

THE FERMAT EQUATION

PETE L. CLARK

1. PYTHAGOREAN TRIPLES AND CONICS

Our goal is to find all integer solutions to $x^2 + y^2 = z^2$.

Step 1: Existence: $3^2 + 4^2 = 5^2$. (Also $(5, 12, 13)$, $(7, 24, 25)$, $(8, 15, 17)$.)

Step 2 (Trivial/Degenerate/Nondegenerate Solutions): Let us stop and ask: is $(3, 4, 5)$ the *simplest* solution to the equation $x^2 + y^2 = z^2$? One is first inclined to say yes; however, there are also simpler solutions if we allow some of x , y and z to equal 0. Indeed, if $z = 0$ then we must have $x = y = 0$ so $(0, 0, 0)$ is a solution. We will call this solution *trivial*, for reasons that will be better appreciated later on. Also if we take $x = 0$ and $y = z$ then we get solutions, say $(0, y, y)$ and by symmetry also $(x, 0, x)$. These solutions are still not of much geometric interest – they correspond to triangles in which one of the legs has length zero – so they are *degenerate* solutions in some sense.

Step 3 (Primitivity): Note that we found infinitely many degenerate solutions: $(x, 0, x) = x(1, 0, 1)$ and also $(0, y, y) = y(0, 1, 1)$. As the algebra indicates, these are obtained by two particular solutions by multiplying each of the three coordinates by a common integer. Indeed this is always possible: if $a^2 + b^2 = c^2$ and C is any integer then also

$$(Ca)^2 + (Cb)^2 = C^2(a^2 + b^2) = C^2c^2 = (Cc)^2,$$

so (Ca, Cb, Cc) is also a solution. Thus by rescaling $(3, 4, 5)$ we will get infinitely many nondegenerate solutions.

Doesn't feel like we have cheated a bit, though? In some sense, in writing down the family of solutions $(3C, 4C, 5C)$ doesn't feel like we have exhibited infinitely many "truly different" solutions. Thus let us call a solution (a, b, c) *primitive* if a , b and c are not simultaneously divisible by any integer $C > 1$. (Note in particular that the trivial solution $(0, 0, 0)$ is imprimitive according to our definition.) Thus it seems convenient to restrict our attention to primitive solutions: in particular, when we start counting solutions to such a polynomial equation, it is more interesting to count primitive solutions than all solutions, since otherwise as soon as there is a single primitive solution there are infinitely many integer solutions.

Now there are certainly other primitive solutions: the next few – ordered in terms of the size of the smallest leg, say – are $(5, 12, 13)$, $(7, 24, 25)$ and $(8, 15, 17)$. But are there infinitely many primitive solutions? How can we find them all?

Step 4 (Reduction to rational solutions): A solution (x, y, z) is nontrivial iff $z \neq 0$;

for any nontrivial integer solution we may divide through by z to get

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

so a nontrivial *integer* solution to $X^2 + Y^2 = Z^2$ gives rise to a *rational* solution to $x^2 + y^2 = 1$. Conversely, given any rational solution to this equation, say

$$(a/b)^2 + (c/d)^2 = 1,$$

just by clearing denominators we will get a nontrivial integer solution to $X^2 + Y^2 = Z^2$, namely

$$(da)^2 + (bc)^2 = (bd)^2.$$

Moreover, we will later verify that if the fractions $\frac{a}{b}$, $\frac{c}{d}$ are written in lowest terms, then the corresponding integral solution is primitive. So we have reduced our task to finding all rational points on the unit circle $x^2 + y^2 = 1$.

What is remarkable is that simple geometric reasoning will give us the answer immediately. First we fix one rational point P_0 on the circle: we could take $(3/5, 4/5)$, but for ease of drawing the picture and doing the calculations, let us take a simpler point: $(-1, 0)$. How to find the others? Well, if $P = (x, y)$ is any other rational point on the unit circle, the unique line joining P_0 to P has rational coordinates – because it passes through two points with rational coordinates. To be even more precise, every nonvertical line passing through $P_0 = (-1, 0)$ is of the form $y - 0 = m(x - (-1)) = m(x + 1)$ where m is the slope. Since the tangent line to the circle at P_0 is vertical, every nonvertical line will intersect the circle at exactly one other point P_m . Moreover, we claim that this second intersection point P_m will have rational coordinates iff its slope m is rational. One direction is immediate: if $P_m = (x_m, y_m)$ has rational coordinates, then $m = \frac{y_m - 0}{x_m + 1}$ is visibly rational. The other direction is a slightly more sophisticated argument: if we plug in the equation $y = m(x + 1)$ to the equation $x^2 + y^2 = 1$, we will get a quadratic equation in x with rational coefficients (since m is rational) and which has two distinct solutions. But in the quadratic formula if we two roots they are either *both* irrational or *both* rational, and since we know that one of the solutions is $x = -1$, the second solution must be rational. Since $y_m = m(x_m + 1)$, then since m and x_m are both rational, so is y_m .

In summary, the rational points on the unit circle $x^2 + y^2 = 1$ are precisely those which are obtained as the intersection points of all possible lines with rational slope passing through $(-1, 0)$.

That's the theoretical perspective, anyway. Let's actually *do* the calculation and see that things work out as claimed. Namely, we will determine the coordinates (x_m, y_m) of the other intersection point of $y = m(x + 1)$ with $x^2 + y^2 = 1$. First plug in y :

$$x^2 + m^2(x + 1)^2 = 1.$$

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0.$$

So we apply the quadratic formula to get the two solutions:

$$x = \frac{-2m^2 \pm \sqrt{4m^4 - 4(1 + m^2)(m^2 - 1)}}{2(1 + m^2)}.$$

Under the radical we have

$$4m^4 - 4(m^2 + 1)(m^2 - 1) = 4(m^4 - (m^4 - 1)) = 4,$$

so that “luckily” $\sqrt{4m^4 - 4(1 + m^2)(m^2 - 1)} = 2$, and we get

$$x = \frac{-2m^2 \pm 2}{2(1 + m^2)} = \frac{-m^2 \pm 1}{1 + m^2}.$$

In other words, one of the solutions is $x = \frac{-m^2 - 1}{m^2 + 1} = -1$ – good! – and the other is $x_m = \frac{1 - m^2}{1 + m^2}$. Thus $y_m = m(1 + \frac{-m^2 + 1}{m^2 + 1}) = \frac{2m}{m^2 + 1}$, so

$$P_m = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$$

is the general rational solution to $x^2 + y^2 = 1$. Put now $m = \frac{u}{v}$, with $\gcd(u, v) = 1$, to get:

$$P_m = \left(\frac{1 - u^2/v^2}{1 + u^2/v^2}, \frac{2u/v}{1 + u^2/v^2} \right) = \left(\frac{v^2 - u^2}{v^2 + u^2}, \frac{2uv}{v^2 + u^2} \right).$$

Now we can clear denominators to get a family of integral solutions

$$(v^2 - u^2)^2 + (2uv)^2 = (v^2 + u^2)^2.$$

As above, up to scaling this must be the most general integral solution, but we are not yet sure about which values of u and v make for a primitive triple. More precisely, the solution will be primitive iff $v^2 + u^2$ is the lowest common denominator of the the x and y coordinates of P_m . If not, we have multiplied through by more than we needed to and will thus not get a primitive integral solution. Equivalently, we are wondering whether $v^2 - u^2, v^2 + u^2$ and $2uv$ can have any common factor.

I claim that the greatest common divisor of these three integers is either 1 or 2. Indeed, if any odd prime p divides both $v^2 - u^2$ and $v^2 + u^2$, it also divides $v^2 + u^2 + v^2 - u^2 = 2v^2$ – so $p \mid v$ – and it divides $v^2 + u^2 - (v^2 - u^2) = 2u^2$ – so $p \mid u$, contradicting $\gcd(u, v) = 1$. Similarly if 4 divided $v^2 \pm u^2$ it would divide $2u^2$ and $2v^2$, which is impossible since u and v are not both even. However, we rather need to worry about the case that u and v are both odd: then 2 divides $v^2 - u^2, 2uv$ and $v^2 + u^2$.

So only in this case did we go slightly too far in clearing denominators. That is, to get primitive solutions it is necessary and sufficient that u and v be relatively prime integers of opposite parity. Summing up, we have now shown all but the very last part of the following:

Theorem 1. (*Classification of Pythagorean Triples*)

- a) *The rational solutions to $x^2 + y^2 = 1$ are $P = (-1, 0)$ and, for every $m \in \mathbb{Q}$, $P_m = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$.*
- b) *For every pair (u, v) of relatively prime integers of opposite parity, $(v^2 - u^2, 2uv, v^2 + u^2)$ is a primitive Pythagorean triple. Every primitive Pythagorean triple (x, y, z) with even y is of this form, and the primitive triples with odd y are obtained by interchanging the first two coordinates.*

The last statement is best reasoned out on your own, and I will let you think about it. Hint: our parameterization seems not to give any triples (x, y, z) with x even and y odd. But go back and look to see that our rational parameterization does

give $(4, 3, 5)$ up to rescaling, and has something to do with the case that u and v are both odd.

1.1. Rational points on conics. The above solution has the merit of giving a *general method* for solving certain kinds of equations. Namely, it will allow us to find all rational points on any *conic*:

$$aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 = 0$$

assuming we can find at least one nontrivial rational solution (which as we will shortly see, is *not* always the case). We explore this issue in the following exercises.

Exercise XX:

a) Show that for any nonzero integer a , the conic

$$aX^2 + bY^2 = a^2Z^2$$

has a nontrivial rational point.

b) Use the above method to find all rational points on $3X^2 + 7Y^2 = 3Z^2$.

Exercise XXG: Show that every conic with rational coefficients is *equivalent* to a conic of the form

$$C_{a,b} : aX^2 + bY^2 = Z^2.$$

for $a, b \in \mathbb{Q}^*$ (in fact we may take a and b in \mathbb{Z}). So the question is, for which pairs $(a, b) \in \mathbb{Q}^\times$ does $C_{a,b}$ have a nontrivial \mathbb{Q} -rational point? This is an interesting problem.

a) Show that $C_{a,-a}$, $C_{a^2,b}$ and $C_{a,1-a}$ always have \mathbb{Q} -rational points.

b) Show that if $C_{a,b}$ has a nontrivial \mathbb{Q} -rational point, then at least one of a and b is positive.

c)* Show that $3X^2 + 5Y^2 = Z^2$ has no nontrivial \mathbb{Q} -rational points. (Suggestion: If there is a nontrivial rational solution there is also a nontrivial integer solution (x, y, z) in which x , y and z are not all divisible by 5 (take, e.g., any primitive solution). First show that 5 does not divide y : this uses properties of the function $\text{ord}_5(n)$ which will be introduced later. Then show that the only solution of the congruence $3X^2 \equiv Z^2 \pmod{5}$ is $X \equiv Z \equiv 0 \pmod{5}$, meaning that x and z are both divisible by 5. Finally, show that this implies that y is divisible by 5, a contradiction.

d)* The above argument shows the following: for p an odd prime and u a positive integer prime to p , the curve $C_{u,p}$ can only have nontrivial rational solutions if the congruence $u \equiv Z^2 \pmod{p}$ has a solution (that is, if u is a *quadratic residue* modulo p).

This exercise of course raises the question: can we give a simple condition on a and b that is necessary and sufficient for $C_{a,b}$ to have a nontrivial rational point? The answer is a resounding *yes*, and is given by a theorem of Legendre. Legendre's Theorem will be one of our main goals in this course.