AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 4(1): 79–85.
DOI:10.3934/Math.2019.1.79
Received: 18 December 2018
Accepted: 09 January 2019
Published: 16 January 2019

Research article

On the gap between prime ideals

Tianyu Ni*

Mathematical College, Sichuan University, Chengdu 610064, China

* **Correspondence:** Email: 18691874630@163.com.

Abstract: We define a *gap* function to measure the difference of two distinct prime ideals in a given number field. In this paper, we determine all quadratic fields and cyclotomic fields satisfying the condition: There exist two distinct prime ideals whose gap is 1.

Keywords: ring of integers; quadratic field; cyclotomic field; prime gap; diophantine equations
Mathematics Subject Classification: 11R04, 11D99

1. Introduction

In the rational number field $\mathbb{Q}$, we say two prime numbers p, q have *gap* k if $p-q = \pm k$ for a positive integer k. Two prime numbers are called *twin primes* if and only if their gap is 2. Studying the pair of prime numbers of a given gap is a main subject in analytic number theory. In this paper, we generalize the definition of gap to a number field.

First, we define the gap function G_K in a number field K.

Definition 1.1. Let K be a number field, $\mathcal{O}_K$ the ring of integers in K, and $\mathrm{Spec}(\mathcal{O}_K)$ the set of prime ideals of $\mathcal{O}_K$. The gap function G_K for K is the map:

$$G_K : \mathrm{Spec}(\mathcal{O}_K) \times \mathrm{Spec}(\mathcal{O}_K) \to \mathbb{Z}\ ;\ G_K(\mathfrak{p}, \mathfrak{q}) = \mathbb{N}\mathfrak{p} - \mathbb{N}\mathfrak{q}$$

for $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_K)$, $\mathbb{N}\mathfrak{p} = (\mathcal{O}_K : \mathfrak{p})$ is the norm of $\mathfrak{p}$.

Then we consider the following questions:

Question 1: Given a number field K and a positive number N, do there exist infinitely many pairs of prime ideals such that their gap $G_K = N$?

Question 1 can be difficult even though $K = \mathbb{Q}$. For example, Question 1 becomes the *twin prime conjecture* when $K = \mathbb{Q}$ and $N = 2$. To study the above question, we first need to study the following question:

Question 2: Given a number field K and a positive number N, do there exist two distinct prime ideals such that their gap $G_K = N$?

Note that if $K = \mathbb{Q}, N = 1$, the only pair of prime numbers satisfying $G_{\mathbb{Q}} = 1$ is $(2, 3)$. However, when K is a number field and $K \neq \mathbb{Q}$, we will show that there may not exist two prime ideals whose gap is 1.

In this paper, we study a very special case of Question 2: K is a quadratic number field or cyclotomic field and $N = 1$. Moreover, we show that if K is a quadratic number field or cyclotomic field that has two distinct prime ideals of gap 1, then the number of such pairs of prime ideals is finite. Thus we give an answer to the Question 1 for a special case.

In particular, we prove the following two results:

Theorem 1.2. *Let $d \neq 1$ be a square-free integer, and K the quadratic field $\mathbb{Q}[\sqrt{d}]$. Then the pairs of prime ideals $\mathfrak{p}, \mathfrak{q}$ with gap 1 in K are as follows: let $\mathfrak{p} \cap \mathbb{Z} = (p), \mathfrak{q} \cap \mathbb{Z} = (q)$,*

1. *$p = 3$ and $q = 2$, where $d \equiv 1, 3, 6, 7, 9, 10 \bmod 12$;*
2. *$p = 5$ and $q = 2$, where $d \equiv 5, 21, 29 \bmod 40$.*

Theorem 1.3. *Let N be a positive integer ($N \neq 1, 2, 3, 4, 6$), K the cyclotomic field $\mathbb{Q}(\zeta_N)$, and O_K the ring of integers of K. Then there exist two distinct prime ideals $\mathfrak{p}, \mathfrak{q}$ of O_K such that $G_K(\mathfrak{p}, \mathfrak{q}) = 1$ if and only if $N = q, 2q$, where q is a Mersenne prime number and $q \neq 3$.*

The proofs of above results are given in section 3. The principal method here is to calculate the decomposition of the prime number in the quadratic field and the cyclotomic field. In section 4 we give several examples. Section 2 is a summary of some results from algebraic number theory which are used throughout the paper.

2. Preliminaries

In this section, we review all the facts we need in the rest of the paper. To study the gap between prime ideals for quadratic fields and cyclotomic fields, we need to know how the prime number p decomposes in their ring of integers.

Lemma 2.1. *Let $d \neq 1$ be a square-free integer, K the quadratic field $\mathbb{Q}[\sqrt{d}]$, $disc(O_K/\mathbb{Z})$ be the discriminant of K, and p an odd prime number. Then we have the following results.*

1. *If p divides $disc(O_K/\mathbb{Z})$, then (p) ramifies in O_K.*
2. *For p not dividing the d, we have*
   (p) is the product the two distinct ideals if and only if d is a square mod p.
   (p) is a prime ideals in $\mathbb{Q}[\sqrt{d}]$ if and only if d is not a square mod p.
3. *For the prime number 2 when $d \equiv 1 \bmod 4$, we have*
   (2) is the product the two distinct ideals in $\mathbb{Q}[\sqrt{d}]$ if and only if $d \equiv 1 \bmod 8$.
   (2) is a prime ideals in $\mathbb{Q}[\sqrt{d}]$ if and only if $d \equiv 5 \bmod 8$.

The proof of Lemma 2.1 can be found in [1].

Lemma 2.2. *Let $N = \Pi_p p^{v_p}$ be the prime factorization of the positive integer N, and let f_p be the smallest positive integer such that*

$$p^{f_p} \equiv 1 \bmod \frac{N}{p^{v_p}}$$

Then one has in the cyclotomic field $\mathbb{Q}(\zeta_N)$ the factorization

$$p = (\mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_r)^{\varphi(p^{v_p})}$$

where $\mathfrak{p}_1, \mathfrak{p}_2, ...\mathfrak{p}_r$ are distinct prime ideals, all of degree f_p.

The proof of Lemma 2.2 can be found in [2]. The following result helps us treat the case when K is a cyclotomic field. And the proof can be found in [3] and [4].

Theorem 2.3 (Mihăilescu)**.** *The only solutions of the equation*

$$x^a - y^b = 1$$

in integers $a, b \geq 2$ and non-zero integers x, y are given by $(\pm 3)^2 - 2^3 = 1$.

3. Proof of the main results

3.1. Proof of Theorem 1.2

Proof. Let $\mathfrak{p}, \mathfrak{q}$ be two distinct prime ideals in $K = \mathbb{Q}[\sqrt{d}]$. Then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$, where p, q are two prime numbers in $\mathbb{Z}$. Now we have

$$G_K(\mathfrak{p}, \mathfrak{q}) = \mathbb{N}\mathfrak{p} - \mathbb{N}\mathfrak{q} = p^{f_p} - q^{f_q}$$

where $f_p = (O_K : \mathfrak{p})$, $f_q = (O_K : \mathfrak{q})$ are the degree of residue fields. Note that the degree of field extension $[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2$ is divided by f_p and f_q, then f_p, f_q can only be 1 or 2. We suppose that $G_K(\mathfrak{p}, \mathfrak{q}) = p^{f_p} - q^{f_q} = 1$. Then

$$p = 3, q = 2, f_p = f_q = 1; p = 2, q = 3, f_p = 2, f_q = 1 \text{ or } p = 5, q = 2, f_p = 1, f_q = 2.$$

Let $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. We list all possible cases:

1. $p = 3, q = 2; f_p = f_q = 1$
   (a) Both 2 and 3 split in $\mathbb{Q}[\sqrt{d}]$. By Lemma 2.1, we have

   $$(\frac{d}{3}) = 1, d \equiv 1 \bmod 8$$

   Therefore $d \equiv 1 \bmod 24$.
   (b) 2 splits in $\mathbb{Q}[\sqrt{d}]$, 3 ramifies in $\mathbb{Q}[\sqrt{d}]$. Then

   $$d \equiv 1 \bmod 8, d \equiv 0 \bmod 3$$

   Therefore, $d \equiv 9 \bmod 24$.
   (c) Both 2 and 3 ramify in $\mathbb{Q}[\sqrt{d}]$. Then

   $$d \equiv 0 \bmod 3, d \equiv 2, 3 \bmod 4$$

   Therefore, $d \equiv 3, 6 \bmod 12$.

(d) 2 ramifies in $\mathbb{Q}[\sqrt{d}]$, 3 splits in $\mathbb{Q}[\sqrt{d}]$. Then

$$(\frac{d}{3}) = 1, d \equiv 2, 3 \bmod 4$$

Therefore, $d \equiv 7, 10 \bmod 12$.

2. $p = 2, q = 3; f_p = 2, f_q = 1$

(a) 2 is a prime ideal in $\mathbb{Q}[\sqrt{d}]$, 3 ramifies in $\mathbb{Q}[\sqrt{d}]$. Then

$$d \equiv 0 \bmod 3, d \equiv 5 \bmod 8$$

Therefore, $d \equiv 21 \bmod 24$.

(b) 2 is a prime ideal in $\mathbb{Q}[\sqrt{d}]$, 3 splits in $\mathbb{Q}[\sqrt{d}]$. Then

$$(\frac{d}{3}) = 1, d \equiv 5 \bmod 8$$

Therefore, $d \equiv 13 \bmod 24$.

3. $p = 5, q = 2; f_p = 1, f_q = 2$

(a) 2 is a prime ideal in $\mathbb{Q}[\sqrt{d}]$, 5 ramifies in $\mathbb{Q}[\sqrt{d}]$. Then

$$d \equiv 0 \bmod 5, d \equiv 5 \bmod 8$$

Therefore, $d \equiv 5 \bmod 40$.

(b) 2 is a prime ideal in $\mathbb{Q}[\sqrt{d}]$, 5 splits in $\mathbb{Q}[\sqrt{d}]$. Then

$$(\frac{d}{5}) = 1, d \equiv 5 \bmod 8$$

Therefore, $d \equiv 21, 29 \bmod 40$.

In summary, $d \equiv 1, 3, 6, 7, 9, 10 \bmod 12$, *or* $d \equiv 5, 21, 29 \bmod 40$.

□

3.2. Proof of Theorem 1.3

Proof. Let $N = \Pi_p p^{v_p}$ be the prime factorization of the positive integer N, $N \neq 1, 2, 3, 4, 6$. And let $\mathfrak{p}, \mathfrak{q}$ be two distinct prime ideals in $K = \mathbb{Q}(\zeta_N)$. Then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$, where p, q are two prime numbers in $\mathbb{Z}$. We suppose that:

$$G_K(\mathfrak{p}, \mathfrak{q}) = \mathbb{N}\mathfrak{p} - \mathbb{N}\mathfrak{q} = p^{f_p} - q^{f_q} = 1 \tag{3.1}$$

where f_p, f_q are the degree of residue fields.

1. $f_p, f_q > 1$: By Theorem 2.3, $p = 3, f_3 = 2; q = 2, f_2 = 3$. Lemma 2.2 implies that

$$3^2 \equiv 1 \bmod \frac{N}{3^{v_3}}, 2^3 \equiv 1 \bmod \frac{N}{2^{v_2}}$$

In other words, $\frac{N}{3^{v_3}} | 8$, $\frac{N}{2^{v_2}} | 7$. The second equation implies that $N = 2^{v_2} \cdot 7$ or 2^{v_2}.

(a) If $N = 2^{v_2}$: then $\frac{N}{3^{v_3}}|8$ implies that $v_3 = 0$ and $N = 2^{v_2}, v_2 \leq 3$. Then we have $v_2 = 1$, $N = 2$, $K = \mathbb{Q}$; $v_2 = 2$, $N = 4$, $K = \mathbb{Q}[\sqrt{-1}]$; $v_2 = 3$, $N = 8$, $K = \mathbb{Q}(\zeta_8)$. However, when $K = \mathbb{Q}(\zeta_8)$, 2 totally ramifies in K, $f_2 = 1 \neq 3$. So $K = \mathbb{Q}(\zeta_8)$ is impossible.

(b) If $N = 7 \cdot 2^{v_2}$: then $\frac{N}{3^{v_3}} = 7 \cdot 2^{v_2}$ doesn't divide 8. So $N = 7 \cdot 2^{v_2}$ is impossible.

Therefore, $f_p, f_q > 1$ is impossible.

2. $f_p = 1$: (3.1) becomes $p - q^{f_q} = 1$. Now $q^{f_q} + 1 = p$ is an odd prime number. Then $q = 2$, $f_2 = 2^n$ for some nonnegative integer n and p is a Fermat prime number. Lemma 2.2 implies that

$$p \equiv 1 \bmod \frac{N}{p^{v_p}}, 2^{2^n} \equiv 1 \bmod \frac{N}{2^{v_2}}$$

In other words, $\frac{N}{p^{v_p}}|(p-1)$ and $\frac{N}{2^{v_2}}|(p-2)$. Therefore, $N = 2^{v_2}$, 2 totally ramifies in K and $f_2 = 2^{2^n} = 1$. From $n = 0$, we obtain $p = 2^{2^n} + 1 = 2 + 1 = 3$, and $2^{v_2}|2$. So $N = 1, 2$.
Therefore, $f_p = 1$ is impossible.

3. $f_q = 1$: (3.1) becomes $2^{f_2} - q = 1$. Now $q = 2^{f_2} - 1$ is a Mersenne prime number. Again, Lemma 2.2 implies that

$$2^{f_2} \equiv 1 \bmod \frac{N}{2^{v_2}}, q \equiv 1 \bmod \frac{N}{q^{v_q}}$$

From the first equation, we obtain $N = 2^{v_2} q^{v_q}$. The second equation shows that $2^{v_2}|(2^{f_2} - 2)$. Note that $f_2 \neq 1$, otherwise $v_q = 0, v_2 = 0, 1$ and $N = 1, 2$. And $2^{f_2} - 2 = 2(2^{f_2-1} - 1)$, $2^{f_2-1} - 1$ is an odd number. Then

(a) If $v_2 = 0$: $N|(2^{f_2} - 1)$ implies that $N = q$. Now we show that f_2 is indeed the smallest positive integer such that

$$2^{f_2} \equiv 1 \bmod \frac{N}{2^{v_2}}$$

If there is a positive integer d, satisfying $d|f_2$ and $2^d \equiv 1 \bmod q$, then $2^d < 2^{f_2} = q + 1$, which leads to a contradiction. Therefore, $N = q$.

(b) If $v_2 = 1$: $\frac{N}{2}|(2^{f_2} - 1)$ implies that $N = 2q$. Similarly, f_2 is indeed the smallest positive integer such that

$$2^{f_2} \equiv 1 \bmod \frac{N}{2^{v_2}}$$

Therefore, $N = 2q$.

In summary, there exist two distinct prime ideals $\mathfrak{p}, \mathfrak{q}$ of O_K such that $G_K(\mathfrak{p}, \mathfrak{q}) = 1$ if and only if $N = q, 2q$, where q is a Mersenne prime number and $q \neq 3$. □

Remark 3.1. Let $K = \mathbb{Q}(\zeta_q)$ or $\mathbb{Q}(\zeta_{2q})$, where q is a Mersenne prime not equal to 3. According to the proof of Theorem 1.3, if $\mathfrak{p}$ and $\mathfrak{q}$ satisfy $G_K(\mathfrak{p}, \mathfrak{q}) = 1$, then $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$, $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$, and $q = 2^{f_2} - 1$ is a Mersenne prime. And let φ be the Euler's totient function. By Lemma 2.2, we have the following decomposition in O_K

$$(2) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_g, (q) = \mathfrak{q}^{q-1}$$

where g is determined by

$$g = \frac{\varphi(q)}{f_2} = \frac{\varphi(2q)}{f_2} = \frac{q-1}{f_2}$$

Let $A^K_{\mathfrak{p},\mathfrak{q}}$ be the set of pairs of prime ideals of *gap* 1, which is

$$A^K_{\mathfrak{p},\mathfrak{q}} = \{(\mathfrak{p},\mathfrak{q})|\mathfrak{p},\mathfrak{q} \text{ are prime ideals in } O_K, G_K(\mathfrak{p},\mathfrak{q}) = 1\}$$

Then the above discussion shows that $\#A^K_{\mathfrak{p},\mathfrak{q}} = g = \frac{q-1}{f_2}$.

4. Examples

In this section, we give some examples of cyclotomic fields satisfying the Theorem 1.3. Recall that a Mersenne prime is of the form $M_n = 2^n - 1$ for some positive integer n. For $n > 2$, the smallest Mersenne prime is $2^3 - 1 = 7$. Then we obtain the following example:

Example 4.1. Let $K = \mathbb{Q}[\zeta_7]$. According to Theorem 1.3, there exists two distinct prime ideals $\mathfrak{p},\mathfrak{q}$ such that $G_K(\mathfrak{p},\mathfrak{q}) = 1$, where $\mathfrak{p}\cap\mathbb{Z} = 2\mathbb{Z}, \mathfrak{q}\cap\mathbb{Z} = 7\mathbb{Z}$. The degree of residue field f_2 is the order of 2 in $(\mathbb{Z}/7\mathbb{Z})^\times$, that is $f_2 = 3$. Therefore, 2 decomposes into $\frac{\varphi(7)}{f_2} = 2$ distinct prime ideals $\mathfrak{p}_1,\mathfrak{p}_2$ in O_K. Moreover, 7 ramifies in O_K with ramification index $e_7 = \varphi(7) = 6$. Explicitly,

$$(2) = \mathfrak{p}_1\mathfrak{p}_2,\ (7) = \mathfrak{q}^6; G_K(\mathfrak{p},\mathfrak{q}) = 2^3 - 7 = 1$$

Example 4.2. $M_7 = 2^{13} - 1 = 8191$ is a Mersenne prime. According to Theorem 1.3, $K = \mathbb{Q}[\zeta_{2\cdot 8191}]$ has two distinct prime ideals $\mathfrak{p},\mathfrak{q}$ such that $G_K(\mathfrak{p},\mathfrak{q}) = 1$, where $\mathfrak{p}\cap\mathbb{Z} = 2\mathbb{Z}, \mathfrak{q}\cap\mathbb{Z} = 8191\mathbb{Z}$. 2 decomposes into $\frac{\varphi(2\cdot 8191)}{f_2} = \frac{8190}{13} = 630$ distinct prime ideals $\mathfrak{p}_1,\mathfrak{p}_2,...,\mathfrak{p}_{630}$ in O_K. 8191 ramifies in O_K with ramification index $e_{8191} = \varphi(8191) = 8190$. Explicitly,

$$(2) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{630},\ (8191) = \mathfrak{q}^{8190}; G_K(\mathfrak{p},\mathfrak{q}) = 2^{13} - 8191 = 1$$

Acknowledgments

The author would like to thank referees for their careful corrections to and valuable comments on the original version of this paper.

Conflict of interest

The authors declare no conflict of interest.

References

1. J.S. Milne, *Algebraic number theory*, Lecture Notes, 1998. Available from: http://www.jmilne.org/math/CourseNotes/ant.html.
2. J. Neukirch, *Algebraic number theory*, Berlin: Springer-Verlag, 1999.
3. P. Mihäilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., **572** (2004), 167–195.

4. T. Metsänkylä, *Catalan's conjecture: Another old Diophantine problem solved*, B. Am. Math. Soc., **41** (2004), 43–57.

AIMS Press