SUMS OF TWO SQUARES IN DIFFERENT RINGS

KEVIN XU

1. Introduction

It is a well-known result that an odd integer prime can be written as the sum of two integral squares if and only if it is congruent to 1 modulo 4. Many proofs have been stated, including the one-line proof by Zagier. However, not much research about the sums of two squares goes beyond this fact, instead talking about the sum of n squares, the sums of two cubes, etc.

It is the purpose of this paper to go more in depth into the sums of two squares, and specifically the sums of squares in different rings. Not only do we find when integers can be expressed as the sum of two integers, we will find out when integers in the ring $\mathbb{Z}[\sqrt{n}]$ can be expressed as the sum of two integers.

I express my sincerest thanks to Simon Rubinstein-Salzedo, who helped guide me through every step along the way.

Date: December 11, 2018.

2. Fermat's Theorem

We begin with the theorem mentioned earlier.

Theorem 2.1 (Euler). *An odd prime can be written as a sum of two integral squares if and only if it is congruent to* 1 *modulo* 4*.*

To simplify matters, we will introduce the *Legendre symbol.*

Definition 2.2. The *Legendre symbol*, usually denoted as $(\frac{a}{p})$, satisfies

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \exists x \mid x^2 \equiv a \pmod p \\ -1 & \nexists x \mid x^2 \equiv a \pmod p \\ 0 & p|a \end{cases}.$$

Corollary 2.3 (Euler's criterion). *For $a, p \in \mathbb{Z}$ and p an odd prime, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Proof. Let us assume that $p \nmid a$, since otherwise then it is trivial. We will handle two cases separately. If $\exists x \mid x^2 \equiv a \pmod p$, then $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$ by Fermat's little theorem. For the other case, denote x as a residue modulo p; we must have $x^2 \not\equiv a \pmod p$ for all x. Following the same steps as the first case gives $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. However, because $a^{p-1} \equiv 1 \pmod p$ (due to Fermat's Little Theorem), if $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$, then $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$, as desired. ■

Theorem 2.4 (Quadratic Reciprocity). *For odd primes p, q,*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Or, if p, q are not both congruent to 3 *modulo* 4*, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

We will not prove this theorem, as it is too long and strays too far from the main topic. However, we will use it later to prove an important theorem. To prove theorem 2.1, we will first need the following lemma:

Lemma 2.5. *Let p be a prime. Then p divides $m^2 + 1$ for some integer m if and only if $p \cong 1 \pmod 4$.*

Proof. Restating the lemma, we want to prove that an odd prime p satisfies

$$\left(\frac{-1}{p}\right) = 1$$

if and only if $p \equiv 1 \pmod 4$. By Corollary 2.3,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

which is 1 if and only if $p \equiv 1 \pmod 4$. ■

Proof of Theorem 2.1. Let $X = \{(a,b) : 0 \leq a, b \leq \lfloor\sqrt{p}\rfloor\}$, and notice that the number of elements in X is $(1 + \lfloor\sqrt{p}\rfloor)^2 > p$. Thus we must have two distinct pairs $(x_1, y_1), (x_2, y_2)$ that are congruent modulo p under the map $(x, y) \mapsto x + sy$, or that $x_1 + sy_1 \equiv x_2 + sy_2 \pmod{p}$ for any integral s. Define $x = x_1 - x_2, y = y_1 - y_2$, so $x^2 \equiv s^2y^2 \pmod{p}$.

From Lemma 2.5, we can choose s such that $s^2 \equiv -1 \pmod{p}$, which gives $x^2 + y^2 \equiv 0 \pmod{p}$. Now, observe that x, y cannot be both 0, and as $0 < x^2 + y^2 \leq 2(\lfloor\sqrt{p}\rfloor)^2 < 2p$, we must have $x^2 + y^2 = p$, completing the proof. ■

Now we have found out which primes are representable as the sum of two integer squares, we can explore a more general question: Which nonnegative integers can be represented in this way?

Theorem 2.6 (Supplement to Theorem 2.1)**.** *An integer $n > 1$ can be represented as the sum of two integer squares if and only every prime factor p satisfying $p \equiv 3 \pmod{4}$ has an even exponent in the prime factorization of n.*

First, we prove two simple lemmas:

Lemma 2.7 (Diophantus)**.** *If m and n can both be represented as a sum of two integer squares, then mn also is representable as a sum of two integer squares.*

Proof. Let $m = a^2 + b^2$ and $n = c^2 + d^2$ where $a, b, c, d \in \mathbb{Z}$. Then $mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$, as desired. ■

Lemma 2.8. *Let $n = x^2 + y^2$ be representable as the sum of two squares. If $p \equiv 3 \pmod{4}$ divides n, then p divides both x and y.*

Proof. Suppose by contradiction that $p \nmid x$. Then there exists $\overline{x}$ such that $x\overline{x} \equiv 1 \pmod{p}$. If we multiply $n = x^2 + y^2$ by $\overline{x}^2$, then $n\overline{x}^2 = (x\overline{x})^2 + (y\overline{x})^2$, and reducing modulo p gives $(y\overline{x})^2 + 1 \equiv 0 \pmod{p}$, or $(y\overline{x})^2 \equiv -1 \pmod{p}$, which by Lemma 2.5 does not have a solution, a contradiction. ■

Remark 2.9. If n can be written as the sum of two squares and $p \equiv 3 \pmod{4}$ is a factor of n, then $\frac{n}{p^2}$ is also a sum of two squares.

Proof of Theorem 2.6. We will first prove that if n has the property that every prime factor congruent to 3 modulo 4 has an even exponent in the prime factorization of n, then n can be represented as the sum of two squares. Let p be some prime factor of n. If $p \equiv 1 \pmod{4}$, then by Theorem 2.1 it can be expressed as the sum of two squares. If $p \equiv 3 \pmod{4}$, then p^2 can be represented as the sum of two squares. Lastly, if $p = 2$, then $p = 1^2 + 1^2$ can be written as the sum of two squares. Thus, the product of these factors, namely n, is also representable as the sum of two squares by Lemma 2.7.

For the other way, Let $n = a^2b$, where a, b are positive integers and b is square-free. If there is a prime $p|b$ with $p \equiv 3 \pmod{4}$, then by Lemma 2.8 $p^2|b$. However, this cannot happen as b is square-free, so we are done. ■

3. The ring of $\mathbb{Z}[\sqrt{n}]$

Now that we have determined which integers can be expressed as the sum of two squares in $\mathbb{Z}$, we will consider the same problem, but with squares in $\mathbb{Z}[\sqrt{n}]$ for integer n where $|n|$ is square-free. We start with some definitions:

Definition 3.1. The set $\mathbb{Z}[\sqrt{n}]$ is defined as all elements of the form $a + b\sqrt{n}$ where $a, b \in \mathbb{Z}$.

Definition 3.2. Let an integer $z \in \mathbb{Z}[\sqrt{n}]$ be expressed as $z = a + b\sqrt{n}$ for $a, b \in \mathbb{Z}$. Then the *norm* of z, denoted as $N(z)$, is defined as $a^2 + nb^2$. The norm has several interesting properties, all of which we will prove later.

Definition 3.3. Integers in $\mathbb{Z}[\sqrt{n}]$ are called *units* if their norm is 1.

Definition 3.4. Let $z \in \mathbb{Z}[\sqrt{n}]$ be expressed as $a + b\sqrt{n}$ where $a, b \in \mathbb{Z}$. Then the *conjugate* of z, denoted as $\overline{z}$, is defined as $a - b\sqrt{n}$. Note that $z\overline{z} = N(z)$.

Definition 3.5. An integer $z \in \mathbb{Z}[\sqrt{n}]$ is *prime* if for all $a, b \in \mathbb{Z}[\sqrt{n}]$ satisfying $z|ab$, $z|a$ or $z|b$.

Definition 3.6. An integer $z \in \mathbb{Z}[\sqrt{n}]$ is *irreducible* if all its factors are in the form of 1 or z, up to units.

There are some rings of the form $\mathbb{Z}[\sqrt{n}]$ where being prime and being irreducible do not mean the same thing. We will not consider these rings in our calculations, and will consider being irreducible as being prime.

Lemma 3.7. *Let $a, b \in \mathbb{Z}[\sqrt{n}]$. Then $N(ab) = N(a)N(b)$.*

Proof. We have $N(ab) = ab \cdot \overline{ab} = ab \cdot \overline{a}\overline{b} = a\overline{a}b\overline{b} = N(a)N(b)$ as desired. ■

We will first begin with the case when $n = -1$, figuring out which Gaussian integers are representable as the sum of two Gaussian squares.

Theorem 3.8. *A Gaussian prime z can be represented as $z_1^2 + z_2^2$ where $z_1, z_2 \in \mathbb{Z}[i]$ if and only if $z \equiv 1 \pmod 2$, or that the real part of z is odd and the imaginary part is even.*

Lemma 3.9. *A Gaussian integer z with a nonzero real and imaginary part is prime if and only if $N(z)$ is prime.*

Proof. Let $z = ab$ where $a, b \in \mathbb{Z}[i]$. Then by Lemma 3.7, $N(z) = N(ab) = N(a)N(b)$. Suppose z is not prime, and so we can choose a, b such that $N(a), N(b) > 1$. Then $N(z) = N(a)N(b)$ is not prime. For the other way, suppose $N(z)$ is not prime. If $p \equiv 3 \pmod 4$ divides $N(z)$, then by Lemma 2.8 $p^2|N(z)$, and $N(z)$ can be written as the product of two sums of squares. If $p \equiv 1 \pmod 4$ divides $N(z)$, by Theorem 2.1 $N(z)$ can be written as the product of two sums of squares. Thus $N(z) = N(a)N(b)$ for some $N(a), N(b) > 1$. We then have $z = ab$ (up to units), so we are done. ■

Now that we have established these, let us begin the proof:

Proof of Theorem 3.8. Let $z = x + yi$ be a Gaussian prime with $x, y \in \mathbb{Z}$, and let $z = z_1^2 + z_2^2$ where $z_1, z_2 \in \mathbb{Z}[i]$. Integers a, b, c, d satisfy $z_1 = a + bi$ and $z_2 = c + di$. Factoring, $z = (z_1 + z_2 i)(z_1 - z_2 i) = (a - d + (b + c)i)(a + d + (b - c)i)$.Because z is a prime in $\mathbb{Z}[i]$, one of the factors is 1 multiplied by a unit, and the other is z multiplied by a unit. Assume without loss of generality that $a - d + (b + c)i = 1$ and $a + d + (b - c)i = z = x + yi$. Then we have the simultaneous equations

$$\begin{aligned} a - d &= 1 \\ b + c &= 0 \\ a + d &= x \\ b - c &= y \end{aligned}$$

Solving these for a, b, c, d, we get $a = \frac{x+1}{2}, b = \frac{y}{2}, c = -\frac{y}{2}, d = \frac{x-1}{2}$. Because these are integers, we must have $x \equiv 1 \pmod 2$ and $y \equiv 0 \pmod 2$, as desired. ∎

Theorem 3.10 (Supplement to Theorem 3.8)**.** *A Gaussian integer $z = x+yi$ where $x, y \in \mathbb{Z}$ and $N(z) > 1$ can be expressed as the sum of two Gaussian squares if and only if every Gaussian prime factor p satisfying $p \equiv i \pmod 2$ has an even exponent in the prime factorization of z.*

We will not prove this theorem because of its similarity to Theorem 2.6, and instead will leave it as an exercise to the reader. Now that we have completed the Gaussian case, we will tackle the sums of squares in $\mathbb{Z}[\sqrt{n}]$ for general n.

Lemma 3.11. *A prime $z \in \mathbb{Z}[\sqrt{n}]$ can be expressed as the sum of two squares in $\mathbb{Z}[\sqrt{n}]$ for positive integer $n > 1$ if and only if it can be factored into the ring $\mathbb{Z}[\sqrt{|n|}, i]$.*

Proof. Suppose $z = x^2 + y^2$ where $x, y \in \mathbb{Z}[\sqrt{n}]$, and denote $a, b, c, d \in \mathbb{Z}$ such that $x = a + b\sqrt{n}, y = c + d\sqrt{n}$. Note

$$z = (a + b\sqrt{n})^2 + (c + d\sqrt{n})^2$$

$$z = (a + b\sqrt{n} + ci + d\sqrt{-n})(a + b\sqrt{n} - ci - d\sqrt{-n}).$$

These factors are both in $\mathbb{Z}[\sqrt{|n|}, i]$, so z can be factored into $\mathbb{Z}[\sqrt{|n|}, i]$. Since all our steps are reversible, we have proven the other direction as well. A sidenote here is that $z = a^2 + nb^2 + c^2 + nd^2 + (2ab + 2cd)\sqrt{n}$, so the coefficient of $\sqrt{n}$ must be even. ∎

Lemma 3.12. *If a prime $p \in \mathbb{Z}$ can be factored into the ring $\mathbb{Z}[\sqrt{D}]$ for nonzero integer D, then $\left(\frac{D}{p}\right) = 1$.*

Proof. Let p have a factor $z = a + b\sqrt{D}$ that is prime in $\mathbb{Z}[\sqrt{-D}]$, so $N(z) > 1$. Because p is an integer prime, $N(z)|p \Rightarrow N(z) = a^2 + Db^2 = p$. Thus $a^2 \equiv p \pmod D$ and $\left(\frac{D}{p}\right) = 1$. ∎

Theorem 3.13. *A prime $z \in \mathbb{Z}[\sqrt{n}]$ with nonzero real and imaginary parts can be written as the sum of two squares in $\mathbb{Z}[\sqrt{n}]$ if and only if $z \equiv 1 \pmod 2$.*

Proof. Due to Lemma 3.11, we wish to find $z \in \mathbb{Z}[\sqrt{n}]$ that can be factored into the ring $\mathbb{Z}[\sqrt{|n|}, i]$. If z can be factored into the ring $\mathbb{Z}[\sqrt{|n|}, i]$, then $N(z)$ can also be factored into the ring and also the subrings $\mathbb{Z}[\sqrt{|n|}]$ and $\mathbb{Z}[i]$. From Lemma 3.12, we must have

$$\left(\frac{-1}{N(z)}\right) = \left(\frac{|n|}{N(z)}\right) = 1.$$

Lemma 2.5 implies that $N(z) \equiv 1 \pmod 4$. Now, using Theorem 2.4, $\left(\frac{|n|}{N(z)}\right) = \left(\frac{N(z)}{|n|}\right) = 1$. To solve this equation, let $z = a + b\sqrt{n}$ where $a, b \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$ with $x^2 \equiv N(z) \equiv a^2 + nb^2 \pmod n$, so $x^2 \equiv a^2 \pmod n$. Because z can be written as the sum of two squares in $\mathbb{Z}[\sqrt{n}]$, then $b \equiv 0 \pmod 2$, which implies $a \equiv 1 \pmod 2$, as desired. ∎

Theorem 3.14 (Generalization of Theorem 3.10)**.** *An integer in $\mathbb{Z}[\sqrt{n}]$, $z = x + y\sqrt{n}$ where $x, y \in \mathbb{Z}$ and $N(z) > 1$, can be expressed as the sum of two squares in $\mathbb{Z}[\sqrt{n}]$ if and only if every prime factor $p|z$ satisfying $p \equiv i \pmod 2$ has an even exponent in the prime factorization of z.*

Just like before, the proof is left as an exercise to the reader. For rings of the form $\mathbb{Z}[\sqrt{n}]$ where being prime is not the same as being irreducible, we would need a different approach. In particular, being prime is the same as being irreducible happens when the class number of $\mathbb{Z}[\sqrt{|n|}, i]$ is 1, which requires further work that we will not delve into.

I have taken the liberty to write up and implement a program dealing with the squares and sums of squares in the ring $\mathbb{Z}[\sqrt{n}]$, which you can find here.

Euler Circle, Palo Alto, CA 94306
E-mail address: `kevinxu144@gmail.com`