Introduction: Pythagorean Triplets

On this first day I want to give you an idea of what sorts of things we talk about in number theory. In number theory we want to study the *natural numbers*, and in particular what we think of as their "multiplicative structure." The natural numbers are fundamentally *discrete*, which means that we can't subdivide them; this fact becomes very important.

I like to think of number theory as being divided into two fields: understanding the structure of the prime numbers (often linked to "analytic number theory"), and finding integer-valued solutions to polynomial equations (often "algebraic number theory"). Both of these topics, as we will see, date back at least to ancient Greece, as well as appearing in ancient Babylonian, Chinese, Indian, and Islamic mathematics texts.

The first couple weeks of the course will focus mostly on the prime numbers; today I want to do an example of a very number theoretical argument in the algebraic vein, which requires essentially no background.

Algebraic Number Theory: Pythagorean Triplets

A famous result from ancient Greece is the Pythagorean theorem, which states that if a right triangle has side lengths of a and b and a hypotenuse of length c, then $a^2 + b^2 = c^2$. Most of you can probably give me a set of integers that solve this equation; two common examples are $(3, 4, 5)$ and $(5, 12, 13)$.

Definition 0.1. A *pythagorean triple* is a triple of integers (a, b, c) that satisfies the equation $a^2 + b^2 = c^2$.

However, it's not actually that easy to find these pythagorean triples. If you pick a random pair of integer side lengths, the hypotenuse will usually not be an integer; famously, the Pythagoreans discovered irrational numbers by considering the right triangle with side lengths $(1, 1, \sqrt{2})$—and then found the concept of irrational numbers so religiously disturbing that revealing it to outsiders punishable by death.

So integer solutions definitely exist, but are not trivial to find. So we might ask how many solutions there are.

Question 0.2. How many pythagorean triples exist?

It turns out that as phrased, this question is actually really easy to answer. (Stop and think about it for a minute). We know that $(3, 4, 5)$ is a pythagorean triple; we can see that

so is $(6, 8, 10)$ and $(9, 12, 15)$ and so on. In general, if (a, b, c) is a pythagorean triple, and n is an integer, then (na, nb, nc) is also a pythagorean triple.

But this seems like cheating! We really only have one solution, we're just "rescaling" it a bunch. We'd like to not "double-count" solutions like this.

Definition 0.3. A *reduced pythagorean triple* is a pythagorean triple (a, b, c) of integers with no common factors.

This prevents double-counting: $(3, 4, 5)$ is a reduced pythagorean triple, but $(6, 8, 10)$ is not. So we now ask a better question:

Question 0.4. How many reduced pythagorean triples exist?

Let's return to the equation $a^2 + b^2 = c^2$. To take into account the "no common factors", we can divide through by c^2, and we get the equivalent equation $(a/c)^2 + (b/c)^2 = 1$. We can no longer ask for integer solutions to this equation since we've divided by c^2, but we can ask for *rational* solutions.

Thus we see that every reduced pythagorean triple gives us a rational solution to the equation $x^2 + y^2 = 1$; it also turns out that every rational solution to $x^2 + y^2 = 1$ gives us exactly one reduced pythagorean triple.

(If $(p/q)^2 + (m/n)^2 = 1$, then $(pn)^2 + (qm)^2 = (qn)^2$, and if p/q and m/n are in lowest terms then pn, qm, qn will have no common factors so we get a unique reduced triple).

Question 0.5. How many rational number solutions does the equation $x^2 + y^2 = 1$ have?

You may notice that this equation is the equation for a circle, and thus we can rephrase this by asking how many rational points there are on a circle. (You might think a circle obviously has infinitely many points. It definitely has infinitely many *real* points, but that doesn't mean it has infinitely many *rational* points; we'll come back to this idea later).

Thus this question has suddenly changed into a question about geometry! (One subset of algebraic number theory techniques is known as "arithmetic geometry"). And since we're studying geometry, we can draw a picture:

We'll draw a picture with four elements:

- The unit circle, centered at zero. (This has the points we're trying to count).
- A point at $(-1, 0)$, the leftmost point of the circle.
- A vertical line $x = 1$ tangent to the rightmost point of the circle.

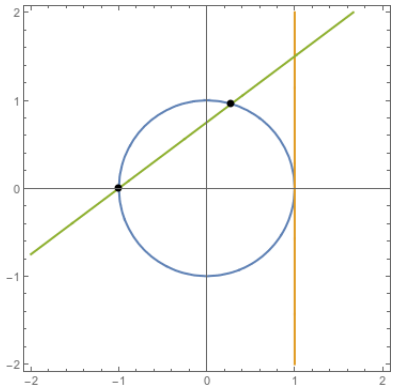

Figure 0.1: Rational Points on the Unit Circle

- A line connecting the point at $(-1, 0)$ to a point $(1, p/q)$ on the vertical line.

For any rational number p/q, the line will intersect the circle in exactly two points: $(-1, 0)$ and one other. Since there are infinitely many rational numbers, this seems like it should answer our question, and tell us that there are infinitely many reduced triples. But we need to make sure that we have a *rational* point. So let's see where the second intersection happens. The equation of this line is:

$$\begin{aligned} y - y_1 &= \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) \\ y - 0 &= \frac{p/q}{1 - (-1)}(x - (-1)) \\ y &= \frac{p}{2q}(x + 1) \end{aligned}$$

We can substitute this in to the equation for the circle and get

$$\begin{aligned} x^2 + \left(\frac{p}{2q}(x+1)\right)^2 &= 1 \\ x^2 + \frac{p^2(x+1)^2}{4q^2} &= 1 \\ 4q^2x^2 + p^2x^2 + 2p^2x + p^2 &= 4q^2 \\ (4q^2 + p^2)x^2 + (2p^2)x + (p^2 - 4q^2) &= 0 \end{aligned}$$

and by the quadratic formula we have

$$\begin{aligned} x &= \frac{-2p^2 \pm \sqrt{4p^4 - 4(4q^2+p^2)(p^2-4q^2)}}{2(4q^2+p^2)} \\ &= \frac{-2p^2 \pm \sqrt{4p^4 - 4(p^4-16q^4)}}{2(4q^2+p^2)} \\ &= \frac{2p^2 \pm \sqrt{64q^4}}{2(4q^2+p^2)} \\ &= \frac{-p^2 \pm 4q^2}{p^2+4q^2}. \end{aligned}$$

One of these possibilities is just $\frac{-p^2-4q^2}{p^2+4q^2} = -1$, which makes sense, since we knew $(-1,0)$ was a solution to the original equation. The other solution is $\frac{4q^2-p^2}{4q^2+p^2}$, which is clearly a rational number. Further, we can solve for y:

$$\begin{aligned} y &= \frac{p}{2q}(x+1) = \frac{p}{2q}\left(\frac{4q^2-p^2}{4q^2+p^2}+1\right) \\ &= \frac{p}{2q}\frac{8q^2}{4q^2+p^2} = \frac{4pq}{4q^2+p^2} \end{aligned}$$

which is clearly a rational number. Thus for every rational number in simplest terms p/q, we have that $\left(\frac{4q^2-p^2}{4q^2+p^2}, \frac{4pq}{4q^2+p^2}\right)$ is a rational solution to $x^2+y^2=1$, and thus we have

Proposition 0.6. *For every rational number p/q in lowest terms, there is a pythagorean triple*

$$\left(4q^2-p^2, 4pq, 4q^2+p^2\right).$$

If p is odd this triple is reduced; if p is even, we can divide through by 4 to get a reduced triple.

$$\left(q^2-p^2/4, pq, q^2+p^2/4\right).$$

Thus there are infinitely many distinct reduced pythagorean triples.

Remark 0.7. We often parametrize the triples as $(q^2-r^2, 2rq, q^2+r^2)$ after a change of variables $r = 2p$.

On a final note, what if we instead look at equations of the form $a^3+b^3=c^3$? Or $a^4+b^4=c^4$, or some other exponent? You might think we could make the same sort of geometric argument, and draw a line and see where it intersects our new shape; here are the corresponding pictures for $x^4+y^4=1$:

But in this case, these lines are somehow very good at avoiding rational points! One of the most significant results in number theory, which was worked on for more than three hundred years, is:

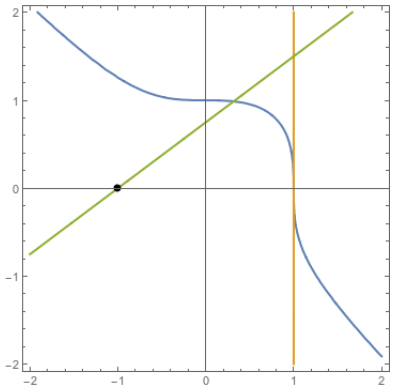

Figure 0.2: $x^3 + y^3 = 1$

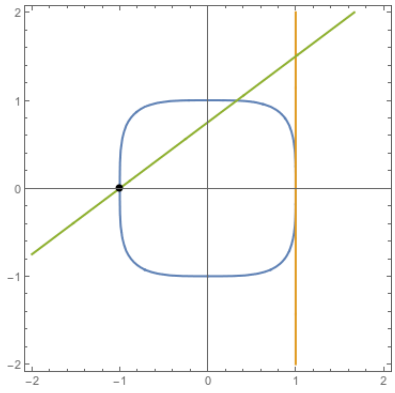

Figure 0.3: $x^4 + y^4 = 1$

Theorem 0.8 (Fermat's Last Theorem (Wiles 1994))**.** *Suppose x and y are rational numbers, and n is a positive integer, with $x^n + y^n = 1$. Then either $n = 1$, $n = 2$, $x = 0$, or $y = 0$.*

That is there are no non-trivial solutions to this equation for $n > 2$.