Math 361 lecture for Monday, Week 1

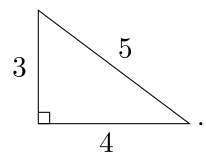
Pythagorean triples

A *Pythagorean triple* is a tuple (x, y, z) of positive integers such that

$$x^2 + y^2 = z^2.$$

It is *primitive* if $\gcd(x, y, z) = 1$.

Example 1. We have $3^2 + 4^2 = 5^2$:



Problem. Find all primitive Pythagorean triples.

First observations.

1. If (x, y, z) is a primitive Pythagorean triple, and m is a positive integer, then (mx, my, mz) is a Pythagorean triple. If (x, y, z) is any Pythagorean triple, then canceling common factors yields a primitive Pythagorean triple.

2. If two of x, y, z in a Pythagorean triple (x, y, z) share a prime factor p, then so does the third. For instance, if $x = px'$ and $z = pz'$, then $y^2 = z^2 - x^2$ is divisible by p. Since p divides y^2 and p is prime, considering the prime factorization of y, we see that p divides y. Thus, for a Pythagorean triple (x, y, z), we have $\gcd(x, y, z) = 1$ if and only if x, y, z are pairwise relatively prime.

3. If (x, y, z) is a primitive Pythagorean theorem, then z must be odd, and exactly one of x and y is even and one is odd. Here are the squares modulo 4:

$$0^2 = 0,\ 1^2 = 1,\ 2^2 = 0,\ 3^2 = 1 \bmod 4.$$

   If a number is odd, then it is 1 or 3 modulo 4, and hence, its square is 1 modulo 4. Similarly, if a number is even, it is 0 or 2 modulo 4, and its square is 0 modulo 4. Since (x, y, z) is primitive, then since we just saw that x, y, z are pairwise relatively prime, at most one of x and y is even. This means that $x^2 + y^2$ is either 1 or 2 modulo 4. However, $z^2 = x^2 + y^2 \neq 2 \bmod 4$, since no square is 2 modulo 4. So $z^2 = x^2 + y^2 = 1$. The result follows.

The key idea we will use to find all Pythagorean triples is the factorization

$$x^2 + y^2 = (x + iy)(x - iy).$$

Define

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

Then $\mathbb{Q}(i)$ is a field. For instance, $\mathbb{Q}(i)$ is closed under multiplication: if $a, b, c, d \in \mathbb{Q}$, then

$$(a + bi)(c + di) = (ac - db) + (ad + bc)i \in \mathbb{Q}(i).$$

Further, if $a + bi \neq 0$, its inverse is

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{1}{a^2 + b^2}(a - bi) = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in \mathbb{Q}(i).$$

The field $\mathbb{Q}(i)$ is the smallest subfield of $\mathbb{C}$ containing i. Define the *Gaussian integers* to be the ring

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

We will define the word "ring" next time. For now, just think of it as a field except that multiplicative inverses of nonzero elements are not guaranteed. For instance, $\mathbb{Z}$, itself, is also a ring.

Factorization in $\mathbb{Z}[i]$. Here, we will see that the relationship between $\mathbb{Q}(i)$ and $\mathbb{Z}[i]$ is much like the relationship between $\mathbb{Q}(i)$ and $\mathbb{Z}[i]$.

Definition 2.

1. Let $a, b \in \mathbb{Z}[i]$. Then a *divides* b, written $a|b$ if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$.
2. An element $u \in \mathbb{Z}[i]$ is a *unit* if $u|1$, i.e., if there exists $v \in \mathbb{Z}[i]$ such that $1 = uv$.
3. An element $p \in \mathbb{Z}[i]$ is *prime* if it is not 0 or a unit and whenever p divides ab for some $a, b \in \mathbb{Z}[i]$, then $p|a$ or $p|b$.

Fact. The ring $\mathbb{Z}[i]$ is a unique factorization domain (UFD). That is, every element nonzero $a \in \mathbb{Z}[i]$ can be written uniquely, up to order, in the form

$$a = u \prod_{i=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are primes, and the e_i are positive integers. (We will go into this topic more deeply later.)

Example 3. It will follow from homework that the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$, and that $1 \pm i$ is prime. Although 2 is prime in $\mathbb{Z}$, it is not prime in $\mathbb{Z}[i]$. Its prime factorization in $\mathbb{Z}[i]$ is

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

Proposition 4. Let (x, y, z) be a primitive Pythagorean triple. Then

$$x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with u a unit.

Proof. Let $p \in \mathbb{Z}[i]$ be an arbitrary prime dividing $x + iy$. It suffices to show that p divides $x+iy$ an even number of times, i.e., p occurs with even multiplicity in the prime factorization of $x + iy$.

Say the prime factorization of z is

$$z = v \prod_{i=1}^{k} p_i^{e_i},$$

with v a unit and the p_i primes in $\mathbb{Z}[i]$. Since

$$(x + iy)(x - iy) = z^2 = v^2 \prod_{i=1}^{k} p_i^{2e_i}$$

and $p|(x + iy)$, it follows that $p = p_i$ for some i and p divides z^2 an even number of times. Since all of the primes in the prime factorization of z^2 come from primes in the factorizations of $x + iy$ and $x - iy$, is suffices to show that p does not divide $(x - iy)$.

For the sake of contradiction, suppose p divides both $x + iy$ and $x - iy$. So p divides $z^2 = (x+iy)(x-iy)$, and since p is prime, it divides z. Further, p divides $(x+iy)-(x-iy) = 2x$. Note that when we talk about dividing here, we mean dividing as elements in the ring $\mathbb{Z}[i]$, not as elements $\mathbb{Z}$. Thus, for instance $p|z$ means there exists $s \in \mathbb{Z}[i]$ such that $z = ps$.

Since (x, y, z) is primitive, it follows that x and z are relatively prime. (Be careful here: this means that x and z share no integer prime factors, and we are concerned about divisibility by p in $\mathbb{Z}[i]$.) As we saw earlier, z is odd. Hence, $2x$ and z are relatively prime integers. Recall that if $a, b \in \mathbb{Z}$, then $\gcd(a, b)$ is an integer linear combination of a and b. Therefore, there exist $m, n \in \mathbb{Z}$ such that

$$2xm + zn = \gcd(2x, z) = 1.$$

Thinking again about division in $\mathbb{Z}[i]$, since p divides both $2x$ and z, it follows that $p|1$, and hence, p is a unit, which contradicts the fact that p is prime. This contradiction completes the proof. $\square$

Corollary 5. The primitive Pythagorean triples are exactly

$$(m^2 - n^2, 2mn, m^2 + n^2) \quad \text{or} \quad (2mn, m^2 - n^2, m^2 + n^2)$$

where $m, n \in \mathbb{Z}_{>0}$ are relatively prime, not both of the same parity, and $m > n$.

Proof. We leave the check that the displayed triples are primitive if and only if m and n are relatively prime and of differing parity as an exercise. (Hint: Rule out the case of a shared factor of 2 first. As part of that case, what goes wrong if m and n have the same parity?)

Next, note that

$$\begin{aligned}(m^2 - n^2)^2 + (2mn)^2 &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2.\end{aligned}$$

for all $m, n \in \mathbb{Z}$. So the displayed triples are Pythagorean triples (we take $m > n$ so that each component is positive).

For the converse, suppose (x, y, z) is a primitive Pythagorean triple. By Proposition 4,

$$(x + iy)(x - iy) = x^2 + y^2 = z^2 \quad \Rightarrow \quad x + iy = uw^2$$

for some $u, w \in \mathbb{Z}[i]$ with u a unit. Write $w = m + ni$ with $m, n \in \mathbb{Z}$. It follows that

$$x + iy = u(m + in)^2 = u((m^2 - n^2) + 2mni).$$

The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. Equating real and imaginary parts, we have

$$(|x|, |y|) = (|m^2 - n^2|, |2mn|) \quad \text{or} \quad (|x|, |y|) = (|2mn|, |m^2 - n^2|).$$

Since $x, y > 0$, the result follows. $\square$

Exercise 6. Show that the Pythagorean triple $(9, 12, 15)$ does not have either of the forms in the corollary. Why isn't that a contradiction? How can you modify the corollary so that it covers all Pythagorean triples?