University of Bordeaux I

Department Of Mathematics

A Survey On Euclidean Number Fields

Author:
M.A. Simachew

Supervisor:
J-P. Cerri

2009

University of Bordeaux I

Department Of Mathematics

A Survey On Euclidean Number Fields

Author:
M.A. Simachew

Supervisor:
J-P. Cerri

Examiners

1. Professor B. Erez — Boas.Erez@math.u-bordeaux1.fr
2. Professor Y. Bilu — Yuri.Bilu@math.u-bordeaux1.fr
3. Professor R. Coulangeon — Renaud.Coulangeon@math.u-bordeaux1.fr
4. Professor J-P. Cerri — Jean-Paul.Cerri@math.u-bordeaux1.fr

To my beloved parents.

Acknowledgements

Above all, I am so grateful to God for everything. My thanks then goes to my supervisor, Jean-Paul Cerri, for his professional help, comments and suggestions throughout the preparation of this memoir in addition to his valuable articles on Euclidean minima. I would also like to thank H. W. Lenstra, Jr. for his many interesting results on the subject of my work; his attendance of my partial presentation in Netherlands and his concerned, detailed and friendly letter-reply to me on the subject.

I am thankful to Boas Erez, Yuri Bilu, Francesco Baldasari, Marco Garutti and Edixhoven together with all the other committee members of *Algant Consortium* who have made possible my great transition to modern mathematical concepts in the areas of *Algebra, Geometry And Number Theory*, (ALGANT). I indeed appreciate the generosity of *European Commission* for the *Erasmus Mundus Masters Program* scholarship. I also thank all my professors in Italy last year and France this year who involved directly or indirectly in my progress in mathematics.

Moreover, I am indebited to *International Relations Office* runners, Muriel Vernay, Delphine Gassiot Casalas, Sylvie Coursiere and Elisa Aghito; my tutors, Alessandra Bertapelle of Padova and Elizabeth Strouse of Bordeaux and all my friends as well.

Last but not least, I am proud to have a wonderful family; I would like to thank them all for every support they have been giving me in life since my existence on earth.

Contents

Chapter 1

Introduction

1.1 Historical Background

The Greek mathematician Euclid of Alexandria (fl. 300 BC) is often called the father of geometry for his contribution to mathematics especially in what we currently call Euclidean Geometry. His *Elements* is the most successful textbook and one of the most influential works in the history of mathematics, serving as the main reference for teaching from the time of its publication until the early 20th century.

Although best known for its geometric results, the *Elements* also includes number theoretic knowledge. It considers the connection between perfect numbers and Mersenne primes[1], the infinitude of prime numbers, Euclid's lemma on factorization which leads to the fundamental theorem of arithmetic on uniqueness of prime factorizations and the Euclidean algorithm for finding greatest common divisor of two numbers.

Euclidean algorithm, the oldest non trivial algorithm that has survived to the present time, was indeed described by him in books 7 and 10 of his *Elements*. He used it for integers in the first and for line segments in the later. However, it is unknown whether this algorithm had existed before him or he discovered it himself.

In the 19th century, the Euclidean algorithm led to the development of new number systems, such as Gaussian integers and Eisenstein integers[2]. In 1815, Carl Gauss used the Euclidean algorithm to demonstrate unique factorization of Gaussian integers. Gauss mentioned the algorithm in his *Disquisitiones Arithmeticae* (1801) as a method for continued fractions.

[1] A perfect number is a positive integer which is the sum of its proper positive divisors; where as a Mersenne prime M_p is a positive prime integer of the form $M_p = 2^p - 1$

[2] Eisenstein integers are complex numbers of the form $a + b\omega$ where a and b are integers and ω is a third primitive root of unity given by $\omega = (-1 + i\sqrt{3})/2 = e^{2\pi i/3}$

Peter Dirichlet described the Euclidean algorithm as the basis for much of number theory. He noted that many results of number theory, such as unique factorization, would hold true for not only the ordinary integers but also any other system of numbers which the Euclidean algorithm could be applied to. Richard Dedekind used Euclid's algorithm to study the nature of algebraic integers, a new general type of numbers containing integers . He was the first to prove Fermat's two-square theorem by using unique factorization of Gaussian integers. He defined the concept of a Euclidean domain. In the closing decades of the 19th century, however, the Euclidean algorithm gradually became eclipsed by Dedekind's more general theory of ideals.

1.2 Some Applications Of Euclidean Algorithm

Euclidean algorithm has extensive theoretical and practical applications not only in mathematics but also in various topics of other related disciplines. It mainly is about computing the greatest common divisor.

* Greatest Common Divisor: Given two integers, a and b, their gcd can be computed efficiently by using the fact that $(a, b) = (b, a - bq)$ where $0 \leq |a - bq| < |b|$.

* Continued Fractions: This is discussed in section 3.5 of the third chapter.

* Bézout's Identity [Extended Eulidean Algorithm]: Given two integers a and b, their gcd, d can be written as $d = xa + yb$ for some integers x and y which can easily be computed by reversing the Euclidean algorithm after finding the d. Hence if the two numbers are coprime, modular inverses of a and b in $\mathbb{Z}/b\mathbb{Z}$ and $\mathbb{Z}/a\mathbb{Z}$ respectively can easily be found.

* Principal Ideals: If $d = (a, b)$, then the ideal of $\mathbb{Z}$ generated by d is $(d) = \{xa + yb, \text{ where } x, y \in \mathbb{Z}\}$. Moreover, we will see the fact that Euclidean domain implies principal ideal domain.

* Unique Factorization Domain: Euclidean Domain$\Rightarrow$PID$\Rightarrow$UFD

* Linear Diophantine Equations: A typical DE, $ax + by = c$ is equivalent to $ax \equiv c \mod b$ or $by \equiv c \mod a$. Hence it is soluble if $(a, b) \mid c$ and in which case, dividing both sides by (a, b), reduces the congruence to its Bézout's relation.

* Chinese Remainder Theorem (CRT): This classic theorem aims at finding an integer that satisfies multiple equivalences in various modular values. i.e.

$$\begin{aligned} x &\equiv x_1 \mod m_1 \\ x &\equiv x_2 \mod m_2 \\ &\cdots \\ x &\equiv x_n \mod m_n \end{aligned}$$

where $(m_i, m_j) = 1$ if $i \neq j$. This can thus be reduced to a single diophantine equation as,

$$x \equiv x_1 M_1 r_1 + x_2 M_2 r_2 + \cdots + x_n M_n r_n \mod M$$

where $M = \prod m_i$, $M_i = M/m_i$ and $r_i = M_i^{-1} \mod m_i$

* Cryptography: As cryptography is the direct application of number theory in real life problems, Euclidean division involves in its many algorithms all often. For instance, the highly secured cryptosystem which is commonly used at the present time in e-commerce, RSA algorithm, involves computing *gcd* and modular inverse. It is very interesting to see how it works:

  Mr. A and Ms. B, the receiver and sender of a secret message, respectively choose very large primes q and p whose lengths are advised to be more than 512 bits for high level of security. Mr. A computes $n = pq$; selects a number $e > 1$ such that $(\phi(n), e) = 1$ and finds its modular inverse $d = e^{-1} \mod \phi(n)$. Here $\phi(n) = (p-1)(q-1)$ as the probability of $p = q$ is negligible for their large random values. He then makes (e, n) public so that the sender uses it for encryption, where as d is his private key. Then Ms. B sends a message to Mr. A (it can be encoded canonically as a number a between 0 and $n-1$ for a sufficiently large n) as b where $b = a^e \mod n$. Then Mr. A decrypts the message as $c = b^d = a^{ed} = a \mod n$. Briefly,

  - Encryption: B should do the following
    - Obtain A's authentic public key (n, e)
    - Represent the message as an integer m in the interval $[0, n-1]$
    - Compute $c \equiv m^e \mod n$ and send the ciphertext c to A
  - Decryption: A should use his private key d obtained by extended Euclidean algorithm to recover m as, $m = c^d \mod n$

  Therefore, the backbone of this cryptosystem is Euclidean algorithm.

1.3 How Did It Develop?

In this section, it is tried to highlight the historical development of the study of Euclidean property with reference to the integer rings of number fields.

To begin with, it is interesting to state the well known *Fermat's Last Theorem* as, there are no positive integers a, b, c and n with $n > 2$ that satisfy

$$a^n + b^n = c^n$$

Gabriel Lamé, a French mathematician who was a member of the *Parisian Académie des Sciences*, announced his colleagues that he claimed to have proved the above theorem of Fermat on March 01, 1847. In his proof, there involved numbers of the following form.

$$z = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}$$

where $\zeta_n^n = 1$, $\zeta_n^k \neq 1$ for every $0 < k < n$ and $a_i \in \mathbb{Z}$ for every i. Nowadays, $\zeta_n = \sqrt[n]{1}$ is called the primitive n^{th} root of unity; and, the set of all numbers of the above form, denoted $\mathbb{Z}[\zeta_n]$, is termed as the ring of integers for the n^{th} cyclotomic field, $\mathbb{Q}(\zeta_n)$.

Lamé supposed, without loss of generality, an odd prime exponent n. It is a clear fact from the theory of *Diophantine Equations* that if p, q, r and n are positive integers such that p and q are without any common factor, then

$$pq = r^n \Rightarrow p = c^n \text{ and } q = d^n \text{ for some positive integers } c \text{ and } d$$

Lamé assumed this above fact would also be true for any $\mathbb{Z}[\zeta_n]$ together with

$$a^n + b^n = 0 \Rightarrow a = -b\sqrt[n]{1} \quad \leftrightsquigarrow \quad a^n + b^n = c^n = \prod_{i=1}^{n}(a + b\zeta_n^i)$$

and finally concluded the proof as either a, b or c should be 0 for $a^n + b^n = c^n$ to hold under the given assumptions.

Joseph Liouville who attended the meeting raised a question if unique factorization could hold in $\mathbb{Z}[\zeta_n]$ for otherwise the proof would be wrong. Lame and Cauchy did not share Liouville's skepticism, but spent the following few months trying to prove his question for any positive integer n though unsuccessful. About two weeks after Lamé's announcement, Wantzel correctly observed that in order to prove that $\mathbb{Z}[\zeta_n]$ is a unique factorization domain, it suffices to show that division with remainder, "norm Euclideanity," holds in it. He illustrated his theorem by considering $n = 4$ and hence dealing with numbers of the form $a + b\sqrt{-1}$, the Gaussian integers. Cauchy apparently

overlooked the fact that $\mathbb{Q}[\zeta_k] = \mathbb{Q}[\zeta_{2k}]$ for any odd positive integer k. Moreover, he later showed that $\mathbb{Q}[\zeta_n]$ where $n = 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15$ are Euclidean rings and $\mathbb{Q}[\zeta_{23}]$ is not.

A few years earlier, there was a parallel development of the idea in Germany in a somehow less straightforward way aiming at generalizing *quadratic reciprocity* for higher degree. The usual *quadratic reciprocity* can be recalled as, for two distinct odd primes p and q, exactly one of the congruences, $p \equiv x^2 \mod q$ and $q \equiv y^2 \mod p$, is solvable if $p, q \equiv 3 \mod 4$. Othewise, they are both solvable or insolvable. Jacobi's result suggested that for higher n, it must be known first if every prime $p \equiv 1 \mod n$ can be written as the norm of an element in $\mathbb{Z}[\zeta_n]$.

This last question of Jacobi is related to some extent to the Liouville's question. In fact, if unique factorization holds in $\mathbb{Z}[\zeta_n]$, then $p = N(z)$ for some $z \in \mathbb{Z}[\zeta_n]$ where $p \equiv 1 \mod n$ is any prime; N denotes the norm. Kummer proved the converse of this last statement beautifully in 1847. Besides, by taking $n = 5, 7, 11, 13, 17$ and 19, he showed that a prime $p \equiv 1 \mod n$ where $p < 1000$ is the norm of some $z \in \mathbb{Z}[\zeta_n]$. As it is impossible to prove this way for all primes, he noted that it suffices to prove unique factorization.

For this, Kummer turned his attention to the sufficient condition Wantzel forwarded, the Euclidean division algorithm. In Watzel's argument, there involved expressing a given $s \in \mathbb{Q}(\zeta_n)$ as,

$$\begin{aligned} s &= a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1} \\ &= (z_0 + q_0) + (z_1 + q_1)\zeta_n + (z_2 + q_2)\zeta_n^2 + \cdots + (z_{n-1} + q_{n-1})\zeta_n^{n-1} \end{aligned}$$

where $z_i \in \mathbb{Z}$ and $q_i \in \mathbb{Q}$ (hence $a_i \in \mathbb{Q}$) such that

$$N(z_0 + z_1\zeta_n + z_2\zeta_n^2 + \cdots + z_{n-1}\zeta_n^{n-1}) < 1$$

With this, the desire to determine whether a given number field is Euclidean or not has then become an interesting area of study by itself.

"The laws of nature are but the mathematical thoughts of God."

Euclid

"If Euclid failed to kindle your youthful enthusiasm,
then you were not born to be a scientific thinker."

Albert Einstein

Chapter 2

Principality And Euclideanity

2.1 Euclidean Function

Let R in general be a commutative ring.

Definition 2.1. A function $\phi : R \to \mathbb{N}$ is said to be a stathm on R or R is called a ϕ-stathm if the condition $\phi(x) = 0 \Leftrightarrow x = 0 \in R$ is satisfied.

Definition 2.2. R is said to be Euclidean if there exists a stathm ϕ on it such that given any $b \neq 0$ and a in R there exist q and r such that $a = bq + r$ with $0 \leq \phi(r) < \phi(b)$ and $\phi(ab) \geq \phi(a)$

Example 2.3. In the followings, ϕ is used to denote a Euclidean function.

- Any field K. $\phi(x) = 1\ \forall x \in K$ if $x \neq 0$ is an obvious case in which all the remainders are 0.
- The ring of integers $\mathbb{Z}$. $\phi(a) = |a|\ \forall a \in \mathbb{Z}$. This is the usual division with remainder of integers where $|\ |$ is the ordinary absolute value.
- The ring of polynomials over a field K, $K[x]$, with the function ϕ that assigns a polynomial $p(x)$ to one more than its degree,

$$\phi(p(x)) = \begin{cases} 0 & \text{if } x = 0 \\ 1 + \text{degree of } p(x) & \text{if } x \neq 0 \end{cases}$$

  This is again the ordinary long division of a polynomial by a non zero polynomial where the degree of constant functions is assumed to be 0.
- The Gaussian integers $\mathbb{Z}[i]$ with the norm function,

$$\phi(a + bi) = | = |a + bi|^2 = a^2 + b^2$$

Indeed, to verify this as an illustrative example, we need to prove that for any two elements α and β in $\mathbb{Z}[i]$, and β non zero, there exist ω and γ such that

$$\alpha = \beta\omega + \gamma \text{ and } \phi(\gamma) < \phi(\beta) \quad \Leftrightarrow \quad \frac{\alpha}{\beta} = \omega + \frac{\gamma}{\beta} \text{ and } |\gamma|^2 < |\beta|^2$$
$$\Leftrightarrow |\frac{\alpha}{\beta} - \omega| = |\frac{\gamma}{\beta}| \text{ and } |\frac{\gamma}{\beta}| < 1 \quad \Leftrightarrow \quad |\frac{\alpha}{\beta} - \omega| < 1$$

But we know that the Gaussian integers form a lattice in the complex plane. The lattice points are those points of the complex plane with two of its coordinates integers with respect to the basis 1 and i. Thus the complex number $\frac{\alpha}{\beta}$ definitely lies in a mesh of the lattice. And clearly, the maximum possible distance of a point from the nearest lattice point is half the length of the diagonal of the mesh, $\frac{\sqrt{2}}{2}$ as shown in the figure below. Therefore, there exists an element $\omega \in \mathbb{Z}[i]$ with the desired property, $|\frac{\alpha}{\beta} - \omega| \leq \frac{\sqrt{2}}{2} < 1$

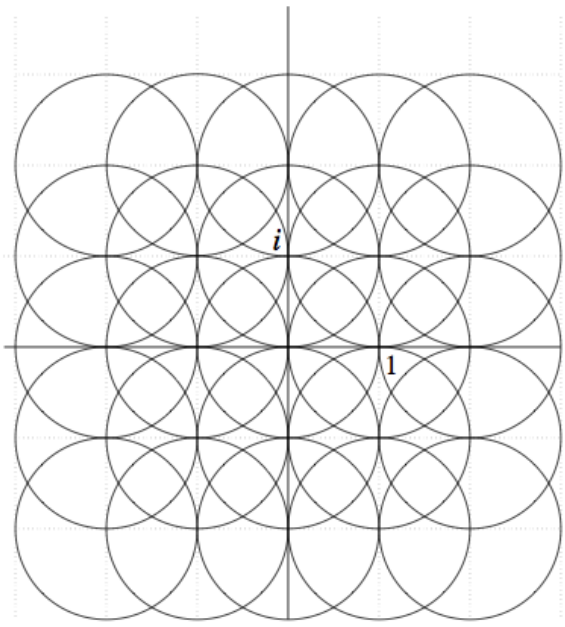


Figure 1. Unit circles with centers the lattice points of $\mathbb{Z}[i]$ in the complex plane

- A principal ideal domain with a finite number of maximal ideals.

Proof. Suppose the set of all the maximal ideals of the domain R be M, i.e.

$$M = \{(m_1), (m_2), \ldots, (m_n)\}$$

If x is taken arbitrarily from the domain, then

$$x = m_1^{\nu_1(x)} \cdot m_2^{\nu_2(x)} \ldots m_n^{\nu_n(x)}$$

where ν_i is the normalized m_i-adic valuation of R.
Claim: ϕ can be defined for each $x \in R$ as,

$$\phi(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 + \sum_{i=1}^{n} \nu_i(x) & \text{if } x \neq 0 \end{cases}$$

Let $\bar{x} \in R/(b)$ for arbitrarily fixed non zero element b of R. It then is needed to be found a representative $x \in R$ of the class $\bar{x}$ with the property $\phi(x) < \phi(b)$. For $\bar{x} = 0$, $x = 0$ can be taken as such a representative. If on the other hand $\bar{x} \neq 0$, let x' be any representative of $\bar{x}$. This implies the existence of some index i satisfying $\nu_i(x') < \nu_i(b)$, for otherwise, $x' \in (b)$ and $\bar{x} = 0$. For this index i,

$$\nu_i(x) = \nu_i(x') < \nu_i(b)$$

for any representative x of $\bar{x}$. For an index j such that $\nu_j(x') \geq \nu_j(b)$, x' can be written as $x' \equiv z_j b \mod (m_j^{1+\nu_j(b)})$ where $z_j \in R$ is well defined mod the ideal (m_j). Chinese Remainder Theorem implies that there exists an element z of R such that $z \equiv (1 - z_j) \mod (m_j)$ for all such indices j. It then follows that $x = x' + (b)$ is a representative of $\bar{x}$ and $x \equiv b \mod (m_j)^{1+\nu_j(b)}$. Thus, $\nu_j(x) = \nu_j(b)$ for all such indices j. But since $\nu_i(x) < \nu_i(b)$ for the other indices i, the desired result, $\phi(x) < \phi(b)$, follows from

$$\sum_{i=1}^{n} \nu_i(x) < \sum_{i=1}^{n} \nu_i(b)$$

□

- An integral domain R equiped with ϕ having the good properties and satisfying moreover

$$\phi(ab) \geq \phi(a) \text{ if } b \neq 0.$$

Theorem 2.4. *Let R be a domain as in the last example. Then*

i. If two elements of R are associates[1]*, their Euclidean values are the same.*

ii. If the Euclidean values of two numbers, where one divides the other, are the same then they are associates.

iii. An element of R is a unit if and only if its Euclidean value is equal to the Euclidean value of 1.

iv. The Euclidean value of any non zero element is greater than the value at 0.

Proof. ϕ is assumed to be the Euclidean function on the domain.

i. Let a and b be associates. Then, we have

$$\phi(a) = \phi(ub) \geq \phi(b)$$

Since u is a unit, $b = au^{-1}$. and similarly, we have

$$\phi(b) = \phi(au^{-1}) \geq \phi(a)$$

Hence they are equal.

ii. By definition of Euclidean function, for the two numbers a and b, there exist q and r such that $a = qb + r$ and $\phi(r) < \phi(b) = \phi(a)$. Moreover, $a \mid b \Rightarrow a \mid r$. Suppose r is non zero. Then $\phi(r) \geq \phi(a)$. Which is impossible according to our assumption. Thus, $r = 0$ and $a = qb$. Since $a \mid b$, q must be a unit, the result follows.

iii. As a is a unit, a and 1 are associates. Then by part i. they have the same Euclidean value. Conversely, $\phi(1) = \phi(a)$ (and $1 \mid a$) implies 1 and a are associates. hence, a is a unit by ii.

iv. By definition of Euclidean function ϕ on R, we have $0 = qa + r$, for some r and q where $\phi(r) < \phi(a)$. $r = 0$ and $\phi(0) < \phi(a)$. Otherwise, $r \neq 0 \Rightarrow q \neq 0 \Rightarrow \phi(r) = \phi((-q)a) \geq \phi(a)$ which is a contradiction.

□

[1] a and b are associates in R, denoted $a \sim b$, if $a = ub$ for some unit $u \in R$

Theorem 2.5. *A Euclidean domain R is principal ideal domain (PID)*

Proof. Since R is Euclidean, it has a Euclidean function, say ϕ. Let I be an ideal of R. If I is the zero ideal then it is clearly principal.
Let I be a non zero ideal. Consider the set of integers D defined as,

$$D = \{\phi(x) : x \in I, x \neq 0\}$$

This set is non empty because the ideal is non zero. Moreover, it is bounded from below due to the fact that $\phi(x) > 0 \ \forall x \in R$. Therefore D has a least element , say $\phi(b)$ where $b \in I$ is non zero. If $a \in I$, since ϕ is Euclidean, then there exist elements q and $r \in R$ such that

$$a = bq + r \text{ where } 0 \leq \phi(r) < \phi(b)$$

Here, I is an ideal. Consequently, $r = a - bq$ belongs to I. Due to the minimality of $\phi(b)$ by assumption, $r = 0$ follows. Hence $a = bq$ and $I = (b)$. i.e every ideal of R is principal or R is PID. □

Corollary 2.6. *A Euclidean domain R is a unique factorization domain.*

Proof. PID ⇒UFD □

Definition 2.7. A number field K is said to be norm-Euclidean if its ring of integers $\mathcal{O}_K$ is Euclidean with respect to the absolute value of the norm N.

Theorem 2.8. *$\mathcal{O}_K$ is norm Euclidean if and only if for every $y \in K$, there exists $x \in \mathcal{O}_K$ such that $N(y - x) < 1$.*

Proof. For the forward implication, let $y \in K$; y can be written as a/b where $a, b \in \mathcal{O}_K$ and $b \neq 0$. By assumption, for these numbers a and b, there exists $q, r \in \mathcal{O}_K$ such that

$$a = bq + r \text{ with } N(r) < N(b).$$
$$a/b = q + r/b \text{ with } N(r)/N(b) < 1$$

The multiplicative property of norm implies $N(r)/N(b) = N(r/b)$.
On top of that, x can be chosen to be q. All these result in

$$N(y - x) = N(a/b - q) = N(r/b) < 1$$

Conversely, let it be assumed that for every $y \in K$, there exists $x \in \mathcal{O}_K$ such that $N(y - x) < 1$. Then given $a, b \in \mathcal{O}_K$ with $b \neq 0$. From the condition, $q \in \mathcal{O}_K$ can be chosen that satisfies $N(a/b - q) < 1$. Taking $r = a - bq$, the following can be found as desired by using the multiplicative property of norm:

$$N(r) = N(a - bq) = N(b(a/b - q)) = N(b)N(a/b - q) < N(b)$$

□

2.2 Motzkin's Result

Motzkin [39] set a criterion for checking whether integral domains in general and rings of integers in particular are Euclidean or not. He set a typical criterion in such a way that Euclidean algorithm is given a new formulation which at first seems a little away from the problem at hand but is indeed a decisive key to the problem.

In his formulation, he introduced his fundamental set on a domain R called the derived sets as follows.

Definition 2.9. In each of the following definitions, R is assumed to be an integral domain.

- A *product ideal* P of R is any subset of $R - \{0\}$ such that

$$P(R - \{0\}) \subseteq P$$

- The *total derived set* of a subset S of R is the set B of all elements of R such that there exists an element a in R for which $a + bR$ is contained in S. i.e

$$B = \{b \in R \mid \exists a \in R \text{ for which } a + bR \subseteq S\}$$

- The *derived set* $S^{'}$ of the subset S is just the intersection of B and S. It is the set of elements in B without those that never belong to S. i.e.

$$\begin{aligned} S^{'} &= B \cap S \\ &= \{b \in S \mid \exists a \in R \text{ for which } a + bR \subseteq S\} \end{aligned}$$

  This set may also be viewed as the set obtained from S by skipping all b such that for every a, b divides some $a + c$ with c not in S.

Remark 2.10. Let the notations be as used in the above definitions.

- $\diamond$ $P_i^{'} \subseteq P_{i+1}$ where $P_i = \{r \in R : |r| \geq i\}$
  In fact, if an element b is taken from $P_i^{'}$ then by the above definition, there is an element a that satisfies $a + bR \subseteq P_i$. Here we note that for any $q \in R$, $a - bq$ can never be zero; otherwise, 0 would belong to the product ideal P_i. Now, taking any such difference with $\mid a - bq \mid < \mid b \mid$, we can see that

$$\begin{aligned} a - bq \in P_i &\Rightarrow \mid a - bq \mid \geq i \text{ and} \\ \mid a - bq \mid < b &\Rightarrow \mid b \mid \geq i + 1 \Rightarrow b \in P_i + 1 \end{aligned}$$

- ◇ If conversely a sequence of product ideals P_i is given with the inclusion $\cdots \subseteq P_2 \subseteq P_1 \subseteq P_0 = R - 0$ where the i^{th} derived set is contained in the $(i+1)^{th}$ product set, then for any given $b \in P_i - P_{i+1}$, then the norm function, $\mid b \mid = i$ is Euclidean. This with the first remark implies the correspondence between a Euclidean algorithm and such a sequence.

- ◇ Of all the Euclidean functions allowed by a ring R, there is a fastest one in the sense that if two sequences P_1 and P_2 with the algorithm constructed above are given, then the algorithm corresponding to P_1 is said to be faster than P_2 if for each i, $P_{1,i} \subseteq P_{2,i}$. This fastest algorithm is defined by repeatedly computing the derived set of P_0 and forming a sequence as $R - \{0\} = P_0 \supseteq P_0^{'} \supseteq P_0^{''} \supseteq \ldots$

Theorem 2.11. *(Motzkin): There is Euclidean algorithm on the domain R if and only if $\bigcap_{i=0}^{\infty} P_0^i = \phi$ where P_0^i represents P_0, $P_0^{'}$ and all the higher derived sets of P_0.*

Universal Side Divisor
For a given domain R, let $\tilde{R}$ denote the set of all units of R and 0.

$$\tilde{R} = R^{\times} \cup \{0\}.$$

Definition 2.12. Let R be an integral domain where $R \neq \tilde{R}$ i.e R, not a field. An element $s \in R - \tilde{R}$ is said to be a side divisor of $d \in R$ if there exists $u \in \tilde{R}$ such that $s \mid (d + u)$. Furthermore, a side divisor is called universal if it is a side divisor for every element in the domain. Precisely, a non unit element of R, $u \neq 0$ is called a universal side divisor if for any $r \in R$ there exists some $\tilde{r} \in \tilde{R}$ such that $u \mid r - \tilde{r}$.

For a given domain R, the Motzkin sets E_i where $i = 0, 1, 2, \ldots$ can also be defined in the reverse process by taking complements of the previous construction in the following sense:
As recalled, derived set P' of P is defined as,

$$P' = P - \{b \in P : \forall a \in R, \quad \exists c \in R - P \text{ such that } b \mid (a + c)\}$$

Hence,

$$\begin{aligned}
&P_0 = R - \{0\} \\
&P_0' = P_0 - R^{\times} = R - R^{\times} - \{0\} \\
&P_0'' = P_0' - S(R) = R - S(R) - R^{\times} - \{0\} \\
&P_0^{(\alpha)} = P_0^{(\alpha-1)} - \{b : \forall a \in R \ \exists c \in R - P_0^{(\alpha-1)} \text{ such that } b \mid (a + c)\}
\end{aligned}$$

It then forms the sequence of inclusions as:

$$R - \{0\} = P_0 \supseteq P_0' \supseteq P_0'' \supseteq \ldots$$

$S(R)$ and $R^\times$ are used above to denote the set of universal side divisors and units respectively of the given domain R.

The complement of the above sets can be considered to start with the set with the least number of elements as follows:

$$\begin{aligned}
E_0 &= \{0\} \\
E_1 &= \{0\} \cup R^\times \\
E_2 &= \{0\} \cup R^\times \cup S(R) \\
E_i &= \{0\} \cup \{a \in R - \{0\} \mid \text{each residue class modulo } a \\
&\qquad \text{contains an element } b \in E_j, j < i\} \\
&= \{0\} \cup \{a \in R - \{0\} : E_{i-1} \cup \{0\} \to \ R/(a) \text{ is on to}\} \\
E_\infty &= \bigcup_{i=0}^{\infty} E_i
\end{aligned}$$

This results in continuous inclusions as

$$\{0\} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$$

Analogously, Motzkin's theorem hence can be restated as follows.

Theorem 2.13. *(Motzkin): There is a Euclidean algorithm on R if and only if $\bigcup_{i=0}^{\infty} E_i = R$. In which case the Euclidean function f is defined as $f(a) = j$ where E_j is the set as above with the least index that contains a.*

f is sometimes referred to as transfinite Euclidean function on account of the ordinal numbers its value assumes as above, the 1^{st}, $2^{\text{nd}} \ldots j^{\text{th}}$ E- set.

If we take $\mathbb{Z}$ as an illustrative example on each of the above sets, we let to have the initial set E_0 containing only 1 element i.e. $\{0\}$ according to the definition. The second set has 1 element to the right and 1 element to the left of 0; so totally containing 3 elements. The third set in a similar pattern contains 3 elements to the right and 3 elements to the left of 0 to totally contains 7 elements based on the definition; as such we have:

$$\begin{aligned}
E_0 &= \{0\} \\
E_1 &= \{-1, 0, 1\} \\
E_2 &= \{-3, -2, -1, 0, 1, 2, 3\} \\
E_i &= \{-2^i - 1, -2^i, \ldots, -2, -1, 0, 1, 2, \ldots, 2^i, 2^i - 1\}
\end{aligned}$$

Hence $\mathbb{Z}$ is a Euclidean domain by Motzkin's theorem since $\bigcup_{i=0}^{\infty} E_i = \mathbb{Z}$.

In the Motzkin construction above, if a domain R does not contain any universal side divisor, then $E_1 = E_2$ or $P_0' = P_0''$. In which case, E_j's or P_0^j's remain equal with each other for any j. If the domain under consideration is not a field, the motzkin criterion for Euclideanity will not hold. Consequently, we have the following result.

Theorem 2.14. *Let R be a domain but not field. If R is with no universal side divisors then it is not Euclidean.*

Based on this key theorem, it was proved that the only imaginary quadratic ring of integers where $P_0' \neq P_0''$, non empty set of universal side divisors, are $-1, -2, -3, -7$ and -11. Therefore, these are the only Euclidean imaginary ring of integers.

2.3 Hooley's Formulations

Under this section, although Artin's conjucture is totally out of the topic at hand and Hooley's proof is entirely about that, it is found to be interesting to see the overview of the formulations used in it. This is due to the fact that Weinberger's proof on Euclidean rings of algebraic integers is mainly based on it. Both papers are similar in that they both are conditional proofs. They indeed assumed the generalized Riemann hypothesis so that analytic notions are embedded in the algebraic proof. The basic difference is their two different topics where Hooley's Artin Conjecture on primitive roots is concerned with numbers where as Weinberger applied those results to ideals for his proof of "Euclideanity." Therefore, the objective of this topic is to see the relevant formulations and notations of Hooley's which Weinberger adapted to our topic.

Artin's Conjecture

If an integer which is neither a perfect square nor -1 is given, there are infinitely many primes where the given integer is a primitive root modulo the primes.

The stronger version

Let $N_a(x)$ denote the number of primes not exceeding x for which a is a primitive root. If a non perfect square integer a is different from -1, then there is a positive constant $A(a)$, dependent on a such that for x tending to infinity,

$$N_a(x) \sim A(a)\frac{x}{\log x}$$

It is known from prime number theorem that $\pi(x)$, the density of primes up to x, tends to $x/\log x$ as x tends to infinity. The constant $A(a)$ measures the proportion of those primes for which $a \leq x$ is a primitive root to the total number of primes up to a very large x,

$$A(a) \sim \frac{N_a(x)}{\pi(x)}$$

The basic observation made here is the criteria for a number to be a primitive root modulo a prime. For a prime p, let $\{q_1, q_2, q_3, \ldots, q_r\}$ be the set of all the prime divisors of $\phi(p)$. The necessary and sufficient condition for the number a to be a primitive root of p is that

$$a^{(p-1)/q_i} \not\equiv 1 \mod p \text{ for each} i$$

In fact, if c is the order of a modulo p, $\phi(p)$ is divisible by c. If moreover, $c \neq \phi(p)$, then c divides $(p-1)/q_i$ for some i. Heuristically, a is a primitive root modulo p if the following two conditions do not hold for any q, prime divisor of $\phi(p)$:

$$p \equiv 1 \text{ mod q} \quad \text{and} \quad a^{(p-1)/q} \equiv 1 \text{ mod p}$$

If q is fixed to find the probability that a prime p satisfies the above two conditions, then by Dirichlet's theorem, $p \equiv 1 \mod q$ (i.e. $q \mid (p-1)$) is true for primes p with frequency $(q-1)^{-1}$.

Moreover, $a^{(p-1)/q} \equiv 1 \mod p$ occurs with a probability of $1/q$. The probability of both events to occur is the product, $(q(q-1))^{-1}$. Finally, the likelihood for the above two events not to occur is $1-(q(q-1))^{-1}$. In other words, this is the probability for the number a to be prime. Therefore, the total value of the probability for all prime q can roughly be

$$\prod_{i=1}^{n}\left(1-\frac{1}{q(q-1)}\right) = 0.3739558136\ldots$$

This value is referred to as the Artin's constant.

Theorem 2.15. *(Hooley) [27] Suppose extended Riemann hypothesis is assumed to be true for Dedekind zeta function over Galois field of the form* $\mathbb{Q}(\sqrt[k_1]{b}\sqrt[k]{1})$ *where* $b \in \mathbb{Z}$*; k is sqare free and* $k_1 \mid k$*, positive integers . Let* a_1 *be the square free part of a. Assume h to be the largest integer such that a is a perfect* h^{th} *power. Let also that*

$$C(h) = \prod_{q|h} \left(1 - \frac{1}{q-1}\right) \prod_{q\nmid h} \left(1 - \frac{1}{q(q-1)}\right)$$

Then as x tends to infinity, we have

$$N_a(x) = C(h)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right) \qquad \text{if } a_1 \not\equiv 1 \mod 4$$

and,

$$N_a(x) = C(h)(1 - \mu(|a_1|) \prod_{q|h, q|a_1} \left(\frac{1}{q-2}\right) \prod_{q\nmid h, q|a_1} \left(\frac{1}{q^2-q-1}\right) \frac{x}{\log x}$$
$$+ O\left(\frac{x \log\log x}{\log^2 x}\right) \qquad \text{if } a_1 \equiv 1 \mod 4$$

Some Notations and Formulations Used

$a \neq -1$ is an integer which is not a perfect square. p and q are primes. k, ξ_1 and ξ_2 are boundary numbers.
Let # denote cardinality and let

$$R(q,p) = \begin{cases} 1 & \text{if } q \mid (p-1) \text{ and } a \text{ is a } q\text{-th power residue mod } p. \\ 0 & \text{otherwise} \end{cases}$$

$$N_a(x) = \#\{p \leq x : a \text{ is a primitive root mod } p\}$$
$$N_a(x,\eta) = \#\{p \leq x : R(q,p) = 0 \text{ for any prime } q \leq \eta\}$$
$$P_a(x,k) = \#\{p \leq x : R(q,p) = 1 \text{ for any } q \mid k\}$$
$$M_a(x,\xi_1,\xi_2) = \#\{p \leq x : R(q,p) = 1 \text{ for some } q : \xi_1 < q \leq \xi_2\}$$

Let us summarize the final equations found by applying several algebraic and analytic methods and see how they are interrelated with each other to result in the Hooley proof. As we pointed out at first, the purpose of studying this is because of the fact that Hooley's approach is analogous to Weinberger's proof. And, the equations are a little simpler and more natural in the level of numbers than ideals. Here, we are going to have the following assumptions. $\xi_1 = \log x/6$, $\xi_2 = \sqrt{x}/(\log^2 x)$, $\xi_3 = \sqrt{x}\log x$.

- $N_a(x) \leq N_a(x, \xi_1)$,
- $N_a(x) \geq N_a(x, \xi_1) - M_a(x, \xi_1, x-1)$,

which implies

$$N_a(x) = N_a(x, \xi_1) + O(M_a(x, \xi_1, x-1)) \qquad (*)$$

To estimate $O(M_a(x, \xi_1, x-1))$, it can be proceeded as

$$M_a(x, \xi_1, x-1) = M_a(x, \xi_1, \xi_2) + M_a(x, \xi_2, \xi_3) + M_a(x, \xi_3, x-1)$$

Analyzing all the terms separately, the followings have been obtained.

1) $M_a(x, \xi_3, x-1) = O\left(\frac{x}{\log^2 x}\right)$

2)[2] $P_a(x, q) = \frac{1}{n} li(x) + O(\sqrt{x}\log(kx)) = O\left(\frac{x}{\log x}\right)$;

3) $M_a(x, \xi_2, \xi_3) \leq \sum_{\xi_2 < q \leq \xi_3} P_a(x, q) = O\left(\frac{x \log\log x}{\log^2 x}\right)$;

4) $M_a(x, \xi_1, \xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P_a(x, q) = O\left(\frac{x}{\log^2 x}\right)$

5) $N_a(x, \xi_1) = \sum_l \mu(l) P_a(x, l) = \frac{A(a)x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$ where

$$A(a) = \begin{cases} \prod_{q|h}\left(1 - \frac{1}{q-1}\right)\prod_{q\nmid h}\left(1 - \frac{1}{q(q-1)}\right) =: \text{ say } C(h), a \not\equiv 1[4] \\ C(h)(1-\mu(|a|))\prod_{q|h, q|a}\left(\frac{1}{q-2}\right)\prod_{q\nmid h, q|a}\left(\frac{1}{q^2-q-1}\right), a \equiv 1[4]; \end{cases}$$

In the 5^{th} equation, l denotes 1 or a positive square-free number whose factors are primes not exceeding ξ_1. μ denotes the the möbius function to eliminate those of non square free elements. Combining these above sub-results, the final result obtained becomes,

$$N_a(x) = \frac{A(a)x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

[2] $li(x)$ is logarithmic integral function given by $li(x) = \int_0^x \frac{dt}{\ln t}$

2.4 Weinberger's Result

The Motzkin's set formation on a commutative ring R can be recalled as $E_0 = \{0\}$ and $E_1 - E_0 = \{a \in R |$ each $\bar{r} \in R/(a)$ contains $0\} = R^\times$

Proof. Let

($\Rightarrow$) Each $\bar{r}$ in $R/(a)$ contains 0.

$$\Rightarrow \text{For each } r, \bar{r} = r + ka = 0, \text{ for } k \in R$$
$$\Rightarrow \text{ take } r = 1, \text{ i.e. } \bar{1} = 1 + ka = 0 \text{ for } k \in R$$
$$\Rightarrow ab = 1 \text{ in } R, \ b = -k \Rightarrow a \in R^\times$$

($\Leftarrow$) Let a be a unit in R taken arbitrarily. We want to show that any arbitrary class in $R/(a)$ contains 0. Fix a random $\bar{r} \in R/(a)$

$$\bar{r} \in R/(a) \Rightarrow \bar{r} = \{r + ka : k \in R \text{ and } r \text{ any representative of the class}\}$$
$$\Rightarrow r + (-ra^{-1})a = 0 \in R/(a)$$

□

$E_j - E_{j-1} = \{a \in R : \text{ each } \bar{r} \in R/(a) \text{ contains an element from } E_{j-1}\}$; as also recalled, R is Euclidean if $R = \cup_{j=1}^{\infty} E_j$. The associated Euclidean function $fR \to \mathbb{N}$ is given as:

$$f(\alpha) = \inf\{j : \alpha \in E_j\} = k \text{ such that } \alpha \in E_k - E_{k-1}.$$

Theorem 2.16. *(Weinberger) [45]*

(1) Assume GRH holds. If K is a number field of class number 1 and its ring of integers, $\mathcal{O}_K$ has infinite unit group, then $\mathcal{O}_K$ is Euclidean.

(2) If the hypotheses of the above theorem are satisfied, every irreducible of $\mathcal{O}_K$ is in E_3

(3) Let $p \in \mathcal{O}_K$ be irreducible so that the corresponding generated ideal $\mathfrak{p} = (p)$ is prime. Set B and D respectively for the multiplicative group and its subgroup as follows,

$$B = \{\mathfrak{b} \subseteq \mathcal{O}_K \text{ an ideal } : (\mathfrak{b}, \mathfrak{p}) = 1\}$$
$$D = \{\mathfrak{d} \in B \text{ ideal } : \mathfrak{d} \equiv (1) \mod \mathfrak{p}\}^3$$

If GRH holds, then every ideal class of $H = B/D$ contains infinitely many primes for which a fixed fundamental unit ε is a primitive root.

[3]For $\mathfrak{m}$ a divisor of K, $\mathfrak{a}, \mathfrak{b}$ two non zero ideals of $\mathcal{O}_K$, $\mathfrak{a} \equiv \mathfrak{b} \mod \mathfrak{m}$ means that $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal ideal (c) such that $\nu_\mathfrak{q}(c) \geq \nu_\mathfrak{q}(\mathfrak{m})$ for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$

Weinberger has shown that (3) $\Rightarrow$ (2) $\Rightarrow$ (1). Structurally, theorem (3) is clearly seen to be the direct analogue to the Artin's conjecture approach of Hooley's conditional proof. Our objective here is to see to what extent they both are interrelated and highlight the basic equations involved.

Some Notations and Formulations Used

As explained so far, the followings are mostly the analogue of Hooley's work with actually further analytic application. The usage of letters and notations are used in a similar way as the above three theorems of Weinberger. Moreover, W is an ideal class of H; ξ_1, ξ_2 and ξ_3 are fixed bounding numbers with a fixed choice of x as used exactly in Hooley's description. i.e

$$\xi_1 = \log x/6, \quad \xi_2 = \sqrt{x}/\log^2 x \text{ and } \xi_3 = \sqrt{x}\log x$$

The key starting point is to notice the fact that ε is not a primitive root of $\mathfrak{p}$ implies the existence of q such that $q \mid N\mathfrak{p} - 1$ and[4] ε is a q^{th} power residue mod $\mathfrak{p}$

$$R(\mathfrak{p}, k) = \begin{cases} 1 & \text{if } k \mid (N\mathfrak{p} - 1) \text{ and } \varepsilon^{(N\mathfrak{p}-1)/k} \equiv 1 \bmod \mathfrak{p} \\ 0 & \text{otherwise} \end{cases}$$

$$\begin{aligned} N(x) &= \#\{\mathfrak{p} \in W : N\mathfrak{p} \leq x, \varepsilon \text{ is a primitive root of } \mathfrak{p}\} \\ N(x, \xi) &= \#\{\mathfrak{p} \in W : N\mathfrak{p} \leq x, R(\mathfrak{p}, p) = 0 \text{ for any prime } q \leq \xi\} \\ P(x, k) &= \#\{\mathfrak{p} \in W : N\mathfrak{p} \leq x, R(\mathfrak{p}, q) = 1 \text{ for any } q \mid k\} \\ M(x, \xi_1, \xi_2) &= \#\{\mathfrak{p} \in W : N\mathfrak{p} \leq x, R(\mathfrak{p}, q) = 1 \text{ for some } q : \xi_1 < q \leq \xi_2\} \end{aligned}$$

By taking $\xi_1 = 1/6 \log x$, the formulation starts from:

$$N(x, \xi_1) - M(x, \xi_1, x - 1) \leq N(x) \leq N(x, \xi_1),$$

which implies

$$N(x) = N(x, \xi_1) + O(M(x, \xi_1, x - 1)).$$

In the second part of the above sum, $M(x, \xi_1, x - 1)$ can be described as the sum of three partitions by making use of $\xi_2 = \frac{\sqrt{x}}{\log^2 x}$ and $\xi_3 = \sqrt{x}\log x$.

$$M(x, \xi_1, x - 1) = M(x, \xi_1, \xi_2) + M(x, \xi_2, \xi_3) + M(x, \xi_3, x - 1).$$

[4] $N_{\mathfrak{p}}$ is to mean the absolute norm of the ideal $\mathfrak{p}$

Hence, the final simplified result was achieved by independently studying those four terms with the knowledge of class field theory and analytic number theory.

A reader who is interested in the detailed proofs can refer to the original papers of Hooley [27] and Weinberger [45]. However it is interesting to mention the main result and the associated sub results here in order to see how Hooley's work is nicely adapted for theorem 2.12 (3).

Further Notations and Assumptions

- B and D are the groups of ideals of $\mathcal{O}_K$ as given in the theorem.
- k is fixed positive integer and ε is a fixed fundamental unit of $\mathcal{O}_K$.
- $L = L_k$ is the normal extension of K given as, $L_k = K(\zeta_k, \varepsilon^{1/k})$.
- $\mathfrak{f}$ denotes the product of the fixed number k and the conductor of D.
- $C(k)$ is the ideal group in K generated by norms of ideals mod $\mathfrak{f}$ of L_k
- Let for a fixed k, $S(k)$ denote the set of all integral ideals $\mathfrak{B}$ in $L = L_k$ prime to $\mathfrak{f}$ with further property that its norm, $N_{L/K}(\mathfrak{B})$, belongs to W. Then the function F is defined as follows,

$$F(k) = \begin{cases} 1 & \text{if } S(k) \neq \phi \\ 0 & \text{otherwise} \end{cases}$$

With the aforementioned notations and assumptions, the results are,

1) $M(x, \xi_3, x-1) = O(\frac{x}{\log^2 x})$

2) $P(x,q) = \frac{1}{n} li(x) + O(\sqrt{x}\log(kx)) = O\left(\frac{x}{\log x}\right)$

3) $M(x, \xi_2, \xi_3) \leq \sum_{\xi_2 < q \leq \xi_3} P(x,q) = O\left(\frac{x \log\log x}{\log^2 x}\right)$

4) $M(x, \xi_1, \xi_2) \leq \sum_{\xi_1 < q \leq \xi_2} P(x,q) = O\left(\frac{x}{\log^2 x}\right)$

5) $N(x, \xi_1) = li(x) \sum_{l} \frac{\mu(l) F(l)}{[C(l) : C(l) \cup D][L_l : K]} + O\left(\frac{x}{\log^2 x}\right)$

In the the last equality, $l \in \{d : q \mid d \text{ and } q \leq \xi_1\}$. In addition to this, μ denotes the möbius function to eliminate out non square-free elements.

Combining these above sub-results, the final result obtained for sufficiently large x becomes:

$$N(x) = P(p)\left(1 - \frac{F(p)[B : C(p)D]}{p[K(\zeta_p) : K]}\right) + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

where

$$P(p) = \frac{li(x)}{[B : D]} \prod_{q \neq p} \left(1 - \frac{1}{q[K(\zeta_q) : K]}\right)$$

In the above expression, as clearly seen, $P(p)$ can never be zero. Moreover, he showed that $[B : C(p)D]$ and $p[K(\zeta_p) : K]$ can not be equal when $F(p)$ is 1; guaranteeing the other factor is also non zero. Thus $N(x)$ is concluded to be infinite.

2.5 Clark, Murty And Harper's Results

Clark's Result [11]
David Clark studied the Euclidean algorithm for Galois extensions of the rational numbers in his Ph.D. thesis (1992) under the supervision of Ram Murty. In his work, he found out a very important criterion for the Euclideanity of a given totally real quartic Galois field (i.e. the corresponding ring of integers).

Theorem 2.17. *Let K be a real quartic Galois field and $\mathcal{O}_K$ be its ring of integers which is PID. If there exists a prime element π with a surjective map from the group of units, $\mathcal{O}_K^\times$, to the prime residue class group $(\mathcal{O}_K/(\pi^k))^\times$ for every integer $k \geq 0$, then $\mathcal{O}_K$ is Euclidean domain.*

Remark 2.18. A prime residue class is a unit in the quotient ring $\mathcal{O}_K/(\pi^k)$. Moreover, a prime π stated with such a property in the theorem is called an admissible or a Wieferich prime.

Before this work, Buchmann and Ford computed all the 165 totally real quartic fields of discriminant less than one million in their paper. Clark then showed the existence of admissible primes in each of those fields which can be taken as an important affirmative evidence for the positive density of such primes. The positive density of admissible primes is not a proven fact rather a conjecture which is naturally adapted from the Artin's conjecture described in the second section of this chapter.

Clark-Murty's Result [12]
About three years after the previous result, Clark collaborated with Murty to generalize the above particular case. It is stated as follows,

Theorem 2.19. *Let R be a PID whose quotient field K is totally real Galois extension of rational numbers with degree n. If there are $m = |n-4|+1$ number of associate prime elements, $\pi_1, \pi_2, \ldots, \pi_m$, in R, such that for each non negative integer k_i, $R^\times$ maps on to $(R/(\pi_1^{k_1}\pi_2^{k_2}\ldots\pi_m^{k_m}))^\times$, then R is Euclidean domain.*

Remark 2.20. In similar way with the above definition, the set $\{\pi_1, \pi_2, \ldots, \pi_m\}$ is called admissible set of primes if for every $b = \pi_1^{k_1}\pi_2^{k_2}\ldots\pi_m^{k_m}$ with k_i any non negative integer, every coprime residue class mod b can be represented by a unit in $\mathcal{O}_K$.

In the last part of their paper, they showed that $\sqrt{14}$ is not Euclidean with respect to the norm.

Harper's Result [24]
In 2000, Harper claimed that he proved $\sqrt{14}$ is Euclidean in his Ph.D thesis. By making use of the major relevant works of the aforementioned researchers on Euclidean problems and specially Clark-Murty's results together with large sieving technique in the number field, he showed his result. Large sieve method for example is a technique by which a relatively large number of residue classes for each modulus are excluded out due to unimportance to the subject under study. The sieve of Eratosthenes is a good simple example of sieving thechnique. Harper's main result is,

Theorem 2.21. *$\sqrt{14}$ is Euclidean domain.*

On the way of proving this claim, he studied many other important contributing results. It is interesting to mention the main ones that have direct and close relevance to our subject,

A variation of Motzkin's criterion has been stated in the paper as follows, Let K be a number field and $\mathcal{O}_K$ be its ring of integers. H_0 be the monoid, algebraic structure with identity element that respects associativity, generated by the unit group and a set of admissible primes. H_j, defined inductively, is let to denote the set of all primes p in $\mathcal{O}_K$ such that every non zero residue class modulo p has a representative in H_{j-1} or H_0. The second simplest set, H_1, hence is solely formed from H_0 as just the set containing primes p such that every residue class mod p is represented by an element of H_0.

Theorem 2.22. *The main sub results included in it are:*

- *A cyclotomic field is Euclidean domain if and only if it is a PID.*
- *Suppose $H_j(x) = \#\{h \in H_j : N(h) \leq x\}$ and $\mathcal{O}_K$ is a PID. If $H_1(x) \gg x/(\log^2 x)$, then $\mathcal{O}_K$ is Euclidean.*
- *If all the primes of $\mathcal{O}_K$ are in $\bigcup_{j=1}^{\infty} H_j$, then it is eulidean*
- *Let K be a real quadratic number field. If $\mathcal{O}_K$ contains a set of two admissible primes and is a PID, then it is eulidean.*
- *If the discriminant of K does not exceed 500 then $\mathcal{O}_K$ is a PID if and only if it is Euclidean.*
- *Suppose $\mathcal{O}_K$ is a PID and contains a set of s admissible primes; suppose also that r is the rank of $\mathcal{O}_K^{\times}$ modulo torsion. Let $d = max\{d' : \zeta_d' \in K\}$. If $r + s \geq 3$ and if there are a and k in $\mathbb{Z}$ satisfying*

  1. *$gcd(a, k) = 1$*
  2. *$gcd(a - 1, k) = d$ and*
  3. *$p \equiv a \mod k$ implies there is a prime there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ with norm p*

  then $\mathcal{O}_K$ is Euclidean.

Harper-Murty's Result [25]
About three years later than his thesis, the preprint of his joint work with Murty was made ready for publishing. This is just a generalization of Harper's previous work to a larger context that includes the abelian extensions. Hence they largely used Harper's work together with Gupta Murty and Murty's work [22]. Their main result is:

Theorem 2.23. *Let K be a finite Galois extension of $\mathbb{Q}$ with unit rank greater than 3. Then its ring of integers, $\mathcal{O}_K$ is Euclidean if and only if it is prinipal ideal domain.*

This theorem can be restated in terms of the degree, n, of the number field instead of the unit rank r. If $r_1 = 0$ then $n = 2r_2$ and $r = r_2 - 1$.
If $r > 0$, then $r > r - r_1/2$. In either case, $r > 3$ whenever $n > 8$. Hence,
Let $K/\mathbb{Q}$ be a finite Galois extension of degree greater than 8. Then $\mathcal{O}_K$ is Euclidean if and only if it is a PID.

Theorem 2.24. *Let $K/\mathbb{Q}$ be a finite abelian extension of degree n with $\mathcal{O}_K$ a PID that contains s admissible primes. Let r be the rank of the unit group. If $r + s \geq 3$, then $\mathcal{O}_K$ is Euclidean if and only if it is PID.*

Chapter 3

Norm As Euclidean Function

3.1 Euclidean And Inhomogeneous Spectra

In this chapter a number field and its ring of integers are denoted by K and $\mathcal{O}_K$. Besides, the group of units of $\mathcal{O}_K$ is denoted by $\mathcal{O}_K^\times$; degree of K by $n = r_1 + 2r_2$ hence of signature (r_1, r_2) and the unit rank by $r = r_1 + r_2 - 1$. Let σ_i, $1 \leq i \leq r_1$ be the r_1 real embeddings of K in $\mathbb{R}$, and τ_j, $\bar{\tau_j}$, where $1 \leq j \leq r_2$, the r_2 pairs of complex embeddings of K in $\mathbb{C}$.

The norm function $N_{K/\mathbb{Q}} : K \to \mathbb{R}$ is defined as:

$$\begin{aligned} N_{K/\mathbb{Q}}(\xi) &= \prod_{i=1}^{r_1} \sigma_i(\xi) \prod_{j=1}^{r_2} \tau_j(\xi) \prod_{j=1}^{r_2} \bar{\tau}_j(\xi) \\ &= \prod_{i=1}^{r_1} \sigma_i(\xi) \prod_{j=1}^{r_2} \left|\tau_j(\xi)\right|^2 \qquad \forall \xi \in K \end{aligned}$$

In computational viewpoint, it is more manageable and easier to change products to sums for many calculations by inserting it in logarithms as,

$$\ln |N_{K/\mathbb{Q}}(\xi)| = \sum_{i=1}^{r_1} \ln |\sigma_i(\xi)| + 2 \sum_{j=1}^{r_2} \ln |\tau_j(\xi)|$$

The logarithmic embedding of $K\backslash\{0\}$ in $\mathbb{R}^{r_1+r_2}$, denoted $\mathcal{L}$, is defined as

$$\mathcal{L}(\xi) = \left(\ln |\sigma_1(\xi)|, \ldots, \ln |\sigma_{r_1+r_2}(\xi)|\right), \quad \forall \xi \in K\backslash\{0\},$$

Definition 3.1. Let $\xi \in K$. The *Euclidean minimum of* ξ is the real number $m_K(\xi)$ defined by

$$m_K(\xi) = \inf\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)| : \quad \Upsilon \in \mathcal{O}_K\}$$

Proposition 3.2. *m_K has the following elementary properties.*

i) $\forall(\xi, \Upsilon, \varepsilon) \in K \times \mathcal{O}_K \times \mathcal{O}_K^{\times},\ m_K(\varepsilon\xi - \Upsilon) = m_K(\xi)$.

ii) $\forall \xi \in K,\ \exists \Upsilon \in \mathcal{O}_K$ *such that* $m_K(\xi) = |N_{K/\mathbb{Q}}(\xi - \Upsilon)|$.

iii) $\forall \xi \in K,\ m_K(\xi) \in \mathbb{Q}$ *and* $m_K(\xi) = 0 \iff \xi \in \mathcal{O}_K$.

Proof. Each of them immediately follows from the definition given above.

i. we clearly see that, for $\alpha \in \mathcal{O}_K$

$$\begin{aligned} m_k(\xi - \alpha) &= \inf\{|N_{K/\mathbb{Q}}((\xi - \alpha) - \beta)| : \beta \in \mathcal{O}_K\} \\ &= \inf\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)| : \Upsilon \in \mathcal{O}_K\};\ \Upsilon = \alpha + \beta \\ &= m_k(\xi) \end{aligned}$$

Besides, from multiplicative property of norm and $|N_{K/\mathbb{Q}}(\varepsilon)| = 1$,

$$|N_{K/\mathbb{Q}}(\varepsilon\xi)| = |N_{K/\mathbb{Q}}(\varepsilon)N_{K/\mathbb{Q}}(\xi)| = |N_{K/\mathbb{Q}}(\xi)|.$$

Combining these, we get the result as desired.

ii. By definition.

iii. As the norm function $N_{K/\mathbb{Q}}$ defined on K is literally the square of a "distance" measure,$N_{K/\mathbb{Q}} : K \to \mathbb{Q}$, hence $m_K(\xi) \in \mathbb{Q}$. Moreover,

$$\begin{aligned} m_K(\xi) = 0 &\implies \inf\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)| : \Upsilon \in \mathcal{O}_K\} = 0 \\ &\implies \exists \alpha \in \mathcal{O}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \alpha)| = 0 \\ &\implies \xi = \alpha \in \mathcal{O}_K \end{aligned}$$

and conversely, we have non negative value of the norm. and hence,

$$\xi \in \mathcal{O}_K \implies N_{K/\mathbb{Q}}(\xi - \xi) = 0 \implies m_K(\xi) = 0$$

□

This definition of m_K on K can also be extended to its analogous minimum on $\bar{K} = K \otimes_{\mathbb{Q}} \mathbb{R}$, the product of the archimedian completions of K, This completion is usually identified as $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ which in turn can also be considered as the set H given below:

$$H = \mathbb{R}^{r_1} \times \Big\{ z \in \mathbb{C}^{2r_2};\ \forall i \in \{1, \ldots, r_2\},\ z_{r_2+i} = \bar{z_i} \Big\},$$

Clearly, $x \in H \Rightarrow x = (x_1, x_2, \ldots, x_n)$ where the first r_1 coordinates in the tuple belong to $\mathbb{R}$, while the last r_2 to $\mathbb{C}$. This is more convenient for easier formulas. If $(x, y) \in H^2$, we shall denote $x.y$ the element z of H defined by $z_i = x_i y_i$ for every i (extension of the product of K). Moreover, an element ξ of K is also in $\bar{K}$ in the sense that the n-tuple $(\sigma_i(\xi))$ is in H.

Definition 3.3. Let $x \in H$. The *inhomogeneous minimum of* x is the real number $m_{\bar{K}}(x)$ defined by

$$m_{\bar{K}}(x) = \inf\Big\{ \prod_{i=1}^{n} |x_i - \sigma_i(\Upsilon)|;\ \Upsilon \in \mathcal{O}_K \Big\}.$$

Of course for $\xi \in K$ we have $m_{\bar{K}}(\xi) = m_K(\xi)$.

Proposition 3.4. *The map $m_{\bar{K}}$ has the following properties:*

i) $\forall (x, \Upsilon, \varepsilon) \in H \times \mathcal{O}_K \times \mathbb{Z}_K^{\times},\ m_{\bar{K}}(x) = m_{\bar{K}}(\varepsilon.x - \Upsilon)$.

ii) $m_{\bar{K}}$ is upper semi-continuous on H.[1]

Proof. The first one is similar to Proposition 3.2. For the second, assume $\lim\limits_{n\to\infty} x_n = x$. We need to show that

$$\lim_{n\to\infty} \sup m(x_n) \leq m(x)$$

For $\varepsilon > 0$ arbitrary,

$$\exists A \in \mathcal{O}_K \text{ such that } |N_{K/\mathbb{Q}}(x - A)| \leq m(x) + \varepsilon/2$$

Moreover, since the norm $N_{K/\mathbb{Q}}$ is a continuous function of H,

$$\begin{aligned} \exists n_0 \text{ such that } |N_{K/\mathbb{Q}}(x_n - A)| &\leq |N_{K/\mathbb{Q}}(x - A)| + \varepsilon/2 \quad \forall n \geq n_0. \\ &\leq m(x) + \varepsilon \end{aligned}$$

We then have by definition and the above last equation, we get

$$\lim_{n\to\infty} \sup m(x_n) \leq |N_{K/\mathbb{Q}}(x - A)| \leq m(x) + \varepsilon$$

□

Remark 3.5. Properties ii. and iii. of Proposition 3.2 cannot be extended to H through $m_{\bar{K}}$. Proposition 3.4 i), with $\varepsilon = 1$, shows that $m_{\bar{K}}$ induces an upper semi-continuous map on H over $\mathcal{O}_K$ which is a compact set (isomorphic to $\mathbb{T}_n$, n- torus), so that $m_{\bar{K}}$ is bounded and attains its maximum on H.

Definition 3.6. The *inhomogeneous minimum of* K, denoted by $M(\bar{K})$, is the positive real number defined by

$$M(\bar{K}) = \sup\{m_{\bar{K}}(x);\ x \in H\} < +\infty.$$

[1] Generally, f is upper semi-continuous at a if $\lim\limits_{x\to a} \sup f(x) \leq f(a)$

Definition 3.7. The *Euclidean minimum of* K, denoted by $M(K)$, is also the positive real number defined by

$$M(K) = \sup\{m_K(\xi);\ \xi \in K\}.$$

Remark 3.8. The Euclidean minimum of K, with respect to the norm $N_{K/\mathbb{Q}}$, also denoted $M(R, N_{K/\mathbb{Q}})$, can be redefined in other words as $M(R, N_{K/\mathbb{Q}})$:

$$\begin{aligned} &= \inf\{k > 0 : \forall \beta \neq 0, \alpha \in \mathcal{O}_K \quad \exists \gamma \in \mathcal{O}_K : |N_{K/\mathbb{Q}}(\alpha - \beta\gamma)| < k|N_{K/\mathbb{Q}}(\beta)|\} \\ &= \inf\{k > 0 : \forall \xi \in K \quad \exists \gamma \in \mathcal{O}_K \text{ with } |N_{K/\mathbb{Q}}(\xi - \gamma)| < k\} \end{aligned}$$

$M(\mathcal{O}_K, N_{K/\mathbb{Q}}) > 1$ means that there exist at least two elements of the domain, say $a, b \in \mathcal{O}_K - \{0\}$, such that for every $q \neq 0$ in $\mathcal{O}_K$, $f(a - bq) > f(b)$. In which case, $N_{K/\mathbb{Q}}$ can not be a Euclidean function on $\mathcal{O}_K$. On the other hand, if $M(\mathcal{O}_K, N_{K/\mathbb{Q}}) < 1$ then for all such numbers a and b, there exists q such that $N_{K/\mathbb{Q}}(a - bq) < N_{K/\mathbb{Q}}(b)$. This makes $\mathcal{O}_K$ Euclidean domain with respect to the given function. However, when $M(\mathcal{O}_K, N_{K/\mathbb{Q}}) = 1$, no conclusion can be made about the Euclideanity with respect to $N_{K/\mathbb{Q}}$ of $\mathcal{O}_K$ as both conditions could happen.

Theorem 3.9. *These above two definitions of Euclidean minimum of a given field are in fact equivalent.*

Proof. Assume m_1 and m_2 to be the Euclidean minimum of K with respect to the two definitions.

$$\begin{aligned} m_1 &:= \inf\{k > 0 : \forall \xi \in K \quad \exists \gamma \in \mathcal{O}_K \text{ with } |N_{K/\mathbb{Q}}(\xi - \gamma)| < k\} \\ m_2 &:= \sup_{\xi \in K} \inf_{\gamma \in \mathcal{O}_K} |N_{K/\mathbb{Q}}(\xi - \gamma)| \end{aligned}$$

Claim: $m_1 = m_2$.
Let $k > m_1$ be arbitrarily taken and fixed. By definition,

$$\begin{aligned} k > m_1 &\Rightarrow \forall \xi \in K \quad \exists \gamma \in \mathcal{O}_K \text{ with } |N_{K/\mathbb{Q}}(\xi - \gamma)| < k \\ &\Rightarrow m_K(\xi) < K \quad \forall \xi \in K \\ &\Rightarrow m_2 \leq k \end{aligned}$$

Since $m_2 \leq k$ is true for any $k > m_1$, $m_2 \leq m_1$ follows.
On the other hand, if any $k > m_2$ is taken, by Proposition 3.4 ii), we have,

$$k > m_2 \Rightarrow \forall \xi \in K \quad \exists \gamma \in \mathcal{O}_K \text{ with } |N_{K/\mathbb{Q}}(\xi - \gamma)| = m_K(\xi) \leq m_2 < k$$

Since $m_1 \leq k$ for all $k > m_2$, $m_1 \leq m_2$ follows. □

By the two definitions, it is clear that $M(K) \leq M(\bar{K})$. In the case $n = 2$ and K is totally real (the complex case is obvious), it has been proved by Barnes and Swinnerton-Dyer (cf [2]), that, in fact, there is an equality, and they have conjectured that there is an element $\xi \in K$ that satisfies $M(\bar{K}) = m_K(\xi)$. Of course, if it is true, we have $M(K) = M(\bar{K}) \in \mathbb{Q}$.
From Definition 3.6 and Proposition 3.2 ii) we can write

$$\forall \xi \in K,\ \exists \Upsilon \in \mathcal{O}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K),$$

which leads to the following definition.

Definition 3.10. $M(\bar{K})$ is said to be *attained* if

$$\forall x \in H,\ \exists \Upsilon \in \mathcal{O}_K \text{ such that } |\prod_{i=1}^{n} x_i - \sigma_i(\Upsilon)| \leq M(\bar{K}).$$

For $n = 2$, this property is not always true. A counter example can be $\mathbb{Q}(\sqrt{13})$ (cf [2], or [32]).

Definition 3.11. The set of values of m_K and $m_{\bar{K}}$ are respectively called the *Euclidean spectrum* and the *inhomogeneous spectrum* of K.

Definition 3.12. The *second inhomogeneous and Euclidean minima* of K are respectively defined by

$$M_2(\bar{K}) = \sup_{\substack{x \in H \\ m_{\bar{K}}(x) < M(\bar{K})}} \Big(m_{\bar{K}}(x) \Big) \quad \text{and}$$
$$M_2(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M(K)}} \Big(m_K(\xi) \Big)$$

By induction, the n^{th} inhomogeneous and Euclidean minima (with $n \geq 2$) can also be defined in a similar notion as follows

$$M_{n+1}(\bar{K}) = \sup_{\substack{x \in H \\ m_{\bar{K}}(x) < M_n(\bar{K})}} \Big(m_{\bar{K}}(x) \Big) \quad \text{and}$$
$$M_{n+1}(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M_n(K)}} \Big(m_K(\xi) \Big)$$

Definition 3.13. $M(\bar{K})$ is said to be *isolated* if $M_2(\bar{K}) < M(\bar{K})$.

3.2 Questions

These previous definitions lead to some questions. For instance, it has been conjectured that, for $n = 2$ and K totally real, $M(\bar{K})$ is isolated, but this has only been proved when $M(\bar{K})$ is "attained" by a finite number of points of H modulo $\mathcal{O}_K$ (cf [2]).

In addition to this, it is likely to ask if there is an equality case between the second Euclidean minimum and inhomogeneous minimum as in the first minima. The answer to the question is negative. when $n = 2$, a good explanation is given by Godwin for the why not. (cf [21]; For related questions, one can refer to Lemmermeyer's survey, [32]): if $K = \mathbb{Q}(\sqrt{73})$, we have $M_2(K) < M_2(\bar{K})$. Nevertheless, as we shall see, there is an equality for $r > 1$ if K is not a CM-field[2], and we can even generalize this phenomenon to the successive minima:

$$\forall p > 1,\ M_{p+1}(\bar{K}) = M_{p+1}(K) < M_p(\bar{K}) = M_p(K),$$

with $\lim_{p\to+\infty} M_p(\bar{K}) = 0$. In this case both spectra are identical, included in $\mathbb{Q}$, and only composed of the successive minima and 0.

Remark 3.14. Without the assumption $r > 1$, the previous limit does not necessarily hold, as can be shown by the simple choice $K = \mathbb{Q}(\sqrt{5})$. In this case, the $M_p(\bar{K})$ form a strictly decreasing sequence and even if it is possible to find $\xi \in K$ with $m_K(\xi)$ arbitrarily small, $\lim_{p\to+\infty} M_p(\bar{K}) = (2 + 2\sqrt{5})^{-1}$.

3.3 General Results

In this section, essential results relevant to the questions mentioned above is given. For more explanation, the reader can refer to J-P Cerri's paper [6].

Theorem 3.15. *Let K be a number field of degree n. If the unit rank r of K is strictly greater than 1, there exists $\xi \in K$ such that*

$$M(\bar{K}) = m_{\bar{K}}(\xi) = m_K(\xi).$$

Corollary 3.16. *For every number field K we have $M(K) = M(\bar{K})$. Moreover if the unit rank of K is strictly greater than 1, then $M(K) = M(\bar{K}) \in \mathbb{Q}$.*

Proof. The equality $M(K) = M(\bar{K})$ is a direct consequence of definitions and Theorem 3.15. The rationality of this number follows from Proposition 3.2 iii). □

[2]CM-field stands for Complex Multiplication field

From the definition of $M(K)$ and the standard definition of *norm-Euclideanity* of number fields, it is already remarked by the other definition that the value of $M(K)$ gives the following information:

- If $M(K) < 1$, K is norm-Euclidean,
- If $M(K) > 1$, K is not norm-Euclidean,
- If $M(K) = 1$, such conclusion is impossible except the case that there is an element ξ of K with $M(K) = m_K(\xi)$; in which case K is not norm-Euclidean,

The above theorem 3.15 and Corollary 3.16 give the following result.

Corollary 3.17. *Let K be a number field with unit rank r such that $r > 1$. If $M(K) = 1$, then K is not norm-Euclidean.*

Let us put now

$$\mathcal{A} = \{z \in H \text{ such that } \prod_{i=1}^{n} |z_i| < 1\}.$$

It is obvious that if $\mathcal{O}_K + \mathcal{A} = H$ then K is norm-Euclidean. H.W. Lenstra Jr. has conjectured that it is in fact an equivalence (cf [33]). Theorem 3.15, implies this is true as far as $r > 1$.

Theorem 3.18. *If the unit rank, r, of a number field K is greater than 1, then*

$$K \text{ is norm-Euclidean} \Longleftrightarrow \mathcal{O}_K + \mathcal{A} = H.$$

Proof. If K is norm-Euclidean, we have $M(K) = M(\bar{K}) \leq 1$. Assume that $M(\bar{K}) = 1$. Then by Theorem 3.15, there exists $\xi \in K$ such that $m_K(\xi) = 1$. But, since K is norm-Euclidean, this is impossible, so that

$$M(K) = M(\bar{K}) = M < 1.$$

Let $z \in H$. We have $m_{\bar{K}}(z) \leq M < 1$ and, by definition of $m_{\bar{K}}(z)$, there exists $Z \in \mathcal{O}_K$ such that

$$\prod_{i=1}^{n} |z_i - \sigma_i(Z)| \leq \frac{M+1}{2} < 1.$$

This implies $\mathcal{O}_K + \mathcal{A} = H$. □

Remark 3.19. In fact we have the following more precise result.
If $\mathcal{A}_k = \{z \in H \text{ such that } \prod_{i=1}^{n} |z_i| \leq k\}$, then

$$K \text{ is norm-Euclidean } \iff \exists\, k \in]0,1[\text{ such that } \mathcal{O}_K + \mathcal{A}_k = H.$$

Let us give now an important corollary of Theorem 3.18 which has already been pointed out by H.W. Lenstra Jr.

Corollary 3.20. *K being given with unit rank strictly greater than 1, the question whether K is norm-Euclidean is decidable.*

The reader can refer to Lenstra's papers [33] for more details.

We can be more precise and look at all the values of $m_{\bar{K}}$ or m_K. It is a remarkable fact that, contrary to what can happen in real degree 2, all these values are rational as far as $r > 1$ and K is not a CM-field (totally complex quadratic extension of a totally real number field). More precisely, inhomogeneous and Euclidean spectra are equal, included in $\mathbb{Q}$ and we have the following result.

Theorem 3.21. *Let K be a number field of degree n. If the unit rank r of K is strictly greater than 1 and if K is not a CM-field, in particular if K is totally real, there exists a strictly decreasing sequence $(r_p)_{p\geq 1}$ of positive rational numbers, which verifies:*

(i) $\lim_{p\to+\infty} r_p = 0.$

(ii) $m_{\bar{K}}(H) = \{r_p;\ p \geq 1\} \cup \{0\}.$

(iii) for each $p \geq 1$ the set of $x \in H$ such that $m_{\bar{K}}(x) = r_p$ is finite modulo $\mathcal{O}_K$ and are points of K, which implies that if $x \notin K$, $m_{\bar{K}}(x) = 0$.

Corollary 3.22. *Under the same hypotheses, $M(\bar{K}) = M(K)$ is attained. If we put $M_1(K) = M(K)$ and $M_1(\bar{K}) = M(\bar{K})$, we have:*

$$\forall p \geq 1,\ M_p(K) = M_p(\bar{K}) \in \mathbb{Q} \ \text{ and } \ M_{p+1}(\bar{K}) < M_p(\bar{K}).$$

In particular, $M(\bar{K})$ is isolated. Moreover $\lim_{p\to+\infty} M_p(\bar{K}) = 0.$

Proof. We know that the set of $x \in H$ such that $m_{\bar{K}}(x) = M(\bar{K})$ is finite modulo $\mathcal{O}_K$ and is included in K, so that Proposition 3.2.ii) gives the first result. The rest is a direct consequence of Theorem 3.21, since by the definitions it is clear that in fact $M_p(K) = M_p(\bar{K}) = r_p$. □

Remark 3.23. It can be interesting to see that things cannot happen in the same way when K is a CM-field, even if $r > 1$ (see [6]). The situation is quite different from that of Theorem 3.21: in fact, if $S_k = \{x \in H;\ m_{\bar{K}}(x) \geq k\}$, we have the equivalence

$$\forall k > 0,\ S_k \text{ is finite modulo } \mathcal{O}_K \iff K \text{ is not a CM-field.}$$

3.4 k-Stage Euclideanity

Cook's k-stage division chain for two numbers α and β of an integral domain R with q_i and r_i 2k numbers in R where i runs from 1 through n, is given by,

$$\begin{array}{rcl} \alpha = \beta q_1 + r_1 & & \alpha/\beta = q_1 + \frac{1}{\beta/r_1} \\ \beta = r_1 q_2 + r_2 & & \beta/r_1 = q_2 + \frac{1}{r_1/r_2} \\ \cdots & & \cdots \\ \cdots & \Rightarrow & \cdots \\ \cdots & & \cdots \\ r_{k-2} = r_{k-1} r_k + r_k & & r_{k-2}/r_{k-1} = q_k + \frac{1}{r_{k-1}/r_k} \end{array}$$

Combining them together, we will get an equation of them following form called continued fraction:

$$\frac{\alpha}{\beta} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ldots \cfrac{1}{q_k}}}}$$

The above continued fraction can for simplicity be defined by $[q_1, q_2, \ldots, q_k]$ (with coefficients $q_i \in R$) i.e.

$$[q_1, q_2, \ldots, q_k] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots \cfrac{1}{q_k}}}$$

Definition 3.24. An integral domain R is said to be a k-stage Euclidean with respect to a given norm N if for every $\alpha, \beta \in R$ and $\beta \neq 0$, there exists an n-stage division chain starting from the given pair of numbers for some $n < k$ in such a way that the last remainder r_k satisfies $N(r_k) < N(\beta)$.

Definition 3.25. R is called an ω-stage Euclidean domain if for every such pairs, there exists a k-stage division chain for some positive integer k such that the last remainder satisfies $N(r_k) < N(\beta)$.

Remark 3.26. .

- n-stage Euclidean R implies m-stage Euclidean R if $m > n$.
- k-stage Euclidean R implies ω-stage Euclidean R for any k
- 1-stage Euclidean domain is the usual Euclidean domain

Remark 3.27. With the aforementioned notion, a division chain can be determined by the sequence of its quotients $q_1, q_2, \ldots, q_k$; and, conversely, any sequence $q_1, q_2, \ldots, q_k$ of elements of R defines a k-stage division chain starting from the pair α and β

Thus,

$$[q_1] = q_1 = \frac{a_1}{b_1} \qquad \text{where } a_1 = q_1, b_1 = 1$$

$$[q_1, q_2] = q_1 + \frac{1}{q_2} = \frac{a_2}{b_2} \qquad \text{where } a_2 = q_1 q_2 + 1, b_2 = q_2$$

$$[q_1, q_2, \ldots, q_k] = \frac{a_k}{b_k} \qquad \text{where } a_k = q_k a_{k-1} + a_{k-2}, b_k = q_k b_{k-1} + b_{k-2}$$

Proposition 3.28. *For α and β elements of R. Let $q_1, \ldots, q_k$ be elements of R. Then the last elements in the k-stage division chain starting from α and β with those q_i's as quotients is related to the continued fraction $\frac{a_k}{b_k}$ as,*

$$\frac{\alpha}{\beta} - \frac{a_k}{b_k} = (-1)^{k-1} \frac{r_k}{\beta b_k}$$

where r_k is the k^{th} remainder in the usual division chain.
i.e. $r_k = r_{k-2} - q_k r_{k-1}$ starting from $r_1 = q_1\beta - \alpha$

Proof. Let us prove equivalently, by induction on i, the equation

$$\alpha b_i - \beta a_i = (-1)^{i-1} r_i$$

since this equation implies the equation on the proposition when $i = k$. The cases $k = 1$ and $k = 2$ are clearly true by the usual division chain as $\alpha - \beta q_1 = r_1$ is true for the first and the following is true for the later, ,

$$\begin{aligned} \alpha b_2 - \beta a_2 &= \alpha q_2 - \beta(q_1 q_2 + 1) \\ &= (\alpha - \beta q_1) q_2 - \beta \\ &= q_2 r_1 - \beta && (r_1 = \alpha - \beta q_1) \\ &= -r_2 && (r_2 = \beta - q_2 r_1) \end{aligned}$$

Now assuming true for $k-2$ and $k-1$ where $k > 2$, we have,

$$\begin{aligned}\alpha b_k - \beta a_k &= \alpha(q_k b_{k-1} + b_{k-2}) - \beta(q_k a_{k-1} + a_{k-2}) \\ &= q_k(\alpha b_{k-1} - \beta a_{k-1}) + (\alpha b_{k-2} - \beta a_{k-2}) \\ &= q_k((-1)^k r_{k-1}) + (-1)^{k-1} r_{k-2} \\ &= (-1)^{k+1}(-q_k r_{k-1} + r_{k-2}) \\ &= (-1)^{k+1} r_k\end{aligned}$$

by the recursive definition of a_i, b_i and the division chain. □

Corollary 3.29. *If α and β be elements in R, then there exists a k-stage division chain starting from the two numbers with least remainder r_k satisfying $N(r_k) < N(\beta)$ if and only if there exists a continued fraction $\frac{a_k}{b_k}$ such that*

$$N\left(\frac{\alpha}{\beta} - \frac{a_k}{b_k}\right) < \frac{1}{N(b_k)}$$

Proof. For the first implication,

$$N\left(\frac{\alpha}{\beta} - \frac{a_k}{b_k}\right) = N\left(\frac{r_k}{\beta b_k}\right) < \frac{1}{N(b_k)}$$

For the other, since a continued fraction $\frac{a_k}{b_k} = [q_1, \ldots, q_k]$ is given in R that satisfies the given inequality, the corresponding division chain can be constructed starting from α and β with q_i's as quotients. Then by the proposition, $N(r_k) < N(\beta)$ follows from

$$\frac{\alpha}{\beta} - \frac{a_k}{b_k} = (-1)^{k+1}\frac{r_k}{\beta b_k} \Rightarrow N\left(\frac{\alpha}{\beta} - \frac{a_k}{b_k}\right) = N\left(\frac{r_k}{\beta b_k}\right) < \frac{1}{N(b_k)}$$

□

Corollary 3.30. *R is a k-stage Euclidean if and only if for every element, α/β of K, there exists a continued fraction $\frac{a_k}{b_k} = [q_1, \ldots, q_k]$ of length n where $n \leq k$ such that*

$$N\left(\frac{\alpha}{\beta} - \frac{a_n}{b_n}\right) < \frac{1}{N(b_n)}$$

Proof. immediate from the above corollary □

Let, for this last part, $K = \mathbb{Q}(\sqrt{n})$ be a number field whose ring of integers is $\mathcal{O}_K$

Proposition 3.31. *$\mathcal{O}_K$ is ω-stage Euclidean if and only if it is k-stage Euclidean for some positive integer k.*

Proposition 3.32.

Suppose a positive integer $n < 47$ is such that $n \equiv 2, 3 \mod 4$ and $n \equiv 1 \mod 3$. If in $\mathcal{O}_K$, there are solutions to $|N(\alpha)| = 2$ and $|N(\alpha)| = 3$, then the ring is 2-stage Euclidean.

Suppose a positive integer $n < 85$ is congruent to $5 \mod 8$. If the fundamental unit of $\mathcal{O}_K$ is of the form $a + bv$, for odd integer b, then the ring is 2-stage Euclidean.

Example 3.33.

n	$\lvert N(\alpha)\rvert = 2$	$\lvert N(\alpha)\rvert = 3$	n	ε
			53	$3 + v$
31	$39 + 7\sqrt{31}$	$11 + 2\sqrt{31}$	61	$17 + 5v$
43	$59 + 9\sqrt{43}$	$13 + 2\sqrt{43}$	69	$11 + 3v$
46	$156 + \sqrt{46}$	$7 + \sqrt{46}$	77	$4 + v$

where $v = \sqrt{n}$ for $n \equiv 1 \mod 4$ or $(1 + \sqrt{n})/2$ for $n \equiv 2, 3 \mod 4$.
In general, the known examples of 2-stage norm Euclidean real quadratic fields are summarized by the following array in terms of n as,

14	22	23	31	38	43	46	47	53
59	61	62	67	69	71	77	89	93
97	101	109	113	129	133	137	149	157
161	173	177	181	193	197	201	213	253

Proposition 3.34. *The ring $\mathcal{O}_K$ of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{n})$ is k-stage Euclidean if and only if it is Euclidean.*

Theorem 3.35. *Let K be a number field with class number 1 and unit rank not less than 1. Assume that GRH holds true. Then K is 4-stage Euclidean. If moreover K has at least one real embedding, then it is a 2-stage Euclidean.*

Chapter 4

"Euclideanity" In Different Degrees

4.1 Quadratic Number Fields

Complex Quadratic Number Fields

Let K be an imaginary quadratic number field, i.e. $K = \mathbb{Q}(\sqrt{-m})$, m a square free positive integer. Generally since Minkowski's conjecture has direct link with the inhomogeneous minima of number fields, the last chapter discusses some important and relevant points about it.

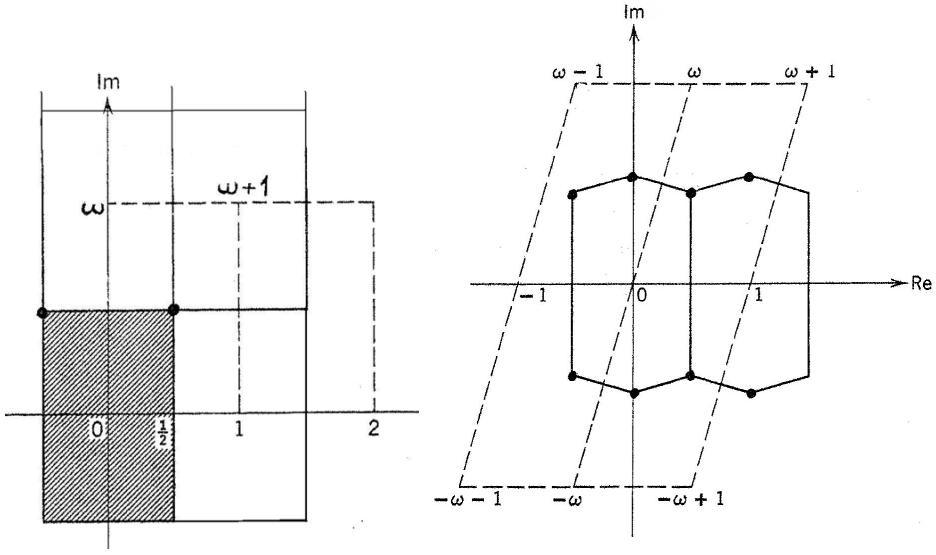
Proposition 4.1. *The ring of integers, $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-m})$ is Euclidean if and only if $m = 1, 2, 3, 7$ and 11. More strongly, they are Euclidean with respect to the norm.*

Proposition 4.2. *The Euclidean minimum $M(K)$ of the ring of integers of $K = Q(\sqrt{-m})$ with respect to the norm is given by*

$$\frac{|m|+1}{4}, \text{ if } R = \mathbb{Z}[\sqrt{-m}], \text{ and}$$

$$\frac{(|m|+1)^2}{16m}, \text{ if } R = \mathbb{Z}\Big[\frac{1+\sqrt{-m}}{2}\Big].$$

Proof. In both cases, the norm $N_{K/Q}(x-z)$ for $x \in K$ and $z \in \mathcal{O}_K$ is the square of the distance between the two points x and z. For the first case, the fundamental domain is a rectangle whose dimensions are $\sqrt{m}$ and 1. The point inside the rectangle at a maximum possible distance from the four vertices (i.e. lattice points), is the mid point of the diagonal as shown in figure (a) below.



(a) The First Case (b) The Second Case

Figure 4.1: Figures showing points of Euclidean minimum

For the second case, the points are found by considering the intersection of the perpendicular bisectors of the left side, diagonal and right side of each parallelogram as shown in figure (b). These are the points at which the Euclidean minimum is achieved up on intersection as shown. Thus they by themselves form a structure looking like honeycomb in the lattice as partly shown in the figure. □

Real Quadratic Number Fields

Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field. Hence, $m \geq 2$ is assumed to be a square free positive integer as above.

Theorem 4.3. *The ring of integers of $K = \mathbb{Q}(\sqrt{m})$ is norm-Euclidean if and only if m is one of the following 16 integers:*

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

Theorem 4.4. *For real quadratic fields K with discriminant d,*

$$\frac{\sqrt{d}}{16 + 6\sqrt{6}} \leq M(K) \leq \frac{1}{4}\sqrt{d}.$$

Proposition 4.5. *Let n be an odd integer, $m = n^2 + 1$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$; then the Euclidean minimum of $\mathcal{O}_K$ is $\frac{n}{2}$, and this minimum is attained exactly at the points $\xi = \frac{1}{2}\sqrt{m} \mod R$.*

Proposition 4.6. *Let $K = \mathbb{Q}(\sqrt{5})$; then $\omega = \frac{1}{2}(1 + \sqrt{5})$ is the fundamental unit of K and $M(K) = \frac{1}{4}$. Moreover, there is an infinite sequence of isolated minima whose $(i+1)^{th}$ term is given by*

$$M_{i+1}(\bar{K}) = \frac{F_{6i-2} + F_{6i-4}}{4(F_{6i-1} + F_{6i-3} - 2)}, \quad \forall i \geq 1$$

where F_i is the i-th Fibonacci number.[1]

The sequence of minima begins with $M_1 = \frac{1}{4}$ as mentioned above; $M_2 = \frac{1}{5}, M_3 = \frac{19}{121}, \ldots, \ldots$ and $M_\infty(\bar{K}) = \lim_{i\to\infty} M_i(\bar{K}) = \dfrac{1}{4\omega}$.

If $C_i(\bar{K})$ or simply C_i denotes the set of all points in $\bar{K}$ at which the minimum value is attained in $M_i(\bar{K})$ i.e.

$$C_i(\bar{K}) = \{x \in \bar{K} : M(x) = M_i(\bar{K})\}$$

then

$$\begin{aligned}
C_1 &= \{(0, \frac{1}{2}), (\frac{1}{2}, 0)\} = \{\frac{1}{2}, \frac{\omega}{2}\} \\
C_2 &= \{(0, \pm\frac{1}{5}), (0, \pm\frac{2}{5})\} = \{\pm\frac{\omega}{5}, \pm\frac{2\omega}{5}\} \\
&\ldots \\
C_i &= \{\xi \in K : \xi \equiv \frac{\omega^{6i-3} + 1}{2(\omega^{6i-2} - 1)}\varepsilon \mod \mathcal{O}_K, \varepsilon \text{ is a unit } \}
\end{aligned}$$

Proposition 4.7. *For $K = \mathbb{Q}(\sqrt{13})$, $M_1(\bar{K}) = \frac{1}{3}$, $M_2(\bar{K}) = \frac{4}{13}$, and*

$$\begin{aligned}
C_1 &= \Big\{\Big(\pm\frac{1}{6}, \frac{1}{6}\Big), \Big(\pm\frac{1}{6} - \frac{1}{6}\eta^k, \pm\frac{1}{6} + \frac{1}{6\sqrt{13}}\eta^k\Big)\Big\} \\
C_2 &= \Big\{\Big(0, \pm\frac{2}{13}\Big), \Big(0, \pm\frac{3}{13}\Big)\Big\}.
\end{aligned}$$

where $k \in \mathbb{N}$ and $\eta = \frac{1}{2}(-3 + \sqrt{13})$. Furthermore, $M_1(\bar{K})$ is not attained.

Proposition 4.8. *Let $K = \mathbb{Q}(\sqrt{23})$; then the first minimum $M_1(\bar{K}) = \frac{77}{46}$ is attained and isolated, whereas $M_2(\bar{K}) = \frac{1}{46}(20\sqrt{23} - 31)$ is not isolated.*

[1] Fibonacci sequence is defined by $F_0 = F_1 = 1; F_{n+1} = F_n + F_{n-1}$.

Proposition 4.9. *In $K = \mathbb{Q}(\sqrt{69})$, we have*

$$\begin{aligned} M_1 &= \tfrac{25}{23}, & C_1 &= \{\pm\tfrac{4}{23}\sqrt{69}\} \\ M_2 &= \tfrac{(3795-345\sqrt{69})}{1058}, & C_2 &= \{(\pm P_k, \pm P_k')\}, \end{aligned}$$

where

$$\begin{aligned} P_k &= \frac{1}{2}\varepsilon^{-k} + \Big(\frac{4}{23} + \frac{1}{2\sqrt{69}}\varepsilon^{-k}\Big)\sqrt{69}, \\ P_k' &= \frac{1}{2}\varepsilon^{-k} - \Big(\frac{4}{23} + \frac{1}{2\sqrt{69}}\varepsilon^{-k}\Big)\sqrt{69}. \end{aligned}$$

where $\varepsilon = \frac{1}{2}(25 + 3\sqrt{69})$ is the fundamental unit in $\mathbb{Q}(\sqrt{69})$.

4.2 Cubic Number Fields

Pure cubic number fields (i.e of the form $\mathbb{Q}(\sqrt[3]{m})$) which are norm-Euclidean are exactly three in number; namely, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$ and $\mathbb{Q}(\sqrt[3]{10})$ which have been determined by Cioffari [9]

Complex Cubic Number Fields.

There are finitely many norm-Euclidean complex cubic number fields. This is proved by Davenport [17]. Good lower bound for $M(\bar{K})$ so far has been found by Cassels [52]. However, Van der Linden [44] noted that this value could seem to be improved to a better bound.

Proposition 4.10. *If K is a complex cubic number field with $d = |\text{discK}|$, then*

$$\frac{\sqrt{d}}{420} \leq M(\bar{K}) \leq \frac{\sqrt[3]{d^2/2}}{16}.$$

Moreover, if K is norm-Euclidean, then $d < 176400$

The following proposition and the upper bound of the above proposition are due to Swinnerton-Dyer [43]

Proposition 4.11. *Let K be the number field defined by the real root α of $f(x) = x^3+2ax-1$ (where $a \geq 1$) and let $R = \mathbb{Z}[\alpha]$. Then $M(K) = M(\bar{K}) = \frac{1}{2}(a^2 - a + 1)$, and this minimum is attained exactly at $\xi \equiv \frac{1}{2}(1 + \alpha + \alpha^2)$ mod R.*

Totally Real Cubic Number Fields.

Proposition 4.12. *If K is a totally real cubic field with discriminant d, then*

$$M(\bar{K}) \leq \frac{1}{8}\sqrt{d}$$

Since $M(\bar{K}) < 1$ implies the corresponding ring of integers is norm Euclidean, the above proposition guarantees that the cubic field with discriminant 49 is norm Euclidean. i.e. $M(\bar{K}) < 7/8 < 1$.
Heilbronn [26] proved that norm-Euclidean cyclic real cubic number fields are finite where as he conjectured the non cyclic ones are infinite.

Real cubic number fields, which moreover are cyclic fields with conductors $\mathfrak{f} = 7, 9, 13, 19, 31, 37, 43, 61$ and 67 are known to be norm Euclidean. On the other hand, those with conductors $73, 79, 97, 139, 151$ and between 163 and 10^4 are not norm Euclidean.This result is due to Smith [42]. Lemmermeyer [31] finally raised the maximum limit to $5 \cdot 10^5$ for the later assertion.

4.3 Quartic Number Fields

Totally Complex Quartic Fields

There are only finite number of norm-Euclidean quartic fields which are totally complex according to the proof of Davenport [16] and Cassels [52]

Proposition 4.13. *If K is a totally complex quartic field and $d =$ discK, then $M(K) > k\sqrt{d}$ for some constant $k > 0$.*

The only norm-Euclidean totally complex cyclic quartic fields are $\mathbb{Q}(\zeta_5)$ and the quartic subfield of $\mathbb{Q}(\zeta_{13})$, where ζ_m denotes a primitive m-th root of unity.

Proposition 4.14. *There are exactly 13 norm Euclidean number fields of the form $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ for a negative integer m where m and n are square free in absolute value; namely,*

$$\begin{array}{llll} \mathbb{Q}(\sqrt{-1}, \sqrt{2}), & \mathbb{Q}(\sqrt{-1}, \sqrt{3}), & \mathbb{Q}(\sqrt{-1}, \sqrt{5}), & \mathbb{Q}(\sqrt{-1}, \sqrt{7}), \\ \mathbb{Q}(\sqrt{-2}, \sqrt{-3}), & \mathbb{Q}(\sqrt{-2}, \sqrt{5}), & \mathbb{Q}(\sqrt{-3}, \sqrt{2}), & \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \\ \mathbb{Q}(\sqrt{-3}, \sqrt{-7}), & \mathbb{Q}(\sqrt{-3}, \sqrt{-11}), & \mathbb{Q}(\sqrt{-3}, \sqrt{17}), & \mathbb{Q}(\sqrt{-3}, \sqrt{-19}) \\ \mathbb{Q}(\sqrt{-7}, \sqrt{5}) & & & \end{array}$$

This result is due to Lemmermeyer [30]

Proposition 4.15. *For m a square-free integer; there are exactly four norm Euclidean complex quartic fields of the form $\mathbb{Q}(\sqrt[4]{-m})$; namely, when m is $2, 3, 7$ or 12.*

Proposition 4.16. *Suppose that K is a norm-Euclidean complex quartic field;*

i) If K contains $k = \mathbb{Q}(\sqrt{2})$, then K is either of the following:

$$k(\sqrt{-1}), \quad k(\sqrt{-3}) \quad or \quad k(\sqrt{-5-2\sqrt{2}})$$

ii) If K contains a real quadratic number field and 2 is totally ramified in K, then

$$K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$$

iii) If K contains a real quadratic number field and 2 is the square of a prime ideal in K, then K is one of the following fields

$$\mathbb{Q}(\zeta_{12}), \quad \mathbb{Q}(\sqrt{-3}, \sqrt{2}), \quad \mathbb{Q}(\sqrt{-3}, \sqrt{-2}) \text{ and } \mathbb{Q}(\sqrt{5}, \sqrt{-2})$$

iv) If $K = \mathbb{Q}(i, \sqrt{a+bi})$ with $i^2 = -1$ and $a + bi \equiv \pm 1 + 2i \mod 4$, then

$$a + bi \in \{\pm 1 + 2i, \pm 3 + 2i, \pm 5 + 2i, \pm 1 + 6i, \pm 7 + 2i\}.$$

Totally Real Quartic Fields

Norm Euclidean totally real quartic fields are finite and have completely been determined. There are some classes of cyclic totally real quartic fields which are not Euclidean with respect to the norm. As highlighted in the first part of Section 2.5, Clark's Ph.D thesis provides us an interesting criterion to determine whether a given real quartic Galois field is Euclidean or not. For example the bicycle field $\mathbb{Q}(\sqrt{14}, \sqrt{22})$ is not norm Euclidean. [32]

Quartic Fields With Unit Rank 2

Proposition 4.17. *There are finitely many norm-Euclidean fields $\mathbb{Q}(\sqrt[4]{m})$.*

The possible value of $m > 0$ for which $\mathbb{Q}(\sqrt[4]{m})$ is norm Euclidean can not be outside the set S as shown by Lemmermeyer [31], where

$$S = \{2, 3, 5, 7, 12, 13, 20, 28, 52, 61, 116, 436\}$$

Currently, the case where $m = 2, 5, 12$ and 20 are known to be norm Euclidean; whereas, $m = 7, 28, 52$ and 436 are not. However, the rest four cases are still open to be determined.

4.4 Survey of Euclidean Minima

In the appendix part A, there are 8 tabular presentations of Euclidean minima of many number fields categorized by their degree. They are directly taken from the doctoral thesis of J-P Cerri [7]. In Table A.1, m refers to the m value in the number field $\mathbb{Q}(\sqrt{m})$ under discussion. T and d_K found in many of these tables respectively represent the number of critical rational points of the fundamental parallelotope of the lattice and the discriminant of the number field K being studied. The letter E is to mean norm-Euclidean.

The following table summarizes each of them according to the data included. The column Total contains the number of cases dealt under each category. In the first table, Table A.1, there are 28 quadratic number fields $K = \mathbb{Q}(m)$ where m is between 103 and 400 that are excluded out due to the large size of their fundamental units, i.e $|\varepsilon| > 10^7$. As shown in table A.5, 156 quintic number fields are presented in which all except only one of them are Euclidean with respect to the norm. The only exception is the field K of discriminant 390,625 which has class number one but has $M(K) = 7/5$. For the number fields of higher degree than 5, little is known about the Euclidean minima. In Table A.6, A.7 and A.8, the first 156 heptic, 132 sextic and 18 octic number fields are surveyed respectively. The m value of the excluded quadratic number fields are listed below. For simplicity, S is let to denote the set of these elements.

139	151	163	166	191	199	211
214	239	241	249	262	271	283
307	311	313	319	331	334	337
358	369	379	382	391	393	394

Table	Number Field	For	Total
Table A.1	Quadratic	m from 2 up to 400 without S	152
Table A.2	Cubic	d_K up to 11,000	108
Table A.3	Cubic	d_K from 11,000 up to 15,000	184
Table A.4	Quartic	d_K up to 40,000	288
Table A.5	Quintic	$d_K$up to 511,000	156
Table A.6	Sextic	d_K up to 5,279,033	156
Table A.7	Heptic	d_K up to 138,031,669	132
Table A.8	Octic	d_K up to 877,268,125	18

Table 4.1: Table description of Some Euclidean minima of number fields

4.5 General Idea

This section mainly discusses the general notions on number fields to be applied for the study of Euclidean number fields of higher degrees in the next chapter.

Let K be an algebraic number field of degree $n = r_1+2r_2$ and discriminant d over $\mathbb{Q}$. And let $\mathcal{O}_K$ be the ring of algebraic integers in K. As K is a separable extension of $\mathbb{Q}$, there exists a primitive or generating element α such that $K = \mathbb{Q}(\alpha)$. Let $f(x)$ be the irreducible monic polynomial in $\mathbb{Q}[x]$ for the primitive element α. Let $\alpha_1, \ldots, \alpha_{r_1}$ be the real roots and $\beta_1, \bar{\beta}_1, \ldots, \beta_{r_2}, \bar{\beta}_{r_2}$ the complex roots appearing in conjugate pairs. Accordingly, we have n embeddings in $\mathbb{C}$ as $\sigma_i : \alpha \mapsto \alpha_i$ for the real ones, $\tau_i : \alpha \mapsto \beta_i$ the complex ones with $\bar{\tau}_i : \alpha \mapsto \bar{\beta}_i$ the corresponding conjugates. Let

$$\begin{aligned}\Phi :& K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \quad \leftrightsquigarrow \\ & x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \tau_1(x), ..., \tau_{r_2}(x), \bar{\tau}_1(x), \ldots, \bar{\tau}_{r_2}(x))\end{aligned}$$

$$\mathcal{N} : \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \to \mathbb{R} \qquad \leftrightsquigarrow \quad x \mapsto \prod_{i=1}^{r_1} |x_i| \prod_{j=1}^{r_2} |x_j \bar{x}_j|$$

The first map is an embedding of K in $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ where as, the later one, when the elements are taken from the image of the first one, is the absolute value of the field norm. Now we see that the image of K by Φ is just n tuples of complex numbers(i.e. $y \in \Phi(K) \Rightarrow y = a_j + b_j i$ where $j = 1, \ldots, n$) Let us consider once again the following function:
$\Psi : \Phi(K) \to \mathbb{R}^n$ given by:

$$\Psi(y) = \Psi((a_j + b_j i)) = (a_j + b_j)$$

By the composing as such, $\Psi \circ \Phi$, K can be embedded in $\mathbb{R}^n$

Proposition 4.18. *$\mathcal{L} = \Psi(\Phi(\mathcal{O}_K))$ is a lattice in $\mathbb{R}^n$ whose fundamental domain has Lebesgue[2] measure of $\sqrt{|d|}$, where d is the discriminant*

Theorem 4.19. *(Hurwitz) There exists an integer $M > 1$ such that*

$$\forall \xi \in K, \quad \exists z \in \mathcal{O}_K \text{ and } j, 0 < j < M \text{ with } N_{K/\mathbb{Q}}(j\xi - z) < 1$$

$\divideontimes$ $\mathcal{O}_K$ is norm Euclidean if and only if M can be chosen to be 2.

[2]Lebesgue measure is a formalization of the intuitive notion of length of a set in $\mathbb{R}$, an area of a set in $\mathbb{R}^2$ and volume in $\mathbb{R}^3$, etc.

Let $\gamma_1, \ldots, \gamma_n$ be a basis of our lattice, $\mathcal{L}$. Then the corresponding fundamental parallelotope with respect to the chosen basis will be given as:

$$P = \{a_1\gamma_1 + \cdots + a_n\gamma_n \text{ where } 0 \leq a_i < 1\}$$

These defined region helps us to relate the field and its ring of integers by $K = P \oplus O_K$.

Since the set P is open and the function $\mathcal{N}$ is continuous on $\mathbb{R}^n$, a neighborhood of the origin in $\mathbb{R}^n$, say U, can be chosen in such a way that for all u and $v \in U, N(u - v) < 1$. Let $\xi \in K$. And let us have translations of the region U by $U_k := k\xi + U, i = 1, 2, 3, \ldots$. Then, for each positive integer k, corresponding to U_k, let V_k be the set formed from U_k by replacing each element ϵ by $\epsilon' \in P$ where $\epsilon' = \epsilon - r, r \in \mathcal{O}_K$. In other words, we are bringing each element of U_k to belong to P by subtracting a suitable element from $\mathcal{O}_K$. Thus, V_k is contained in P for each k. Moreover, the volume of each V_k is equal to the volume of U. Therefore, if M is taken to be greater than $\mu(F)/\mu(U)$, then at least two sets V_{k_1} and $V_{k_2}, 1 \leq k_1 < k_2 \leq M$ will intersect. That is:

$$\exists u_1, u_2 \in U; \lambda_1, \lambda_2 \in \mathcal{O}_K \text{ such that } k_1\xi + u_1 - \lambda_1 = k_2\xi + u_2 - \lambda_2$$

Finally, if we set $j = k_2 - k_1$ and $z = \lambda_2 - \lambda_1$, we get:

$$\begin{aligned} N_{K/\mathbb{Q}}(j\xi - z) =& N_{K/\mathbb{Q}}((k_2 - k_1)\xi - (\lambda_2 - \lambda_1)) \\ =& N_{K/\mathbb{Q}}(k_2\xi - \lambda_2 - k_1\xi + \lambda_1) \\ =& N_{K/\mathbb{Q}}(u_1 - u_2) < 1 \end{aligned}$$

This way of proving whether a number field is Norm Euclidean based on the sets U, U_k and V_k, where $k = 1, 2, 3, \ldots$ is sometimes impossible due to the fact that we are not able to find such a suitable set U such that $\mu(F)/\mu(U) < M = 2$. To avoid such failure, Lenstra formed a new sequence $\omega_1, \ldots, \omega_M$ instead of just $\{1, 2, \ldots, M\}$ where each ω_i is taken from $\mathcal{O}_K$ and the difference between any two distinct elements from the sequence is a unit in $\mathcal{O}_K$. Thus under the analogous construction on the new sequence, we can state the result as, there is an integer $M > 1$ such that for each $\xi \in K$, there is $z \in \mathcal{O}_K$ and indices $i, j; 0 < i < j < M$ such that $N_{K/\mathbb{Q}}((\omega_i - \omega_j)\xi - z) < 1$. From this we can have:

$$\begin{aligned} N_{K/\mathbb{Q}}(\xi - z(\omega_i - \omega_j)^{-1}) =& N_{K/\mathbb{Q}}(\xi - z(\omega_i - \omega_j)^{-1}) \cdot 1 \\ =& N_{K/\mathbb{Q}}((\omega_i - \omega_j)\xi - z)N_{K/\mathbb{Q}}(\omega_i - \omega_j) \\ =& N_{K/\mathbb{Q}}((\omega_i - \omega_j)\xi - z) < 1 \end{aligned}$$

As such, $\mathcal{O}_K$ can be concluded to be Euclidean with respect to norm function. Therefore for $\mathcal{O}_K$ to be norm Euclidean, there should exist long enough sequence $\{\omega_i\}_{i=1}^n$ and such that $\omega_i - \omega_j$ should belong to $\mathcal{O}_K^\times$ These leads us to the following formal definition of Lenstra's sequences and theorem.

Exceptional Sequences

In this section, although the original work of Lenstra is revised in the next chapter for cyclotomic fields and as his method can also be adapted to other non cyclotomic number fields of higher degree, it is quite useful to see it here as well.

Definition 4.20. A sequence $\omega_1, \ldots, \omega_n$ of elements of $\mathcal{O}_K$ is said to be a unit differential or an exceptional sequence of length n if the n elements are all distinct and for all $i, j; i \neq j$, $\omega_i - \omega_j \in \mathcal{O}_K^\times$.

Definition 4.21. Lenstra's constant of a number field K, denoted by $\lambda(K)$ is the positive integer k such that the field has an exceptional sequence of maximal length k. i.e. if $\omega_1, \ldots, \omega_k$ is an exceptional sequence of maximal length, then $\lambda(K) = k$ is termed as Lenstra's constant of K.

The length of exceptional sequence is bounded. If $\lambda'(K)$ is the minimal norm of a non zero proper ideal of $\mathcal{O}_K$, then $\lambda(K) \leq \lambda'(K)$.

Theorem 4.22. *Let the degree of the number field K be $n := r_1 + 2r_2$ where r_1 and r_2 are the number of real and complex embeddings in order. Then there exist constants $\alpha_{r_1,r_2} > 0$ with the following property: if K contains an exceptional sequence of length $m > \alpha_{r_1,r_2}\sqrt{d}$, then K is norm-Euclidean, where $\alpha_{r_1,r_2} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}$*

Proposition 4.23. *Let p be prime, $\zeta = \zeta_p$ a primitive p-th root of unity, and $K = \mathbb{Q}(\zeta)$. Then the sequence*

$$\left\{\omega_j = \frac{\zeta_p^j - 1}{\zeta_p - 1}\right\}_{1 \leq j \leq p}$$

shows that $\lambda(K) = \lambda'(K) = p$.

Theorem 4.24. *Let K be an algebraic number field of discriminant d and degree n over $\mathbb{Q}$. Let $N_{K/\mathbb{Q}}$ be the absolute value of the field norm. If $U \subseteq \mathbb{R}^n$ is a bounded Lebesgue measurable set with positive Lebesgue measure μ; such that, $N_{K/\mathbb{Q}}(u - v) < 1 \quad \forall u, v \in U$, then K is Euclidean if $\lambda(K) > \delta^*(U)\sqrt{d}$ where $\delta^*(U)$ is the center packing constant of U as given in DefinitionB.24*

Proof. We need to find $z \in \mathcal{O}_K$ for $x \in K$ chosen randomly; such that $N_{K/\mathbb{Q}}(x-y) < 1$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be the Lenstra's sequence of $\mathcal{O}_K$ with

$$m > \delta^*(U)\sqrt{d}$$

But, by definition of center packing constant,

$$m > \delta^*(U)\sqrt{d} \Leftrightarrow m\mu(U)/\sqrt{d} > \delta(U)$$

According to the system of translates of U given by $\mathbf{U} = \{U + \omega_i x + \alpha\}$ where $i : 1, 2, \ldots, m$ and $\alpha \in \mathcal{O}_K$. By Proposition B.27,

$$\rho_+(\mathbf{U}) = m\mu(U)/\sqrt{d} \quad \text{and thus } \rho_+(\mathbf{U}) > \delta(U)$$

This and the definition of δ imply $\mathbf{U}$ is not a packing of U. There then exist at least a pair of distinct (i, α) and j, β with $1 \leq i \leq m, 1 \leq j \leq m$ and α, $\beta \in \mathcal{O}_K$ such that

$$(U + \omega_i x + \alpha) \cap (U + \omega_j x + \beta) \neq \varnothing$$

$$\text{i.e. } \exists u, v \in U \text{ such that } u + \omega_i x + \alpha = v + \omega_j x + \beta$$

. If ω_i and ω_j are not distinct, then

$$\alpha - \beta = v - u$$

Since

$$u, v \in U \Rightarrow N_{K/\mathbb{Q}}(u - v) < 1 \text{ and } \alpha \in \mathcal{O}_K \Rightarrow N_{K/\mathbb{Q}}(\alpha - \beta) \in \mathbb{Z}$$

implying a contradicting result, $\alpha = \beta$, to the distinct hypothesis. Hence ω_i and ω_j are distinct elements in the sequence (their difference is a unit in $\mathcal{O}_K$). Finally, if we set $y = (\beta - \alpha)/(\omega_i - \omega_j)$, then

$$N_{K/\mathbb{Q}}(x - y) = N_{K/\mathbb{Q}}\Big(\frac{U - v}{\omega_i - \omega_j}\Big) = N_{K/\mathbb{Q}}(u - v) < 1$$

□

Corollary 4.25. *Let K be an algebraic number field of discriminant d and degree $n = r_1 + r_2$, where r_1 and r_2 respectively are the number of real and pairs of complex embeddings of K. It is Euclidean if and only if*

$$\lambda(K) > (n!/n^n)(4/\pi)^{r_1}\sqrt{d}$$

As can be noted clearly, this corollary makes Theorem 4.22 stronger.

Let K be a number field; in order to prove that $|N_{K/\mathbb{Q}}|$ is a Euclidean function on $\mathcal{O}_K$ it is sufficient to find a function $F : K \to \mathbb{R}$ such that

a) $|N_{K/\mathbb{Q}}(\alpha)| \leq F(\alpha)$ for all $\alpha \in K$;

b) for all $\xi \in K$, there is a $\gamma \in \mathcal{O}_K$ such that $F(\xi - \gamma) < 1$.

Gauss introduced a measure $\mathfrak{g}_K$ on K which is defined as,

$$\mathfrak{g}_K(\alpha) = \sum_{\sigma \in \mathrm{Gal(K/\mathbb{Q})}} |\sigma(\alpha)|^2$$

Lenstra has used it to find Euclidean cyclotomic fields as treated in the next chapter. This function can be modified slightly in the following manner where n is the degree of the extension.

$$\mu_K(\alpha) = \frac{1}{n} \sum_{\sigma \in \mathrm{Gal(K/\mathbb{Q})}} |\sigma(\alpha)|^2$$

where the sum is over all n embeddings $\sigma : K \to \mathbb{R}$.

If $K \subseteq L$ are number fields, and $n = [K : \mathbb{Q}]$, then μ has the following properties:

a. $|N_{K/\mathbb{Q}}(\alpha)| \leq \mu(\alpha)^{n/2}$;

b. $\mu_L(\alpha) - \mu_L(\alpha - \beta) = \mu_K\big(\frac{1}{(L:K)}\mathrm{Tr_{L/K}}(\alpha)\big) - \mu_{\mathrm{K}}\big(\frac{1}{(\mathrm{L:K})}\mathrm{Tr_{L/K}}(\alpha) - \beta\big)$ for all $\alpha \in L, \beta \in K$.

c. If $L = K(\zeta_m)$, then $(L : K)\mu_L(\alpha) = \frac{1}{m}\sum_{j=1}^{m} \mu_K\big(\mathrm{Tr_{L/K}}(\alpha\zeta_{\mathrm{m}}^{\mathrm{j}})\big)$.

Chapter 5

Euclideanity In Cyclotomic Fields

5.1 Introduction

In this chapter, although special attention is given to the usual cyclotomic fields, some other CM-Fields are also discussed briefly at last from the work of J-P. Cerri.

Let $\mathbb{Q}(\zeta_n)$ be used to denote a cyclotomic field corresponding to the n^{th} primitive root of unity. It has the following basic properties,

- The Galois group of the cyclotomic extension $K = \mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, denoted Gal(K/$\mathbb{Q}$) is isomorphic to the unit group of $\mathbb{Z}/n\mathbb{Z}$.
  More precisely,
  $$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$
  $$a \mod n \longleftrightarrow \zeta_n \mapsto \zeta_n^a$$

- $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ for $n \equiv 2 \mod 4$. Indeed, we have,
  $$\zeta_{2n}^2 = (e^{\frac{2\pi i}{2n}})^2 = \zeta_n \Rightarrow \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{2n})$$
  ; and conversely,
  $$\zeta_{2n} = 1 \cdot e^{\frac{2\pi i}{2n}} = -e^{\frac{2n\pi i}{2n}} e^{\frac{2\pi i}{2n}} = -e^{\frac{(n+1)2\pi i}{2n}} = -\zeta_n^{\frac{n+1}{2}} \in \mathbb{Q}(\zeta_n)$$

- The degree of the cyclotomic extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is the Euler ϕ value of n that counts integers co-prime with n in $\mathbb{Z}/n\mathbb{Z}$ i.e.
  $$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$

- For relatively prime integers m and n,

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q} \text{ and } \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$$

- The only ramified primes in $\mathbb{Q}(\zeta_n)$ are the primes that divide n. i.e.

$$p \text{ is ramified in } \mathbb{Q}(\zeta_n) \iff p \mid n$$

- If d is a positive divisor of n, then the degree of the extension of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\zeta_d)$ is equal to the ratio of the Euler phi value of n to that of d. That is to mean,

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_d)] = \frac{\phi(n)}{\phi(d)}$$

- The ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}(\zeta_n)$.

By the second property, it should be noted that there is no need to consider the n^{th} cyclotomic field in the case that $n \equiv 2 \mod 4$ or $n = 4k+2$ for some k, because it is exactly the same as the corresponding odd number indexed cyclotomic field, $\mathbb{Q}(\zeta_{2k+1})$ for some positive integer k.

Theorem 5.1. *(Masley and Montgomery) [37] The ring of integers $\mathbb{Z}[\zeta_n]$ is a principal ideal domain if and only if n is one of the following 30 possible integrs:*

1	3	4	5	7	8	9	11	12	13
15	16	17	19	20	21	24	25	27	28
32	33	35	36	40	44	45	48	60	84

In other words, there are precisely 30 cyclotomic number fields of class number 1. Moreover, among these, the first 12 of them along with $n = 20$ and $n = 24$ are known to be norm Euclidean. Lenstra has shown that $\mathbb{Q}(\zeta_{32})$ is not norm Euclidean.

Theorem 5.2. *A cyclotomic field is Euclidean if and only if it is principal ideal domain*

Proof. By Theorem 2.16 of Weinberger and Theorem 5.1 above. □

In the previous chapter, we have introduced Lenstra's general condition for a number field to decide if its ring of integers is Euclidean. In particular, the idea can be nicely adapted to cyclotomic fields. Therefore, we will make use of the very important corollary once again to prove some of them for being Euclidean.

p	n	r_2	$n!/n^n$	$\lvert d\rvert$	M
2	1	0	1	1	1
3	2	1	1	3	1.103
5	4	2	6	125	1.7
7	6	3	3/2	7^5	4.13
11	10	5	$9!/10^9$	11^9	58.96

Table 5.1: The bound M for the first five primes

Let us recall the bounding corollary 4.25 as,

$$\lambda(K) > (n!/n^n) \cdot (4/\pi)^{r_2} \cdot \sqrt{|d|} := M$$

where the degree of $\mathbb{Q}(\alpha)$ is $n = r_1 + 2r_2$ and d is its discriminant.

Here for the p^{th} cyclotomic field, p prime, we can construct an exceptional sequence as follows,

$$0, 1, (\zeta_p^2 - 1)/(\zeta_p - 1), (\zeta_p^3 - 1)/(\zeta_p - 1), \ldots, (\zeta_p^{p-1} - 1)/(\zeta_p - 1)$$

That is to mean for each positive integer $i \in [1, p]$,

$$\omega_i = (\zeta_p^i - 1)/(\zeta_p - 1) = \zeta_p^{i-1} + \zeta_p^{i-2} + \cdots + 1$$

This shows that the maximum length M is never less than p. Now, let us summarize, by the table below, the bounds for the first five cyclotomic fields, i.e for $p = 2, 3, 5, 7$ and 11. To do this we need to evaluate the discriminant of each cyclotomic fields given above.
The discriminant of the m^{th} cyclotomic field, $\mathbb{Q}(\zeta_m)$, is given by the formula:

$$d = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}$$

For our specific case however m is a prime p. Hence we have

$$|d| = p^{p-2}$$

Clearly, by the aid of Theorem 4.22 given in the last part of the previous chapter, the first four cyclotomic fields are Euclidean but it doesn't help us to make any conclusions for the 11^{th} cyclotomic field. In fact, we can not have a better bound on M when $p \geq 11$. The following proposition guarantees the why not.

Proposition 5.3. *Let K be an algebraic number field of degree n. If*

$$L := \min\{|\mathcal{O}_K/\mathfrak{p}| : \mathfrak{p} \subset \mathcal{O}_K \text{ is a proper ideal }\}$$

then

$$2 \leq \lambda(K) \leq L \leq 2^n$$

Proof. The first inequality is true because $\{0, 1\}$ is always an exceptional sequence for any such given ring. So is the last inequality. Indeed, if we consider the principal ideal $2\mathcal{O}_K$, we get $L \leq 2^n$, So L is always finite. Then for the middle inequality, $\lambda(K) \leq L$, suppose $\omega_1, \ldots, \omega_k$ are the elements of any exceptional sequence of $\mathcal{O}_K$. Let I be any proper ideal of $\mathcal{O}_K$. Since $\omega_i - \omega_j \ \forall 1 \leq i < j \leq k$ are all units, they can not be contained in the ideal I. The elements $\omega_1, \ldots, \omega_k$ are all pairwise incongruent modulo I. This implies that k can never be greater than the cardinality of $\mathcal{O}_K/I$. Therefore, $\lambda(K) \leq L$. □

In the above method, we are able to say that the first four cyclotomic fields are definitely Euclidean. But again, Lenstra extends the method to prove a lot more cyclotomic Euclidean fields. In this section, there are some repetitions that has already been discussed in the last section of the preceding chapter including definitions. This has been done to get rid of ambiguity of this specific case from the general setting.

For this other method, another size function is going to be used in the next section instead of the norm function used so far. This new size function is in fact the Gauss measure which has been introduced lastly in the previous chapter.

5.2 Definitions, Remarks And First Results

As usual, the notation K is used as an algebraic number field; $\mathcal{O}_K$ is its ring of integers; $n = r_1 + 2r_2$ as the degree of K over $\mathbb{Q}$ and $K_{\mathbb{R}}$ as given below

$$K_{\mathbb{R}} = K \otimes \mathbb{R} \simeq_{\mathbb{R}} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad \text{where } n = r_1 + 2r_2$$

- The general measure on $K_{\mathbb{R}}$ is defined as,

$$\mu : K_{\mathbb{R}} \to \mathbb{R} \text{ such that } x \mapsto \mu(x) = \sum_{\sigma \in Hom(K,\mathbb{C})} |\sigma(x)|^2$$

- The fundamental domain is given by,

$$F = \{x \in K_{\mathbb{R}} : \mu(x) \leq \mu(x - y) \quad \forall y \in \mathcal{O}_K\}$$

  Here F is a compact subset of $K_{\mathbb{R}}$ that satisfies $K_{\mathbb{R}} = F + \mathcal{O}_K$

- Let c be the maximum value of μ in F. Then a number c' is termed as a bound for F if $c' \geq c$. Furthermore, a bound c' is said to be usable if for every $x \in F \cap K$ such that $\mu(x) = c'$, there exists a root of unity $\zeta \in \mathcal{O}_K$ satisfying $\mu(x - \zeta) = c'$. With this definition, a bound that strictly exceeds the value of c is usable as c' is the maximum possible value for F.

- Arithmetic-Geometric mean inequality (i.e. G.M $\leq$ A.M) gives rise to $N(x)^2 \leq (\mu(x)/d)^d$ for $x \in K_{\mathbb{R}}$ where N is the norm function.

- When a specific cyclotomic field is considered, for instance $\mathbb{Q}(\zeta_m)$, the notations μ, F and c used in the above definitions are replaced by μ_m, F_m and c_m respectively for the sake of simplicity and avoidance of confusion.

- For a ring $\mathcal{O}_K$ to be Euclidean, since any unique factorization domain is integrally closed in its fraction field K, it is assumed in this section that no cube root of unity is contained in $K - \mathcal{O}_K$.

Lemma 5.4. *If an element x of K satisfies $|\sigma(x)|^2 = 1$ and $|\sigma(x - \zeta)|^2 = 1$, for some $\sigma \in Hom(K, \mathbb{C})$, $\zeta \in \mathcal{O}_K$ a root of unity, then x belongs to $\mathcal{O}_K$*

Proof. If we let $y := \sigma(-xu^{-1}) \in \mathbb{C}$, then $y\bar{y} = 1$ and $y + \bar{y} = -1$ by the above inequalities and homomorphic property of the function σ. Thus y is a cube root of unity. Furthermore, as σ is injective, the pre-image of y must also be a cube root of unity in K. But by the last remark noted above, $-xu^{-1}$ should also belong to $\mathcal{O}_K$. Finally, since u is assumed to be in $\mathcal{O}_K$, $x = (-u^{-1})(-u) \in \mathcal{O}_K$ follows. □

Proposition 5.5. *If the degree n of K is a usable bound for F, then $\mathcal{O}_K$ is norm Euclidean.*

Proof. It is remarked in advance that $F + \mathcal{O}_K = K_{\mathbb{R}}$. Hence in order to show that $\mathcal{O}_K$ is Euclidean, it suffices to show that for every element x in F, there exists an element $r \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(x - r) < 1$. $x \in F$ implies $\mu(x) \leq n$ for n is just a bound.
case 1 : $\mu(x) < n$
This implies $N_{K/\mathbb{Q}}(x) < 1$ since $\mu(x)/n < 1$ and arithmetic-geometric mean inequality remark. Thus $N_{K/\mathbb{Q}}(x - 0) < 1$.
case 2 : $\mu(x) = n$
By definition of usable bound, there exist a root of unity $\zeta \in \mathcal{O}_K$ such that $\mu(x) = \mu(x - \zeta)$. Again from $\mu(x)/n = 1$ and the arithmetic-geometric inequality remark, we have

$$N_{K/\mathbb{Q}}(x) \leq \sqrt{(\mu(x)/n)^n} = 1 \text{ and } N_{K/\mathbb{Q}}(x - \zeta) \leq \sqrt{(\mu(x - \zeta)/n)^n} = 1$$

case 2.1 : at least one of them is strict inequality
If the first inequality is strict, $N_{K/\mathbb{Q}}(x - 0) \leq 1$ is obtained, where as for the possibility of strict inequality of the second one, $N_{K/\mathbb{Q}}(x - \zeta) \leq 1$ can be considered as ζ belongs to $\mathcal{O}_K$.
case 2.2 : $N_{K/\mathbb{Q}}(x)^2 = (\mu(x)/n)^n = 1$ and $N_{K/\mathbb{Q}}(x - \zeta)^2 = (\mu(x - \zeta)/n)^n = 1$
In this case, the values of $|\sigma(x)|^2$ are all the same for each n number of homomorphisms, σ's. In the same way, $|\sigma(x - \zeta)|^2 = |\sigma'(x - \zeta)|^2$ for all $\sigma, \sigma' : K \to \mathbb{C}$, $\mathbb{R}$-algebra homomorphisms. Now, since $N_{K/\mathbb{Q}}(x)^2 = 1$ (i.e our case) and
$N_{K/\mathbb{Q}}(x) = \prod_{\sigma} |\sigma(x)|^2$, we have $|\sigma(x)|^{2n} = 1$. This in turn implies $|\sigma(x)|^2 = 1$.
Similarly, $|\sigma(x - \zeta)|^2 = 1$. From the above lemma, it then follows that $x \in R$ contradiction against $x \in F - \{0\}$. □

This is the main result of Lenstra's paper of Euclid's algorithm in cyclotomic fields. To determine those cyclotomic fields whose ring of integers are Euclidean by making use of this criterion, it is essential to study this usable bounds more closely.

5.3 Bounds From Other Bounds

In the appendix part, the definition of trace is recalled. For a little further extension of the same function to $K_{\mathbb{R}}$, let us make clear the notations clear before they are going to be used in the following propositions.

$\mathrm{Tr_m}$ is to denote the extension of the usual trace function to $K_{\mathbb{R}}$ where the subject field is $\mathbb{Q}(\zeta_m)$. Thus, $\mathrm{Tr} : \mathbb{Q}(\zeta_\mathrm{m}) \to \mathbb{Q}(\zeta_\mathrm{m})$ can be extended to $\mathrm{Tr_m} : \mathrm{K}_{\mathbb{R}} \to \mathrm{K}_{\mathbb{R}}$.
The trace Tr and the general measure μ can be related as follows,

$$\mathrm{Tr}(\mathrm{x}\bar{\mathrm{x}}) = \sum_{\sigma} \sigma(\mathrm{x}\bar{\mathrm{x}}) = \sum_{\sigma} \sigma(\mathrm{x})\sigma(\bar{\mathrm{x}}) = \sum_{\sigma} \sigma(\mathrm{x})^2 = \mu(\mathrm{x})$$

In addition to the extended trace considered above, a relative trace can be defined. For b and m positive integers such that $b \mid m$, considering $\mathbb{Q}(\zeta_m)$ as extension of $\mathbb{Q}(\zeta_b)$, we have the trace function. From now on, let us reserve the notation Tr for the extended trace function of $K := \mathbb{Q}(\zeta_m) \to K' := \mathbb{Q}(\zeta_b)$ to $K_{\mathbb{R}} \to K'_{\mathbb{R}}$. More precisely,
if $x \in K_{\mathbb{R}}$ and $G = \mathrm{Gal(K/K')}$, then $\mathrm{Tr} : \mathrm{K}_{\mathbb{R}} \to \mathrm{K}_{\mathbb{R}'}$ sends x to $\sum_{\sigma \in G} \sigma(x)$

Remark 5.6. The extended trace function Tr defined above commutes with complex conjugation. Moreover, for positive integers b and m where b divides m, $\mathrm{Tr_m} = \mathrm{Tr_b} \circ \mathrm{Tr}$

In the following two lemmas and the base proposition, b and m are positive integers where b divides m; K and K' denote $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_b)$; $e = [K : K'] = \phi(m)/\phi(b)$.

Lemma 5.7. *Let x and y be elements taken from $K_{\mathbb{R}}$ and $K'_{\mathbb{R}}$ respectively. If we set $s := e(\mu_b(\mathrm{Tr(x)/e}) - \mu_\mathrm{b}(\mathrm{Tr(x)/e - y}))$, then $s = \mu(x) - \mu(x - y)$*

Proof. We have noted in advance that $\mu_j(x) = \mathrm{Tr_j}(\mathrm{x}\bar{\mathrm{x}})$ for any positive integer j. Then,

$$\begin{aligned} s :&= e(\mu_b(\mathrm{Tr(x)/e}) - \mu_\mathrm{b}(\mathrm{Tr(x)/e - y})) \\ &= e\mathrm{Tr_b}(\mathrm{Tr(x)}\bar{\mathrm{y}}/\mathrm{e} + \mathrm{Tr}(\bar{\mathrm{x}})\mathrm{y}/\mathrm{e} - \mathrm{y}\bar{\mathrm{y}}) \\ &= \mathrm{Tr_b}(\mathrm{Tr(x)}\bar{\mathrm{y}} + \mathrm{Tr}(\bar{\mathrm{x}})\mathrm{y} - \mathrm{ey}\bar{\mathrm{y}}) \\ &= \mathrm{Tr_b}(\mathrm{Tr}(\mathrm{x}\bar{\mathrm{y}}) + \mathrm{Tr}(\bar{\mathrm{x}}\mathrm{y}) - \mathrm{Tr}(\mathrm{y}\bar{\mathrm{y}})) \\ &= \mathrm{Tr_m}(\mathrm{x}\bar{\mathrm{y}} + \bar{\mathrm{x}}\mathrm{y} - \mathrm{y}\bar{\mathrm{y}}) \\ &= \mu_m(x) - \mu_m(x - y) \end{aligned}$$

□

Lemma 5.8. *Let K be $\mathbb{Q}(\zeta_m)$ as reminded. If x belongs to $K_{\mathbb{R}}$, then*

$$\mu_m(x) = 1/m \sum_{i=1}^{m} \mu_b \mathrm{Tr}(\mathrm{x}\zeta_\mathrm{m}^\mathrm{j})$$

Proof. Let G be the Galois group K over K'. Then,

$$\begin{aligned}
\sum_{i=1}^{m} \mu_b \mathrm{Tr}(\mathrm{x}\zeta_{\mathrm{m}}^{\mathrm{i}}) &= \sum_{i=1}^{m} \mu_b \left(\sum_{\sigma \in G} \sigma(x\zeta_m^i) \right) \\
&= \mathrm{Tr_b} \left(\sum_{\mathrm{i}=1}^{\mathrm{m}} \sum_{\sigma \in \mathrm{G}} \sum_{\sigma' \in \mathrm{G}} \sigma(\mathrm{x})\sigma(\zeta_{\mathrm{m}}^{\mathrm{i}})\sigma'(\bar{\mathrm{x}})\sigma'(\zeta_{\mathrm{m}} - \mathrm{i}) \right) \\
&= \mathrm{Tr_b} \left(\sum_{\sigma \in \mathrm{G}} \sum_{\sigma' \in \mathrm{G}} \sigma(\mathrm{x})\sigma'(\bar{\mathrm{x}}) \left(\sum_{\mathrm{i}=1}^{\mathrm{m}} (\sigma(\zeta_{\mathrm{m}})\sigma'(\zeta_{\mathrm{m}})^{-1})^{\mathrm{i}} \right) \right) \\
&= \mathrm{Tr_b} \sum_{\sigma \in \mathrm{G}} \sigma(\mathrm{x})\sigma(\bar{\mathrm{x}})\mathrm{m} \qquad (*) \\
&= m\mathrm{Tr_b}(\mathrm{Tr}(\mathrm{x}\bar{\mathrm{x}})) = \mathrm{mTr_m}(\mathrm{x}\bar{\mathrm{x}}) = \mathrm{m}\mu_{\mathrm{m}}(\mathrm{x})
\end{aligned}$$

Here equation (*) follows for the following reason. In the inner most sum of the preceding equation, $\zeta := \sigma(\zeta_m)\sigma'(\zeta_m)^{-1})$ is the m^{th} root of unity. On one hand, if $\sigma = \sigma'$, $\sigma(\zeta_m\zeta_m^{-1}) = 1$, hence $\sum_{i=1}^{m} 1 = m$. On the other hand, if they are different, $\sum_{i=1}^{m} \zeta_m^i = 0$, thus, only the same sigma is remained (non vanishing case). □

Proposition 5.9. *$c_m \leq e^2 c_b$. Moreover, If c' is a usable bound for F_b, then e^2c' is a usable bound for F_m.*

Proof. Let $x \in F_m$. Taking $y \in \mathbb{Z}[\zeta_b]$, the first lemma implies $\mathrm{Tr(x)/e} \in \mathrm{F_b}$. Similarly, since $x \in F_m \Rightarrow x\zeta_m^i \in F_m$ where $i = 0, 1, 2, \ldots, \zeta_m^{m-1}$, taking $y \in \mathbb{Z}[\zeta_b]$ and applying the lemma, we have $\mathrm{Tr}(\mathrm{x}\zeta_{\mathrm{m}}^{\mathrm{i}}) \in \mathrm{F_b}$ for the first m non negative integers. Thus, for every integer $i \in \mathbb{Z}$,
$\mu_b(\mathrm{Tr}(\mathrm{x}\zeta_{\mathrm{m}}^{\mathrm{i}})) = \mathrm{e}^2\mu_{\mathrm{b}}(\mathrm{Tr}(\mathrm{x}\zeta_{\mathrm{m}}^{\mathrm{i}})/\mathrm{e}) \leq \mathrm{e}^2\mathrm{c_b}$. Then from the second lemma, it follows that $\mu_m(x) \leq e^2c_b$. Hence, e^2c_b is a bound for F_m as desired.
For the "moreover" part, by definition of usability of the bound c' of F_b , there exists a root of unity $\zeta \in \mathbb{Z}[\zeta_b]$ such that $\mu_b(\mathrm{Tr(x)/e} - \zeta) = \mathrm{c}'$. Then taking $y = \zeta$ and applying the first lemma, we obtain $\mu_m(x-\zeta) = \mu_m(x) = e^2c'$. □

Remark 5.10. If the positive integers m and b are divisible by the same prime numbers, then $c_m = e^2c_b$

This first result of Lenstra at once identifies all the previously determined Euclidean cyclotomic fields by various mathematicians at different time. This is just by considering $\mathbb{Q}$ as the first and simplest cyclotomic field, whose root

of unity is literally $\zeta_1 = 1$. We know that $c_1 = max\{|x|^2 : x \in F_1\}$. Here $\mu_1(x) = |x|^2$ as we have only the identity homomorphism. But again, since $x \in F_1$, it should satisfy $|x|^2 \leq |x - y|^2$ for all $y \in \mathbb{Z}$. This notion is the same as the Euclidean minimum of $\mathbb{Z}[i]$, i.e. $1/4$, we illustrated as an example by the corresponding lattice diagram in the second Chapter, but even weaker. Hence, $|x|^2 \leq |x - y|^2 \leq 1/4$. Now for m^{th} cyclotomic field, $e = \phi(m)/\phi(1) = \phi(m)$. Combining these two and the above proposition, $\phi(m)/4$ is a usable bound for F_m. Then Proposition 5.5 recovers the five Euclidean cyclotomic fields, i.e. the case where m is $1, 3, 4, 5, 8$ and 12.

In the following, the more important method of Lenstra's will be revised. This method is to find a usable bound for F_p when p is prime. As any positive integer m is a product of prime factors, we are able to use this forthcoming result with the above proposition to estimate the usable bound for F_m. Let us briefly introduce the concept of positive definite quadratic forms.

Let $k \geq 2$ be an integer and let V be an (n-1) dimensional $\mathbb{R}$ vector space with a basis $\{e_i\}_{i=1}^{k-1}$. Let also that $e_k = -\sum_{i=1}^{n-1} e_i$. We can also view $\{e_i : i = 1, 2, \ldots, k\}$ as linearly dependent generating set.

5.4 Usable Bounds From Quadratic Forms

Definition 5.11. Given $x \in V$. The positive definite quadratic form q on V at x is defined as,

$$q(x) = q\left(\sum_{i=1}^{k} x_i e_i\right) = \sum_{1 \leq i \leq k} (x_i - x_j)^2$$

The symmetric bilinear form induced by q, denoted (,) is given as,

$$V \times V \to \mathbb{R} \qquad (x, y) \mapsto \frac{1}{2}(q(x+y) - q(x) - q(y)) \quad [= \frac{1}{4}q(x+y) - q(x-y)]$$

Basic Properties

- For a scalar c, $q(cx) = q\left(\sum_{i=1}^{k} cx_i e_i\right) = \sum_{1 \leq i < \leq j \leq k} (cx_i - cx_j)^2 = c^2 q(x)$,
  hence the name quadratic.

- $(x,x) = \frac{1}{4}(q(x+x) - q(x-x)) = q(x)$.
- Since $e_i = e_i + \sum_{j \neq i} 0e_j$ or $e_i = 0e_i + \sum_{j \neq i} -e_j$ for each i, we have that $(e_i, e_i) = q(e_i) = k - 1$
- For $i \neq j$, taking $e_i + e_j = e_i + e_j + \sum_{l \neq i,j} 0e_l$, it then follows that $q(e_i + e_j) = (k-2)(1+1) = 2k - 4$, hence $(e_i, e_j) = -1$.

Let L be the subgroup of V generated by $\{e_i : i = 1, 2, \ldots, k\}$. L is a lattice in V whose rank is $n-1$ whose fundamental domain E, which is a compact subset of V, is given by,

$$\begin{aligned} E &= \{x \in V : q(x) \leq q(x-y) \qquad \forall y \in L\} \\ &= \{x \in V : (x,y) \leq \frac{1}{2}q(y) \qquad \forall y \in L\} \end{aligned}$$

Proposition 5.12. *Let $t := \max\{q(x) : x \in E\}$. The set of points $x \in E$ for which $q(x)$ is the maximum, t, is*

$$\left\{ \frac{1}{k} \sum_{i=1}^{k} i e_{\sigma(i)} \text{ where } e_{\sigma(i)} \text{ is a permutation of the } k \text{ generators} \right\}$$

Moreover, $t = (k^2 - 1)/12$.

The proof of this proposition is apparently long with a series of lemmas but merely linear algebraic computation. The interested reader can refer to the original and detailed proof of Lenstra.

Proposition 5.13. *If k is a prime number, $c_k = (k^2 - 1)/12$ is a usable bound for F_k*

Proof. Let $K = \mathbb{Q}(\zeta_k)$. Since the primality of k implies $\sum_{i=1}^{k} \zeta_k^i = 0$, the $\mathbb{R}$- algebra $K_{\mathbb{R}}$ is generated by $\{\zeta_k^i : i = 1, 2, \ldots, k\}$. Now, if k elements, $x_1, x_2, \ldots, x_k$, are given from $\mathbb{R}$,

$$\begin{aligned} \mu_k \left(\sum_{i=1}^{k} x_i \zeta_k^i \right) &= \mathrm{Tr_k} \left(\sum_{\mathrm{i=1}}^{\mathrm{k}} \sum_{\mathrm{j=1}}^{\mathrm{k}} \mathrm{x_i x_j \zeta_k^{i-j}} \right) \qquad (\text{since } \mu_k(y) = \mathrm{Tr_k(y\bar{y})}) \\ &= k \sum_{i=1}^{k} x_i^2 - \sum_{i=1}^{k} \sum_{j=1}^{k} x_i x_j \\ &= \sum_{1 \leq i < j \leq k} (x_i - x_j)^2 \end{aligned}$$

Consequently, the two quadratic spaces $K_{\mathbb{R}}, \mu_k$ and V, q are isomorphic by the map $\zeta_n^i \mapsto e_i$ for each i from 1 through k. Thus $\mathbb{Z}[\zeta_k]$ and F_k correspond to L and E respectively. Moreover, $c_k = t = (k^2 - 1)/12$ and the set of elements, x, in F_k for which $\mu_k(x) = c_k$ is given by,

$$X := \{1/k \sum_{i=1}^{k} i\zeta_k^{\sigma(i)} : \sigma \text{ is a permutation of 1, 2,..., k}\}$$

Let any $x \in X$ be taken with the corresponding permutation. Without the loss of generality, $\sigma(0) = \sigma(k)$ can be set. Then,

$$x - \zeta_k^{\sigma(k)} = \frac{1}{k} \sum_{i=1}^{k-1} i\zeta_k^{\sigma(i)} = \frac{1}{k} \sum_{j=1}^{k} j\zeta_k^{\sigma(j-1)} \in X$$

Therefore, as $\mu_k(x - \zeta_k^{\sigma(k)}) = c_k$, c_k is concluded to be usable. □

5.5 Theorem(Lenstra)

Theorem 5.14. *If $m \neq 16, 24$ is a positive integer where $\phi(m) \leq 10$, then $\mathbb{Z}[\zeta_m]$ is norm Euclidean.*

Proof. As remarked so far, for $m = 1, 3, 4, 5, 8$ and 12, we have

$$\begin{aligned} c_1 = 1/4 < 1 = \phi(1) \\ c_3 = 2/3 < 2 = \phi(3) \\ c_4 \leq 2^2/4 = 1 < 2 = \phi(4) \\ c_5 = 2 < 4 = \phi(5) \\ c_8 \leq 4^2/4 = 4 = \phi(8) \\ c_{12} \leq 4^2/4 = 4 = \phi(12) \end{aligned}$$

Now by using Proposition 5.9 and proposition 5.13 for $m = 7, 9, 11, 15$ and 20, we have,

$$\begin{aligned} c_7 = 4 < 6 = \phi(7) \\ c_9 \leq 3^2 c_3 = 6 = \phi(9) \\ c_{11} = 10 = \phi(11) \\ c_{15} \leq 2^2 c_5 = 8 = \phi(15) \\ c_{20} \leq 2^2 c_5 = 8 = \phi(20) \end{aligned}$$

Since the bound $\phi(m)$ is usable for F_m for all m considered above, $\mathbb{Z}[\zeta_m]$ is norm Euclidean by Proposition 5.5 □

Although the above result of Lenstra has identified many norm Euclidean cyclotomic fields, there have also been discovered other cyclotomic fields of the same type by another methods.

Other CM-Fields J-P Cerri [4], the supervisor of this paper, has developed a computer-aided algorithm to show that $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$ is indeed Euclidean with respect to the norm. It has been done by showing that the Euclidean minimum of its maximal real subfield, $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{2}}}\right)$, is indeed $1/2$. He has also found that, if $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\sqrt{3}}}\right)$, we have $M(K) = M(\bar{K}) = 1/2$. By the same method, it has been shown that the Euclidean minimum of $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$ is also $1/2$ hence it is Euclidean as conjectured by H. Cohn and J. Deutsch.

Some other norm Euclidean cyclotomic fields were also discovered by R. Quême and Niklasch [40] by improving Lenstra's first method.

Chapter 6

Minkowski's Conjecture

6.1 Why Minkowski Here?

General Case
Let Λ be a lattice in $\mathbb{R}^n$; $\{\alpha_i\}$ and $\{e_i\}$ where $i = 1, 2, \ldots, n$ be any $\mathbb{Z}$-basis and the canonical basis respectively. Then

$$x \in \mathbb{R}^n \Rightarrow x = \sum_{i=1}^{n} x_i \alpha_i \quad \text{where } x_i \in \mathbb{R}$$

$$X \in \mathbb{Z}^n \Rightarrow X = \sum_{i=1}^{n} X_i \alpha_i \quad \text{where } X_i \in \mathbb{Z}$$

The corresponding fundamental parallelotope, F, to the given basis α_i's is then given as,

$$F = \{\sum_{i=1}^{n} a_i \alpha_i \text{ where } a_i \in \mathbb{R} \text{ and } 0 \leq a_i < 1, \text{ for each } i\}$$

All the elements of the basis $\{\alpha_i\}_{i=1}^{n}$ can be written in terms of the canonical basis as,

$$\alpha_i = \sum_{j=1}^{n} m_{i,j} e_j \quad \text{where } m_{i,j} \in \mathbb{R}$$

The matrix M obtained by considering the coefficients, $M = (m_{i,j})$, is invertible; otherwise, the n elements α_i's can not be linearly independent. On one hand, the absolute value of the determinant of this matrix clearly gives the volume of the fundamental parallelotope, Vol(F). This volume is independent on the choice of basis.

$$\text{Vol(F)} = |\det \text{M}| = \det \Lambda$$

On the other hand, let $x \in \mathbb{R}^n$ and $X \in \Lambda$ given, and define f as,

$$f(x - X) = |\prod_{i=1}^{n}(x_i - X_i)|$$

For a fixed element x from $\mathbb{R}^n$, let us denote by g the minimum value of $f(x - X)$ for some $X \in \Lambda$. i.e.

$$g(x) = \inf_{X \in \Lambda} f(x - X)$$

If $M(\Lambda)$ is used to denote the maximum value g can have for $x \in \mathbb{R}^n$, i.e.

$$M(\Lambda) = \sup\{g(x) : x \in \mathbb{R}^n\}$$

This maximum value has the important property that if D is a diagonal invertible matrix of dimension $n \times n$, then

$$M(D\Lambda) = M(\Lambda)|\prod_{i=1}^{n} d_{i,i}|$$

Totally Real Number Fields

Let K be a totally real number field of degree n, $\bar{K} = K \otimes_{\mathbb{Q}} \mathbb{R}$ and $\mathcal{O}_K$ its ring of integers. Let us recall all the notations and definitions used in the third chapter. $m_K, m_{\bar{K}}, M(K), M(\bar{K})$, the homogeneous and Euclidean minima. σ_i where $i = 1, 2, \ldots, n$ are all the real embeddings in our case.

By the map $K \to \mathbb{R}^n$ defined by $\xi \mapsto (\sigma_1(\xi), \sigma_2(\xi), \ldots, \sigma_n(\xi))$, there is n-tuple representing each element. Now, if $\xi \in K$ and $X \in \mathcal{O}_K = \Lambda$, we have,

$$f(\xi - X) = |N_{K/\mathbb{Q}}(\xi - X)|$$

and hence

$$g(\xi) = \inf_{X \in \Lambda} f(x - X) = m_K(\xi)$$

If $x \in \mathbb{R}^n$, $g(x) = m_{\bar{K}}(x)$; hence, $M(\bar{K}) = M(\Lambda)$

To put it in simple terms, it is clear that a given algebraic number field is Euclidean if and only if $\forall x \in K \quad \exists X \in \mathcal{O}_K$ such that $N(x - X) < 1$. To thus make use of this criterion of checking a number field for Euclideanity, it is vital to study $M(K) = \sup_{x \in K} \inf_{X \in \mathcal{O}_K} N(x - X)$. As $\mathcal{O}_K$ forms a lattice of the same dimension in the number field K of degree n. The conjecture of Minkowski , that is stated in the next section, can be directly adapted to number fields in computing the Euclidean minima.

6.2 Minkowski's Conjecture

Keeping the notations used in the preceding section in mind, Minkowski's conjecture can be stated in a short inequality as,

$$\boxed{M(\Lambda) \leq \frac{\mathrm{Vol}(\Lambda)}{2^n}}$$

In the conjecture, as reminded above, n is the dimension of the space in which the lattice Λ is considered. $M(\Lambda)$ is to denote the upper bound, i.e

$$M(\Lambda) = \sup_{x \in \mathbb{R}^n} \inf_{X \in \Lambda} f(x - X)$$

From the number field view point, the above conjecture gives rise to the following parallel statement as its consequence, where $N_{\mathbb{Q}/K}$ is used as usual to denote the usual norm function on K.

If K is a totally real number field over the rational numbers with degree n and discriminant d, then for every element $x \in K$, there exists $y \in \mathcal{O}_K$ such that

$$|N_{\mathbb{Q}/K}(x - y)| \leq \frac{\sqrt{d}}{2^n}$$

The conjecture has been proved for $n = 1, 2, 3, 4, 5, 6$. The paper of three mathematicians which is made available very recently claimed to have proven the conjecture for n=7. The idea is highlighted by stating their main theorem after some of the previous results on the area. For clearer reference, the names of mathematicians who are credited to the proof of the conjecture for different values of n in different time is shown in the following table.

n	Proved by	Year
1	Euclid	$\approx$ 280 BC
2	Minkowski	1901
3	Remak	1923
4	Dyson	1948
5	Skubenko	1976
	Bambah-Woods	1980
6	McMullen	2005
7	Hans-Gill, Raka, Sehmi	2009

Table 6.1: The conjecture has been proved up to $n = 7$

Definition 6.1. A matrix $D \in M_n(\mathbb{R})$ is said to be DOTU if it can be decomposed as A=DOTU where,

- D is diagonal and invertible matrix;
- O belongs to $O_n(\mathbb{R})$;
- T is upper triangular with diagonal entries equal 1; and,
- U belongs to $GL_n(\mathbb{Z})$.

Precisely, the set of such sort of matrices can be given as,

$$\mathbf{\Gamma} = \left\{ \begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} \text{ where } x_i > 0 \quad \forall i \text{ and } \prod a_i = 1 \right\} \subseteq SL_n(\mathbb{R})$$

This set Γ is a diagonal subgroup of $SL_n(\mathbb{R})$

Theorem 6.2. *(MacBeath) If a lattice $\Lambda \in \mathbb{R}^n$ admits a $\mathbb{Z}$ basis whose coordinates (in the canonical basis of $\mathbb{R}^n$) give a DOTU matrix, or in another words, if $\Lambda = D\mathbb{Z}^n$ with D a DOTU, then Minkowski's conjecture holds for the given lattice.*

Proof. As D and U can be removed from the matrix A, we can assume that $A = OT$ and $\Lambda = OT\mathbb{Z}^n$ with $\text{Vol}(\Lambda) = 1$. Precisely, the aim is to prove that

$$\forall x \in \mathbb{R}^n \quad \exists X \in \mathbb{Z}^n \text{ such that } \prod_{i=1}^{n} |x_i - (OTX)_i| \leq 2^{-n}$$

If $e_i \in \mathbb{R}^n$ is used to denote the i^{th} column of O, all the n e_i's form the orthonormal basis of $\mathbb{R}^n$. Hence, writing x as a linear combination of this basis is possible as, $x = a_1e_1 + \cdots + a_ne_n$ If we let $X \in \mathbb{Z}^n$, then

$$x - OTX = y_1e_1 + \cdots + y_ne_n$$

where

$$\begin{cases} y_n &= a_n - X_n \\ y_{n-1} &= a_{n-1} - X_{n-1} - t_{n-1,n}X_n \\ \vdots &= \vdots \\ y_1 &= a_1 - X_1 - t_{1,2}X_2 - \ \ldots \ - t_{1,n}X_n \end{cases}$$

Then, $X_n, X_{n-1}, \ldots,$ are chosen successively in such a way that for each i, $|y_i| \leq 1/2$ to result in the following:

$$||x - OTX||^2 = \sum_{i=1}^{n} y_i^2 \leq \frac{n}{4} \qquad i.e. \quad \sum_{i=1}^{n}(x_i - (OTX)_i)^2 \leq \frac{n}{4}$$

Finally, the arithmetic-geometric mean inequality implies

$$\prod_{i=1}^{n} |x_i - (OTX)_i| \leq 2^{-n}$$

□

A more general result that gives rise to the above case as its specific consequence can be stated as follows.
If Λ is a unimodular lattice in $\mathbb{R}^n$, then

$$\sup_{x \in \mathbb{R}^n} \inf_{y \in \Lambda} \{N(x - y)\} \leq 2^{-n}$$

Moreover, they will be equal if and only if $\Lambda = D\mathbb{Z}^n$ for some $D \in \Gamma$.

6.3 McMullen's Approach

Mc Mullen in his paper [38] proved a more general proposition that implies Minkowski's conjecture to hold true for $n = 6$. His proof is based on the topological dimension theory, as reflected in the combinatorics of open covers of $\mathbb{R}^n$ and the n-torus $\mathbb{T}^n$. Topology of torus, compressibility/incompressibility, Poincaré Lemma and the knowledge of lattices are to mention the main mathematical entities used to obtain the result. This proof makes the previous proofs clearer and gives a basic ground to aim at greater n values.

Let Λ be a lattice in $\mathbb{R}^n$ and [1]

$$|\Lambda| := \inf\{|y| : |y| \text{ is Euclidean length of y} \neq 0 \text{ in } \Lambda\}$$
$$|N(\Lambda)| := \inf\{N(y) : N(y) \text{ is Euclidean norm of y} \neq 0 \text{ in } \Lambda\}$$

Definition 6.3. If an element $y \in \Lambda$ is such that $|y| = |L|$, it is called minimal. Moreover, Λ is said to be a well rounded lattice if its minimal vectors generate $\mathbb{R}^n$.

Here also, as used in the previous chapter, the arithmetic-geometric inequality results in the following for any $x \in \mathbb{R}^n$.

$$N(x)^{\frac{1}{n}} \leq \frac{|x|}{\sqrt{n}}$$

He therefore stated the general propositions as follows and claims that proving them is sufficient for the proof of Minkowski's conjecture for a given value of n

Proposition 6.4. *Let Γ be the set of all DOTU matrices as denoted in the preceding section. Then for any lattice Λ in $\mathbb{R}^n$, there is an element $D \in \Gamma$ such that $D\Lambda$ is well rounded; and the covering radius of any well ordered unimodular lattice satisfies*

$$\sup_{x \in \mathbb{R}^n} \inf_{y \in \Lambda} |x - y| \leq \frac{\sqrt{n}}{2}$$

Moreover in the latter proposition, the two expressions are equal if and only if $\Lambda = B\mathbb{Z}$ for some $B \in SO_n(\mathbb{R})$.

It should be recalled from Birch and Swinnerton-Dyer's proof [3] of any counter example to Minkowski's conjecture with minimal dimension must satisfy $N(L) > 0$. i.e. $\Gamma\Lambda$ must have compact closure in the space of lattices $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$.

Theorem 6.5. *(McMullen) [38] Given Λ, a lattice in $\mathbb{R}^n$. If the orbit closure[2] of the lattice Λ is compact, then it meets the locus of well-ordered lattices.*

Corollary 6.6. *If the second part of the general proposition holds for every $k \leq n$, then Minkowski's Conjecture will also hold true for all lattices in $\mathbb{R}^k$, for every $k \leq n$.*

Corollary 6.7. *Minkowski's conjecture holds for $n = 6$.*

[1] $|y|$ and $|N(y)|$, the Euclidean length and norm of y, are respectively given by, $|y|^2 = |x_1|^2 + \cdots + |x_n|^2$ and $N(x) = |x_1 \cdot x_2 \ldots x_n|$

[2] The orbit closure of the lattice Λ is $\overline{\Gamma \cdot \Lambda} \subset SL_n(\mathbb{R})/SL_n(\mathbb{Z})$

6.4 The Recent Result For $n = 7$

Hans-Gill, Raka and Semhi's mutual work for the proof of Minkowski's conjecture with $n = 7$ has been made available this year from journals of Science Direct [23].
Their approach is proving for $n = 7$ a general conjecture of Woods that implies the proof of a well known conjecture stated below and thereby proving Minkowski's conjecture for the case.

- Conjecture 1: If Λ is a lattice in the Euclidean space $\mathbb{R}^n$, every closed sphere of radius $\sqrt{n}/2$ contains a point of the lattice.

This conjecture was proved by Woods [46], [47], [48] in his three papers at different time for $n = 4, 5, 6$. It was also shown to be true for $n = 3$ by Remak [41], Davenport [15] and Mahler [36]. This current proof for the case $n = 7$ then follows the Remak-Davenport approach of proving this conjecture and one other conjecture given below; and finally concluding the proof of Minkowski's for n=7. The second conjecture is,

- Conjecture 2: For any given lattice $\Lambda \in \mathbb{R}^n$, there is an ellipsoid of equation
$$\sum_{i=1}^{n} a_i x_i^2 < 1$$
which contains no point of the lattice other than the origin but its boundary contains n linearly independent points of the lattice.

Since the statement of Woods' conjecture they stated and used for their proof is related in the usage of notations and variables, it is a good idea to restate minkowski's conjecture in their own way as,

- Conjecture (Minkowski): Let $L_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n$ where $i = 1, 2, \ldots, n$ be n linear forms in n variables, $x_1, \ldots, x_n$. Suppose also that the determinant $\det A$ of the matrix formed from the coefficients $a_{i,j}$, i.e. $A = (a_{i,j})$ be non zero. Then for any given $r = (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, there exists an element $z = (z_1, z_2, \ldots, z_n) \in \mathbb{Z}^n$ such that
$$|(L_1 + r_1) \ldots (L_n + r_n)| \leq |\det A|/2^n$$
where the variables in L_i are substituted by $z = (z_1, z_2, \ldots, z_n)$

The more general conjecture than the first one was forwarded by Woods. Let Λ be a lattice in the Euclidean space $\mathbb{R}^n$. Quadratic forms reduction theory introduced by Korkine and Zolotareff [28], [29] guarantees the possibility of choosing a cartesian coordinate system in $\mathbb{R}^n$ in such a way that the lattice has a basis $\{b_i, i = 1, 2, \ldots, n\}$ of the form

$$\begin{aligned} b_1 &= (A_1, 0, 0, \ldots, 0) \\ b_2 &= (a_{2,1}, A_2, 0, ..., 0) \\ b_3 &= (a_{3,1}, a_{3,2}, A_3, \ldots, 0) \\ b_n &= (a_{n,1}, a_{n,2}, a_{n,3}, \ldots, A_n) \end{aligned}$$

where A_i is positive for each index i from 1 through n. Moreover, If another lattice Λ' is considered in the $n - i + 1$ $\mathbb{R}$ Euclidean space for each i, with a basis $b'_j, j = i, i + 1, i + 2, \ldots, n$

$$\begin{aligned} b'_i &= (A_i, 0, 0, \ldots, 0) \\ b'_{i+1} &= (a_{i+1,i}, A_{i+1}, 0, \ldots, 0) \\ b'_{i+2} &= (a_{i+2,i}, a_{i+2,i+1}, A_{i+2}, \ldots, 0) \\ b'_n &= (a_{n,i}, a_{n,i+1}, a_{n,3}, \ldots, a_{n,n-1}, A_n) \end{aligned}$$

Then any two points of the lattice are at a distance of at least A_i apart.

- Conjecture (Woods): If the product of all the A_i's from 1 to n is 1, $\prod_{i=1}^{n} A_i = 1$, and for each i, $A_i \leq A_1$, then any closed sphere of radius $\sqrt{n}/2$ in n Euclidean space contains a point of the lattice.

Theorem 6.8. *(Hans-Gill, Raka and Semhi) [23] Woods' conjecture holds for $n = 7$. Equivalently, If A_i's are as above such that $A_1 A_2 \ldots A_7 = 1$ and $A_i \leq A_1$ for $i = 1, 2, 3, 4, 5, 6$ and 7, then any closed sphere in $\mathbb{R}^7$ of radius $\sqrt{7}/2$ contains a point of the lattice.*

The theorem has used the following main lemmas in each of which the lattice Λ with value $d(\Lambda)$ is assumed to be reduced in the sense of Korkine and Zolotareff. Moreover, the critical determinant of the unit sphere with center at the origin in $\mathbb{R}^n$ is denoted by $\Delta(S_n)$.

1. If $2\Delta(S_{n_1} A_1^n) \geq d(\Lambda)$ then any closed sphere in $\mathbb{R}^n$ of radius r given as,

$$r = A_1[1 - (A_1^n \Delta(S_{n+1})/d(\Lambda))^2]^{1/2}$$

contains a point of the lattice.

2. For a fixed integer i with $1 \leq i \leq n-1$, let Λ_1 in $\mathbb{R}^i$ and Λ_2 in $\mathbb{R}^{n-i}$ be lattices with their reduced bases $\{p_i, i = 1, 2, ..., i\}$ and $\{q_j, j = i+1, i+2, \ldots, n\}$ respectively, where

$p_1 = (A_1, 0, 0, \ldots, 0)$ $\quad$ $q_{i+1} = (A_{i+1}, 0, 0, \ldots, 0)$
$p_2 = (a_{2,1}, A_2, 0, \ldots, 0)$ $\quad$ $q_{i+2} = (a_{i+2,i+1}, A_{i+2}, 0, \ldots, 0)$
$p_3 = (a_{3,1}, a_{3,2}, A_3, \ldots, 0)$ $\quad$ $q_{i+3} = (a_{i+3,i+1}, a_{i+3,i+2}, A_{i+3}, \ldots, 0)$
$p_i = (a_{i,1}, a_{i,2}, a_{i,3}, \ldots, A_i)$ $\quad$ $q_n = (a_{n,i+1}, a_{n,i+2}, a_{n,3}, \ldots, a_{n,n-1}, A_n)$

   If any sphere in $\mathbb{R}^i$ of radius r_1 contains a point of the first lattice and if any sphere in $\mathbb{R}^{n-i}$ of radius r_2 contains a point of the second lattice, then any sphere in $\mathbb{R}^n$ of radius $\sqrt{(r_1^2 + r_2^2)}$ contains a point of the main lattice $\Lambda \in \mathbb{R}^n$.

3. For all relevant i, $A_{i+1}^2 \geq \frac{3}{4}A_i^2$ and $A_{i+2}^2 \geq \frac{2}{3}A_i^2$

4. For $n = 3, 4, 5, 6$ and 7, $\Delta(S_n) = 1/\sqrt{2}, 1/2, 1/2\sqrt{2}, \sqrt{3}/8$ and $1/8$ respectively.

For the proof, they used Woods' notations and approach of his three papers. It is by supposing that there is a sphere of radius $\sqrt{7}/2$ in $\mathbb{R}^7$ that does not contain any point from the lattice Λ satisfying the hypothesis of Woods' conjecture for $n = 7$ and finding a contradiction afterwards. Since the conjecture considers each of the 7 A_i's, it is needed to consider all the possible cases for its proof. Let $A = A_1^2, B = A_2^2, C = A_3^2, D = A_4^2, E = A_5^2, F = A_6^2$ and $G = A_7^2$. Since $\det(\Lambda) = \prod A_i = 1$ has been assumed, the product $ABCDEFG = 1$. Let $\Lambda_i, i = 1, 2, 3, 4$ be lattices in $\mathbb{R}^1$ with basis $(A_1), (A_2), (A_3), (A_4)$ respectively; and let Λ_5 be a lattice in $\mathbb{R}^3$ having basis of $(A_5, 0, 0), (a_{6,5}, A_6, 0), (a_{7,5}, a_{7,6}, A_7)$. Any closed 1-sphere of radius $1/2A_i$, $i = 1, 2, 3, 4$ contains a point of Λ_i correspondingly. The first lemma can guarantee that if $2\Delta(S_4)A_5^3 \geq A_5A_6A_7$ then any closed 7-sphere of radius r given by

$$r = \sqrt{A_5 \left(1 - \left[\frac{A_5^6 \Delta(S_4)^2}{EFG}\right]\right)}$$

contains a point of the lattice Λ_5. Moreover, by repeated application of the second lemma, if the same condition as above (i.e $2\Delta(S_4)A_5^3 \geq A_5A_6A_7$) holds, then any 7-sphere of radius r' given by

$$r' = \sqrt{\frac{1}{4}(A + B + C + D + 4E) - \left[\frac{A_5^8 \Delta(S_4)^2}{EFG}\right]}$$

contains a point of the corresponding lattice. This radius should exceed $\sqrt{7}/2$, otherwise, it would contradict the assumption.

Here as $\Delta(S_4) = 1/2$ the above condition can be reduced to,

$$2\Delta(S_4)A_5^3 \geq A_5A_6A_7 \Rightarrow A_5^6 \geq (A_5A_6A_7)^2 \Rightarrow E^2 \geq FG$$

Besides, ABCD is the multiplicative inverse of EFG since the total product is 1. Hence, we have the following inequality:

$$\begin{aligned} E^2 \geq FG &\Longrightarrow r' > \sqrt{7}/2 \\ &\iff \sqrt{\frac{1}{4}(A+B+C+D+4E) - \left[\frac{A_5^8\Delta(S_4)^2}{EFG}\right]} > \sqrt{7}/2 \\ &\iff A+B+C+D+4E-E^4ABCD > 7 \end{aligned}$$

Let the above inequality be denoted by (1,1,1,1,3) since it shows the ordered partition of 7 and makes it easy to apply the second lemma. In a similar way, inequality (1,1,1,1,1, 2) is

$$\begin{aligned} 2F \geq G &\Longrightarrow A+B+C+D+E+4F-2F^2/G > 7 \\ &\Longrightarrow A+B+C+D+E+2G > 7 \qquad (\text{for } 4F-2F^2/G \leq 2G) \\ &\Longrightarrow A+B+C+D+E+4F-2F^3ABCD > 7 \quad (\text{for } \textstyle\prod A_i = 1) \end{aligned}$$

Inequality (4,1,1,1) corresponding to the ordered partition (4,1,1,1) of 7 is

$$A^4EFG \geq 2 \Longrightarrow 4A - \frac{1}{2}A^5EFG + E + F + G > 7$$

In the case of $A \leq 1$, there is equality of all A, B, C, D, E, F, G to 1 because $A_i \leq A_1 \forall i : 1, 2...7$. Thus Woods' conjecture is satisfied using the corresponding inequality, (1,1,1,1,1,1,1). Furthermore, the lattice Λ has no point enclosed in the sphere of radius A_1 whose center is at the origin. Hence $\Delta(A_1S_7) \leq 1$. Since $\Delta(S_7) = 1/8$, $A^7 \leq 64$ or equivalently, $A < 2$. Therefore, since the case for $A \leq 1$ is just the stated case in the above few lines, only $A > 1$ is considered along with the two cases (i.e. ≥ 1 and < 1) for each of B, C, D, E, F and G results in 2^6 different cases which have been analyzed in their work. They have remarked that there are alternative ways to get a contradiction in many cases. The interested reader is advised to refer their original work [23]

6.5 Related Results

After Minkowski put the bound for his conjecture, various related good bounds have been proved; but of course weaker ones. Each of the results listed is indeed a better bound than the preceding ones. Using the notations directly as in the section of Minkowski's conjecture, the table summarizes those main results discovered. They precisely have proved that the inequality below is true with the given corresponding information in the table.

$$\boxed{M(\Lambda) \leq \frac{\text{Vol}(\Lambda)}{2^{n/2} x_n}}$$

where x_n is listed in the table for each result.

Year	Credited to	x_n	Remark
1934	Cebotarev	1	———
1940	Mordell	$(1+(\sqrt{2}-1)^n)$	———
1949	Davenport	a_n	$\lim_{n\to\infty} a_n = 2e-1$
1958	Woods	b_n	$\lim_{n\to\infty} b_n = 2(2e-1)$
1963	Bombieri	c_n	$\lim_{n\to\infty} c_n = 3(2e-1)$
1978	Skubenko	$e^{-2}n^{1/3}(\log n)^{-2/3}$	For large n
1982	Narzuleav and Skubenko	$e^{-25.6}n^{3/7}(\log n)^{-4/7}$	For large n

Table 6.2: Related bounds to Minkowskis conjecture

As an illustrative example, the proof of Cebotarev is shown below

Theorem 6.9. *(Cebotarev) Keeping the notations the same as used in Minkowiski's conjecture,*

$$M(\Lambda) \leq \frac{\text{Vol}(\Lambda)}{2^{n/2}}$$

Proof. We can suppose that $\text{Vol}(\Lambda) = 1$. We need to prove that for $x \in \mathbb{R}^n$, $m_\Lambda(x) \leq 2^{-n/2}$. For simpler notation, let $m = m_\Lambda(x)$.

$$\begin{aligned} m > 0 \Rightarrow & \exists X \in \Lambda \text{ with } \mathcal{N}(x-X) < \frac{m}{1-\varepsilon} \qquad \text{for a small } \varepsilon \\ \Rightarrow & \exists t \in [0,\varepsilon) \text{ such that } \mathcal{N}(x-X) = \frac{m}{1-t} \end{aligned}$$

If we now consider the new lattice Λ' given by,

$$\Lambda' = \Big\{ \Big(\frac{Y_i - X_i}{x_i - X_i} \Big)_{1 \le i \le n} : Y = (Y_1, \ldots, Y_n) \in \Lambda \Big\}$$

its volume $\mathrm{Vol}(\Lambda')$ is equal to $(1-t)/m$. Since $\prod_{i=1}^{n} |x_i - Y_i| \ge m \quad \forall Y \in \Lambda$, we have,

$$\prod_{i=1}^{n} |1 - Y_i'| \ge 1 - t \text{ and } \prod_{i=1}^{n} |1 + Y_i'| \ge 1 - t \quad \forall Y' \in \Lambda'$$

so that

$$\prod |1 - Y_i'^2| \ge (1-t)^2 \qquad (\star)$$

This final inequality implies that for ε small, there does not exist a non zero $Y' \in \Lambda'$ such that

$$|Y_i'| < \sqrt{1 + (1-t)^2}$$

Indeed, If there was such a Y', it would follow for each i that

$$-1 \le Y_i'^2 - 1 < (1-t)^2 \le 1$$

On one hand, for a given i,

$$Y_i' - 1 > -(1-t)^2 \Rightarrow \prod_{i=1}^{n} |1 - Y_i'^2| < (1-t)^2$$

which contradicts equation($\star$) above.
On the other hand, for every i,

$$-1 \le Y_i'^2 - 1 \le -(1-t)^2 \Rightarrow |Y_i'| \le \sqrt{1 - (1-t)^2} \le \sqrt{2t}$$

This is again impossible for ε is small number. Therefore, there does not exist a non zero $Y' \in \Lambda'$ in the cube C' given below:

$$C' = \{x' \in \mathbb{R}_n : |x_i'| < \sqrt{1 + (1-t)^2} \text{ for each } i\}$$

Minkowski convex body theorem then implies

$$\mathrm{Vol(C')} \le 2^{\mathrm{n}} \mathrm{Vol}(\Lambda') = 2^{\mathrm{n}} \frac{1 - \mathrm{t}}{\mathrm{m}} \Rightarrow 2^{\mathrm{n}} (1 + (1 - \mathrm{t}^2))^{\mathrm{n}/2} \le 2^{\mathrm{n}} \frac{1 - \mathrm{t}}{\mathrm{m}}$$

As $\varepsilon \to 0$, $t \to 0$. Then finally $m \le 2^{-n/2}$ is obtained as desired. $\square$

The following is mainly credited to Eva Bayer's 2006 result on upper bounds of Euclidean minima [20]. Let K as usual be an algebraic number field with degree n and absolute discriminant d.

1. If K is an algebraic number field of degree n and discriminant d satisfies

$$M(K) \leq \frac{|d|}{2^n}.$$

2. If p is a positive odd prime number and if the algebraic number field K is of the form $K = \mathbb{Q}(\zeta_{p^k} + \zeta_{p^k}^{-1})$ with degree n and discriminant d, then Minkowiski's conjecture holds, i.e.

$$M(K) \leq \frac{\sqrt{|d|}}{2^n}.$$

$\Rightarrow$ For $k = 1$, $K = [\mathbb{Q}(\zeta_p + \zeta_p^{-1})] \Rightarrow n = (p-1)/2$, hence

$$M(K) \leq \frac{\sqrt{d}}{2^{\frac{p-1}{2}}}.$$

3. If K is the nth cyclotomic field, i.e. $K = \mathbb{Q}(\zeta_n)$, then

$$M(K) \leq \frac{\sqrt{|d|}}{2^{\phi(n)}}.$$

For her main results, the knowledge of ideal lattices, sphere packing, covering invariant, thin fields and thin ideal classes have been used together with other number theoretic concepts.

Appendix A

List Of Tables

Here we give the results that J.-P. Cerri [7] and [5] has extended the previous less number of data given by Lemmermeyer [32] and Quême [40].

• Notations :

- K is a number field of degree n,
- $M(K)$ is the Euclidean minimum of K
- $M(\bar{K})$ is the inhomogeneous minimum of K
- When $n = 3$, E indicates that K is norm-Euclidean.
- T is number of critical rational points in a fundamental domain,
- E means norm-Euclidean
- d_K is discriminant of K

• Table A.1 : $n = 2$.

For $n = 2$ (i.e. $K = \mathbb{Q}(\sqrt{m})$ for some square free integer m), the tables complete those that can be found in Lemmermeyer's paper [32] which has given $M(K)$ of $\mathbb{Q}(\sqrt{m})$ for $2 \leq m \leq 102$. J.-P Cerri then has further computed it for such m between 103 and 400, with only 28 exceptions as mentioned in Section 4.4. These indeed could be computed in multi-precision.

• Table A.2 and A.3 : $n = 3$.

For $n = 3$, in a similar way, Table A.2 has completed those left indeterminate by the update version of Lemmermeyer [32] for discriminant not exceeding 11,000; In fact, all of them are norm Euclidean.

Table A.3 is devoted to number fields of discriminant more than 11,000 but less than 15,000, not studied in [32]. The Euclidean minimum is only given for number fields which are not norm-Euclidean; otherwise letter E written.

• Table A.4 : $n = 4$

For $n = 4$, the Euclidean minima of the 286 number fields of discriminant less than 40000 have been computed. The Euclidean nature of a large number of them has already been found by Quême [40] but he had left some fields indeterminate. In fact, some of these last ones are not norm-Euclidean, although they have class number one (i.e. for $d_K = 18432$, 34816 and 35152).

• Table A.5 : $n = 5$

For $n = 5$, there were only 25 number fields which are known to be norm-Euclidean by Quême [40]. However, after him, the Euclidean minima of the 156 number fields of discriminant less than 511,000 are determined. With one exception, they have all been found to be norm-Euclidean.

• Tables A.6, A.7 and A.8 : $n = 6$, 7, and 8 respectively.

For $n \geq 6$, very little was known on the fields of degree greater than 5. Cerri has also treated the first 156 sextic, 132 heptic and 18 octic number fields and found them all to be norm-Euclidean.

A.1 Quadratic Number Fields

m	T	$M(K)$	m	T	$M(K)$
103	2	1129671/455054	105	2	8/7
106	4	13967/8010	107	2	637/214
109	4	8709209/7425625	110	1	11/4
111	1	11/4	113	4	3514159/2408708
114	2	343/114	115	4	289554/140875
118	2	835775/306918	119	2	1121/238
122	1	11/2	123	2	393/82
127	2	21904533/9461246	129	2	64/43
130	1	7/2	131	2	4440376/1390041
133	2	299/171	134	2	194659/72963
137	4	4543/3488	138	1	17/4
141	2	275/188	142	1	21/4
143	1	11/2	145	2	3/2
146	1	23/4	149	4	95/61
154	1	15/4	155	1	7/2
157	4	436/217	158	2	539/158
159	2	275/106	161	2	34/23
165	2	41/15	167	2	1909/334
170	1	13/2	173	2	36/13
174	2	115/24	177	2	88/59
178	2	1377/356	179	2	21395567/8380422
181	4	2876/1305	182	1	7/2
183	1	7/2	185	4	113/68
186	2	20947/7502	187	2	729/187
190	2	292671/104044	193	4	k_1
194	1	25/4	195	1	13/2
197	2	7/4	201	2	1844723/1030192
202	4	183203/68276	203	1	11/2
205	2	81/41	206	2	110615/29767
209	2	1467/931	210	1	15/4
213	2	187/71	215	2	361/86
217	4	k_2	218	1	11/2
219	2	805/146	221	2	55/17
222	1	13/2	223	2	2997/446

m	T	$M(K)$	m	T	$M(K)$
226	1	15/2	227	2	3079/454
229	4	49/15	230	1	13/2
231	2	923/154	233	4	3715882019/2144801348
235	2	441/94	237	2	227/79
238	2	24294/5831	246	2	66726/14801
247	2	344693/85293	251	2	12735720/3674891
253	2	3877/1863	254	1	29/4
255	1	15/2	257	2	2
258	1	31/4	259	2	2958475/847226
263	2	1046501/278254	265	4	233/138
266	2	3085/684	267	2	847/178
269	4	517/269	273	2	272/91
274	1	9/2	277	4	5788/2613
278	2	2777/556	281	4	1808417155581/1131100315025
282	2	23231/4704	285	2	71/19
286	2	4068289/1123672	287	2	4433/574
290	1	17/2	291	2	1509/194
293	4	64/17	295	2	1868333/506250
298	4	k_3	299	2	3865/832
301	2	38751/22747	302	2	29948063/8553244
303	2	24489/5046	305	2	529/244
309	2	240/103	310	1	19/4
314	4	3241351/785000	317	4	20231/7925
318	1	29/4	321	2	260/107
322	1	33/4	323	1	17/2
326	1	35/4	327	1	17/2
329	2	784/423	330	1	31/4
335	2	5171/1206	339	2	1000945/195942
341	2	767/279	345	2	40/23
346	1	11/2	347	2	2671668/641603
349	4	k_4	353	4	k_5
354	2	316991/57348	355	2	1419/284
357	2	89/21	359	2	6265/718
362	1	19/2	365	4	81/19
366	2	7290735/1815848	370	1	15/2
371	1	25/4	373	4	k_6
374	2	4225/748	377	2	1459/464

m	T	$M(K)$	m	T	$M(K)$
381	2	1501/508	383	2	2057/383
385	2	60263/27380	386	2	569023/111554
389	4	533549/262964	390	1	29/4
395	1	17/2	397	4	31061844/11881813
398	1	37/4	399	1	19/2

Where the constants k_1, k_2, k_3, k_4, k_5 and k_6 are given as follows:

$$k_1 = \frac{20470649447051}{12448646853700}$$
$$k_2 = \frac{344451856454}{230887817937}$$
$$k_3 = \frac{1297639985683}{335473872500}$$
$$k_4 = \frac{711233433}{339296404}$$
$$k_5 = \frac{52222023079}{20314230788}$$
$$k_6 = \frac{187701339}{104775700}$$

A.2 Cubic Number Fields ($d_K < 11000$)

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
1593	2	1/3	2177	2	1/3	2713	8	1/3
2993	2	1/3	3137	12	209/485	3173	1	1/2
3252	2	5/9	3261	1	1/2	3281	4	9/13
3316	1	1/2	3325	2	7/10	3356	2	1/2
3368	2	1/2	3496	2	13/16	3508	8	113/178
3540	1	1/2	3569	8	7/17	3576	2	1/2
3580	2	1/2	3592	2	5/8	3596	2	1/2
3604	1	1/2	3624	2	1/2	3732	1	1/2
3736	2	1/2	3753	6	11/27	3873	2	3/5
3877	1	1/2	3892	2	7/10	3941	2	7/12
3957	1	1/2	4104	2	1/2	4281	8	79/225
4344	2	1/2	4364	2	1/2	4409	?	$[1/3, 6/17[$
4481	3	1/2	4493	2	31/36	4596	1	1/2
4597	1	1/2	4628	1	1/2	4641	2	9/11
4649	4	9/13	4692	1	1/2	4749	1	1/2
4765	3	1/2	4825	2	47/80	4841	20	11/27
4844	2	1/2	4852	1	1/2	4853	4	27/53
4857	8	3/7	4860	2	25/36	4892	2	1/2
4933	1	1/2	5073	?	$[1/3, 10/27[$	5081	4	7/9
5172	2	5/9	5204	3	1/2	5261	2	3/4
5300	3	3/4	5325	1	1/2	5333	1	1/2
5353	6	5/13	5356	2	1/2	5368	2	1/2
5373	1	1/2	5468	2	1/2	5477	1	1/2
5497	3	1/2	5529	2	7/9	5556	1	1/2
5613	1	1/2	5620	2	7/10	5621	1	1/2
5624	2	1/2	5629	1	1/2	5637	1	1/2
5685	1	1/2	5697	4	7/17	5724	1	7/8
5741	1	1/2	5780	2	23/34	5821	4	7/8
5853	1	1/2	5901	2	9/16	5912	2	5/9
5925	4	137/180	5940	1	1/2	5980	2	13/20
6053	1	1/2	6088	2	25/32	6092	2	1/2
6108	2	1/2	6133	1	1/2	6153	2	5/9
6184	2	23/32	6209	6	83/133	6237	1	1/2
6268	4	17/32	6396	2	1/2	6420	2	1/2

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
6453	1	1/2	6508	1	5/8	6549	1	1/2
6556	2	25/32	6557	1	1/2	6584	2	1/2

A.3 Cubic Number Fields ($d_K \in (11000, 15000)$)

d_K	$M(K)$	d_K	$M(K)$	d_K	$M(K)$	d_K	$M(K)$
10661	E	10929	E	10941	E	10949	E
10997	E	11013	E	11,020	E	11028	E
11032	E	11045	E	11057	E	11060	E
11085	E	11092	E	11097	33/27	11109	E
11124	5/4	11137	E	11188	5/4	11197	31/8
11289	E	11293	E	11316	E	11321	E
11324	3/2	11348	9/4	11380	E	11401	167/151
11417	11/3	11421	49/36	11448	E	11476	E
11505	E	11545	E	11576	E	11608	E
11637	5/4	11641	E	11656	11/8	11665	E
11672	E	11688	E	11697	E	11705	213/193
11757	E	11772	E	11777	27/17	11789	E
11821	23/16	11829	E	11848	E	11849	19/9
11853	E	11880	E	11881	E	11884	E
11885	E	11965	23/8	12001	E	12065	1
12081	152/149	12092	E	12140	E	12177	E
12188	E	12197	3/2	12216	E	12248	E
12269	E	12284	E	12309	E	12317	25/22
12325	E	12333	E	12401	E	12409	E
12436	E	12441	E	12552	E	12577	49/19
12632	E	12652	E	12657	E	12660	23/18
12664	E	12685	E	12700	E	12724	E
12744	E	12765	23/20	12788	E	12821	E
12849	E	12852	E	12925	E	13069	E
13089	E	13117	E	13148	E	13153	7/5

d_K	$M(K)$	d_K	$M(K)$	d_K	$M(K)$	d_K	$M(K)$
13172	E	13189	E	13204	E	13245	E
13257	E	13269	E	13273	E	13332	E
13333	E	13396	E	13433	E	13460	9/8
13473	E	13537	E	13549	41/36	13564	E
13576	11/8	13577	E	13589	E	13608	E
13652	E	13676	3/2	13684	E	13688	E
13689_1	53/39	13689_2	13/3	13693	31/22	13748	E
13765	E	13768	5/2	13785	E	13801	67/17
13861	17/8	13877	E	13897	E	13905	E
13916	16/9	13925	5/4	13928	E	13932	95/48
13972	E	14013	2	14036	45/44	14056	19/16
14089	27/7	14129	E	14141	E	14165	E
14189	E	14197	3/2	14229	E	14296	E
14316	E	14360	E	14376	E	14385	E
14388	E	14389	E	14397	9/4	14408	E
14420	E	14424	E	14457	E	14505	8/7
14516	E	14520	40/33	14597	E	14609	E
14653	E	14661	7/2	14668	E	14680	E
14769	E	14824	E	14825	E	14836	E
14876	E	14945	33/5	14956	E	14964	E
14969	E	14977	E	14993	E		

The number fields of discriminant 13689 are respectively generated by a root of $X^3 - 39X - 26$ ($d_K = 13689_1$) and $X^3 - 39X - 91$ ($d_K = 13689_2$).

A.4 Quartic Number Fields

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
725	20	1/11	1125	4	1/5	1600	3	1/4
1957	2	1/3	2000	3	1/4	2048	1	1/2
2225	6	1/4	2304	1	1/2	2525	8	1/5
2624	3	1/4	2777	1	1/2	3600	3	1/4
3981	2	1/3	4205	16	1/5	4225	6	1/4
4352	1	1/2	4400	3	1/4	4525	8	1/5
4752	2	1/3	4913	6	1/4	5125	4	1/5
5225	6	1/4	5725	8	1/9	5744	3	1/4
6125	16	11/49	6224	1	1/2	6809	1	1/2
7053	2	1/3	7056	2	1/3	7168	1	1/2
7225	6	1/4	7232	2	1/2	7488	1	1/2
7537	1	1/2	7600	3	1/4	7625	6	1/4
8000	6	5/16	8069	4	1/5	8112	2	1/3
8468	1	1/2	8525	8	1/5	8725	16	1/9
8768	3	1/4	8789	4	1/5	8957	4	1/3
9225	6	1/4	9248	2	1/2	9301	2	1/3
9792	6	7/16	9909	2	1/3	10025	6	1/4
10273	1	1/2	10304	2	1/2	10309	52	9/53
10512	3	1/4	10816	3	1/4	10889	1	1/2
11025	6	1/4	11197	2	1/3	11324	1	1/2
11344	1	1/2	11348	2	1/2	11525	8	1/5
11661	6	1/3	12197	12	13/37	12357	4	1/3
12400	3	1/4	12544	1	1/2	12725	40	1/11
13025	6	1/4	13068	1	1/2	13448	1	1/2
13525	8	1/5	13625	6	1/4	13676	1	1/2
13725	12	9/25	13768	1	1/2	13824	1	1/2
13888	3	1/4	13968	2	1/2	14013	4	1/3
14197	18	9/37	14272	2	1/3	14336	1	1/2
14400	6	5/16	14656	1	1/2	14725	28	9/29
15125	20	31/121	15188	2	1/2	15317	2	1/2
15529	1	1/2	15952	1	1/2	16225	6	1/4
16317	12	17/49	16357	2	1/3	16400	3	1/4
16448_1	1	1/2	16448_2	2	1/2	16609	1	1/2
16997	8	1/5	17069	4	1/3	17417	1	1/2

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
17424	2	1/2	17428	2	1/2	17600	6	11/16
17609	1	1/2	17725	16	1/9	17989	2	1/3
18097	2	1/3	18432	1	7/4	18496	2	9/16
18625	6	1/4	18688	1	1/2	18736	2	1/3
19025	6	1/4	19225	6	1/4	19429	2	1/3
19525	8	1/5	19600	3	1/4	19664	2	1/2
19773	4	9/13	19796	2	1/2	19821	2	1/3
20032	3	1/4	20225	6	1/4	20308	2	1/2
20808	1	1/2	21025	6	1	21056	3	1/4
21200	1	1/2	21208	1	1/2	21308	1	1/2
21312	1	1/2	21469	2	1/3	21568	2	1/2
21725	28	11/29	21737	6	1/4	21801	2	1/3
21964	1	1/2	22000	6	9/16	22221	4	1/3
22545	1	1/2	22592	2	1/2	22676	2	1/2
22784	1	1/2	22896	4	1/3	23252	2	1/2
23297	1	1/2	23301	2	1/3	23377	1	1/2
23525	8	1/5	23552	1	1/2	23600	3	1/4
23665	1	1/2	23724	1	1/2	24197	2	1/2
24336	4	1/3	24400	8	9/25	24417	1	1/2
24437	8	1/5	24525	8	9/25	24749	6	1/7
24832	1	1/2	24917	4	1/3	25088	2	1/2
25225	6	1/4	25488	2	1/2	25492	2	1/2
25525	8	1/5	25717	2	1/3	25808	1	1/2
25857	4	1/3	25893	4	1/3	25961	1	1/2
26032	2	1/3	26125	4	1/5	26176	3	1/4
26224	2	1/3	26225	6	1/4	26525	8	1/5
26541	4	1/3	26569	1	1/2	26825	1	1/2
26873	2	7/8	27004	1	1/2	27225	6	1/4
27329	1	1/2	27472	1	1/2	27648	1	3/4
27725	28	16/29	27792	4	1/3	28025	6	1/4
28224_1	6	5/16	28224_2	6	7/16	28400	3	1/4
28473	1	1/2	28669	4	1/5	28677	2	1/3
28749	5	7/16	29237	4	1/3	29248	3	1/4
29268	2	1/2	29813	30	13/77	29952	1	3/4
30056_1	3	1/2	30056_2	1	1/2	30125	4	1/5
30273	1	1/2	30400	6	5/16	30512	3	1/4
30544	1	1/2	30725	?	$[1/11, 8/59[$	30776	1	1/2

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
30972	1	1/2	30976	1	1/2	31225	6	1/4
31288	1	1/2	31532	1	1/2	31600	3	1/4
31744	1	1/2	31808	2	1/2	32081	1	1/2
32225	6	1/4	32368	2	1/3	32448	6	1/3
32625	6	1	32737	1	1/2	32821	2	1/3
32832	2	1/3	33097	1	1/2	33344	3	1/4
33424	2	1/3	33428	2	1/2	33452	1	1/2
33489	1	1/2	33525	8	11/25	33625	6	1/4
33709	2	1/3	33725	50	19/121	33813	2	1/2
33844	2	1/2	34025	6	1/4	34196	2	1/2
34225	6	9/16	34704	3	1/4	34816	1	7/4
34868	2	1/2	35013	6	1/3	35125	4	1/5
35136	1	1/2	35152	4	16/13	35225	6	1/4
35312	4	1/3	35392	3	1/4	35401	2	1/3
35537_1	1	1/2	35537_2	1	1/2	35537_3	1	1/2
35856	2	1/3	36025	6	1/4	36416	3	1/4
36517	12	13/49	36677	14	11/29	36761	1	1/2
36928	2	1/2	37108	2	1/2	37229	4	1/3
37349	4	9/13	37485_1	16	17/49	37485_2	4	1/3
37489	1	1/2	37525	8	1/5	37773	4	1/3
37885	2	1/3	37952	2	1/2	38000	6	5/16
38225	6	1/4	38720	1	1/2	38725	?	$[1/9, 3/16[$
38864	3	1/4	39377	4	1/3	39528	1	1/2
39600	6	9/16	39605	2	1/2	39744	1	1/2
39800	1	1/2						

The number fields of discriminant, d_K =16448 are respectively generated by a root of $X^4-2X^3-6X^2+2$ ($d_K = 16448_1$) and $X^4-2X^3-7X^2+8X+14$ ($d_K = 16448_2$); of d_K =28224 by a root of $X^4 - 10X^2 + 4$ ($d_K = 28224_1$) and $X^4 - 2X^3 - 13X^2 + 14X + 7$ ($d_K = 28224_2$); of d_K =35537 by a root of $X^4 - 2X^3 - 9X^2 + 5X + 16$ ($d_K = 35537_1$), $X^4 - X^3 - 8X^2 - 3X + 4$ ($d_K = 35537_2$) and $X^4-2X^3-5X^2+5X+4$ ($d_K = 35537_3$); of d_K =37485 by a root of $X^4-X^3-7X^2+X+1$ ($d_K = 37485_1$) and $X^4-X^3-8X^2+12X-3$ ($d_K = 37485_2$) respectively as in the table.

A.5 Quintic Number Fields

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
14641	10	1/11	24217	4	1/5	36497	2	1/3
38569	6	1/7	65657	2	1/3	70601	6	1/7
81509	1	1/2	81589	1	1/2	89417	2	1/3
101833	4	1/5	106069	1	1/2	117688	1	1/2
122821	3	1/4	124817	2	1/3	126032	1	1/2
135076	1	1/2	138136	1	1/2	138917	2	1/3
144209	2	1/3	147109	1	1/2	149169	2	1/3
153424	1	1/2	157457	2	1/3	160801	2	1/3
161121	4	1/3	170701	3	1/4	173513	8	1/9
176281	8	1/5	176684	1	1/2	179024	1	1/2
180769	8	1/5	181057	4	1/3	186037	1	1/2
195829	1	1/2	202817	2	1/3	205225	4	1/3
207184	1	1/2	210557	3	1/4	216637	1	1/2
218524	1	1/2	220036	1	1/2	220669	1	1/2
223824	1	1/2	223952	1	1/2	224773	1	1/2
230224	2	1/2	233489	6	1/7	236549	1	1/2
240133	1	1/2	240881	4	1/5	242773	3	1/4
245992	1	1/2	246832	1	1/2	249689	4	1/5
255877	3	1/4	265504	2	1/2	270017	2	1/3
273397	1	1/2	274129	4	1/5	284897	2	1/3
287349	2	1/3	288385	4	1/3	288565	3	1/4
288633	2	1/3	294577	4	1/3	301117	1	1/2
301909	1	1/2	303952	1	1/2	305617	4	1/5
307145	2	1/3	307829	3	1/4	310097	2	1/3
310257	4	1/3	312617	2	1/3	313905	2	1/3
320837	1	1/2	324301	1	1/2	328784	2	1/2
329977	2	1/3	331312	1	1/2	339509	2	1/3
341692	1	1/2	345065	2	1/3	347317	3	1/4
352076	1	1/2	352588	1	1/2	354969	2	1/3
355309	1	1/2	356173	3	1/4	356789	3	1/4
357977	4	1/5	368464	2	1/2	369849	2	1/3
372289	2	1/2	373057	6	1/7	375116	1	1/2
375145	8	1/5	379077	1	1/2	379477	1	1/2
380224	2	1/2	386404	1	1/2	387268	1	1/2

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
390625	2	7/5	394064	1	1/2	394657	2	1/3
395721	2	1/3	396520	1	1/2	398885	1	1/2
401584	2	1/2	403137	4	1/3	404185	4	1/5
404744	1	1/2	406264	2	1/2	410677	1	1/2
414677	1	1/2	416249	8	1/5	419969	12	1/7
420460	1	1/2	421096	1	1/2	422069	1	1/2
422077	1	1/2	423537	2	1/3	423904	2	1/2
427569	2	1/3	429937	4	1/5	442552	1	1/2
446609	2	1/3	449617	12	1/7	449733	1	1/2
450277	3	1/4	453712	1	1/2	453749	1	1/2
454057	4	1/3	457904	1	1/2	459513	2	1/3
459533	3	1/4	460708	1	1/2	463341	1	1/2
463477	3	1/4	466809	4	1/3	470117	2	1/3
475333	3	1/4	475929	2	1/3	481097	4	1/5
482689	8	1/5	483273	2	1/3	484105	8	1/5
486337	2	1/2	488149	1	1/2	493049	6	1/7
495317	3	1/4	501289	8	1/5	503376	1	1/2
504568	2	1/2	509324	1	1/2	510889	2	1/2

A.6 Sextic Number Fields

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
300125	168	1/29	371293	12	1/13	434581	24	1/13
453789	6	1/7	485125	8	1/9	592661	6	1/7
703493	48	1/13	722000	3	1/4	810448	3	1/4
820125	8	1/9	905177	14	1/8	966125	4	1/5
980125	8	1/9	1075648	6	1/7	1081856	6	1/7
1134389	6	1/7	1202933	4	1/5	1229312	12	1/7
1241125	4	1/5	1259712	2	1/3	1279733	12	1/7
1292517	8	1/9	1312625	3	1/4	1387029	2	1/3
1397493	2	1/3	1416125	4	1/5	1528713	14	1/8
1541581	4	1/5	1683101	12	1/7	1767625	3	1/4
1868969	1	1/2	1922000	3	1/4	1995125	30	1/11
1997632	7	1/8	2115281	14	1/8	2235125	24	1/9
2249737	14	1/8	2286997	2	1/3	2323397	2	1/3
2415125	30	1/11	2460365	8	1/5	2495261	2	1/3
2501557	2	1/3	2540864	1	1/2	2565429	2	1/3
2591125	4	1/5	2623625	3	1/4	2624293	12	1/7
2661761	1	1/2	2666432	7	1/8	2737625	3	1/4
2738000	3	1/4	2782261	2	1/3	2803712	1	1/2
2806769	6	1/7	2812877	8	1/5	2847089	1	1/2
2847312	2	1/3	2850125	24	1/9	2854789	132	1/13
2908477	8	1/5	2936696	1	1/2	2990117	2	1/3
3022625	3	1/4	3027661	12	1/7	3072812	1	1/2
3081125	4	1/5	3086597	4	1/3	3094889	12	1/7
3151861	2	1/3	3162625	3	1/4	3184733	6	1/7
3195392_1	1	1/2	3195392_2	18	1/7	3296573	12	1/7
3319769	1	1/2	3356224	1	1/2	3359232	7	1/8
3389609	1	1/2	3418281	14	1/8	3438125	8	1/5
3455125	8	1/9	3477989	4	1/5	3486377	3	1/4
3512000	6	1/4	3527069	60	1/13	3549501	4	1/3
3570125	12	1/5	3662336	6	1/7	3697873	1	1/2
3706688	2	1/3	3728437	2	1/3	3728753	14	1/8
3822093	2	1/3	3829849	3	1/4	3916917	2	1/3
3928381	2	1/3	4016873	6	1/7	4022000	6	1/4
4086536	1	1/2	4125937	1	1/2	4126869	8	1/9

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
4141568	1	1/2	4148928	24	8/49	4170688	2	1/3
4181517	2	1/3	4218557	6	1/7	4222000	6	1/4
4224413	8	1/5	4227136	8	1/5	4254689	1	1/2
4274669	6	1/7	4284928	7	1/8	4305125	50	11/101
4308028	1	1/2	4383253	4	1/5	4418000	6	1/4
4418197	2	1/3	4443861	2	1/3	4448597	12	1/7
4456256	12	1/7	4462625	3	1/4	4507648	1	1/2
4537077	2	1/3	4588625	3	1/4	4601153	1	1/2
4642000	3	1/4	4667249	3	1/4	4733829	2	1/3
4755281	1	1/2	4758548	1	1/2	4778125	4	1/5
4820125	8	1/9	4823921	1	1/2	4824572	1	1/2
4829696	1	1/2	4838537	4	1/5	4840784	3	1/4
4847625	3	1/4	4851125	4	1/5	4905125	12	1/5
4918997	10	1/11	4950125	12	1/5	4966677	4	1/3
5030996	1	1/2	5061125	4	1/5	5061656	1	1/2
5090861	4	1/5	5101781	6	1/7	5160733	6	1/7
5163008	1	1/2	5173625	3	1/4	5192000	3	1/4
5224841	3	1/4	5274997	36	1/13	5279033	1	1/2

A.7 Heptic Number Fields

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
20134393	6	1/7	25164057	2	1/3	25367689	12	1/13
28118369	6	1/7	30653489	2	1/3	31056073	6	1/7
32354821	3	1/4	32567681	8	1/9	34554953	6	1/7
35269512	6	1/7	39610073	4	1/5	39829313	2	1/3
41153941	3	1/4	41455873	4	1/5	41783473	4	1/5
42855577	6	1/7	43242544	3	1/4	43723857	2	1/3
46643776	1	1/2	49960857	2	1/3	52011969	2	1/3
55073801	6	1/7	55078981	7	1/8	55311169	4	1/5
57936017	2	1/3	58355513	4	1/5	61136809	4	1/5
63128113	6	1/7	65698681	12	1/7	65845693	4	1/5
67159593	6	1/7	68249369	2	1/3	69012929	8	1/9
69678137	4	1/5	69836041	10	1/11	70244521	4	1/5
75602713	4	1/5	75630121	4	1/5	77004029	1	1/2
78373945	4	1/5	78534833	8	1/9	79044293	6	1/7
79397476	1	1/2	79438057	4	1/5	80750473	10	1/11
81323773	1	1/2	81437164	1	1/2	82916101	3	1/4
83266101	3	1/4	83934569	4	1/5	84506041	4	1/5
84824233	16	1/9	86278889	6	1/7	88337321	2	1/3
88383761	8	1/9	88537609	10	1/11	89211436	1	1/2
89781929	4	1/5	89916129	2	1/3	91138133	2	1/3
92507681	12	1/7	93364693	3	1/4	93679973	3	1/4
95402689	4	1/5	96309817	2	1/3	96703369	12	1/7
97212489	2	1/3	97824733	3	1/4	98167689	6	1/7
98295577	20	1/11	99230049	2	1/3	100069857	2	1/3
100269173	1	1/2	100660489	6	1/7	100907057	4	1/5
101109161	4	1/5	101206153	4	1/5	102872809	4	1/5
105058897	4	1/3	105391453	1	1/2	105486613	1	1/2
105537053	7	1/8	105708673	4	1/5	107164437	2	1/3
107680489	12	1/7	107704601	4	1/5	108526193	2	1/3
109652617	4	1/5	110251433	4	1/5	110921461	3	1/4
112831453	3	1/4	112873193	4	1/5	113269137	2	1/3
114059549	3	1/4	114075673	4	1/5	114477761	6	1/7
117757033	2	1/3	117806905	8	1/5	118768997	1	1/2
118870813	1	1/2	118892393	4	1/5	119084961	2	1/3

d_K	T	$M(K)$	d_K	T	$M(K)$	d_K	T	$M(K)$
119292949	3	1/4	119605529	2	1/3	120077752	1	1/2
120230212	1	1/2	120275469	1	1/2	120299213	6	1/7
120919849	2	1/3	124666793	2	1/3	124893376	1	1/2
5439409	24	1/13	125834753	2	1/3	126039593	2	1/3
126123101	3	1/4	126284149	8	1/5	126993449	6	1/7
128513177	2	1/3	129629693	7	1/8	129673145	4	1/5
130548149	6	1/7	130696737	4	1/3	130840257	2	1/3
132205961	6	1/7	134317789	6	1/7	134407793	2	1/3
134589773	3	1/4	135384281	8	1/9	135877157	2	1/3
136997732	1	1/2	137185481	6	1/7	138031669	7	1/8

A.8 Octic Number Fields

d_K	T	$M(K)$	d_K	T	$M(K)$
282300416	15	1/16	309593125	18	1/19
324000000	15	1/16	410338673	30	1/16
432640000	15	1/16	442050625	30	1/16
456768125	10	1/11	483345053	10	1/11
494613125	36	1/19	582918125	20	1/11
656505625	30	1/16	661518125	10	1/11
707295133	12	1/13	733968125	10	1/11
740605625	30	1/16	803680625	10	1/11
852038125	20	1/11	877268125	20	1/11

Appendix B

Basic Definitions And Concepts Used

B.1 Riemann Hypothesis

Before stating the hypothesis, let us recall elementary definitions to supplement Hooley's result.

Euler's generalization of Fermat's Little Theorem is stated as if $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that the $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\text{mod } n)$ where $\phi(n)$ is the Euler ϕ function counting the integers between 1 and n that are coprime to n. This fundamental theorem naturally invites us to investigate exponents that result in its congruence with 1 under the given coprime restriction. It further raises the minimal exponent question to give the same congruence.

Definition B.1. (Order) Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ where a and n are relatively prime. Then the *order* of the number a modulo n is the smallest exponent e such that $a^e \equiv 1 (\text{mod } n)$, denoted by $e = ord_n(a)$. In which case, a is said to belong to the exponent e modulo n.

It is clear that the modular order of an integer is equivalent to the order of the element in the group $(\mathbb{Z}/n\mathbb{Z})^*$

Proposition B.2. *Let $a \in \mathbb{Z}$ and $n, c \in \mathbb{N}$. Then $a^c \equiv 1 (mod\ n)$ if and only if $ord_n(a)$,say α, divides c. In particular, $\alpha \mid \phi(n)$.*

Proof. $(\Longleftarrow) : c = \alpha q$ for some $q \in \mathbb{N}$ clearly implies $a^c \equiv (a^\alpha)^q \equiv 1 (\text{mod } n)$. $(\Longrightarrow) : a^c \equiv 1 (\text{mod } n) \Rightarrow c \geq \alpha$ by definition. Then Division Algorithm gives us q and r where $0 \leq r < \alpha \Rightarrow 1 \equiv a^c \equiv (a^\alpha)^q a^r \equiv a^r \ (\text{mod } n)$. But again by definition of order of an element given above $r = 0$ □

Definition B.3. (Primitive Root) If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that the $\gcd(a, n) = 1$, then a is said to be a *primitive root modulo* n if $ord_n(a) = \phi(n)$. If for $b \in \mathbb{Z}$, $b \equiv a^\beta \pmod{n}$ for the given primitive element a, then the integer β is called the *index* of the integer b modulo n to the *base* a.

Definition B.4. The *Riemann zeta function* is defined to be the complex valued function given by the series

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{B.1}$$

which is absolutely convergent for all complex numbers s with $\Re(s) > 1$.

Some properties of the zeta function are listed below.

- For all s with $\Re(s) > 1$, the zeta function satisfies the *Euler product formula*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \tag{B.2}$$

where the product is taken over all positive integer primes p, and converges uniformly in a neighborhood of s. This is the direct consequence of unique factorization of positive integers values of n. In fact, it is clear to observe the following:

$$\begin{aligned}\zeta(s) : &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} (1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{2^{2s}} + \frac{1}{5^s} + \frac{1}{2^s}.\frac{1}{3^s} + \dots) \\ &= \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots) = \prod_p \frac{1}{1 - p^{-s}}\end{aligned}$$

The final equality is because of the fact that for each prime p, the given geometric progression converges to the value $(1 - p^{-s})^{-1}$

- The zeta function has a meromorphic continuation to the entire complex plane with a simple pole at $s = 1$, of residue 1, and no other singularities.

- The zeta function satisfies the *functional equation*

$$\zeta(s) = 2^s \pi^{s-1} \sin \frac{\pi s}{2} \Gamma(1 - s) \zeta(1 - s), \tag{B.3}$$

for any $s \in \mathbb{C}$ (where Γ denotes the Gamma function).

Distribution of primes

The Euler product formula (B.2) given above expresses the zeta function as a product over the primes $p \in \mathbb{Z}$, and consequently provides a link between the analytic properties of the zeta function and the distribution of primes in the integers. As the simplest possible illustration of this link, we show how the properties of the zeta function given above can be used to prove that there are infinitely many primes.

If the set S of primes in $\mathbb{Z}$ were finite, then the Euler product formula

$$\zeta(s) = \prod_{p \in S} \frac{1}{1 - p^{-s}}$$

would be a finite product, and consequently $\lim_{s \to 1} \zeta(s)$ would exist and would equal

$$\lim_{s \to 1} \zeta(s) = \prod_{p \in S} \frac{1}{1 - p^{-1}}.$$

But the existence of this limit contradicts the fact that $\zeta(s)$ has a pole at $s = 1$, so the set S of primes cannot be finite.

A more sophisticated analysis of the zeta function along these lines can be used to prove both the analytic prime number theorem and Dirichlet's theorem on primes in arithmetic progressions[1].

Zeros of the zeta function

A *nontrivial zero* of the Riemann zeta function is defined to be a root $\zeta(s) = 0$ of the zeta function with the property that $0 \leq \Re(s) \leq 1$. Any other zero is called *trivial zero* of the zeta function.

The reason behind the terminology is as follows. For complex numbers s with real part greater than 1, the series definition (B.1) immediately shows that no zeros of the zeta function exist in this region. It is then an easy matter to use the functional equation (B.3) to find all zeros of the zeta function with real part less than 0 (it turns out they are exactly the values $-2n$, for n a positive integer). However, for values of s with real part between 0 and 1, the situation is quite different, since we have neither a series definition nor a functional equation to fall back upon; and indeed to this day very little is known about the behavior of the zeta function inside this critical strip of the complex plane.

[1] In the case of arithmetic progressions, one also needs to examine the closely related Dirichlet L–functions in addition to the zeta function itself.

It is known that the prime number theorem is equivalent to the assertion that the zeta function has no zeros s with $\Re(s) = 0$ or $\Re(s) = 1$.

The celebrated *Riemann hypothesis* asserts that all nontrivial zeros s of the zeta function satisfy the much more precise equation $\Re(s) = 1/2$.

The generalized Riemann hypothesis

The *Dirichlet L-series* associated to a Dirichlet character χ is the series

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

It converges absolutely and uniformly in the domain $\Re(s) \geq 1 + \delta$ for any positive δ, and admits the Euler product identity

$$L(\chi, s) = \prod_{p} \frac{1}{1 - \chi(p)p^{-s}}$$

where the product is over all primes p, by virtue of the multiplicativity of χ. In the case where $\chi = \chi_0$ is the trivial character mod m, we have

$$L(\chi_0, s) = \zeta(s) \prod_{p|m} (1 - p^{-s}),$$

where $\zeta(s)$ is the Riemann Zeta function.

Therefore, the Generalized Riemann Hypothesis (GRH), as its name indicates, generalizes the Riemann hypothesis which can be stated as,
neither the Riemann zeta nor any Dirichlet L series has a zero with real part of s larger than $1/2$.

If this hypothesis were true, it would have profound consequences on many mathematical problems like the distribution of primes in the arithmetic progression, Hooley's approach to Artin's conjecture and Weinberger's Euclidean problem.

B.2 Algebraic Number Fields

Definition B.5. (Number Field And Degree) An algebraic number field or a number field K is a subfield of the complex numbers, $\mathbb{C}$ which is a finite extension of the rational numbers, $\mathbb{Q}$. The degree n of this field extension , usually denoted by $|K : \mathbb{Q}|$ is its dimension when viewed as a $\mathbb{Q}$ vector space.

Based on this positive integral value of the degree, number fields can be categorized in to quadratic, cubic, quartic, quintic, etc. corresponding to degree 2, 3, 4, 5, etc. respectively.

Definition B.6. (Roots of Unity) A *root of unity* is a number ω such that some power ω^n, where n is a positive integer, equals to 1.

Specifically, if K is a field, then the nth roots of unity in K are the numbers ω in K such that $\omega^n = 1$. Equivalently, they are all the roots of the polynomial $X^n - 1$. No matter what field K is, the polynomial can never have more than n roots. Clearly 1 is an example; if n is even, then -1 will also be an example. Beyond this, the list of possibilities depends on K.

- If K is the set of real numbers, then 1 and -1 are the only possibilities.

- If K is the field of the complex numbers, the fundamental theorem of algebra assures us that the polynomial $X^n - 1$ has exactly n roots (counting multiplicities). Comparing $X^n - 1$ with its formal derivative, nX^{n-1}, we see that they are coprime, and therefore all the roots of $X^n - 1$ are distinct. That is, there exist n distinct complex numbers ω such that $\omega^n = 1$.

  If $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$, then all the nth roots of unity are: $\zeta^k = e^{2\pi ki/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$ for $k = 1, 2, \ldots, n$.

  If drawn on the complex plane, the nth roots of unity are the vertices of a regular n-gon centered at the origin and with a vertex at 1.

- If K is a finite field having p^a elements, for p a prime, then *every* nonzero element is a $p^a - 1$th root of unity (in fact this characterizes them completely; this is the role of the Frobenius operator). For other n, the answer is more complicated. For example, if n is divisible by p, the formal derivative of $X^n - 1$ is nX^{n-1}, which is zero since the characteristic of K is p and n is zero modulo p. So one is not guaranteed that the roots of unity will be distinct. For example, in the field of two elements, $1 = -1$, so there is only one square root of 1.

If an element ω is an nth root of unity but is not an mth root of unity for any $0 < m < n$, then ω is called a primitive nth root of unity. For example, the number ζ defined above is a primitive nth root of unity. If $\omega \in \mathbb{C}$ is a primitive nth root of unity, then all of the primitive nth roots of unity have the form ω^m for some $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$.

Definition B.7. (Cyclotomic Field) Let K be a field and let $\bar{K}$ be a fixed algebraic closure of K. A cyclotomic extension of K is an extension field of the form $K(\zeta)$ where $\zeta \in \bar{K}$ is a root of unity.

A *cyclotomic field* (or *cyclotomic number field*) is a cyclotomic extension of $\mathbb{Q}$. These are all of the form $\mathbb{Q}(\omega_n)$, where ω_n is a primitive nth root of unity.

Given a primitive nth root of unity ω_n, its minimal polynomial over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_n(x) = \prod_\omega (x - \omega)$. Thus, $[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \varphi(n)$, where φ denotes the Euler phi function.

Remark B.8. If n is a positive integer and m is an integer such that $\gcd(m, n) = 1$, then ω_n and ${\omega_n}^m$ are primitive nth roots of unity and generate the same cyclotomic field.

Definition B.9. (Ring of Integers) Let K be a number field. The ring of integers of K, usually denoted by $\mathcal{O}_K$, is the set of all elements $\alpha \in K$ which are roots of some monic polynomial with coefficients in $\mathbb{Z}$, i.e. those $\alpha \in K$ which are integral over $\mathbb{Z}$ i.e., $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

The only rational numbers which are roots of monic polynomials with integer coefficients are the integers themselves. Thus, the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Let $\mathcal{O}_K$ denote the ring of integers of $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. Then:

$$\mathcal{O}_K \cong \begin{cases} \mathbb{Z} \oplus \frac{1+\sqrt{d}}{2}\mathbb{Z}, & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z} \oplus \sqrt{d}\,\mathbb{Z}, & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

In other words, if we let

$$\alpha = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \mod 4, \\ \sqrt{d}, & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

then

$$\mathcal{O}_K = \{n + m\alpha : n, m \in \mathbb{Z}\}.$$

For $K = \mathbb{Q}(\zeta_n)$ a cyclotomic extension of $\mathbb{Q}$, where ζ_n is a primitive nth root of unity, the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, i.e.

$$\mathcal{O}_K = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \ldots + a_{n-1}\zeta_n^{n-1} : a_i \in \mathbb{Z}\}.$$

Definition B.10. (Norm And Trace) Let $|K : \mathbb{Q}| = n$ be the degree of K or equivalently the number of automorphisms, σ of K in the Galois group Gal(K/$\mathbb{Q}$) that fix rational numbers. The norm $N_{K/\mathbb{Q}}(\alpha)$ and trace $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}$ of an element α in K are rational numbers defined as,

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma\in\ \mathrm{Gal(K/\mathbb{Q})}} \sigma(\alpha) \quad \text{and} \quad \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(\alpha) = \sum_{\sigma\in\mathrm{Gal(K/\mathbb{Q})}} \sigma(\alpha)$$

Specifically if we take an element $q \in \mathbb{Q}$, since all the automorphisms fix rational numbers, we will have

$$N_{K/\mathbb{Q}}(\alpha) = q^n \quad \text{and} \quad \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(\alpha) = \mathrm{nq}$$

Here we note that norm and trace are multiplicative.

Definition B.11. (Congruency In Modular Ideal) Let α and β be algebraic integers in an algebraic number field K and $\mathfrak{m}$ a non-zero ideal in the ring of integers of K. We say that α and β are *congruent modulo the ideal* $\mathfrak{m}$ in the case that $\alpha-\beta \in \mathfrak{m}$. This is denoted by

$$\alpha \equiv \beta \pmod{\mathfrak{m}}.$$

This congruence relation divides the ring of integers of K into equivalence classes, which are called the *residue classes modulo the ideal* $\mathfrak{m}$.

Definition B.12. (Norm of Ideal) Let K be an algebraic number field and $\mathfrak{a}$ a non-zero ideal in K. The absolute norm of ideal $\mathfrak{a}$ means the number of all distinct residue classes modulo $\mathfrak{a}$.

Remark B.13. The norm of an ideal $\mathfrak{a}$ of K is finite; and satisfies:

- $N(\mathfrak{ab}) = N(\mathfrak{a})\cdot N(\mathfrak{b})$
- $N(\mathfrak{a}) = 1 \quad \Leftrightarrow \quad \mathfrak{a} = (1)$
- $N((\alpha)) = |N(\alpha)|$
- $N(\mathfrak{a}) \in \mathfrak{a}$
- If $N(\mathfrak{p})$ is a rational prime, then $\mathfrak{p}$ is a prime ideal.

Definition B.14. (Discriminant) Let $\{v_1, v_2, \ldots, v_n\}$ be an integral basis of $\mathcal{O}_K$, basis as $\mathbb{Z}$ module and let $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be the set of embeddings of K in $\mathbb{C}$. Then the discriminant of K, denoted by Δ_K, is defined to be the

square of the determinant of $n \times n$ matrix M such that $m_{i,j} = \sigma_i(v_j)$

$$\Delta_K = \det^2 \begin{pmatrix} \sigma_1(v_1) & \sigma_1(v_2) & \dots & \sigma_1(v_n) \\ \sigma_2(v_1) & \sigma_2(v_2) & \dots & \sigma_2(v_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(v_1) & \sigma_n(v_2) & \dots & \sigma_n(v_n) \end{pmatrix}$$

- **Quadratic number field:** If d be a square free integer, then the discriminant of $K = \mathbb{Q}(\sqrt{d})$ is given by,

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \equiv 2, 3 \mod 4 \end{cases}$$

- **Cyclotomic number field:** If $\phi(m)$ is the Euler's totient function, the discriminant of the m^{th} cyclotomic field $K_m = \mathbb{Q}(\zeta_m)$ is given as,

$$\Delta_{K_m} = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}$$

Definition B.15. (Real and Complex Embedding) Since any algebraic number field K is a subfield of $\mathbb{C}$, its embedding in $\mathbb{C}$ can be discussed in two categories.

1. A real embedding of L is an injective field homomorphism

$$\sigma \colon L \hookrightarrow \mathbb{R}$$

2. An imaginary or a complex embedding of L is an injective field homomorphism

$$\tau \colon L \hookrightarrow \mathbb{C}$$

such that $\tau(L) \nsubseteq \mathbb{R}$.

3. We denote Σ_L the set of all embeddings, real and complex, of L in $\mathbb{C}$ (note that all of them must fix $\mathbb{Q}$, since they are field homomorphisms).

We note that if σ is a real embedding then $\bar{\sigma} = \sigma$, where $\bar{\cdot}$ denotes the complex conjugation automorphism:

$$\bar{\cdot} \colon \mathbb{C} \to \mathbb{C} \quad \text{where } (\overline{a + bi}) = a - bi$$

On the other hand, if τ is a complex embedding, then $\bar{\tau}$ is another complex embedding, so the complex embeddings always come in pairs $\{\tau, \bar{\tau}\}$.

Let $K \subseteq L$ be another subfield of $\mathbb{C}$. Moreover, assume that $[L : K]$ is finite (this is the dimension of L as a vector space over K). We are interested in the embeddings of L that fix K pointwise, i.e. embeddings $\psi \colon L \hookrightarrow \mathbb{C}$ such that

$$\psi(k) = k, \quad \forall k \in K$$

For any embedding ψ of K in $\mathbb{C}$, there are exactly $[L : K]$ embeddings of L such that they extend ψ. In other words, if φ is one of them, then

$$\varphi(k) = \psi(k), \quad \forall k \in K$$

Thus, by taking Id_K, there are exactly $[L : K]$ embeddings of L which fix K pointwise.

Hence we know that the order of Σ_L is $[L : \mathbb{Q}]$. The number $n = [L : \mathbb{Q}]$ is usually decomposed as

$$[L : \mathbb{Q}] = r_1 + 2r_2$$

where r_1 is the number of embeddings which are real, and $2r_2$ is the number of complex embeddings appearing in pairs, one being the conjugate of the other.

Ring of integers as Dedekind domain

The ring $\mathcal{O}_K$ of an algebraic number field K is Dedekind domain. i.e

1. It is Noetherian.
2. Every non zero prime ideal is maximal.
3. It is integrally closed.

Consequently, it has a lot of interesting attributed properties. Some of them are just the analogous notions to elementary properties of integers. Let us mention some of them as follows:

- Every non trivial ideal can be represented as a product of prime ideals; furthermore, this product is unique up to reordering if $\mathcal{O}_K$ is principal ideal domain (PID)
- An ideal $\mathbf{a}$ is divisible by an ideal $\mathbf{b}$ if there exist a suitable ideal $\mathbf{c}$ such that $\mathbf{a} = \mathbf{bc}$. In particular, in $\mathcal{O}_K$, this happens if $\mathbf{a} \subseteq \mathbf{b}$.
- Every principal fractional ideal is invertible and the set of all invertible fractional ideals forms a group under multiplication.

- If $\mathbf{a} = \prod_{\mathbf{p}} \mathbf{p}^{\nu_{\mathbf{a}}(\mathbf{p})}$ and $\mathbf{b} = \prod_{\mathbf{p}} \mathbf{p}^{\nu_{\mathbf{b}}(\mathbf{p})}$. Then
  - Their product $\mathbf{ab}$ is given as, $\mathbf{ab} = \prod_{\mathbf{p}} \mathbf{p}^{\nu_{\mathbf{a}}(\mathbf{p})+\nu_{\mathbf{b}}(\mathbf{p})}$
  - Their *gcd*, $(\mathbf{a}, \mathbf{b})$ is given as, $(\mathbf{a}, \mathbf{b}) = \prod_{\mathbf{p}} \mathbf{p}^{\min\{\nu_{\mathbf{a}}(\mathbf{p}),\nu_{\mathbf{b}}(\mathbf{p})}$
  - Their *lcm*, $[\mathbf{a}, \mathbf{b}]$ is given as, $[\mathbf{a}, \mathbf{b}] = \prod_{\mathbf{p}} \mathbf{p}^{\max\{\nu_{\mathbf{a}}(\mathbf{p}),\nu_{\mathbf{b}}(\mathbf{p})}$
  - $\mathbf{a} \cdot \mathbf{b} = (\mathbf{a}, \mathbf{b})[\mathbf{a}, \mathbf{b}]$

.

Definition B.16. (Unit Group and Torsion Subgroup) The group of units or simply the unit group associated to a number field K, denoted by $\mathcal{O}_K^\times$ is a multiplicative group of elements of $\mathcal{O}_K$, its ring of integers, that have multiplicative inverses in $\mathcal{O}_K$ itself. The corresponding torsion subgroup of $\mathcal{O}_K^\times$ is defined as $\mathrm{Tor}(\mathcal{O}_K^\times) = \{u \in \mathcal{O}_K^\times : u^n = 1 \text{ for some } n \in \mathbb{N}\}$

Theorem B.17. *(Dirichlet) The group $\mathcal{O}_K^\times$ is a product of finite cyclic group of rank $r = r_1 + r_2 - 1$, called the unit rank where r_1 and r_2 are the number of real and pairs of imaginary embeddings.*
An element of $\mathcal{O}_K$ is a unit if and only if the absolute value of its norm is 1.

Definition B.18. (Fundamental Units) The finite subset $H = \{\eta_1, \eta_2, \ldots, \eta_t\}$ of $\mathcal{O}_K$ is called the set of its fundamental units if every unit ε of $\mathcal{O}_K$ is a power product of elements of H, multiplied by a root of unity:

$$\varepsilon = \zeta \cdot \eta_1^{k_1} \eta_2^{k_2} \ldots \eta_t^{k_t}$$

Conversely, every such element ε of the field is a unit of R.

Dirichlet's unit theorem gives all units of an algebraic number field $K = \mathbb{Q}(\alpha)$ i.e. its ring of integers, in the unique form

$$\varepsilon = \zeta^n \eta_1^{k_1} \eta_2^{k_2} \ldots \eta_t^{k_t},$$

where ζ is a primitive w^{th} root of unity in $\mathbb{Q}(\alpha)$, the η_j's are the fundamental units of $\mathbb{Q}(\alpha)$, $0 \leqq n \leqq w-1$, $k_j \in \mathbb{Z}\ \forall j$, $t = r+s-1$.

- The case of a real quadratic field $\mathbb{Q}(\sqrt{m})$, the square-free $m > 1$: $r = 2,\ s = 0,\ t = r+s-1 = 1$. So we obtain

  $$\varepsilon = \zeta^n \eta^k = \pm \eta^k,$$

  because $\zeta = -1$ is the only real primitive root of unity ($w = 2$). Thus, every real quadratic field has infinitely many units and a unique fundamental unit η.

  For example: If $m = 3$, then $\eta = 2+\sqrt{3}$;

- The case of any imaginary quadratic field $\mathbb{Q}(\alpha)$; here $\alpha = \sqrt{m}$, the square-free $m < 0$: The conjugates of α are the pure imaginary numbers $\pm\sqrt{m}$, hence $r = 0,\ 2s = 2,\ t = r+s-1 = 0$. Thus we see that all units are

$$\varepsilon = \zeta^n.$$

1) $m = -1$. The field contains the primitive fourth root of unity, e.g. i, and therefore all units in the Gaussian field $\mathbb{Q}(i)$ are i^n, where $n = 0,\ 1,\ 2,\ 3$.

2) $m = -3$. The field in question is a cyclotomic field containing the primitive third root of unity and also the primitive sixth root of unity, namely

$$\zeta = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6};$$

hence all units are $\varepsilon = (\frac{1+\sqrt{-3}}{2})^n$, where $n = 0,\ 1,\ \ldots,\ 5$, or, equivalently, $\varepsilon = \pm(\frac{-1+\sqrt{-3}}{2})^n$, where $n = 0,\ 1,\ 2$.

Definition B.19. (Möbius function) Möbius function, denoted by μ, is a multiplicative function defined for all positive integers n to have values -1, 0 or 1 depending of the factorization property of the given integer. It is defined as,

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1. \\ 0 & \text{if } n \text{ is not square-free} \\ (-1)^r & \text{if n is square free with r distinct prime factors.} \end{cases}$$

Definition B.20. (Decomposition Group) Let A be a Noetherian integrally closed integral domain with field of fractions K. Let L be a Galois extension of K and denote by B the integral closure of A in L. Then, for any prime ideal $\mathfrak{p} \subset A$, the Galois group $G := \mathrm{Gal(L/K)}$ acts transitively on the set of all prime ideals $\mathfrak{P} \subset B$ containing $\mathfrak{p}$. If we fix a particular prime ideal $\mathfrak{P} \subset B$ lying over $\mathfrak{p}$, then the stabilizer of $\mathfrak{P}$ under this group action is a subgroup of G, called the *decomposition group* at $\mathfrak{P}$ and denoted $D(\mathfrak{P}/\mathfrak{p})$. In other words,

$$D(\mathfrak{P}/\mathfrak{p}) := \{\sigma \in G \mid \sigma(\mathfrak{P}) = (\mathfrak{P})\}.$$

If $\mathfrak{P}' \subset B$ is another prime ideal of B lying over $\mathfrak{p}$, then the decomposition groups $D(\mathfrak{P}/\mathfrak{p})$ and $D(\mathfrak{P}'/\mathfrak{p})$ are conjugate in G via any Galois automorphism mapping $\mathfrak{P}$ to $\mathfrak{P}'$.

Definition B.21. (Inertia Group) Write l for the residue field $B/\mathfrak{P}$ and k for the residue field $A/\mathfrak{p}$. Assume that the extension l/k is separable. Any

element $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, by definition, fixes $\mathfrak{P}$ and hence descends to a well defined automorphism of the field l. Since σ also fixes A by virtue of being in G, it induces an automorphism of the extension l/k fixing k. We therefore have a group homomorphism

$$D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \text{Gal(l/k)},$$

and the $\mathfrak{P}$ kernel of this homomorphism is called the inertia group of $\mathfrak{P}$, and written $T(\mathfrak{P}/\mathfrak{p})$. It turns out that this homomorphism is actually surjective so that there is an exact sequence

$$1 \longrightarrow T(\mathfrak{P}/\mathfrak{p}) \longrightarrow D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \text{Gal(l/k)} \longrightarrow 1$$

Definition B.22. (Artin Symbol) Let L/K be a Galois extension of number fields, with rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. For any finite prime $\mathfrak{P} \subset L$ lying over a prime $\mathfrak{p} \in K$, let $D(\mathfrak{P})$ denote the decomposition group of $\mathfrak{P}$, let $T(\mathfrak{P})$ denote the inertia group of $\mathfrak{P}$, and let $l := \mathcal{O}_L/\mathfrak{P}$ and $k := \mathcal{O}_K/\mathfrak{p}$ be the residue fields. The exact sequence

$$1 \longrightarrow T(\mathfrak{P}) \longrightarrow D(\mathfrak{P}) \longrightarrow \text{Gal(l/k)} \longrightarrow 1$$

yields an isomorphism $D(\mathfrak{P})/T(\mathfrak{P}) \cong \text{Gal(l/k)}$. In particular, there is a unique element in $D(\mathfrak{P})/T(\mathfrak{P})$, denoted $[\mathfrak{P}, L/K]$, which maps to the q^{th} power Frobenius map $Frob_q \in \text{Gal(l/k)}$ under this isomorphism (where q is the number of elements in k). The notation $[\mathfrak{P}, L/K,]$ is referred to as the Artin symbol of the extension L/K at $\mathfrak{P}$.

Definition B.23. (Conductor) Let L/K be a finite abelian extension of number fields, and let $\mathcal{O}_K$ be the ring of integers of K. There exists an integral ideal $\mathcal{C} \subset \mathcal{O}_K$, divisible by precisely the prime ideals of K that ramify in L, such that

$$((\alpha), L/K) = 1, \quad \forall \alpha \in K^*,\ \alpha \equiv 1 \mod \mathcal{C}$$

where $((\alpha), L/K)$ is the Artin map.
The largest one of those type of ideals of $\mathcal{O}_K$ is termed as the conductor of the finite abelian extension L/K.
Here Comparison is made possible due to existence mentioned above. Indeed, if two ideals $\mathcal{C}, \mathcal{C}'$ satisfy the given property, so does their sum $\mathcal{C} + \mathcal{C}'$
More precisely, If $L = K(\theta)$ is a finite abelian extension of the number field K with θ primitive element, then the conductor is given as,

$$\mathfrak{f} = \{x \in L : x\mathcal{O}' \subset \mathcal{O}[\theta]\}$$

where $\mathcal{O}$ is a valuation ring of K , where as $\mathcal{O}'$ is its integral closure in L

B.3 A Little On Packing Theory

This section is to briefly highlight the concept of packing as it has important application to design a criterion for checking if a number field is Euclidean.

Definition B.24. The following are some definitions and brief notions.

- Let $U \subseteq \mathbb{R}^n$ be a set with finite positive Lebesgue measure $\mu(U)$. Given a sequence $\{a_k\}_{k\in I}$ of points of $\mathbb{R}^n$, the system of translates of U, denoted by $\mathbf{U}$, is defined relative to the terms of the sequence as

$$\mathbf{U} = \{S : S = U + a_k, \quad k \in I\}$$

- A sequence of subsets of $\mathbb{R}^n$, S_1, S_2 ..., is said to form a packing if $S_i \cap S_j = \varnothing$ for every $i \neq j$

- Let $C \subseteq \mathbb{R}^n$ be a half-open, half-closed cube of side length s, centered at the point $x = (x_1, \ldots, x_n)$, i.e.

$$C = \{(y_1, \ldots, y_n) : y_i - s/2 \leq x_i < y_i + s/2 \quad \forall i\}$$

  and let $\mathbf{U}$ be a system of translates of some Lebesgue measurable set U with some Lebesgue measure μ relative to some sequence, say $\{a_i\}_{i\in I}$, then the corresponding upper and lower densities with respect to the given cube C, denoted by $\rho_+(\mathbf{U}, C)$ and $\rho_-(\mathbf{U}, C)$, are defined as follows,

$$\rho_+(\mathbf{U}, C) = \frac{1}{\mu(C)} \sum_{(U+a_i)\cap C\neq\varnothing} \mu(U+a_i) \quad \text{and} \quad \rho_-(\mathbf{U}, C) = \frac{1}{\mu(C)} \sum_{(U+a_i)\subseteq C} \mu(U+a_i)$$

  In general terms, these densities of $\mathbf{U}$, are defined as

$$\rho_+(\mathbf{U}) = \lim_{s(C)\to\infty} \sup \rho_+(\mathbf{U}, C) \quad \text{and} \quad \rho_-(\mathbf{U}) = \lim_{s(C)\to\infty} \inf \rho_-(\mathbf{U}, C)$$

  Note that $\rho_-(\mathbf{U}) \leq \rho_+(\mathbf{U})$

- Let U be as used above and D be the set of systems of translates $\mathbf{U}$ of U such that $\rho_+(\mathbf{U}) < \infty$. If $D' \subseteq D$ is the set of systems of translates which form packings in to U, then the packing density, denoted by $\delta(U) = \sup_{\mathbf{U}\in D'} \rho_+(\mathbf{U})$. If moreover μ is a Lebesgue measure, the center packing constant of U, denoted $\delta^*(U)$, is the ratio of its packing density to its Lebesgue measure. i.e.

$$\delta^*(U) = \delta(U)/\mu(U)$$

Proposition B.25. *Let U a subset of $\mathbb{R}^n$ and $\mathbf{U}$ a system of translates of U be given as above. If $\mathbf{U}$ forms a packing, then $\rho_+(U) \leq 1$*

Proof. Let U be contained in some cube of side length $s(U)$. Let a cube C, whose side length is $s(C)$, is centered at arbitrarily chosen $x \in \mathbb{R}^n$. Then all the translates $U + a_i$'s that intersect C lie in the cube C', where C' is a cube centered at x with side length $s(C) + 2s(U)$. Since $\mathbf{U}$ is a packing, the sets $U + a_i$ and $U + a_j$ are mutually disjoint as far as $i \neq j$. It then follows that,

$$\sum_{(U+a_i)\cap C \neq \varnothing} \mu(U + a_i) \leq [s(C) + 2s(U)]^n$$

Dividing both sides by $\mu(C) = [s(C)]^n$ results in

$$\rho_+(\mathbf{U}, C) \leq [1 + 2s(U)/s(C)]^n \Rightarrow \rho_+(\mathbf{U}) \leq \lim_{s(C)\to\infty} \sup[1 + 2s(U)/s(C)]^n = 1$$

□

Corollary B.26. *With U and $\mathbf{U}$ as in the proposition, $\delta(U) \leq 1$*

Finally let us state below the main proposition in this section without proof.

Proposition B.27. *Let $U \subseteq \mathbb{R}^n$ be a bounded set with positive Lebesgue measure, and let $C \subseteq \mathbb{R}^n$ be a closed cube with edges in the directions parallel to the basis vectors; let T be a non-singular affine transformation. Let $a_1, \ldots, a_m$ be any points in $\mathbb{R}^n$ and $b_1, b_2, \ldots$ be any enumeration of the lattice $[s(C)\mathbb{Z}]^n \subseteq \mathbb{R}^n$. For $i = 1, 2 \ldots m$ and $j = 1, 2 \ldots$, if $\mathbf{K}$ and $T\mathbf{K}$ denote*

$$K = \{U + a_i + b_j\} \quad \text{and } \{T(U + a_i + b_j)\}$$

then

$$\rho_+(\mathbf{K}) = \rho_+(T\mathbf{K}) = \rho_-(\mathbf{K}) = \rho_-(T\mathbf{K}) = m\mu(U)/\mu(C)$$

Bibliography

[1] R. Akhtar, Cyclotomic Euclidean number fields, thesis (1995)

[2] E.S. Barnes and H.P.F Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms I, *Acta Mathematica* **87** (1952), 259-323, The inhomogeneous minima of binary quadratic forms II, *Acta Mathematica* **88** (1952), 279-316.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer, On the inhomogeneous minimum of the product of n linear forms. *Mathematika* **3** (1956), 25-39.

[4] J.-P. Cerri, De l'Euclidianité de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ et $\mathbb{Q}\Big(\sqrt{2+\sqrt{2+\sqrt{2}}}\Big)$ pour la norme, *Journal de Théorie des Nombres de Bordeaux* **12** (2000), 103-126.

[5] J.-P. Cerri, Euclidean minima of totally real number fields: Algorithmic determination, *Mathematics of Computation* **76** (2007), 1547-1575.

[6] J.-P. Cerri, Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1, *J. Reine Angew. Math.* **592** (2006), 49-62

[7] J.-P. Cerri, Spectres Euclidiens et inhomogènes des corps de nombres, Thèse Université de Nancy 1 (2005).

[8] J. W. S. Cassels, The inhomogeneous minima of binary quadratic, ternary cubic, and quaternary quartic forms, *Proc. Cambridge Phil. Soc.* **48** (1952), 72-86

[9] V. Cioffari, The Euclidean condition in pure cubic and complex quartic fields, *Math. Comp.* **33** (1979), 389-398

[10] D. A. Clark, On k-stage Euclidean Algorithms for Galois extensions of $\mathbf{Q}$, *Manuscripta Math.* **90** (1996), 149-153

[11] D. A. Clark, The Euclidean algorithm for Galois extensions of the rational numbers, Ph. D. thesis, McGill University, Montreal (1992)

[12] D. A. Clark and M. R. Murty, The Euclidean Algorithm in Galois Extensions of **Q**, *J. Reine Angew. Math.* **459** (1995), 151-162

[13] G.E. Cooke, P and J. Weinberger, On the construction of Division Chains in Algebraic Number Rings, with Applications to SL_2, *Commun. Algebra* **3** (1975), 481–524.

[14] G. Cooke, The weakening of the Euclidean property for integral domains and application to algebraic number theory I, II, *J. Reine Angew. Math.* **282, 283** resp. (1976, 1977 resp.), 133-156, 71-85 resp.

[15] H. Davenport, A simple proof of Remaks theorem on the product of three linear forms, *J. London Math. Soc.* **14** (1939) 47-51.

[16] H. Davenport, Euclid's algorithm in certain quartic fields, *Trans. Amer. Math. Soc.* **68** (1950), 508-532.

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

[18] Eva Bayer-Fluckiger, JeanPaul Cerri and Jerome Chaubert, Euclidean minima and central division algebras

[19] Eva Bayer-Fluckiger and Gabriele Nebe, On the Euclidean Minimum of some real number fields,*Journal de theorie des nombres de Bordeaux* **17** (2005), 437-454

[20] Eva Bayer-Fluckiger, Upper bounds for Euclidean minima of algebraic number elds, *Journal of Number Theory* **121** (2006), 305-323

[21] H.J. Godwin, On the inhomogeneous minima of certain norm-forms, *J. London Math. Soc.* **30** (1955), 114-119.

[22] R. Gupta, M. Murty, V. Murty, The Euclidean algorithm for S-integers, *Canad. Math. Soc. Conference Proc.* **7** (1987), 189-201

[23] R.J. Hans-Gill, M. Raka and R. Sehmi, On conjectures of Minkowski and Woods for n = 7, *Journal of Number Theory* **129** (2009) 1011-1033

[24] M. Harper, $\mathbb{Z}[\sqrt{14}]$ is Euclidean, *Canad. J. Math. Vol.* **56** (1), (2004) 55-70

[25] M. Harper, R. Murty, Euclidean rings of algebraic integers, Canad. *J. Math. Vol.* **56** (1), (2004), 71-76

[26] H. Heilbronn, On Euclids algorithm in real quadratic fields, *Proc. Cambridge Phil. Soc.* **34** (1938), 521-526

[27] C. Hooley, On Artin's conjecture. *J. reine angew. Math,* **225** (1967) 209-220

[28] A. Korkine and G. Zolotareff, Sur les formes quadratiques, *Math. Ann.* **6** (1873) 366-389;

[29] A. Korkine and G. Zolotareff, Sur les formes quadratiques positives, *Math. Ann.* **11** (1877) 242-292.

[30] F. Lemmermayer, Euclids algorithm in quartic CM-fields, *preprint*

[31] F. Lemmermeyer, Euklidische Ringe, Diplomarbeit, Heidelberg 1989

[32] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Expositiones Mathematicae* (1995), 385-416.

[33] H.W. Lenstra Jr., Euclidean number fields 1, 2 and 3 , The Mathematical Intelligencer, *Springer-Verlag* (1979, 1980, 1980 resp.), 6-15; 73-77; 99-103 resp.

[34] H.W Lenstra, Jr., Euclidean number fields of large degree, *Inventiones math.* **38**, (1977) 237-254

[35] H. W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, *J. London Math. Soc.* **10** (1975), 457-465

[36] K. Mahler, On a property of positive definite ternary quadratic forms, *J. London Math. Soc.* (2) **15** (1940) 305-320

[37] J. M. Masley, H. L. Montgomery, Cyclotomic fields with unique factorization, *Reine Angew Math.* **286/287**(1976), 248-256

[38] C.T. McMullen, Minkowskis conjecture, well-rounded lattices and topological dimension, *J. Amer. Math. Soc.* **18** (2005), 711-734

[39] T. Motzkin, The Euclidean algorithm, *Bull. Am. Math. Soc.* **55** (1949), 1142-1146

[40] G. Niklasch and R. Quême, An improvement of Lenstra's criterion for Euclidean number fields: The totally real case, *Acta Arith.* **58** (1991), 157-168

[41] R. Remak Verallgemeinerung eines Minkowskischen Satzes, *Math. Z.* **17** (1923) 1-34, *Math. Z.* **18** (1923) 173-200.

[42] J. R. Smith, On Euclids algorithm in some cyclic cubic fields, *J. London Math. Soc.* **44** (1969), 577-582

[43] H. P. F. Swinnerton-Dyer, The inhomogeneous minima of complex cubic norm forms, *Proc. Cambridge Phil. Soc.* **50** (1954), 209-219

[44] F. J. van der Linden, Euclidean rings with two infinite primes, Ph.D. thesis, *Univ. Amsterdam* (1984)

[45] P. J. Weinberger, On Euclidean rings of algebraic integers, *Proc. Symp. Pure Math.* **24** Analytic number theory, AMS, (1973), 321-332

[46] A.C. Woods, The densest double lattice packing of four spheres, *Mathematika* **12** (1965) 138-142.

[47] A.C. Woods, Lattice coverings of five space by spheres, *Mathematika* **12** (1965) 143-150.

[48] A.C. Woods, Covering six space with spheres, *J. Number Theory* **4** (1972) 157-180.

Reference Books

[49] S. Alaca and K.S. Williams, Introductory algebraic number theory, Cambridge University Press (2004)

[50] E. Artin and J. Tate, Class field theory, notes of a Seminar at Princeton, AMS (1990)

[51] Z.I. Borevich and I.R. Shafarevich, Number Theory, Academic Press (1966)

[52] J.W.S. Cassels and A. Fröhlich, Algebraic number theory, Academic Press (1967)

[53] A. Fröhlich and M.J. Taylor, Algebraic number theory, Cambridge University Press (1993)

[54] H. Hardy and M. Wright, An introduction to the theory of numbers, Fifth edition, (1979)

[55] K. Ireland and M. Rosen, A classical introduction to modern number theory, Second Edition, Springer (1990)

[56] G.J. Janusz, Algebraic number fields, Second Edition, Academic Press (1996)

[57] N. Kobliz, A course in number theory and cryptography, Second Edition, Springer (1994)

[58] S. Lang, Algebraic number theory, Second Edition, Springer (1994)

[59] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of applied cryptography, CRC Press (1997)

[60] J.S. Milne, Class field theory, Lecture note for Math 776 at University of Michigan (1997)

[61] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Third Edition Springer (2004)

[62] J-P. Serre, A course in arithmetic, Springer (1996)

[63] L.C. Washington, Introduction to cyclotomic fields, Second Edition, Springer (1982)