1 Rational Points on Curves

1.1 The Pythagorean Theorem

One of the most fundamental theorems in geometry is the *Pythagorean theorem*, which says that the side lengths X, Y, and Z of a right triangle satisfies

$$X^2 + Y^2 = Z^2.$$

When X, Y, and Z are all integers, we call (X, Y, Z) a *Pythagorean triple*. Some famous Pythagorean triples are

$$(3, 4, 5), (5, 12, 13), (8, 15, 17), \ldots$$

How many Pythagorean triples are there? Well, if we start with any triple (say $(3, 4, 5)$), then we get infinitely many triples just by considering all multiples of the triple:

$$(3, 4, 5), (6, 8, 10), (9, 12, 15), \ldots$$

That was a little easy, so let's instead consider *primitive Pythagorean triples*. The triple (X, Y, Z) is called primitive if X, Y, and Z don't share a common factor. So $(3, 4, 5)$ is primitive, but $(6, 8, 10)$ and $(9, 12, 15)$ are not; the triple $(5, 12, 13)$ is primitive, but $(10, 24, 26)$ is not. How many primitive Pythagorean triples are there?

It turns out that there are also infinitely many primitive Pythagorean triples. One way to see this is by taking the sequence of perfect squares, and considering the difference between neighboring terms.

$$1 \xrightarrow{+3} 4 \xrightarrow{+5} 9 \xrightarrow{+7} 16 \xrightarrow{+9} 25 \xrightarrow{+11} \ldots$$

We see that differences of neighboring squares are just the odd integers! Indeed, we have

$$(n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

There are infinitely many odd integers that are also perfect squares. Now whenever $2n + 1 = m^2$ for some integer m, we see that $(m, n, n + 1)$ is a Pythagorean triple. Since the positive integers n and $n + 1$ can't share a common factor, it follows that $(m, n, n + 1)$ is a primitive Pythagorean triple. Therefore, we conclude that there are infinitely many primitive Pythagorean triples.

The triples $(3, 4, 5)$ and $(5, 12, 13)$ are examples of these triples of the form $(m, n, n + 1)$. However, the primitive triple $(8, 15, 17)$ is not of this form. Therefore, our argument above shows that there are infinitely many primitive Pythagorean triples, but we haven't yet found all of the primitive Pythagorean triples.

Let's take our question one step further. The goal of today's lecture is to answer

*Q: What are **all** of the primitive Pythagorean triples?*

In other words, we'll try to find some formula that will give us every single Pythagorean triple.

1.2 Diophantine Equations

Our goal is to solve the equation

$$X^2 + Y^2 = Z^2, \quad X, Y, Z \in \mathbb{Z}.$$

The problem of finding integer solutions to a polynomial equation belongs to the study of *Diophantine equations.* The study of Diophantine equations is one of the most ancient branches of mathematics, dating back to mathematicians such as Pythagoras (c. 500 BC), Pappus of Alexandria (c. 350 BC), and its namesake Diophantus (c. 250 CE). The Pythagorean theorem gives one of the most fundamental and historically important Diophantine equations.

Let's assume that (X, Y, Z) is a primitive triple, so that the integer side lengths X, Y, and Z don't share a common prime factor. Now since

$$X^2 = Z^2 - Y^2,$$

if Y and Z are both multiples of a prime p then X is also a prime multiple of p. Repeating for Y and Z, we see that if (X, Y, Z) is a primitive triple, then no pair of sides $(X, Y), (Y, Z)$, or (Z, X) share a common prime factor.

In particular, the point (x, y) defined

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}$$

satisfies that (i) x and y are both rational numbers and (ii) the fractions X/Z and Y/Z are reduced.

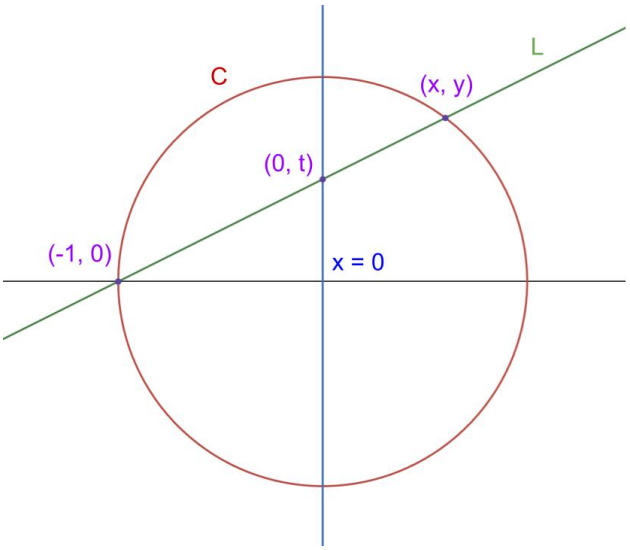
We will call such a point (x, y) with $x, y \in \mathbb{Q}$ a *rational point.* In particular, we have that (x, y) satisfies

$$x^2 + y^2 = 1,$$

which is the equation for a circle. We see that the problem of finding a primitive Pythagorean triple is equivalent to the problem of finding a rational point on the circle!

$$X^2 + Y^2 = Z^2,\ X, Y, Z \in \mathbb{Z} \quad \longleftrightarrow \quad x^2 + y^2 = 1,\ (x, y) \in \mathbb{Q}^2.$$

Now let's tackle this new question. We want to find all the rational points on a circle: we can do so using the power of geometry. Consider the following diagram.



Let C be the unit circle defined by the equation $x^2 + y^2 = 1$. Our idea is to project the points of C onto the y-axis from the point $(-1, 0)$. Let L be a line passing through the points $(-1, 0)$ and $(0, t)$. The equation of L is then

$$y = t(x + 1).$$

The line L intersects C at two points: once at $(-1, 0)$, and once at (x, y). To solve for the values for x and y in terms of t, we can solve the system of equations

$$\begin{cases} y & = t(x+1) \\ x^2 + y^2 & = 1. \end{cases}$$

Substituting, we have

$$x^2 + t^2(x+1)^2 = 1 \implies (x+1)((1+t^2)x - 1 + t^2) = 0,$$

which give the x-values

$$x = -1, \frac{1-t^2}{1+t^2}.$$

Substituting $y = t(x + 1)$, we find that the line L intersects C at the points

$$(x, y) = (-1, 0), \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

We can also find t from x and y since

$$t = \frac{y}{x+1}.$$

Importantly, we see that x and y are rational functions of t, and conversely that t is a rational function of x and y. This means that whenever t is a rational number ($t \in \mathbb{Q}$), then x and y are rational numbers ($x, y \in \mathbb{Q}$), and *vice versa*. In particular, every rational point on C is parametrized (represented) by some rational point on L!

Therefore, let $t = m/n$ be a rational number, where m and n do not share any common prime factors. Then its corresponding point on C is

$$x = \frac{1-t^2}{1+t^2} = \frac{n^2-m^2}{n^2+m^2}, \quad y = \frac{2t}{1+t^2} = \frac{2mn}{n^2+m^2}.$$

These describe all of the rational points on C!

Now to recover our original question about primitive Pythagorean triples (X, Y, Z), note that we have

$$\frac{X}{Z} = \frac{n^2-m^2}{n^2+m^2}, \quad \frac{Y}{Z} = \frac{2nm}{n^2+m^2}.$$

Since we said that X/Z and Y/Z are reduced, there exists some positive integer $\lambda \in \mathbb{Z}$ satisfying

$$\lambda X = n^2 - m^2, \quad \lambda Y = 2nm, \quad \lambda Z = n^2 + m^2.$$

We'd like to show that $\lambda = 1$. Note that λ divides $n^2 - m^2$ and $n^2 + m^2$, so also divides their sum $2n^2$ and their difference $2m^2$. Since n and m do not share any prime divisors, it follows that λ divides 2, and therefore $\lambda = 1$ or $\lambda = 2$.

We make a key observation: in a primitive Pythagorean triple (X, Y, Z), the integers X and Y can not both be odd. If this were the case, then $X^2 + Y^2 \equiv 2 \pmod 4$, but the square Z^2 can only be

equivalent to 0 or 1 mod 4. Therefore, one of X and Y are even, and the other is odd. Thus, let's first only consider triples such that X is odd.

Suppose that $\lambda = 2$. The quantity $n^2 - m^2 = 2X$ is then even, but is not a multiple of 4 since we are assuming X is odd. In other words, $n^2 - m^2 \equiv 2 \pmod 4$. But if n and m are both integers, then $n^2 - m^2$ can only be one of $0, 1$, or 3 mod 4. This is a contradiction, and hence $\lambda = 1$.

Therefore, when X is odd and Y is even, all primitive Pythagorean triples are given by

$$X = n^2 - m^2, \quad Y = nm, \quad Z = n^2 + m^2.$$

To get the triples such that X is even and Y is odd, we can interchange X and Y from above.

These formulas give all of the primitive Pythagorean triples as we vary n and m! (With n and m coprime). For example, when $n = 37$ and $m = 18$, we have

$$X = 1045, \quad Y = 1332, \quad Z = 1693$$

Indeed, we see

$$1045^2 + 1332^2 = 2866249 = 1693^2.$$