# Prime Sums of Squares

Aidan Hennessey

December 2023

## 1 Overview

In number theory, the question naturally arises "which integers $n$ can be written $n = a^2 + b^2$ for integers $a$ and $b$?". It turns out that this question is easy to answer for composite numbers if you know the answer for the primes. The answer for primes, first proven by Gauss, is 2, along with all the primes which are 1 mod 4. This result is far from trivial, and proofs of it often include a lot of hairy algebra. These notes give a slick proof of Gauss's result using a variety of machinery that we have developed over the course of the course.

The proof can be broken into steps as follows:

1. Convert the question to one about factoring primes, and thus prime ideals, in $\mathbb{Z}[i]$
2. Make heavy use of the third isomorphism theorem for rings to reduce the question to one about squares in $\mathbb{F}_p$
3. Show that $-1$ is a square in $\mathbb{F}_p$ if and only if $p = 2$ or $p \equiv 1 \mod 4$
4. (Bonus) Show how this can be used to determine if composite numbers are sums of squares

## 2 Primes in $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ is a PID, so just like the integers, it has its own unique factorization of elements into primes. A natural question to ask is then, how do the normal integers factor in this bigger ring, $\mathbb{Z}[i]$? By unique factorization in $\mathbb{Z}$, it suffices to know how prime integers factor. Suppose a prime integer $p$ factors into non-units in $\mathbb{Z}[i]$. Then, because $p$ is real, the factors must be complex conjugates. Thus,

$$p = (a + bi)(a - bi) = a^2 + b^2.$$

Similarly, if $p = a^2 + b^2$ for some integers $a$ and $b$, then $p$ factors as $p = (a + bi)(a - bi)$ in $\mathbb{Z}[i]$. We now take a moment to show two basic results which will allow us to bring in various ring theory machinery.

**Lemma 1.** A principal ideal $(p)$ in an integral domain $R$ is prime if and only if $p$ is prime in $R$.

**Lemma 2.** In a PID, an element is prime if and only if it is irreducible.

If you're not convinced, these are good exercises to try as a way study for the final next week. Putting everything together, the upshot is that $p$ is a sum of squares if and only is the ideal $(p)$ is *not* prime in $\mathbb{Z}[i]$.

## 3 The Magic

We now introduce the star player in this proof.

**Theorem 1** (The Third Isomorphism Theorem for Rings)**.** Let $I$ be an ideal in a ring $R$. Then, there is a bijection

$$\{\text{Ideals of } R \text{ that contain } I\} \longrightarrow \{\text{ideals of } R/I\}, \qquad J \longmapsto J/I,$$

where $J/I$ is the set of cosets

$$J/I = \{a + I : a \in J\}.$$

Furthermore, let $J$ be an ideal of $R$ that contains $I$. Then, $J$ is prime if and only if $J/I$ is prime, $J$ is maximal if and only if $J/I$ is maximal, and there is an isomorphism of quotient groups

$$\frac{R/I}{J/I} \cong R/J.$$

Recall that our goal is to determine when $(p)$ is a prime ideal of $\mathbb{Z}[i]$. This is equivalent to determining whether $\mathbb{Z}[i]/(p)$ is an integral domain. We will make repeated use of the third isomorphism theorem to massage $\mathbb{Z}[i]/(p)$ into a more familiar form. First, observe that

$$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1).$$

This should feel familiar to the way we typically construct field extensions. The explicit isomorphism is determined by sending $i$ to $x$. Now, we apply the third isomorphism theorem. Here, $\mathbb{Z}[x]$ plays the role of $R$, $(x^2 + 1)$ plays the role of $I$, and $(p)$ plays the role of $J/I$. Plugging in,

$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[x]/(x^2 + 1)}{(x^2 + 1, p)/(x^2 + 1)} \cong \frac{\mathbb{Z}[x]}{(x^2 + 1, p)}.$$

Now we apply the theorem again, but this time we let $(p)$ take the role of $I$.

$$\frac{\mathbb{Z}[x]}{(x^2 + 1, p)} \cong \frac{\mathbb{Z}[x]/(p)}{(x^2 + 1, p)/(p)} \cong \frac{\mathbb{F}_p[x]}{(x^2 + 1)}.$$

The final ring should look familiar. It's a polynomial ring over a field, quotiented out by a principal ideal. Because polynomial rings over fields are PIDs, lemmas 1 and 2 tell us that the ideal is prime if and only if the generator, $x^2 + 1$, is irreducible in $\mathbb{F}_p[x]$. A degree 2 polynomial is reducible if and only if it has a root. So, all that's left to do is determine when $x^2 + 1$ has a root mod $p$, i.e. when $-1$ is a square mod $p$.

# 4 Squares in $\mathbb{F}_p$

In $\mathbb{F}_2$, $-1 = 1$, so $-1 = 1 = 1^2$ is a square. For the odd primes, we show the following result.

**Theorem 2.** $-1$ is a square modulo an odd prime $p$ if and only if $p$ is congruent to 1 modulo 4.

*Proof.* Any unit with multiplicative order 2 squares to 1, so it is a root of $x^2 - 1$. Recall that over a field, a polynomial of degree $d$ has at most $d$ roots. $x^2 - 1$ has $-1$ and 1 as roots, and in $\mathbb{F}_p$ for $p \geq 3$, $-1 \neq 1$, so $-1$ and 1 are the *only* roots of $x^2 - 1$. 1 has order 1, so the only element in the unit group with order 2 is $-1$.

If $a^2 = -1$, then $a^4 = (a^2)^2 = (-1)^2 = 1$, so $a$ has order 4. On the other hand, any element $a$ with order 4 squares to an element with order 2. $-1$ is the only such element, so we must have $a^2 = -1$. Thus, $-1$ is a square in $\mathbb{F}_p$ if and only if $\mathbb{F}_p^\times$ contains an element of order 4.

Recall that the unit group $\mathbb{F}_p^\times$ of the finite field $\mathbb{F}_p$ is cyclic. Thus, it has an element of order 4 if and only if its order is a multiple of 4.

$$\#F_p^\times = p - 1$$

so $-1$ is a square in $\mathbb{F}_p^\times$ if and only if $p - 1 \equiv 0 \mod 4$, i.e. if $p \equiv 1 \mod 4$. □

# 5 Putting it all together

In summary, we have the following chain of equivalences:

$$\begin{aligned} p = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z} &\iff (p) \text{ is not prime in } \mathbb{Z}[i] \\ &\iff \mathbb{Z}[i]/(p) \text{ is not an integral domain} \\ &\iff \mathbb{F}_p[x]/(x^2+1) \text{ is not an integral domain} \\ &\iff (x^2+1) \text{ is not prime in } F_p[x] \\ &\iff x^2+1 \text{ is reducible in } F_p[x] \\ &\iff -1 \text{ is a square modulo } p \\ &\iff p = 2 \quad \text{or} \quad p \equiv 1 \mod 4 \end{aligned}$$

Now, let's use this to classify all integers. Let $n$ be a positive integer. Suppose $n = a^2 + b^2 = (a - bi)(a + bi)$ for integers $a$ and $b$. Let $a + bi$ split into prime factors (in $\mathbb{Z}[i]$) as

$$a + bi = (x_1 + y_1 i)(x_2 + y_2 i) \cdots (x_k + y_k i).$$

By applying complex conjugation to each side, we obtain the prime factorization

$$a - bi = (x_1 - y_1 i)(x_2 - y_2 i) \cdots (x_k - y_k i).$$

Now, multiply the two equations, and group complex conjugate terms:

$$n = a^2 + b^2 = (a + bi)(a - bi) = (x_1 + y_1 i)(x_1 - y_1 i) \cdots (x_k + y_k i)(x_k - y_k i)$$

So, when you factor $n$ in $\mathbb{Z}[i]$, the prime factors come in complex conjugate pairs. Prime integers of the form $4t + 3$ are still prime in $\mathbb{Z}[i]$ (this is one half of what we spent the first two pages proving) so whenever any such prime $p$ appears in the prime factorization of $n$, it must come in pairs ($p$ is its own complex conjugate). Thus, $n$'s prime factorization has an even number of each prime of the form $4t + 3$.

It turns out that this condition is not only necessary, but in fact sufficient to determine whether $n$ is a sum of squares! To see this, suppose $n$'s prime factorization has an even exponent on all primes of the form $4t+3$. Factor $n$ in $\mathbb{Z}$ as

$$n = c^2 p_1 p_2 \cdots p_k,$$

where each $p_j$ is a distinct prime. By hypothesis, each $p_j$ is 2 or 1 mod 4, so it can be written as a sum of squares, $p_j = a_j^2 + b_j^2 = (a_j + b_j i)(a_j - b_j i)$. Doing this for all $p_j$,

$$n = c^2 (a_1 + b_1 i)(a_1 - b_1 i)(a_2 + b_2 i)(a_2 - b_2 i) \cdots (a_k + b_k i)(a_k - b_k i).$$

Now, multiply all the $(a_j + b_j i)$'s together into one big $A + Bi$, and similarly multiply all the $(a_j - b_j i)$'s to get $A - Bi$. Plugging in,

$$n = c^2 (A + Bi)(A - Bi) = c^2 (A^2 + B^2) = (cA)^2 + (cB)^2,$$

as desired.