Returning to the problem of studying Diophantine equations in the integers, we can use these ideas to build one of the most powerful techniques in number theory. This technique does not always work, but even when it fails, its nearly-working is still extremely interesting. For instance, this thinking is what leads to the ideas of the zeta and L-functions, and can be thought of as somehow behind two of the seven million dollar Millennium prize problems. To explain, we have to begin with an example whose solution goes back to the ancient Greeks.

We will consider the problem of characterizing the Pythagorean triples. You have probably seen these in school. To recap, they are simply triples of positive integers $a, b, c \in \mathbb{N}$ such that $a^2 + b^2 = c^2$. For instance, a few triples are given by $(3, 4, 5)$ and $(5, 12, 13)$. Of course, these really arise from a geometric problem. Namely, a triple of numbers is a Pythagorean triple if and only if they are the side lengths of a right triangle. How can you write down all such triples? The first observation is that one can rescale triangles by considering similar triangles. That is, any triple (a, b, c) can be rescaled to (Na, Nb, Nc). For instance, $(3, 4, 5)$ also gives rise to the triples $(9, 12, 15)$ and $(30, 40, 50)$. Similarly, one can divide out any common factors from a, b, c. Thus, it is sufficient to determine the set of *primitive Pythagorean triples*, i.e., those for which $(a, b, c) = 1$.

How should we determine all solutions to this equation? The first observation is that the polynomial $f(a, b, c) = a^2 + b^2 - c^2$ is *homogenous*, meaning that all terms have the same degree. Equivalently, $f(xa, xb, xc) = x^2 f(a, b, c)$. Thus, we can divide by c^2 (side lengths of triangles are positive) to obtain the equivalent formulation $(a/c)^2 + (b/c)^2 = 1$. Renaming $x = a/c$ and $y = b/c$, we obtain $x^2 + y^2 = 1$. Thus, we have found a *rational* point (one with rational coordinates) on the unit circle. Conversely, given a rational point $x^2 + y^2 = 1$ on the unit circle, we can find a common denominator N of x and y and multiply through to get $(Nx)^2 + (Ny)^2 = N^2$, where all terms are integers. Thus, we have shown the following.

Lemma. *There is a one-to-one correspondence between rational points on the unit circle and Pythagorean triples.*

This geometric recasting of the problem is very handy. We can find all Pythagorean triples this was as follows. Take any rational point on the unit circle. For convenience, basically to make the formulas simple, let's consider the point $P = (-1, 0)$. Given any rational point on the unit circle $Z = (x, y)$, the line from P to Z has rational slope equal to $y/(x + 1)$. Conversely, any line with rational slope m through P will intersect the circle at precisely one other rational point on the circle. You can think of the slope as another way to parameterize all the possible angles. The only points which won't correspond to Pythagorean triples are the trivial ones, which have $y = 0$. These correspond to $m = 0$, where the line intersects the circle at $(1, 0)$, and the degenerate case $m = \infty$, where the line is tangent and intersects the circle twice at $(-1, 0)$.

Thus, we can find all triples by first taking intersections with all lines of slope $0 < m \in \mathbb{Q}$. Suppose that $m = p/q$. Then using the point-slope form of the equation, the line of slope m through P is:

$$L\colon y = m(x + 1) = \frac{p}{q}(x + 1).$$

To compute the other intersection point, we plug this into the equation of the circle $x^2 + y^2 = 1$ to obtain:

$$1 = x^2 + \frac{p^2}{q^2}(x + 1)^2 = \left(1 + \frac{p^2}{q^2}\right) x^2 + 2\frac{2p^2}{q^2}x + \frac{p^2}{q^2},$$

or

$$0 = \left(1 + \frac{p^2}{q^2}\right) x^2 + \frac{2p^2}{q^2}x + \left(\frac{p^2}{q^2} - 1\right).$$

Using the quadratic formula, we find that the discriminant is $4p^4/q^4 - 4(p^2/q^2 + 1)(p^2/q^2 - 1) = 4p^4/q^4 - 4(p^4/q^4 - 1) = 4$, and so

$$x = \frac{-\frac{2p^2}{q^2} \pm 2}{2\left(1 + \frac{p^2}{q^2}\right)} = \frac{-p^2 \pm q^2}{(q^2 + p^2)},$$

so $x = -1$ (this corresponds to the point P), or $x = (q^2 - p^2)/(q^2 + p^2)$. Plugging back into the equation of the line shows that the other point has y-coordinate

$$\frac{p}{q}\left(\frac{q^2-p^2}{q^2+p^2}+1\right) = \frac{p}{q}\left(\frac{2q^2}{q^2+p^2}\right) = \frac{2pq}{q^2+p^2}.$$

Using the one-to-one correspondence above, we have shown the following.

Proposition 1. *As p, q range over all coprime integers, $q \neq 0$, the numbers*

$$a = q^2 - p^2, \qquad b = 2pq, \qquad c = q^2 + p^2$$

yield all Pythagorean triples.

On the homework, you will address to what extent there is redundancy in this formula. Essentially, you can generate all Pythagorean triples using less numbers p and q together with rescalings, but you have to do some gcd calculations to deduce the exact result.

This beautiful geometric proof was already known to the Greeks. It is natural to ask about the same question for other curves. Given an algebraic plane curve C, meaning one defined by the equation $f(x, y) = 0$ for a polynomial $f(x, y)$, how can we compute all rational points on it? Surprisingly, it turns out that this problem is closely connected to the topology of the curve. We wont' have much time to delve into the details, but instead of studying the rational solutions, one can first consider the easier question of determining all complex points on the curve. Since the complex numbers are "two-dimensional", every curve becomes a surface when viewed as a set of complex solutions. It is a very general theorem that all surfaces like this, up to stretching, that is, "topologically", are the "the same" as a sphere with a number of holes in it. This number of holes is called the *genus* g of the surface. For example, if $g = 0$, the surface is essentially a sphere, and if $g = 1$ it is a torus, or doughnut. A genus two surface looks like a doughnut with two holes. The genus is closely correlated to the degree of f in our case. The crazy thing is that studying the topology of the surface over the complex numbers should have little to do with the set of rational solutions. However, it turns out that it has much to do with our ability to classify rational points. Roughly speaking, the higher the degree of f is, the higher the genus and the harder the problem.

The case where we can give a complete answer is for the curves of genus zero. These correspond just to $\deg(f) \leq 2$. The degree 1 case is essentially elementary, but the degree 2 case contains much deep number theory. For instance, the Pythagorean triples. Hasse developed an eponymous principle for detecting rational points on curves. The philosophy is as follows. Any number $x \in \mathbb{Q}$ is automatically in $\mathbb{R}$. Similarly, for every prime p, $\mathbb{Q} \subseteq \mathbb{Q}_p$. Thus, if one has a rational point, then one must also have a point over $\mathbb{Q}_p$ for every prime as well as a real point in $\mathbb{R}$ (we sometimes call this the "infinite" prime). This is very much in line with how we have given counterexamples to other theorems in this class. For instance, thanks to Hensel's Lemma, finding a root of a polynomial over $\mathbb{Q}_p$ often reduces to a finite computation in $\mathbb{F}_p$, and indeed we have often said that an equation wasn't solvable as there was a congruence obstruction. That is, we have said that if there is no solution in $\mathbb{Z}/m\mathbb{Z}$ for some m, then the equation also has no solution in $\mathbb{Z}$.

On the other hand, finding whether an equation has a root in $\mathbb{R}$, or $\mathbb{Q}_p$ is usually pretty easy. Basically, because we have calculus. Over $\mathbb{R}$, we have the intermediate value theorem, and over $\mathbb{Q}_p$, we have Hensel's Lemma. For instance, the curve $x^2 + y^2 = -1$ has no rational solutions, as it doesn't have any real solutions. When is the converse true? That is, when does the "local data" of a root in every $\mathbb{Q}_p$ and over $\mathbb{R}$ "lift" to a "global" root in $\mathbb{Q}$. Amazingly, for curves of genus zero, this turns out to be exactly an if and only if statement.

The following theorem solidified this philosophy as a standard in modern number theory. It concerns *quadratic forms*, which are simply polynomials in any number of variables which are homogenous of degree 2 (for instance, $3x^2 + 5y^2 + 7yz - z^2$).

Theorem 0.1 (Hasse-Minkowski Local-Global theorem)**.** *Let $Q(x_1, \dots, x_n)$ be a rational quadratic form in at least 2 variables. Let P be the set of primes consisting of 2 and all odd primes dividing a numerator or denominator of a coefficient of Q. Then for $c \neq 0$, $Q(x) = c$ has a rational solution if and only if it has a $\mathbb{Q}_p$ solution for every prime $p \in P$, and a real solution. If $c = 0$, then $Q(x) = 0$ has a non-zero solution if and only if it has a non-zero solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every $p \in P$.*

Thus, it is usually a finite check to detect if a quadratic form has solutions! Now that we can detect if curves of *degree* 2 have rational solutions, how might one go about finding *all* rational solutions? It turns out that the Greek-style proof as in the case of Pythagorean triples always works. Namely, given such a curve, one first uses the local-to-global principle to find if there are any solutions, and then if there is one, you can use it as a base point and find all solutions by drawing lines of rational slope through it and intersecting.

We say that a quadratic form *represents* a number N if there are inputs $x_1, \dots, x_n$ such that $Q(x_1, \dots, x_n) = N$. It is always a finite check as to whether a quadratic form represents an integer N with integer inputs, since squares are positive and the integers are discrete. A priori, it is not a finite check for rational numbers, since they are dense in $\mathbb{R}$. However, The Hasse-Minkowski theorem does say that it is always a finite check. This is a shocking result. Another interesting question is given a quadratic form, which numbers does it represent? For any particular number this is now a finite check, but it still seems like an infinite check as N ranges. However, Bhargava and Hanke showed the very famous recent result, known as the "290-theorem". Here, we say that a form is *positive-definite* if it only takes positive values for non-zero inputs.

Theorem 0.2 (Bhargava and Hanke)**.** *If a positive definite quadratic form represents the integers $1, 2, \dots, 290$, then it represents all integers.*

For instance, we have seen that the quadratic form $x^2 + y^2$ does not represent integers that are 3 (mod 4). However, we will later prove Lagrange's Theorem, which states that $x^2 + y^2 + z^2 + w^2$ does represent all natural numbers. That is, all positive integers are a sum of four squares. This will take some work for us. However, if we assumed the work of Bhargava and Hanke, we would simply have to check the claim integers from 1 to 290 on a computer to guarantee it continues to hold for all positive integers.

What about curves of higher degree? The problem quickly becomes difficult. For instance, if one wants to study Fermat's Last Theorem, you want to study whether there are integer solutions on the curve $x^n + y^n = z^n$, or, since this is a homogenous polynomial, whether there are any non-trivial rational points on the *Fermat curve* $x^n + y^n = 1$. Unfortunately, as this problems famed difficulty attests to, this is not so easy. It is not too hard to show that it suffices to study the case of exponent an odd prime p or $p = 4$ ($p = 2$ isn't included since there are rational solutions on that curve, given by Pythagorean triples). Mod p, there is always a non-trivial solution to the Fermat equation in exponent p. Specifically, in the next lesson, we will learn about Fermat's Little Theorem, which implies that $x^p \equiv 1 \pmod{p}$ for all $(x, p) = 1$. Thus, for non-zero congruences classes x and y, $x^p + y^p \equiv x + y \equiv 1 \pmod{p}$, which is easily solvable. Hensel's lemma then allows one to lift this to a solution in $\mathbb{Q}^p$ (note that differentiation kills x^p modulo p). It is also easy to find real solutions. For instance, let $y = 1/2$, and then it is clear that there is a p-th root of $1 - y^p$, since this is a positive number.

In general, the local-global principle becomes false as soon as the degree of the polynomial one wishes to study is 3. In this case, the curve has genus 1. Such curves have a special name: they are called *elliptic curves*. These are important tools in number theory, and are the basis of much modern cyrptography as well as a key tool to prove things like Fermat's Last Theorem. The reason these curves are so interesting is precisely that the local-global principle is false so that the theory is less elementary, but the local-global principle's failure is still fairly minor, so one can still prove false results. For curves of degree at least 5, that is, of genus at least 2, very little is known in general. If we have time we may return to this beautiful theory. The other nice property is that doughnuts can

easily be turned into nice examples of groups, and this group law for elliptic curves does not exist for curves of higher genus.

A famous example is the elliptic curve of Selmer, given by the equation

$$3x^3 + 4y^3 + 5z^3 = 0.$$

It turns out that this has a non-trivial solution in every $\mathbb{Q}_p$ and in $\mathbb{R}$, but no rational solutions. How would one show results like this? The idea is that over $\mathbb{R}$, it is pretty simple (just pick y and z more or less arbitrarily and solve for x), and over $\mathbb{Q}_p$, one needs to apply Hensel's Lemma. This leads to some cubic congruences that one needs to solve. In order to make further progress on studying curves like this, or giving a more robust theory of things like quadratic forms, we need to finally understand a theory of quadratic and cubic congruences modulo primes p. This will be one of our major goals later in the course, and we will see that there is an elegant theory for quadratic congruences mod primes.