Lecture 2: Sums of squares

In lecture we discussed different ways of "counting" Pythagorean triples. In this problem set we start developing a different but related question. This is a long set of problems – if you get tired, you should skip to the end and watch the youtube video linked there!

The starting point is the following question:

Question 0.1. Which integers d can be written as the sum of two squares?

For each of the following integers, check if it can be written as the sum of two squares, and if it can, record how to do it. (You don't need to complete the entire table if it gets boring.)

number	Sum of 2 squares?	number	Sum of 2 squares?	number	Sum of 2 squares?
6		19		32	
7		20		33	
8		21		34	
9		22		35	
10		23		36	
11		24		37	
12		25		38	
13		26		39	
14		27		40	
15		28		41	
16		29		42	
17		30		43	
18		31		44	

It's hard to see a pattern! Try to formulate a conjecture just for the prime numbers:

number	Sum of 2 squares?	number	Sum of 2 squares?
3		29	
5		31	
7		37	
11		41	
13		43	
17		47	
19		53	
23		59	

Can you see a pattern for the primes?

1 Gaussian integers

Our analysis of this problem will rely on complex numbers. (If you need a refresher on multiplication and division for complex numbers, now is a good time to have someone explain it to you!)

Definition 1.1. The Gaussian integers $\mathbb{Z}[i]$ are the complex numbers $a + bi$ where both a, b are integers.

Graphically, $\mathbb{Z}[i]$ looks like the integer points in the complex plane $\mathbb{C}$. Note that the product of two Gaussian integers will still be a Gaussian integer. (Thus Gaussian integers form a mathematical object called a *ring*.)

The key fact about multiplication in $\mathbb{Z}$ is the existence of prime factorizations. Let's formulate a version of this statement which allows both positive and negative numbers. An integer p (positive or negative) is said to be prime if its only divisors are $1, -1, p, -p$. Here is one statement of the fundamental theorem of arithmetic:

Theorem 1.2. *Let n be a number that is not $0, \pm 1$. Then we can write*

$$n = cp_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

where $c = \pm 1$, the a_i are positive integers, and each p_i is a positive prime number. This decomposition is "essentially unique": the only ambiguity is the order of the prime factors.

It turns out that $\mathbb{Z}[i]$ also admits a similar theory! Suppose that $x, z \in \mathbb{Z}[i]$. We will say that x divides z, and write $x|z$, if there is some other element $y \in \mathbb{Z}[i]$ satisfying $xy = z$. Our first goal is to understand the divisibility relation in $\mathbb{Z}[i]$.

1) Does $1 - i$ divide $-5 + 3i$?

2) Does $2 - 2i$ divide $-7 + 4i$?

3) Does $4 + 5i$ divide $14 + 3i$?

The key tool for understanding divisibility in $\mathbb{Z}[i]$ is the norm:

$$N(a + bi) = a^2 + b^2$$

In other words, $N(z)$ is the distance from z to the origin in the complex plane.

4) Prove the following properties of the norm:

a) For every $x, y \in \mathbb{Z}[i]$ we have $N(xy) = N(x)N(y)$.

b) If $x|z$ then $N(x)|N(z)$.

Using the norm, answer the following questions:

5) There is a set of special Gaussian integers in $\mathbb{Z}[i]$ that are called units: $1, -1, i, -i$.

   a) Prove that the units divide every Gaussian integer.

   b) Show that the units are the only Gaussian integers which divide every Gaussian integer.

   An equivalent way of identifying the units is the set of all divisors of 1.

6) Find all the factors of 2 in $\mathbb{Z}[i]$.

7) Find all the factors of $3 - i$ in $\mathbb{Z}[i]$.

8) Find all the factors of 5 in $\mathbb{Z}[i]$.

Every Gaussian integer $x \in \mathbb{Z}[i]$ that is not 0 or a unit will have at least eight factors: $\pm 1, \pm i, \pm x, \pm ix$. We call these "trivial factors" (since they don't contain any interesting information about x).

Definition 1.3. A Gaussian integer x is prime if the only divisors of x are the trivial factors.

It turns out that there is a very tight relationship between the primes in $\mathbb{Z}[i]$ and the primes in $\mathbb{Z}$. The following exercises are intended to tease out this relationship:

9) Note that an integer p that is prime in $\mathbb{Z}$ need not be prime in $\mathbb{Z}[i]$. (What are some examples?) However, it is also possible that a prime number p remains prime in $\mathbb{Z}[i]$. Show that 7 and 11 are primes in $\mathbb{Z}[i]$.

10) Show that if a Gaussian integer x has $N(x) = p$ for a prime number p then x is prime. In particular, conclude that if an integer p is prime in $\mathbb{Z}$ but not prime in $\mathbb{Z}[i]$ then every non-trivial factor of p is prime. (What are some examples?)

11) Show that a prime p in $\mathbb{Z}$ will fail to be prime in $\mathbb{Z}[i]$ if and only if we can write $p = a^2 + b^2$ for some integers a, b.

The following theorem is an analogue of the prime factorization theorem that holds in $\mathbb{Z}[i]$. Let's call a Gaussian integer $a + bi$ positive if $a > 0$ and $b \geq 0$. Note that every non-zero Gaussian integer has a unique conjugate that is positive.

Theorem 1.4. *Let x be a Gaussian integer that is not 0 or a unit. Then we can write*

$$x = u\rho_1^{a_1}\rho_2^{a_2}\dots\rho_k^{a_k}$$

where u is a unit, the a_i are positive integers, and each ρ_i is a positive prime in $\mathbb{Z}[i]$. This decomposition is "essentially unique": the only ambiguity is the order of the prime factors.

If we take this theorem for granted, we can completely describe the primes in $\mathbb{Z}[i]$:

12) Given a Gaussian integer $x = a + bi$, we denote its conjugate by $\overline{x} = a - bi$. Show that x is prime if and only if $\overline{x}$ is prime.

13) Suppose that x is a prime Gaussian integer. Using unique factorization in $\mathbb{Z}[i]$, show that $N(x) = x\overline{x}$ is either a prime number or the square of a prime.

14) Put together all the work we have done so far to describe a complete list of the primes in $\mathbb{Z}[i]$:

    a) The four prime factors of 2: $1 + i$, $1 - i$, $-1 - i$, $-1 + i$.

    b) For the odd primes p in $\mathbb{Z}$ which cannot be written as a sum of two squares we have four associated primes: $\pm p, \pm ip$.

    c) For the odd primes p in $\mathbb{Z}$ which can be written as a sum of two squares $p = a^2 + b^2$ we have eight associated primes: $\pm a \pm bi$ and $\pm b \pm ai$.

2 Finding solutions

Finally we return to our starting question: which integers d can be written as a sum of two squares? Our starting point is the following theorem (which is too hard to leave as an exercise):

Theorem 2.1 (Fermat, Euler)**.** *An odd prime $p \in \mathbb{Z}$ can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

So, the primes which are 1 more than a multiple of 4 will factor in $\mathbb{Z}[i]$, while the primes which are 3 more than a multiple of 4 will remain prime in $\mathbb{Z}[i]$. Using this property, we can answer our original question:

Theorem 2.2. *A positive integer d can be written as the sum of two squares if and only if in the prime factorization of d (inside of $\mathbb{Z}$) every prime that is congruent to 3 mod 4 appears an even number of times.*

Here are the steps to prove this theorem:

15) Let's consider the prime factorization of d inside of $\mathbb{Z}$. It will be helpful to separate out the primes depending on their congruence class mod 4:

$$d = 2^c p_1^{a_1} \dots p_k^{a_k} q_1^{b_1} \dots q_l^{b_l}$$

where each p_i is 1 more than a multiple of 4 and each q_i is 3 more than a multiple of 4. Using our classification of Gaussian primes, explain how to determine the prime factorization of d inside of $\mathbb{Z}[i]$.

16) Show that a positive integer d is a sum of two squares in $\mathbb{Z}$ if and only if there is a Gaussian integer x such that $n = x \cdot \overline{x}$. Explain why this is the same as saying that the prime factors of d in $\mathbb{Z}[i]$ can be assigned into "pairs" which have the same norm: half to divide x and half to divide $\overline{x}$.

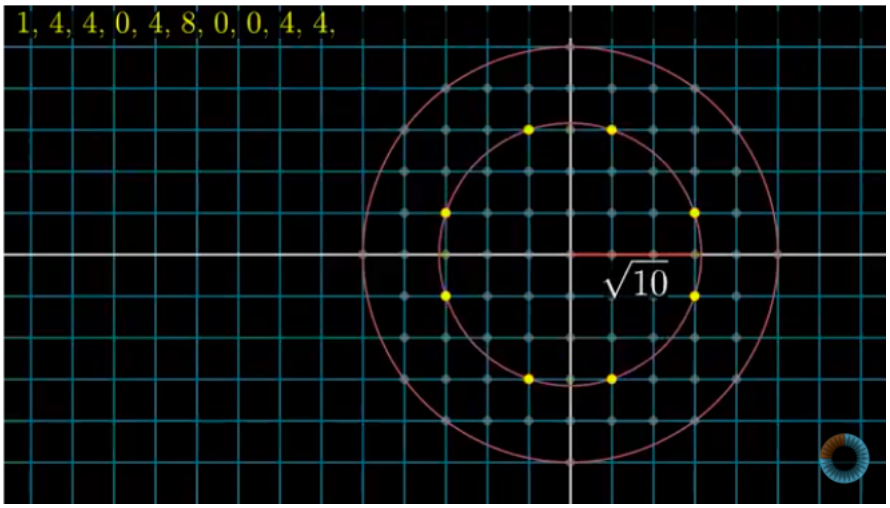
17) Combine the previous exercises to prove Theorem 2.2.

3 Counting points on the circle

We next discuss an "upgrade" of our original question:

Question 3.1. Suppose that d can be written as a sum of two squares. How many different integer pairs (a, b) satisfy $d = a^2 + b^2$?

This is the same thing as asking: how many integer points lie on the circle of radius $\sqrt{d}$?



8 points on the circle of radius $\sqrt{10}$

For example there are twelve different integer points on the circle of radius 50:

$$(\pm 5, \pm 5), (\pm 7, \pm 1), (\pm 1, \pm 7).$$

18) Try generating some data for small values of d. (Unfortunately it will probably be hard to spot any patterns.)

A great way to think about this question is to use complex numbers. Note that we have:

$$d = a^2 + b^2 \qquad \Leftrightarrow \qquad d = (a + ib)(a - ib)$$

In other words, our original question can be rephrased:

Question 3.2. Suppose that d is a positive integer. How many different ways are there to factor d in $\mathbb{Z}[i]$ as a product of a Gaussian integer x and its conjugate: $d = x \cdot \overline{x}$?

We can approach this question using prime factorizations. First let's factor d inside of $\mathbb{Z}$. It will be helpful to separate out the primes depending on their congruence class mod 4:

$$d = 2^c p_1^{a_1} \dots p_k^{a_k} q_1^{b_1} \dots q_l^{b_l}$$

where each p_i is 1 more than a multiple of 4 and each q_i is 3 more than a multiple of 4. If d can be written as a sum of two squares, then each b_i is even. So instead let's write:

$$d = 2^c p_1^{a_1} \dots p_k^{a_k} q_1^{2b_1} \dots q_l^{2b_l}$$

Using our earlier description of primes in $\mathbb{Z}[i]$, we can upgrade this to a prime factorization in $\mathbb{Z}[i]$. (Remember, to make our prime factorization unique we insist that each Gaussian prime lies in the upper right hand quadrant.) Each q_i is already a Gaussian prime. The factor 2 becomes the square of a prime (up to units): $2 = (-i)(1 + i)^2$. Each factor p_i splits into a product of two different Gaussian primes $p_i = (-i)(a + bi)(b + ai)$. Altogether our prime factorization is

$$d = u(1 + i)^{2c} \rho_1^{a_1} \widehat{\rho}_1^{a_1} \dots \rho_k^{a_k} \widehat{\rho}_k{}^{a_k} q_1^{2b_1} \dots q_l^{2b_l}$$

where u is the unit $(-i)^{c + \sum a_i}$ and ρ_i and $\widehat{\rho}_i$ are two Gaussian primes whose norms are the same.

Now let's think about how to choose an x such that $x \cdot \overline{x} = d$. Looking at prime factorizations, both x and $\overline{x}$ will consist of exactly half of the Gaussian primes dividing d. Furthermore, these primes must occur in pairs: the Gaussian primes of norm N must be split evenly between x and $\overline{x}$.
It is a little easier to count if we insist that x lie in the upper right quadrant.

19) Suppose x lies in the upper right hand quadrant. Explain why:

a) Exactly half of the primes $(1+i)^{2c}$ must divide x.

b) Exactly half of the primes $q_i^{2b_i}$ must divide x.

c) Out of the prime factors $\rho_i^{a_i} \cdot \widehat{\rho}_i^{a_i}$, we have $a_i + 1$ different ways of choosing which primes are assigned to x and which are assigned to $\overline{x}$.

20) Show that the number of ways that d can be written as a sum of two squares is $4\prod_{i=1}^{k}(a_i+1)$.

Remark 3.3. You might guess that our analysis will have an interesting interaction with Gauss' circle problem. And you would be right! Please watch the 3Blue1Brown youtube video on this topic titled "Pi hiding in prime regularities":
`https://youtu.be/NaL_Cb42WyY`