Math 126 Number Theory

Prof. D. Joyce, Clark University

28 Mar 2006

Due Friday. Page 155: exercises 1, 2, 7. Choose one of the three and write it up completely. Whichever one you choose, find all those solutions where the three numbers in the solution are relatively prime. (In 1 and 2, you can do that because the equations are homogeneous; in 7 that's part of the specific instructions.)

Try to write it up as well as any of the proofs in the text, or at least as well as I do in my notes and answer sheets. Every sentence should be complete; every variable that's introduced should be explained; every equation should be connected with words to what has gone on before; and, of course, the logic should be correct.

Don't try to write up the final proof until understand what it will be. First, you have to find out what the solutions to the equation are. That takes some analysis. After you have what you think are all the solutions, then develop the proof that shows that you have all the solutions. It may take a couple of drafts to work it up completely. Go over what you've written and be sure that you haven't left anything out.

Due Monday. Page 161: exercises 3, 5. Choose one and write it up completely. Same instructions as for Friday's assignment.

Second test. Wednesday, April 5.

Last time. We analyzed Pythagorean triples which are triples (x, y, z) of positive integers such that $x^2 + y^2 = z^2$. We were particularly interested in primitive Pythagorean triples, those where the greatest common divisor (x, y, z) is 1, because all others are multiples of the primitive ones. Here's what we did.

We tried the method of factoring. We couldn't factor $x^2 + y^2$. (You can if you use complex numbers, since $x^2+y^2 = (x+iy)(x-iy)$, but we didn't go that route.) So we converted the equation to $x^2 = z^2 - y^2$ so we could use factor the difference of two squares. That gave us the equation

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

The next problem was to factor x^2 so that one factor equalled $z + y$ while the other equalled $z - y$.

We rejected the factoring $x^2 = xx$ with $x = z+y$ and $x = z - y$ because then y would be 0, and we're only looking for positive solutions to the Pythagorean equation.

Next we factored x^2 as $x^2 \cdot 1$ with

$$\begin{cases} x^2 &= z + y \\ 1 &= z - y \end{cases}$$

That pair of equations is equivalent to

$$\begin{cases} z &= (x^2 + 1)/2 \\ y &= (x^2 - 1)/2 \end{cases}$$

Thus, we found some solutions when x is an odd number greater than 1, namely,

$$(x, y, z) = \big(x, (x^2 - 1)/2, (x^2 + 1)/2\big).$$

Here are the first few of them in a table.

x	$(x^2-1)/2$	$(x^2+1)/2$
3	4	5
5	12	13
7	24	25
9	40	41
11	60	61

We noted that these were all primitive Pythagorean triples since y and z differed by 1.

Incidentally, this particular sequence of Pythagorean triples is attributed to the early Pythagoreans. Perhaps Pythagoras himself knew of them.

Next, we tried another factoring $x^2 = a^2b^2$ with

$$\begin{cases} a^2 = z + y \\ b^2 = z - y \end{cases}$$

and, of course, $a > b$. This was a generalization of the previous factoring since that just had $b = 1$. That pair of equations has the solution

$$\begin{cases} z = (a^2 + b^2)/2 \\ y = (a^2 - b^2)/2 \end{cases}$$

Now we have solutions

$$(x, y, z) = \big(ab, (a^2 - b^2)/2, (a^2 + b^2)/2\big)$$

when a and b have the same parity (so that y and z are integers). We noted that a and b needed to be relatively prime in order that the triple be primitive. Therefore a and b both need to be odd.

This construction turns out to be precisely Euclid's as it appears in Proposition 29 of Book X of his *Elements*. A table of the first few of these Pythagorean triples is on a separate sheet.

By the way, besides the sequence of Pythagorean triples mentioned above (the ones where $b = 1$) there's also another sequence attributed to Plato. For that, $b = a - 2$. The first few triples in this sequence are

$$(3, 4, 5), (15, 8, 17), (35, 12, 37), (63, 16, 65).$$

They can also be parameterized as

$$(x, y, z) = (k^2 - 1, 2k, k^2 + 1)$$

with k a positive even number.

Today. We'll prove the Pythagorean triples we found last time are all of them. We'll see how Pythagorean triples form an Abelian group. We'll also begin examining Fermat's method of descent and follow Fermat's use of it to prove $x^4 + y^4 = z^4$ has no nontrivial solutions.

We found all the Pythagorean triples last time. But we haven't proved that we found them all. We need to show that every primitive Pythagorean triple (x, y, z) is of the form

$$(x, y, z) = \big(ab, (a^2 - b^2)/2, (a^2 + b^2)/2\big)$$

where a and b are relatively prime odd numbers, $a > b \geq 1$.

All we have to do is prove that the only factoring of $x^2 = AB$ with $A = z + y$ and $B = z - y$ that we need to consider is when $x^2 = a^2b^2$ with $A = a^2$ and $B = b^2$. There's only one factoring that's more general, and that's $x^2 = a^2b^2c^2$ with $A = a^2c$ and $B = b^2c$. That leads to the solution

$$\begin{cases} z = (a^2c + b^2c)/2 \\ y = (a^2c - b^2c)/2 \end{cases}$$

Now, note that if an odd prime p divides c, then p also divides all three of x, y, and z, leading to a nonprimitive triple. Thus, we conclude no odd prime divides c.

On the other hand, 2 could divide c. Then, of course, $x = abc$ would be even, but y and z could still be odd. But we know not both x and y are even (for then z would be even and the triple wouldn't be primitive), so we could specify at the outset that x is odd (by switching it with y if it's not), and thus 2 does not divide c.

Hence $c = 1$. That shows the factoring we used was the most general that leads to a primitive Pythagorean triple. Q.E.D.

There is another common parameterization of the Pythagorean triples besides the one we found. For that parameterization, we assume x is odd and y is even (just like with our parameterization), then

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$$

where where u and v are positive relatively prime integers with $u > v$. It's easy to work out the formulas connecting these two parameterizations. They are $a = u + v$, $b = u - v$, $u = \frac{1}{2}(a + b)$, and $v = \frac{1}{2}(a - b)$.

Trigonometry and the group associated to Pythagorean triples. It is not obvious, but there is a way of taking any two Pythagorean triples and constructing another one. Here's how we can see the group. The original equation $x^2+y^2=z^2$ is a homogeneous equation in three variables where we're looking for integral solutions. We can dehomogenize it to get a nonhomogeneous equation where we're looking for rational solutions as follows. Divide the equation by z^2 to get

$$(x/z)^2+(y/z)^2=1$$

and rename the rational number x/z as X and the rational number y/z as Y. That gives us the equation

$$X^2+Y^2=1$$

of the unit circle. (Note that there's a faster way to get this equation. Just set z to 1.)

Since we only want rational solutions to this equation, we can call rational solutions the points on the *rational unit circle.* A few of the points on this rational curve are

$$(\tfrac{3}{5},\tfrac{4}{5}),(\tfrac{4}{5},\tfrac{3}{5}),(\tfrac{5}{13},\tfrac{12}{13}),(-\tfrac{5}{13},\tfrac{12}{13}),(1,0),(0,-1).$$

Since the circle doesn't lie entirely in the first quadrant of the plane, we shouldn't ignore points that have negative coordinates; likewise, we shouldn't ignore the four points that have zero coordinates.

Now, how can we add two of these points? We can interpret them as angles! We can certainly add two angles together. For instance, 60° plus 75° equals 135°. We do have to be careful about adding angles whose sum is greater than 360°. For instance, 180° and 270° should be 90°, but all we have to do is make 360° equal to 0°, and that we can do if we take degrees modulo 360. In symbolic notation, the group of angles is $\mathbf{R}/360\mathbf{Z}$. This group is the *circle group.* Depending on what you scale you use for measuring angles, you might take $\mathbf{R}/2\pi\mathbf{Z}$ or $\mathbf{R}/\mathbf{Z}$ instead.

Now, we don't have the actual angle θ. What we have is (X,Y) where $X^2+Y^2=1$. In other words we have the cosine and sine of the angle.

$$(X,Y)=(\cos\theta,\sin\theta).$$

Recall the sum formulas for cosine and sine.

$$\begin{aligned}\cos(\theta+\phi)&=\cos\theta\cos\phi-\sin\theta\sin\phi\\ \sin(\theta+\phi)&=\sin\theta\cos\phi+\cos\theta\sin\phi\end{aligned}$$

If $(U,V)=(\cos\phi,\sin\phi)$ are the corresponding coordinates for the angle ϕ, and

$$(S,T)=(\cos(\theta+\phi),\sin(\theta+\phi))$$

are the coordinates for the sum of the angles $\theta+\phi$, then these two formulas give

$$\begin{aligned}S&=XU-YV\\ T&=YU+XV\end{aligned}$$

These give us an addition formula for points on the unit circle. Let's use the symbol $\oplus$ for this addition.

$$(X,Y)\oplus(U,V)=(XU-YV,YU+XV).$$

From the difference formulas for cosine and sine, there's a subtraction formula, too.

$$(X,Y)\ominus(U,V)=(XU+YV,YU-XV)$$

Note that the zero element of this group is the point $(1,0)$ corresponding to 0°.

An example addition:

$$\begin{aligned}(\tfrac{3}{5},\tfrac{4}{5})\oplus(\tfrac{5}{13},\tfrac{12}{13})&=(\tfrac{3}{5}\cdot\tfrac{5}{13}+\tfrac{4}{5}\cdot\tfrac{12}{13},\tfrac{4}{5}\cdot\tfrac{5}{13}-\tfrac{3}{5}\cdot\tfrac{12}{13})\\ &=(\tfrac{63}{65},-\tfrac{16}{65})\end{aligned}$$

This group structure can be carried over to Pythagorean triples (x,y,z) but only if two Pythagorean triples are considered to be the same if they only differ by scaling. Thus (x,y,z) and $(\lambda x,\lambda y,\lambda z)$ are to be considered the same where λ is any nonzero constant. We can turn a a rational point (X,Y) on the unit circle into a Pythagorean triple by adding a third coordinate with value 1 to get $(X,Y,1)$ thereby undoing the process we started out with. The corresponding formulas in homogeneous coordinates (x,y,z) for $\oplus$ can be found by working from the nonhomogeneous coordinates (X,Y). Here's how. First write the addition formula with the extra coordinate.

$$(X,Y,1)\oplus(U,V,1)=(XU-YV,YU+XV,1).$$

Next, replace X by x/z, Y by y/z, U by u/w, and V by v/w.

$$(\tfrac{x}{z}, \tfrac{y}{z}, 1) \oplus (\tfrac{u}{w}, \tfrac{v}{w}, 1) = (\tfrac{xu}{zw} - \tfrac{yv}{zw}, \tfrac{yu}{zw} + \tfrac{xv}{zw}, 1).$$

Now we clear the denominators for each point. We'll replace $(\frac{x}{z}, \frac{y}{z}, 1)$ by (x, y, z) by multiplying each coordinate by z. Likewise, we'll multiply each coordinate of $(\frac{u}{w}, \frac{v}{w}, 1)$ by w, and multiply each coordinate of the last point by zw. We end up with the formula

$$(x, y, z) \oplus (u, v, w) = (xu - yv, uy + xv, zw).$$

The formula for subtraction is

$$(x, y, z) \ominus (u, v, w) = (xu + yv, uy - xv, zw).$$

The zero element is $(1, 0, 1)$. An example addition:

$$(3, 4, 5) \oplus (5, 12, 13) = (63, -16, 65).$$

Fermat's method of descent. Early in the semester we used the following axiom, equivalent to mathematical induction, or the principle of minimization (also called the well-ordering principle).

Axiom. There is no infinite decreasing sequence of positive integers.

Euclid used this principle frequently in his *Elements.* Fermat used it in number theory, too. Fermat would take a particular Diophantine equation, suppose that there was one solution, and look for a way to produce a smaller solution from it. If this worked without fail, then he would have an infinite decreasing sequence of solutions and could conclude that no solution could exist. On the other hand, if the descent stopped with an actual solution, reversing the process would lead to more solutions.

We'll look at Fermat's proof that $x^4 + y^4 = z^4$ has no positive integral solutions. Actually, he proved something stronger, that the Diophantine equation $x^4 + y^4 = z^2$ has no solutions.

Theorem. There are no positive integral solutions of

$$x^4 + y^4 = z^2.$$

Proof: Suppose that x, y, z is a solution.

First, we want to reduce to the case where x and y are relatively prime. Let d be the greatest common divisor of them, and let $x_1 = x/d$ and $y_1 = y/d$. Then

$$d^4(x_1^4 + y_1^4) = z^2.$$

Therefore, $d^4|z^2$, so $d^2|z$. Let $z_1 = z/d^2$. Then

$$x_1^4 + y_1^4 = z_1^2.$$

We now have a smaller solution where x_1 and y_1 are relatively prime.

Now we may suppose that x, y, z is a solution where $(x, y) = 1$. Following Fermat, we need to find a smaller solution, and in this case that means a solution with a smaller value for z.

Note that $(x^2)^2 + (y^2)^2 = z^2$, so (x^2, y^2, z) is a primitive Pythagorean triple. It turns out that using the alternate parameterizations of primitive Pythagorean triples works better here than the parameterization we found. We'll take x^2 odd, then

$$(x^2, y^2, z) = (u^2 - v^2, 2uv, u^2 + v^2)$$

where where u and v are positive relatively prime integers with $u > v$. Note that $x^2 = u^2 - v^2$, so $x^2 + v^2 = u^2$. Therefore, (x, v, u) is another Pythagorean triple, and it's primitive since u and v are relatively prime. Therefore,

$$(x, v, u) = (s^2 - t^2, 2st, s^2 + t^2)$$

where where s and t are positive relatively prime integers with $s > t$.

Now, $y^2 = 2uv$. Since u and v are relatively prime, and u is odd (because (x, v, u) is a primitive Pythagorean triple), therefore u and $2v$ are relatively prime. But y^2 is their product, so each of u and $2v$ is a square. Let

$$u = z_2^2 \quad \text{and} \quad 2v = c^2,$$

and since c is even, let $c = 2d$ so that $v = 2d^2$. Since $v = 2st$, therefore

$$st = v/2 = d^2.$$

But s and t are relatively prime, and their product is a square d^2, therefore each is a square. Let

$$x_2^2 = s \quad \text{and} \quad y_2^2 = t.$$

Finally, since $s^2 + t^2 = u$, therefore

$$x_2^4 + y_2^4 = z_2^2.$$

The new value z_2 is smaller than the old value z since

$$z_2 \leq z_2^4 = u^2 < u^2 + v^2 = z.$$

Thus, we have shown that if (x, y, z) is a solution for the equation $x^4 + y^4 = z^2$, then there is another solution with a smaller value of z. As this process can be repeated without end, that yields an infinite descending sequence of positive integers, which is impossible. Thus, the equation has no positive integral solutions. Q.E.D.