Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/13/20240744

Factoring primes and sums of two squares

Zirui Jiang

The University of Manchester, Manchester, M13 9PL, United Kingdom

ziruij@163.com

Abstract. Mathematicians began to study a series of properties about numbers a long time ago, and a new field of mathematics, the number theory, was born from this. Some special properties of numbers in the number theory make mathematicians use the knowledge of group theory to make some ingenious answers when considering some problems. In the analytic number theory, equations related to numbers have always been a concern of mathematicians. The most famous Fermat's last theorem also brought long-term troubles to countless mathematicians and was finally proved by the British mathematician Wiles. Many famous theorems also prove that some problems in the number theory can be solved by thinking in relation to other algebraic knowledge. This paper focuses on the factoring primes and constructs prime ideals of $O_F = \mathbb{Z}[\alpha]$ lying above a prim p from irreducible factors of $\overline{f_\alpha} \in \mathbb{Z}[p[x]$. The paper also shows that these are all prime ideals lying above p . Based on these theorems and definitions, as a simple application of the theory, this paper first considers which primes can be written as sums of two squares, then the second part of this paper gives the answer: p is a sum of two squares if and only if $p \equiv 1 \, mod \, 4$.

Keywords: Primes, Sums of Squares, Algebraic Number Theory, Mathematics.

1. Introduction

For algebraic number theory [1], the overall understanding process starts with defining some basic algebraic number theory annotations, such as algebraic numbers and integers [2], number fields, rings of integers, norm and discriminant, fractional ideals, and class groups and lattices. As one of the most essential parts of algebraic number theory, factorising prime numbers into prime ideals of a ring of integers and applying it in the case of simple number fields (such as quadratic fields) is very important intermediate knowledge. Only after mastering the basic definition and such a decomposition relationship can the following Minkowski's first theorem be introduced to try to compute class numbers and class groups of simple number fields. This paper can be divided into two parts, describing the process of decomposition of prime ideals and the corresponding applications, respectively. To be more specific, it discusses what kind of prime numbers can be written in the form of a sum of two integer squares, which is a very classical part of algebraic number theory.

The most important part of the first part is that if we give a number field, give the corresponding ring of integers and have a minimal polynomial, then we can perform in the given number field for some given prime numbers. break down. The second part gives more inspiration when we consider an algebraic decomposition problem, in addition to analyzing the properties of the number itself, we can also use the

DOI: 10.54254/2753-8818/13/20240744

properties of groups, rings, and fields on the basis of group theory. Considering the problem, this actually inspires us to think about the problem from many aspects when facing Fermat's last theorem.

2. Factoring primes

2.1. Some basic definitions

Several concepts of algebraic number theory have a pivotal role [3]: numbers, polynomials, and equations. So this paper gives definitions of some of the core terms before discussing the central issues. First of all, for numbers that people have a lot of contact with, the more special numbers in algebraic number theory are algebraic numbers and transcendental numbers [4]. Based on this background, the following are some definitions.

Definition 2.1. A complex number $\alpha \in \mathbb{C}$ is called algebraic if there is a non-zero polynomials $f \in \mathbb{Q}[x]$ with $f(\alpha) = 0$. If α is not algebraic, it is called transcendental.

Definition 2.2. The number field generated by an algebraic number $\alpha \in \mathbb{C}$ is the smallest subfield of $\mathbb{C}$ that contains α. We denote this field by $\mathbb{Q}(\alpha)$.

A subfield $F \cap \mathbb{C}$ is an algebraic number field (or a number field) if $F = \mathbb{Q}(\alpha)$ for an algebraic number $\alpha \in \mathbb{C}$.

Definition 2.3. A complex number $\alpha \in \mathbb{C}$ is an algebraic integer if there is a monic polynomial $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.

Definition 2.4. Let F be a number field. The ring $\mathcal{O}_F = \overline{\mathbb{Z}} \cap F$ consisting of all algebraic integers in F is called the ring of integers of F, where the set $\overline{\mathbb{Z}}$ of algebraic integers is a subring of $\mathbb{C}$.

2.2. Prime ideals

Lemma 2.5. Let F be a number field and $P \subseteq \mathcal{O}_F$ a non-zero prime ideal [5]. Then $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, so $P \cap \mathbb{Z} = \langle p \rangle \subseteq \mathbb{Z}$, for a prime p.

Proof. If $a, b \in P \cap \mathbb{Z}$, $r \in \mathbb{Z}$, then $a + b \in P \cap \mathbb{Z}$, $ra \in P \cap \mathbb{Z}$, then $P \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. If we have $a, b \in \mathbb{Z}$ such that $ab \in P \cap \mathbb{Z}$, since P is a prime ideal, then $a \in P$ or $b \in P$. Since $a, b \in \mathbb{Z}$, we can get $a \in P \cap \mathbb{Z}$ or $b \in P \cap \mathbb{Z}$, thus $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Let $\alpha \in P$, $\alpha \neq 0$. We konw that $N(\alpha) \in P \cap \mathbb{Z}$, and $N(\alpha) \neq 0$. Hence, $P \cap \mathbb{Z} \neq 0$. As a non-zero prime ideal of $\mathbb{Z}$, it must have the form $P \cap \mathbb{Z} = \langle p \rangle$ for a prime p.

Definition 2.6. Let p be a prime. The prime ideals $P_1, ..., P_r$ appearing in the prime ideal factorization $p\mathcal{O}_F = P_1^{e_1} ... P_r^{e_r}$ of $p\mathcal{O}_F$ are said to be lying above p [6].

Lemma 2.7. Let p be a prime, P a prime ideal of $\mathcal{O}_F$. Then P lies above p if and only if $P \cap \mathbb{Z} = \langle p \rangle \subseteq \mathbb{Z}$.

Proof. If P lies above p, it appears in the prime ideal factorisation of $p\mathcal{O}_F$. Thus, $p\mathcal{O}_F = P^e ... P_r^{e_r} \subseteq P$. Then, $p \in P \cap \mathbb{Z}$. Since $P \cap \mathbb{Z}$ is a prime ideal $\langle q \rangle \subseteq \mathbb{Z}$ by Lemma 2.5, with q is a prime, then it can get $q \mid p$, thus $q = p$.

If $P \cap \mathbb{Z} = \langle p \rangle$, then $p \in P$, thus $p\mathcal{O}_F \subseteq \mathbb{Z}$, by the properties of ideals of $\mathcal{O}_F$: "To contain is to divide", thus $P \mid p\mathcal{O}_F$. Therefore, if $p\mathcal{O}_F = P_1^{e_1} ... P_r^{e_r}$ is the prime ideal factorisation of $p\mathcal{O}_F$, we must have $P = P_i$ for some i.

DOI: 10.54254/2753-8818/13/20240744

Theorem 2.8. Let F be a number field and assume that $O_F = \mathbb{Z}[\alpha]$, for some $\alpha \in O_F$. Let p be prime and $g \in \mathbb{Z}[x]$ a monic polynomial, such that $\overline{g} \in \mathbb{Z}_p[x]$ is irreducible over $\mathbb{Z}_p$ and divides $\overline{f_\alpha}$ where f_α is the minimal polynomial. Then the ideal $P = \langle p, g(\alpha) \rangle$ is a prime ideal of O_F. Moreover, P lies above p and $N(P) = p^{deg(g)}$.

*Proof. We consider t*he residue class field $F = \mathbb{Z}_p[x] / \langle \overline{g} \rangle$. Recall that $\mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[x]\}$. A function $\phi : \mathbb{Z}[\alpha] \to F$ is defined by setting $\phi(f(\alpha)) = \overline{f} + \langle \overline{g} \rangle$. If $f(\alpha) = h(\alpha)$, then f_α divides $f - h$, thus $f - h = qf_\alpha$ where $q \in [\![\ ][x]$. By Gauss Lemma, it is found that $\lambda \in [\![\ ç\ \{0\}$, such that $\lambda f_\alpha, \lambda^{-1} q \in \mathbb{Z}[x]$. Since f_α is monic, then $\lambda \in \mathbb{Z}$. However, $\lambda^{-1} q \in \mathbb{Z}[x]$ implies that $q \in \mathbb{Z}[x]$. Thus $f = h + qf_\alpha$ where $q \in \mathbb{Z}[x]$. Since $\overline{g} \nmid \overline{f_\alpha}$, then $\overline{f_\alpha} \in \langle \overline{g} \rangle$, thus $\overline{f} + \langle \overline{g} \rangle = \overline{h} + \overline{q}\,\overline{f_\alpha} + \langle \overline{g} \rangle = \overline{h} + \langle \overline{g} \rangle$ and ϕ is well defined. It is clearly a ring homomorphism and subjective. Consider the ideal $P = ker(\phi)$ of $\mathbb{Z}[\alpha] = O_F$. By the First Isomorphism Theorem, $\phi' : O_F / P \to F$ is an isomorphism, then O_F / P is a field with $p^{deg(g)}$ elements. Therefore, P is a maximal ideal of O_F and a prime ideal with $N(P) = p^{deg(g)}$.

We just need to show that $P = \langle p, g(\alpha) \rangle$. First, since $\overline{p} = 0$, we have $\phi(p) = \overline{p} + \langle \overline{g} \rangle = 0_F$. Moreover, $g(\alpha) \in P$, as $\phi(g(\alpha)) = \overline{g} + \langle \overline{g} \rangle = 0_F$. Thus $\langle p, g(\alpha) \rangle \subseteq P$. Conversely, let $f(\alpha) \in P$. Then $\overline{f} \in \langle \overline{g} \rangle$, so $\overline{f} = \overline{h}\overline{g}$, for some $h \in \mathbb{Z}[x]$. Then the polynomials f and $h\ g$ are congruent modulo p, so all coefficients of $f - hg$ are divisible by p. Hence, there is a polynomial $r \in \mathbb{Z}[x]$, such that $f = hg + pr$. Plugging in α, $f(\alpha) = h(\alpha)g(\alpha) + pr(\alpha) \in \langle p, g(\alpha) \rangle$ is obtained. Thus $P = \langle p, g(\alpha) \rangle$. Since $p \in P$, we have $p \in P \cap \mathbb{Z}$. By Lemma 2.5, $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ that contains p, thus $P \cap \mathbb{Z} = \langle p \rangle$. By Lemma 2.7, it shows that P lies above p.

2.3. Factoring prime

Theorem 2.9. Let F be a number field and assume that $O_F = \mathbb{Z}[\alpha]$ for some $\alpha \in O_F$. Let p be prime and $\overline{f_\alpha} = \overline{g_1}^{e_1} \ldots \overline{g_r}^{e_r}$ be the factorization of $\overline{f_\alpha} \in \mathbb{Z}_p[x]$[7] into irreducibles. That is, $g_1, \ldots, g_r \in \mathbb{Z}[x]$ are monic polynomials, such that the $\overline{g_i}$ are distinct and irreducible in $\mathbb{Z}_p[x]$, and $e_1, \ldots, e_r \in \bullet$. Then the prime ideals of O_F lying above p are precisely the ideals $P_i = \langle p, g_i(\alpha) \rangle$, for $i \in \{1, \ldots, r\}$. The ideal $\langle p \rangle = pO_F$ of O_F factorises into prime ideals as $pO_F = P_1^{e_1} \ldots P_r^{e_r}$.

Proof. It is known from Theorem 2.8 that all P_i are prime ideals with $N(P_i) = p^{d_i}$, where $d_i = deg(g_i)$. From the factorization $\overline{f_\alpha} = \overline{g_1}^{e_1} \ldots \overline{g_r}^{e_r}$, it can get $d_1 e_1 + \ldots + d_r e_r = deg(f_\alpha)$, since all g_i are monic, $deg(\overline{g_i}) = deg(g_i)$. For arbitrary ideals I, J_1, J_2 of O_F, Equation (1) is obtained:

$$(I + J_1)(I + J_2) = II + IJ_1 + IJ_2 + J_1 J_2 \subseteq I + I + I + J_1 J_2 = I + J_1 J_2. \tag{1}$$

Applying this inductively to the $P_i = \langle p, g_i(\alpha) \rangle = \langle p \rangle + \langle g_i(\alpha) \rangle$, Equation (2) is obtained:

$$P_1^{e_1} \ldots P_r^{e_r} \subseteq \langle p \rangle + \langle g_1(\alpha) \rangle^{e_1} \ldots \langle g_r(\alpha) \rangle^{e_r} = \langle p, g_1(\alpha)^{e_1} \ldots g_r(\alpha)^{e_r} \rangle = \langle p \rangle. \tag{2}$$

DOI: 10.54254/2753-8818/13/20240744

The last equality holds due to $\overline{f_\alpha} = \overline{g_1}^{e_1} ... \overline{g_r}^{e_r}$, as then p divides all coefficients of $f_\alpha - g_1^{e_1} ... g_r^{e_r}$, so $g_1^{e_1} ... g_r^{e_r} = f_\alpha + ph$, for some $h \in \mathbb{Z}[x]$. But then $g_1(\alpha)^{e_1} ... g_r(\alpha)^{e_r} = f_\alpha(\alpha) + ph(\alpha) = ph(\alpha) \in p\mathcal{O}_F = \langle p \rangle$.

Thus, $\langle p \rangle$ $P_1^{e_1} ... P_r^{e_r}$ is obtained and hence $\langle p \rangle = P_1^{k_1} ... P_r^{k_r}$ with $0 \le k_i \le e_i$. Hence, the P_i is indeed the only prime ideals of $\mathcal{O}_F$ lying above p . Moreover, Equation (3) is obtained:

$$p^{deg(f_\alpha)} = p^{[F:\mathbb{Q}]} = | N(P) | = N(\langle p \rangle) = N(P_1)^{k_1} ... N(P_r)^{k_r} = p^{d_1 k_1 + ... + d_r k_r}. \quad (3)$$

Compare this to $d_1 e_1 + ... + d_r e_r = deg(f_\alpha)$ to conclude that $k_i = e_i$ for all i .

3. Primes as sums of two squares

Lemma 3.1. Let p be an odd prime, such that $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$. Then $p \equiv 1 \ mod \ 4$.

Proof. Since $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0 \ mod \ 4$ and $3^2 = 9 \equiv 1 \ mod \ 4$, we found that squares are always congruent to 0 or 1 modulo 4 . If p is a sum of two squares, then $p \equiv 0, 1, 2 \mod 4$. Then $p \equiv 0 \ mod \ 4$ is impossible and the only prime congruent to 2 modulo 4 is 2 .

The less trivial reverse direction will be proved, showing that every prime $p \equiv 1 \ mod \ 4$ can be written as $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$. This will be done by factoring the ideal $p\mathbb{Z}[i]$ in the ring of integers $\mathbb{Z}[i]$ of $\mathbb{Q}(i)$. The factorisation depends on the roots of $f_i = x^2 + 1$ in $\mathbb{Z}_p$.

Lemma 3.2. Let $p \equiv 1 \ mod \ 4$ be a prime. Then -1 is a square modulo p , i.e., there is $c \in \mathbb{Z}$ with $-1^2 \equiv c \ mod \ p$.

Proof. Let $\overline{g}$ be a generator of $\mathbb{Z}_p^\times$, then $\mathbb{Z}_p^\times = \langle \overline{g} \rangle$ and write $p - 1 = 4k$. By Fermat's Little Theorem, then $\overline{1} = \overline{g}^{p-1} = \overline{g}^{4k}$. The polynomial $x^2 - \overline{1} = (x - \overline{1})(x + \overline{1})$ has only two roots $x = \pm \overline{1}$. Thus $\overline{g}^{2k} = \pm \overline{1}$. If $\overline{g}^{2k} = \overline{1}$, so $\overline{g}$ can not generate all of $\mathbb{Z}_p^\times$, as then $\overline{g}^{2k+j} \equiv \overline{g}^j \ mod \ p$, so the powers $\overline{g}^j$, for $i \in \{0, ..., p-1\}$ capture only $2k = (p-1)/2$ elements of $\mathbb{Z}_p^\times$. Hence, $-\overline{1} = \overline{g}^{2k} = (\overline{g}^k)^2$ and thus, -1 is a square modulo p .

Theorem 3.3. Let p be an odd prime. Then p is a sum of two squares if and only if $p \equiv 1 \ mod \ 4$ [8,9].

Proof. From Lemma 3.1, it is known that the "only if" part has been proved, so let us prove the "if" part. Let $F = \mathbb{Q}(i)$, then $\mathcal{O}_F = \mathbb{Z}[i]$. Consider the factorisation of the ideal $p\mathcal{O}_F$ and note that $f_\alpha = x^2 + 1$. By Lemma 3.2, there is $c \in \mathbb{Z}$, such that $-1 \equiv c^2 \ mod \ p$. Thus Equation (4) is obtained:

$$\overline{f_\alpha} = x^2 + \overline{1} = x^2 - \overline{c}^2 = (x + \overline{c})(x - \overline{c}). \quad (4)$$

If $c \equiv -c \ mod \ p$, then $2c \equiv 0 \ mod \ p$. Since $p > 2$, so there is only one possible value: $c = p$, but that is impossible because $c^2 \equiv -1 \ mod \ p$, thus $c \not\equiv -c \ mod \ p$, so these are two distinct roots. Hence, p is split in $\mathcal{O}_F$ and $p\mathcal{O}_F = P_1 P_2$, for two distinct prime ideals P_i with $N(P_i) = p$. Since every ideal of $\mathbb{Z}[i]$ is principle. Hence, $P_1 = \langle \pi \rangle$, for some $\pi = a + bi \in \mathbb{Z}[i]$. Since $\pi \in \mathbb{Z}[i]$ and $\pi \neq 0$, then Equation (5) is obtained:

$$p = N(P_1) = N(\langle \pi \rangle) = | N(\pi) | = (a + bi)(a - bi) = a^2 + b^2. \quad (5)$$

DOI: 10.54254/2753-8818/13/20240744

4. Conclusion

This paper describes the process of decomposition of prime ideals and the corresponding applications: i.e., it discusses what kind of prime numbers can be written in the form of a sum of two integer squares and we got the result that for odd prime p , it is a sum of two squares if and only if $p \equiv 1 \, mod \, 4$,this part is a very classical part of algebraic number theory, on the basis of which if Minkowski bound and class groups, etc. are introduced, the property of the unique factorization domain (UFD) can be used to solve some problems about the Diophantine equations [10]. For instance, it can be shown that there are no $x, y \in \mathbb{Z}$ with $x^2 + 5 = y^2$, which in the long run will be useful for the proof of Fermat's Last Theorem.

In the proof of the theorem, we use the fact that every ideal in $\mathbb{Z}[i]$is principle, we did not present the proof of this result in the article due to space constraints. Also, Theorem 2.9 can be applied to many number fields, but not all of them, that is because the assumption $O_F = \mathbb{Z}[\alpha]$, for some algebraic integer α . But for many number fields, such an α does not exist, we just found such α for quadratic and cyclotomic fields. Therefore, the results given in this article actually have certain limitations. On the basis of this problem, we can gradually try to use the idea of decomposition to consider proof of the special case of the Fermat's last theorem for regular primes.

References

[1] Bhaskar, J. (2008). Sum of two squares. https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf.

[2] Homeworkhelp. Com and Inc. Factoring and Primes (High School Math).

[3] Stewart, I. and Tall, D. (2001). Algebraic Number Theory and Fermat's Last Theorem: Third Edition. A K Peters/CRC Press. ISBN-10: 1568811195. ISBN-13: 978-1568811192.

[4] Edwards, H. M. (1977). Fermat's last theorem: A genetic introduction to algebraic number theory. In: Graduate Texts in Mathematics. Springer New York, NY.

[5] Stein, M. R. and Dennis, R. K. (1989). Algebraic K-Theory and Algebraic Number Theory: Comtemporar Math., 83. American Mathematical Society, Providence.

[6] Rosen, K. H. (2000). Elementary number theory and its applications. Addison Wesley. ISBN-10: 0201870738. ISBN-13: 978-0201870732.

[7] Zagier, D. (1990). A One-Sentence Proof That Every Prime p $1(\mathrm{mod}\,4)$ Is a Sum of Two Squares. In: American Mathematical Monthly 97(2), 144.

[8] Honsberger, R. (1970). Writing a Number as a Sum of Two Squares. In Ingenuity In Mathematics (Anneli Lax New Mathematical Library, pp. 61-66). Mathematical Association of America. doi:10.5948/UPO9780883859384.012.

[9] Vladimirovich, D. V. and Genadievna, S. A. (2017). A generalization of fermat's theorem on sum of two squares. Austrian Journal of Technical and Natural Sciences.

[10] Ore, O. (1988). Number theory and its history (Dover Books on Mathematics). Dover Publications. ISBN-10: 0486656209. ISBN-13: 978-0486656205.