x + 18279$	$(3, \frac{1}{39}a^2 - \frac{1}{3}a - \frac{802}{13})$
10753	$x^3 - x^2 - 3584x + 76864$	$(5, a+2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
10789	$x^3 - x^2 - 3596x - 55943$	$(43, a)$
10831	$x^3 - x^2 - 3610x + 78625$	$(3, \frac{1}{15}a^2 + \frac{8}{5}a - \frac{479}{3})$
10837	$x^3 - x^2 - 3612x + 83485$	$(5, a)$
10861	$x^3 - x^2 - 3620x + 66775$	$(17, a + 4)$
10867	$x^3 - x^2 - 3622x + 20929$	$(3, a + 1)$
10891	$x^3 - x^2 - 3630x - 46791$	$(11, \frac{1}{11}a^2 + \frac{7}{11}a - \frac{2375}{11})$
10903	$x^3 - x^2 - 3634x - 26248$	$(19, a - 4)$
10909	$x^3 - x^2 - 3636x + 54949$	$(7, a + 2)$
10993	$x^3 - x^2 - 3664x - 74101$	$(5, a + 2)$
11047	$x^3 - x^2 - 3682x + 36005$	$(17, a - 6)$
11059	$x^3 - x^2 - 3686x + 86424$	$(3, a)$
11119	$x^3 - x^2 - 3706x - 82363$	$(7, a + 1)$
11131	$x^3 - x^2 - 3710x - 42875$	$(5, \frac{1}{35}a^2 - \frac{1}{35}a - 70)$
11161	$x^3 - x^2 - 3720x - 14468$	$(5, a + 2)$
11173	$x^3 - x^2 - 3724x + 84832$	$(3, -\frac{1}{12}a^2 - \frac{13}{4}a + \frac{619}{3})$
11197	$x^3 - x^2 - 3732x + 26541$	$(3, \frac{1}{39}a^2 - \frac{10}{39}a - \frac{837}{13})$
11239	$x^3 - x^2 - 3746x + 46621$	$(5, \frac{1}{35}a^2 - \frac{2451}{35})$
11251	$x^3 - x^2 - 3750x - 85841$	$(17, a + 2)$
11287	$x^3 - x^2 - 3762x - 67304$	$(13, a - 3)$
11299	$x^3 - x^2 - 3766x + 89555$	$(11, a - 2)$
11317	$x^3 - x^2 - 3772x + 59519$	$(31, \frac{1}{31}a^2 + \frac{7}{31}a - \frac{2042}{31})$
11329	$x^3 - x^2 - 3776x + 20560$	$(5, \frac{1}{40}a^2 - \frac{13}{40}a - \frac{125}{2})$
11353	$x^3 - x^2 - 3784x - 841$	$(5, a - 2)$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
11383	$x^3 - x^2 - 3794x + 54807$	$(3, a)$
11437	$x^3 - x^2 - 3812x + 9319$	$(19, a + 1)$
11443	$x^3 - x^2 - 3814x - 84763$	$(7, a)$
11467	$x^3 - x^2 - 3822x - 87489$	$(31, a + 1)$
11497	$x^3 - x^2 - 3832x - 39175$	$(5, a + 1)$
11503	$x^3 - x^2 - 3834x + 11929$	$(37, a + 11)$
11527	$x^3 - x^2 - 3842x - 29031$	$(3, \frac{1}{39}a^2 + \frac{7}{39}a - \frac{859}{13})$
11551	$x^3 - x^2 - 3850x + 64600$	$(3, \frac{1}{30}a^2 + \frac{13}{10}a - \frac{253}{3})$
11587	$x^3 - x^2 - 3862x + 14591$	$(31, a - 5)$
11593	$x^3 - x^2 - 3864x + 42937$	$(23, a + 10)$
11617	$x^3 - x^2 - 3872x - 91215$	$(3, \frac{1}{3}a^2 - \frac{38}{3}a - 856)$
11677	$x^3 - x^2 - 3892x + 92551$	$(17, a + 1)$
11689	$x^3 - x^2 - 3896x + 17317$	$(23, a + 10)$
11701	$x^3 - x^2 - 3900x - 73673$	$(47, a + 7)$
11719	$x^3 - x^2 - 3906x + 82467$	$(13, a + 6)$
11731	$x^3 - x^2 - 3910x + 81248$	$(11, \frac{1}{22}a^2 + \frac{19}{22}a - \frac{1358}{11})$
11743	$x^3 - x^2 - 3914x + 64369$	$(17, a + 3)$
11821	$x^3 - x^2 - 3940x - 87563$	$(3, -\frac{1}{15}a^2 + \frac{14}{5}a + \frac{2638}{15})$
11827	$x^3 - x^2 - 3942x + 35919$	$(3, \frac{1}{39}a^2 - \frac{7}{39}a - 68)$
11833	$x^3 - x^2 - 3944x + 96417$	$(3, \frac{1}{3}a^2 + \frac{34}{3}a - 880)$
11839	$x^3 - x^2 - 3946x + 70157$	$(41, a + 15)$
11863	$x^3 - x^2 - 3954x - 39104$	$(13, a + 1)$
11923	$x^3 - x^2 - 3974x - 2208$	$(7, -\frac{1}{21}a^2 - \frac{61}{21}a + \frac{890}{7})$

Continued on next page

Table 5.1

f	*polynomial*	*admissible prime*
11941	$x^3 - x^2 - 3980x + 97297$	$(5, \frac{1}{5}a^2 + \frac{33}{5}a - \frac{2653}{5})$
11953	$x^3 - x^2 - 3984x + 64192$	$(17, a + 2)$
11959	$x^3 - x^2 - 3986x + 77512$	$(43, a + 10)$
11971	$x^3 - x^2 - 3990x + 8424$	$(3, \frac{1}{42}a^2 - \frac{61}{42}a - \frac{440}{7})$

Bibliography

[1] S. Alaca, K. S. Williams, *Introductory algebraic number theory,* Cambridge University Press, 2003.

[2] V. Buniakovsky, *Sur les diviseurs numeriques invariables des fonctions rationnelles entieres,* Mem Acad. Sci. St Petersburg 6 (1857), 305 – 329.

[3] H. Chatland and H. Davenport, *Euclid's algorithm in quadratic number fields*, Canadian Journal of Mathematics **2** (1950), 289 – 296.

[4] D. A. Clark, M. Ram Murty, *The Euclidean algorithm for Galois extensions,* Journal für die reine und angewandte Mathematik.459(1995), 151–162.

[5] A. Clark, *A quadratic field which is Euclidean but not norm-Euclidean,* Manuscripta Mathematica 83 (1994), 327 – 330.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer Verlag (1993).

[7] H. Davenport, *Euclid's algorithm in cubic fields of negative discriminant*, Acta Math. 84 (1950), 159 –179.

[8] D. S. Dummit, R. M. Foote, *Abstract Algebra,* John Wiley & Sons, 2004.

[9] J. Esmonde, M. Ram Murty, *Problems in Algebraic Number Theory,* Graduate texts in Mathematics. Springer-Verlag New York, Inc.

[10] H. Graves, M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions,* J. Number Theory 133 (2013), 1809 –1813.

[11] H. J. Godwin, J. R. Smith, *On the Euclidean nature of four cyclic cubic fields,* Math. Comp. 60 (1993), 421– 423.

[12] R. Gupta, M. Ram Murty, V. Kumar Murty, *The Euclidean algorithm for S-integers,* In: Number Theory (eds. H. Kisilevsky and J. Labute), CMS Conf. Proc. 7 (1987), 189 – 201.

[13] K. Győry, *On the* abc *conjecture in algebraic number fields,* Acta Arith. 133 (2008), no. 3, 281 – 295.

[14] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean,* Canad. J. Math. 56 No.1,(2004), 55 – 70.

[15] H. Heilbronn, *On Euclid's algorithm in cubic self-conjugate fields*, Proc. Cambridge Philosophical Society, Vol. 46 (1950), 377 – 382.

[16] C. Hooley, *On Artin's conjecture,* J. Reine Agew. Math. 225 (1967), 209 – 220.

[17] G. J. Janusz, *Algebraic Number Fields*, Providence, R. I., AMS (1996).

[18] J.W. Jones, D.P. Roberts, *A database of number fields*, Volume 17, Issue 1 2014, 595 – 618.

[19] F. Lemmermeyer,

List of publications

1. (with M. Ram Murty, K. Srinivas) *Admissible primes and Euclidean quadratic fields*, (submitted).

2. (with K. Srinivas) *Non-Wieferich primes in number fields and abc conjecture*, Czechoslovak Mathematical Journal, (*accepted* for publication).

3. (with K. Srinivas) *A note on Euclidean cyclic cubic fields*, Journal of the Ramanujan Mathematical Society, (*accepted* for publication).