Last time we completely characterized which integers can be written as the sum of two squares, by using the arithmetic of the Gaussian integers $\mathbb{Z}[i]$. One step of our proof was left incomplete, however:

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

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

Proof: Note that $|\pi|^2 \in \mathbb{Z}$ and $|\pi|^2 > 0$. We will consider the prime factorization in $\mathbb{Z}$ and compare this to the prime factorization in $\mathbb{Z}[i]$. Uniqueness of factorization (in both $\mathbb{Z}$ and $\mathbb{Z}[i]$) will allow us to win.

Consider the prime factorization of $|\pi|^2$ in $\mathbb{Z}$, say

$$|\pi|^2 = p_1 p_2 \cdots p_k \tag{$\dagger$}$$

where $p_j \in \mathbb{Z}$ are rational primes. On the other hand $|\pi|^2 = \pi\bar{\pi}$, and both $\pi$ and $\bar{\pi}$ are Gaussian primes. By the FTA for $\mathbb{Z}[i]$, this factorization is unique up to ordering and units; in other words, any prime factorization of $|\pi|^2$ in $\mathbb{Z}[i]$ uses *exactly two* Gaussian primes. On the other hand, each $p_j$ is divisible by a Gaussian prime, whence there are at most two rational primes in the factorization ($\dagger$). In other words, $k = 1$ or 2.

- If $k = 1$, then $|\pi|^2 = p$, whence $p = \pi\bar{\pi}$. But this means $p \in S$, so by Fermat's Two-Squares Theorem we know $p = 2$ or $p \equiv 1 \pmod 4$.
- If $k = 2$, then $|\pi|^2 = \pi\bar{\pi} = p_1 p_2$. By the FTA for $\mathbb{Z}[i]$ we deduce that both $p_1$ and $p_2$ are prime in $\mathbb{Z}[i]$, whence by our work from last class,

  $$p_1 \equiv 3 \pmod 4.$$

  Moreover, the FTA for $\mathbb{Z}[i]$ also implies $p_1 = u\pi$ for some unit $u \in \mathbb{Z}[i]$, whence

  $$p_1 = |p_1| = |u\pi| = |\pi|.$$

  Thus $|\pi|^2 = p_1^2$.

Putting the cases $k = 1$ and $k = 2$ together concludes the proof. □

This concludes our characterization of $S$, the numbers that can be written as the sum of two squares. What about sums of 3 squares? Or 4 squares? Or 5 squares? It turns out that the last question is redundant:

Theorem (Lagrange, 1770): Every $n \geq 0$ is the sum of four squares.

We won't prove this, but I encourage you to look up Lagrange's original proof (using the 'method of descent') – you have all the tools to fully understand it. Among other things, the first step of the proof will look quite familiar: it turns out that the set of all numbers that can be written as a sum of four squares is closed under multiplication, so it suffices to study which primes can be written as a sum of four squares.

As was the case with the two-squares theorem, the fact that being the sum of four squares is preserved under multiplication isn't at all obvious. In the case of two squares, we saw this by changing perspectives from $\mathbb{Z}$ to the Gauss integers $\mathbb{Z}[i]$. Similarly, for four squares, one can see the multiplicative property by rephrasing the problem as being about properties of the *Hurwitz integers*:

$$\mathcal{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}.$$

Here $i, j, k$ are generalizations of the imaginary number $i$, and generate the set of *quaternions*; they satisfy $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$ and $ki = j$. One can develop a theory of primes and prime factorization in $\mathcal{H}$ that is analogous to what happens in $\mathbb{Z}$ and $\mathbb{Z}[i]$, with a few changes. The first change is that the size of a Hurwitz integer $a + bi + cj + dk$ is measured by $\sqrt{a^2 + b^2 + c^2 + d^2}$, which explains why the Hurwitz integers are useful to prove Lagrange's theorem! (Indeed, it's not hard to verify that size of the product of two Hurwitz integers is the product of their individual sizes.)

A more fundamental difference between $\mathcal{H}$ and $\mathbb{Z}[i]$ or $\mathbb{Z}$ is that multiplication isn't commutative, and also that factorization into primes isn't quite unique. However, it turns out to be close enough that one can develop a slightly weaker version of the FTA, which is good enough to give a nice proof of Lagrange's theorem.

What about sums of three squares? Do they generate all integers? Nope: 7 cannot be written as the sum of three squares. Some playing around should convince you that numbers that are 7 (mod 8) can't be written as the sum of three squares, but this doesn't tell the whole story (e.g. 28 can't be written as a sum of three squares). Legendre was able to characterize sums of three squares:

Legendre's 3-squares Theorem: An integer $n \geq 0$ is the sum of three squares if and only if $n \neq 4^k(8\ell + 7)$.

The proof of this theorem is much harder than the proofs for two- or four-squares. One reason for this is that there's no 'three-dimensional' analogue of the Gaussian or Hurwitz integers. (In fact, it was Hamilton's failure to come up with a three-dimensional version of $\mathbb{C}$ that led him to invent the quaternions. For more on this, look up Frobenius' theorem on

real division algebras.)

It seems like we've now answered all the questions about sums of squares: there are complete descriptions of which integers can and cannot be written as the sum of two or three squares, and every positive integer can be written as the sum of four squares. There are other questions one may ask, however. For example, note that some integers can be represented in multiple different way as sums of squares, e.g.

$$25 = 5^2 + 0^2 = 4^2 + 3^2.$$

In how many ways can a number be written as a sum of squares? Amazingly, there are exact formulas! Let $r_k(n)$ denote the number of ways of writing $n$ as the sum of $k$ squares; thus

$$r_2(n) := \{(a, b) \in \mathbb{Z} : n = a^2 + b^2\},$$

so for example we have $r_2(1) = 4$. It turns out that

$$r_2(n) = 4 \sum_{d|n} \chi(d) \qquad \text{where} \qquad \chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv -1 \pmod 4 \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

(Note that $\chi$ is completely multiplicative and has period 4; these two properties make it a *Dirichlet character*, a type of function that plays a fundamental role in current number theory research. This topic is outside the scope of this course, but you will learn about it in a course on analytic number theory.)

The formula for $r_4(n)$ is also relative simple:

Theorem (Jacobi, 1860's): $r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d.$

The proof is beautiful, and uses Fourier Analysis. The starting point of the proof is to consider the function

$$\Theta(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z}$$

Some playing around should convince you that

$$\Theta(z)^4 = \sum_{k \geq 0} r_4(k) e^{2\pi i k z}.$$

This is where Fourier Analysis plays a role: it allows us to extract coefficients of such sums. Also crucial to the proof are some nice transformation properties of the $\Theta$ function. We will

not prove this theorem in this course, but the proof can be found in many places, e.g. Stein and Shakarchi's introductory textbook on Fourier Analysis.

You might think that everything about sums of squares must have been discovered a long time ago, but this is not the case. Before describing some extremely recent developments, let me first state a classical conjecture due to Euler (in a letter to Goldbach in 1750):

Euler's Conjecture: Every odd $n \geq 1$ can be written as $n = a^2+b^2+c^2+d^2$ such that $a+b+c+d = 1$.

Example: $3 = 1^2 + 1^2 + (-1)^2 + 0^2$ and $1 + 1 - 1 + 0 = 1$.

Theorem (Sun-Sun, 2016): Every $n \geq 1$ can be written as $n = a^2 + b^2 + c^2 + d^2$ such that $a + b + c + d = m^2$ for some $m \in \mathbb{Z}$. (They also proved a version of this with $m^2$ replaced by $m^3$.)

Many of these results can be unified using the following notation:

$$\mathscr{S}(n) := \{a + b + c + d : n = a^2 + b^2 + c^2 + d^2\}.$$

- Lagrange's theorem asserts that $\mathscr{S}(n) \neq \varnothing$.
- Euler's Conjecture says that $1 \in \mathscr{S}(n)$ for all odd $n$.
- Sun-Sun's theorem says $\mathscr{S}(n)$ must contain a perfect square and a perfect cube.

More generally, what can we say about $T \in \mathscr{S}(n)$?

- We know $T \equiv n \pmod 2$, since

$$T = a + b + c + d \equiv a^2 + b^2 + c^2 + d^2 = n \pmod 2.$$

- By the Cauchy-Schwarz inequality we have

$$T^2 = (a + b + c + d)^2 \leq (a^2 + b^2 + c^2 + d^2)(1^2 + 1^2 + 1^2 + 1^2) = 4n,$$

  whence $T \leq 2\sqrt{n}$.

It turns out that in most circumstances, these two conditions tell the whole story:

Theorem (Goldmakher-Pollack, 2018): If $4 \nmid n$, then $\mathscr{S}(n) = \{T \equiv n \pmod 2 : |T| \leq 2\sqrt{n}\}$.

There's a more complicated description one can give for those $n$ that are multiples of 4. It turns out that both Euler's conjecture and Sun-Sun's theorem are immediate consequences.