Last time we began exploring the set

$$S := \{x^2 + y^2 : x, y \in \mathbb{Z}\} = \{0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34 \ldots\}$$

We observed that $n \in S$ if and only if $n = a^2 + b^2 = (a + bi)(a - bi)$ where $a \pm bi \in \mathbb{Z}[i]$, the *Gaussian integers*.

Before discussing $\mathbb{Z}[i]$ further, we recalled some basic facts about $\mathbb{C}$, the set of all complex numbers.

Definition (Complex conjugate) Given $z \in \mathbb{C}$, say $z = x + iy$ with $x, y \in \mathbb{R}$. The *complex conjugate of* z, denoted $\overline{z}$, is defined

$$\overline{z} := x - iy.$$

Note that

$$z\overline{z} = x^2 + y^2 = |z|^2,$$

where $|z|$ is the distance from z to 0. Both the absolute value and complex conjugation have nice properties:

Properties. Given $s, z \in \mathbb{C}$. Then

1. $\overline{s + z} = \overline{s} + \overline{z}$
2. $\overline{sz} = \overline{s}\,\overline{z}$
3. $|s + z| \leq |s| + |z|$ (the 'triangle inequality')
4. $|sz| = |s|\,|z|$

We can now state a criterion for membership in S quite succinctly in terms of our new notation:

Proposition: $n \in S$ if and only if $n = |\alpha|^2$ for some $\alpha \in \mathbb{Z}[i]$.

Great: we've taken a problem comprehensible by a third-grader and recast it in a language that makes it look more complicated. But there's one enormous advantage to changing our perspective: it allows us to see some structure in S that we weren't able to observe before:

Corollary: If $m, n \in S$, then $mn \in S$.

Proof. Given $m, n \in S$, we have $m = |\alpha|^2$ and $n = |\beta|^2$ for $\alpha, \beta \in \mathbb{Z}[i]$. Then $mn = |\alpha|^2|\beta|^2 = |\alpha\beta|^2$ and $\alpha\beta \in \mathbb{Z}[i]$, so $mn \in S$. □

This motivates the following question: which primes are in S? Let's take a look:

In S	Not in S
2, 5, 13, 17, 29, ...	3, 7, 11, 19, 23, 31,...

Jacob's Conjecture: $p \in S$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.
This is called *Fermat's Two-Squares Theorem*. One direction of the proof isn't too bad:

Proof of $\Rightarrow$:
We showed previously that if $n \in S$, then $n \not\equiv 3 \pmod 4$. So if $p \in S$, then $p \not\equiv 3 \pmod 4$, but $p \not\equiv 0 \pmod 4$ since p is prime, and $p \not\equiv 2 \pmod 4$ unless $p = 2$, so then either $p = 2$ or $p \equiv 1 \pmod 4$. ♣

The other direction (every prime that's 2 or $\equiv 1 \pmod 4$ is the sum of two squares) is significantly harder to prove. We will use the arithmetic of the Gaussian integers, in particular studying when a prime factors. What does this mean?

Recall the FTA in $\mathbb{Z}$: any number can be written (in an essentially unique way) as a product of primes. Why stop at primes? Because they're indivisible – they cannot be broken down into smaller pieces. But as soon as we expand from the world of $\mathbb{Z}$ to the world of $\mathbb{Z}[i]$, this is no longer true: we have $2 = (1+i)(1-i)$ and $5 = (2+i)(2-i)$. Thus, we might say that in the Gaussian integers, 2 and 5 are no longer prime, since they can be broken down into smaller pieces. Are these pieces smaller? How does one compare the size of two Gaussian integers? Absolute value, of course! Let's make this all precise:

Definition: Given $\alpha, \beta \in \mathbb{Z}[i]$.

1. We say α *is smaller than* β iff $|\alpha| < |\beta|$.
2. We say α is *composite* if and only if $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{Z}[i]$ both smaller than α.
3. We say α is *prime* if and only if α is not composite and α is not a unit.
4. We say $u \in \mathbb{Z}[i]$ is a *unit* if and only if $|u| = 1$.

Notice that we now have two kinds of primes: $p \in \mathbb{Z}$ that cannot be broken down as a product of two smaller *integers* and $\alpha \in \mathbb{Z}[i]$ that cannot be broken down as a product of two smaller *Gaussian integers*. To distinguish these, we call the former 'rational primes', and the latter *Gaussian primes*. Note that $2 = (1+i)(1-i)$ and $5 = (2+i)(2-i)$ are rational primes, but not Gaussian primes. Inspired by these examples, we guess the following:

Proposition: If a rational prime p is composite in $\mathbb{Z}[i]$ then $p = \pi\overline{\pi}$ for some $\pi \in \mathbb{Z}[i]$.

Proof of Proposition: Given a rational prime p that's composite in $\mathbb{Z}[i]$. Then by definition we can write p as a product of two smaller Gaussian integers, say, $p = \beta\gamma$ with $\beta, \gamma \in \mathbb{Z}[i]$ such that $|\beta|, |\gamma| < |p| = p$. Then $p^2 = |p|^2 = |\beta\gamma|^2 = |\beta|^2|\gamma|^2$. Note that $|\beta|^2, |\gamma|^2 \in \mathbb{Z}$, so we have two integers whose product is the square of a (rational) prime. Thus either $|\beta|^2 = 1$, $|\beta|^2 = p$, or $|\beta|^2 = p^2$. The first and third options can't happen, since β and γ are both smaller than p, whence $p = |\beta|^2 = \beta\overline{\beta}$. □

Of course the converse of the above proposition is also true. Thus we see that a rational prime p is composite in the Gaussian integers iff $p = \pi\overline{\pi}$, which happens iff $p \in S$. In other words, our question about which primes are the sums of two squares is secretly the same as asking which rational primes are also Gaussian primes!

To prove Jacob's Conjecture it now suffices to show that p is composite in $\mathbb{Z}[i]$ for every rational prime $p \equiv 1 \pmod 4$.

Claim: Given a rational prime p, if $p \equiv 1 \pmod 4$, then p is composite in $\mathbb{Z}[i]$.
Proof: If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$, so for some $x \in \mathbb{Z}$ we have $x^2 \equiv -1 \pmod p$. This means $p \mid x^2 + 1 = (x+i)(x-i)$, where $x \pm i$ are both Gaussian integers. If p were prime in $\mathbb{Z}[i]$, then we would have $p \mid x+i$ or $p \mid x-i$. But this is impossible, since $\frac{x \pm i}{p} = \frac{x}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i]$. Thus p must be composite in $\mathbb{Z}[i]$.

BUT WAIT! We are implicitly using an unproven fact about $\mathbb{Z}[i]$: that if a (Gaussian) prime divides the product of two (Gaussian) integers, then it must divide one of them. (Recall that we proved the analogous statement in $\mathbb{Z}$ at the start of the term.) It turns out that this holds in $\mathbb{Z}[i]$. Indeed, more is true:

Fundamental Theorem of Arithmetic for $\mathbb{Z}[i]$:
Any $\alpha \in \mathbb{Z}[i]$ can be written as a product of Gaussian primes $\alpha = \pi_1\pi_2\cdots\pi_k$. Moreover, the π_j's are unique up to order and units.

To clarify the uniqueness up to units bit, consider the two apparently different factorizations

$$5 = (2+i)(2-i) = (1-2i)(1+2i).$$

However, the factors are actually the same up to units, since

$$1 - 2i = (-i)(2+i) \qquad \text{and} \qquad 1 + 2i = i(2-i).$$

A bit of thought shows that this isn't actually different than the case of $\mathbb{Z}$; we were able to avoid mentioning units earlier because we only worked with *positive* integers. If we had written down an FTA for all of $\mathbb{Z}$ instead, it would look exactly like the one we just wrote for $\mathbb{Z}[i]$.

The proof of the FTA for $\mathbb{Z}[i]$ is essentially identical to the one for $\mathbb{Z}$, apart from one important subtlety that you will explore on Problem Set 8.

We've now characterized all the (rational) primes p that are sums of two squares: we've proved that $p \in S$ iff $p = 2$ or $p \equiv 1 \pmod 4$. What about the other (non-prime) numbers in S? Since S is closed under multiplication, any products of such primes must also be in S (e.g. $10 \in S$). But this isn't the full story, since for example $9 \in S$, and 9 isn't generated by 2 or primes $\equiv 1 \pmod 4$. Of course, 9 has to be in S since it's already a square; more generally, all numbers of the form p^2 where $p \equiv 3 \pmod 4$ must also be in S, as well as anything else forced to belong to S by closure under multiplication. It turns out this is now the full story: every element of S is generated by 2, all $p \equiv 1 \pmod 4$, and all p^2 with $p \equiv 3 \pmod 4$. We can state this in a cleaner way:

Theorem: A nonzero $n \in S$ if and only if $\nu_p(n)$ is even for all $p \equiv 3 \pmod 4$.
Proof:
$(\Leftarrow)$: We just proved this! ✓
$(\Rightarrow)$: Given $n \in S$, we know $n = |\alpha|^2$ for some $\alpha \in \mathbb{Z}[i]$, whence $n = \alpha\overline{\alpha}$. Consider the prime factorization (in $\mathbb{Z}[i]$) of α, say

$$\alpha = \pi_1\pi_2\cdots\pi_k$$

where $\pi_j \in \mathbb{Z}[i]$ are all prime. Then

$$n = \alpha\overline{\alpha} = \pi_1\overline{\pi_1}\pi_2\overline{\pi_2}\cdots\pi_k\overline{\pi_k} = |\pi_1|^2|\pi_2|^2\cdots|\pi_k|^2.$$

The theorem immediately follows from the following:

Lemma: For any prime $\pi \in \mathbb{Z}[i]$ we have

$$|\pi|^2 = \begin{cases} 2 & \text{or} \\ p & \text{for some } p \equiv 1 \pmod 4 \text{ or} \\ p^2 & \text{for some } p \equiv 3 \pmod 4. \end{cases}$$

We'll prove this lemma next time. □