Math 5330
Spring 2018

Notes:
Pythagorean Triples

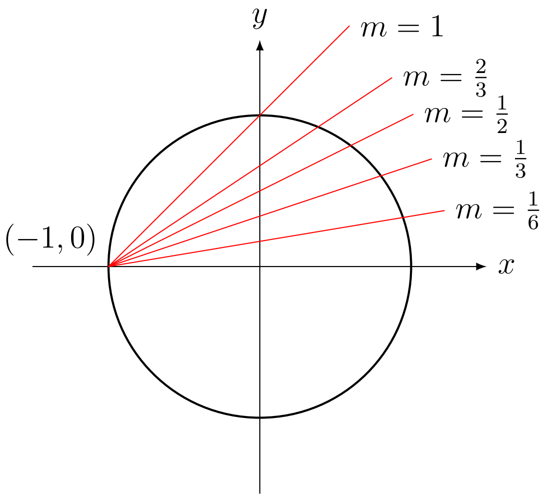
Many people know that $3^2 + 4^2 = 5^2$. Less commonly known are $5^2 + 12^2 = 13^2$ and $7^2 + 24^2 = 25^2$. Such a set of integers is called a Pythagorean Triple. The reason for the name is the relation to the Pythagorean Theorem: The sum of the squares of the lengths of the sides of a right triangle is equal to the square of the length of the hypotenuse. Thus, a Pythagorean triple is a set of integers that form the sides and hypotenuse of a right triangle.

There are infinitely many Pythagorean triples. In fact, $6^2 + 8^2 = 10^2$, $9^2 + 12^2 = 15^2$, and in general, $(3k)^2 + (4k)^2 = (5k)^2$. This is not terribly satisfying since all these triples are related to the triple (3, 4, 5). Geometrically, all triangles with sides $3k$, $4k$, and $5k$ are similar. There are also infinitely many fundamentally different Pythagorean triples. Here is a simple way to construct infinitely many triples of a specific form. Suppose we wish to find all triples (x, y, z) with $x^2 + y^2 = z^2$ and $z = y + 2$. We can just follow our noses: set $x^2 + y^2 = (y + 2)^2$. Multiplying this out, we get $x^2 = 4y + 4$. The problem with this is for a given y it might be hard to tell if $4y + 4$ is a perfect square, and we need it to be a square if we are to find x. To get around this, solve for y instead of x: $y = \frac{x^2-4}{4}$. We still have a problem: we need $x^2 - 4$ to be divisible by 4. But this is a much easier problem to fix: we can just let x be even. Let's introduce a new parameter, k. We let $x = 2k$, assuring that x is even. Then $y = \frac{(2k)^2-4}{4} = k^2 - 1$. Finally, $z = y + 2 = k^2 + 1$, so our triple (x, y, z) can be written $(2k, k^2 - 1, k^2 + 1)$. In fact, this always works, provided $k > 1$ giving us infinitely many Pythagorean triples. As an example, when $k = 4$, this gives the triple (8, 15, 17), and indeed, $8^2 + 15^2 = 64 + 225 = 289 = 17^2$.

Is it possible to find **all** Pythagorean triples? Since there are infinitely many, a better question would be to find a simple way to describe all Pythagorean triples. In fact, there are several methods to do this. I will give three(!) such methods in this set of notes.

A Geometric approach

If $x^2 + y^2 = z^2$, then dividing by z^2 gives $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$, an equation of the form $a^2 + b^2 = 1$ where a and b are rational numbers (instead of integers). Similarly, if $a^2 + b^2 = 1$ for rational numbers a and b, and z is the least common multiple of the denominators of a and b, then $(za)^2 + (zb)^2 = z^2$ and za and zb will be integers. Thus, finding integer solutions to $x^2 + y^2 = z^2$ is equivalent to finding all rational solutions to $x^2 + y^2 = 1$. That is, we wish to find all rational points on the unit circle. (A rational point is a point in which both coordinates are rational numbers.) This may not sound like progress, but there is a simple geometric approach to getting all rational points on the circle (and in general, rational points on any conic section.) First, we find one particular rational point. This can be hard for some curves, but it is easy for the circle. I will select the point (-1, 0). I could have picked lots of other points instead, but this one will lead to the nicest formulas. Next, consider all lines with rational slope which pass through (-1, 0).



Such lines have equation $y = m(x + 1)$. The point of using a line passing through (-1, 0) is that the line will intersect the circle again in the first quadrant (positive x, y) if the slope is between 0 and 1. If we call the second point (a, b), then we solve $x^2+y^2 = 1$ and $y = m(x+1)$ simultaneously. We have $x^2 + (m(x + 1))^2 = 1$, or $(m^2 + 1)x^2 + 2m^2x + m^2 - 1 = 0$. Since we know $x = -1$ is one solution to this quadratic, we know it must have $x + 1$ as a factor. In fact, $(x + 1)((m^2 + 1)x + m^2 - 1) = 0$, so the other solution is

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

Since $y = m(x + 1)$, we have

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

and the point is

$$(a, b) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right). \tag{1}$$

Note that if m is rational, then by the form of a and b, they must both be rational as well. Conversely, if a and b are rational, then m must be rational as well. The reason for this is that m is the slope of the line through (-1, 0) and (a, b). This line will have slope $m = \frac{b}{a+1}$, a rational number if a and b are rational. What this means is that there is a one-to-one correspondence between rational points on the circle in the first quadrant and rational numbers m with $0 < m < 1$. Formula (1) is called a **rational parameterization** of the circle: Every rational point is given in terms of some other variable, a parameter, m.

But we are interested in Pythagorean triples, so now we start the somewhat unpleasant task of going from a rational point on the circle to a Pythagorean triple. Since m is rational, we may write $m = \frac{q}{p}$ where p and q are positive integers. Since $0 < m < 1$, we may assume that $p > q > 0$. We have

$$a = \frac{1-m^2}{1+m^2} = \frac{1-\frac{q^2}{p^2}}{1+\frac{q^2}{p^2}} = \frac{p^2-q^2}{p^2+q^2}, \quad \text{and} \quad b = \frac{2m}{m^2+1} = \frac{2\frac{q}{p}}{\frac{q^2}{p^2}+1} = \frac{2pq}{p^2+q^2}.$$

Since $a = \frac{x}{z}$ and $b = \frac{y}{z}$, we have that $(x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2)$ is a Pythagorean triple for every choice of integers $p > q > 0$. Note that once we have found this, we can check it easily:

$$\begin{aligned} x^2 + y^2 &= \quad (p^2-q^2)^2 \quad + \quad (2pq)^2 \\ &= p^4 - 2p^2q^2 + q^4 \quad + \quad 4p^2q^2 \\ &= p^4 + 2p^2q^2 + q^4 \\ &= (p^2+q^2)^2 \qquad = \quad z^2. \end{aligned}$$

Some examples:

p	q	x	y	z
2	1	3	4	5
3	1	8	6	10
3	2	5	12	13
4	1	15	8	17
4	2	12	16	20
4	3	7	24	25

Not all Pythagorian triples can be found this way, however! A simple example is $(x, y, z) = (4, 3, 5)$, which cannot occur since $y = 2pq$ implies that y is even. As a more complicated example, $(x, y, z) = (15, 20, 25)$ cannot occur. In this case, we would need $2pq = 20$ so $pq = 10$. Moreover, $p > q > 0$, so we are left with the cases $p = 10$, $q = 1$ or $p = 5$, $q = 2$. These lead to the triples (99, 20, 101) and (21, 20, 29), neither of which is (15, 20, 25).

How can this be? We got EVERY positive rational solution to $a^2 + b^2 = 1$ by the procedure we outlined. In the case of the triple (15, 20, 25), the corresponding values of a and b are $a = \frac{15}{25}$ and $b = \frac{20}{25}$. But $\frac{15}{25} = \frac{3}{5}$ and $\frac{20}{25} = \frac{4}{5}$. Thus, many different Pythagorean triples come from the same rational point on $x^2 + y^2 = 1$. In fact, if $x^2 + y^2 = z^2$, then for any rational number d, $(dx)^2 + (dy)^2 = d^2x^2 + d^2y^2 = d^2(x^2 + y^2) = d^2z^2 = (dz)^2$, so if (x, y, z) is a Pythagorean triple, then so is (dx, dy, dz) for any rational number d for which all three of dx, dy, dz are integers. This gives us our first real theorem of the course.

Theorem 1 *Every Pythagorean triple has the form*

$$(d(p^2 - q^2),\ 2dpq,\ d(p^2 + q^2))$$

for some integers p and q with $p > q > 0$ and some positive rational number d.

It is customary to modify the problem of finding all Pythagorean triples as follows: Suppose that any two of x, y, z are divisible by some integer, n. Then it is easy to see that the third is also divisible by n. In this case, if we write $x = x_1n$, $y = y_1n$, $z = z_1n$, then $x^2+y^2 = z^2 \Rightarrow n^2x_1^2+n^2y_1^2 = n^2z_1^2$, so $x_1^2+y_1^2 = z_1^2$. Because of this, we usually only look for Pythagorean triples in which no two numbers have any factors in common. If two numbers have no common factor, they are called **relatively prime**. If (x, y, z) is a Pythagorean triple with x, y, z pairwise relatively prime, we call it a **primitive** Pythagorean triple. That is, (3, 4, 5) is primitive, (15, 20, 25) is not. What all this shows is that every Pythagorean triple has the form (nx, ny, nz) where (x, y, z) is primitive.

Suppose that (x, y, z) is a primitive Pythagorean triple. Then exactly one of x, y, z must be even. This is because odd + odd = even, odd + even = odd, even + odd = odd, even + even = even, and we can't have this fourth case because the triple would not be primitive. Moreover, it turns out that z can't be the even. To see this, suppose that z is even, but the triple is primitive. This means x and y are odd. With all this, we can write $x = 2m + 1$, $y = 2n + 1$, $z = 2p$, for some integers m, n, p. Plugging in, $(2m + 1)^2 + (2n + 1)^2 = (2p)^2$, or $4m^2 + 4m + 4n^2 + 4n + 2 = 4p^2$. But this last equation has no integer solutions: If we divide by 2 we get $2p^2 = 2(m^2 + m + n^2 + n) + 1$. That is, we would need $2p^2$ to be both even and odd. So it must be that one of x, y is even, and the other and z are odd. It is customary to arbitrarily decide that we will pick y to be even and x to be odd. That is, we ignore (8, 15, 17), but consider (15, 8, 17) instead. Of course this means we skip some Pythagorean triples. To get all of them, we switch x and y.

Theorem 2 *Every primitive Pythagorean triple (x, y, z) in which y is even has the form*

$$(p^2 - q^2,\ 2pq,\ p^2 + q^2)$$

for some integers p and q where $p > q > 0$, p and q are relatively prime, and one of p and q is even. Conversely, if $p > q > 0$, p and q are relatively prime, and one of them is even, then $(p^2 - q^2,\ 2pq,\ p^2 + q^2)$ is a primitive Pythagorean triple.

Proof: The converse is easier. We know that for any integers p, q with $p > q > 0$, that $(p^2 - q^2,\ 2pq,\ p^2 + q^2)$ is a Pythagorean triple. What we must show is that the triple is primitive when p and q are relatively prime and one of them is even. Suppose that there is a common divisor, d for (x, y, z). Then d is a common divisor for $p^2 - q^2$ and $p^2 + q^2$. Since one of p and q is even and the other is odd, both of these expressions are odd, so d must be odd. A common trick: If d divides two numbers, then it must divide their sum and their difference (and any integer combination of the two numbers.) As a consequence, d is a divisor of the sum, $2p^2$ and the difference, $2q^2$. Since d is odd, we can ignore the 2, so d is a divisor of p^2 and q^2. Since p^2 and q^2 have a common factor, so do p and q, contradicting the hypothesis that they are relatively prime. Thus, $(p^2 - q^2,\ 2pq,\ p^2 + q^2)$ is a primitive Pythagorean triple.

For the other direction, let (x, y, z) be a primitive Pythagorean triple in which y is even. From the geometric construction, there is a rational number, m, with $0 < m < 1$ for which

$$\frac{x}{z} = \frac{1-m^2}{1+m^2}, \qquad \frac{y}{z} = \frac{2m}{1+m^2}.$$

We may write $m = \frac{q}{p}$ where p and q are relatively prime. Thus, we have relatively integers $p > q > 0$ for which

$$\frac{x}{z} = \frac{p^2-q^2}{p^2+q^2}, \qquad \frac{y}{z} = \frac{2pq}{p^2+q^2}.$$

Next, suppose that p and q are both odd. If we write $p = 2m+1$, $q = 2n+1$, then

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

From this, it follows that x must be even (the numerator is divisible by at least 4, the denominator is divisible only by 2.) This contradicts the assumption that y is even and x is odd. Consequently, one of p and q has to be even, as desired. This completes the proof. ■

Pythagorean triples from an algebraic approach

Everything above was based on the geometric idea that rational solutions of the equation $x^2 + y^2 = 1$ can be found by considering lines of rational slope passing through one fixed rational point on the curve (we used (-1, 0) because it was the most convenient point to use). We now look at things from a purely algebraic point of view that goes back at least to Euclid. Again, we restrict our attention to primitive Pythagorean triples. Suppose that (x, y, z) is a primitive Pythagorean triple and that y is even. Then $x^2 + y^2 = z^2$ can be rearranged:

$$y^2 = z^2 - x^2 = (z+x)(z-x) = 4\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

Letting $u = \dfrac{z+x}{2}$, $v = \dfrac{z-x}{2}$, $y = 2y_1$, we have $4y_1^2 = 4uv$, or $y_1^2 = uv$. We can show that u and v are relatively prime: if d is a divisor of both u and v, then d is a divisor of their sum, $u + v$ and their difference, $u - v$. But $u + v = z$, $u - v = x$, so d would have to be a divisor of x and z. Since x and z are relatively prime, $d = 1$.

Theorem 3 *If the product of two relatively prime positive integers is a square, then both integers are squares.*

We will prove this later. As an example, $12 \times 75 = 900 = 30^2$. Even though neither 12 nor 75 is a square, this does not contradict the theorem because they are not relatively prime. What the theorem says is the only way to write 900 as the product of two relatively prime positive integers is to use squares. We can certainly do this in many ways: $900 = 2^2 \times 15^2 = 5^2 \times 6^2$, for example.

If we believe Theorem 3, then $uv = y_1^2$, with u and v relatively prime, so $u = p^2$ and $v = q^2$ for some integers p and q, which are relatively prime. Now $x = u - v = p^2 - q^2$, $z = u + v = p^2 + q^2$, and $y^2 = 4uv = 4p^2q^2$ so $y = 2pq$. Thus, we again have $(x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2)$.

This may seem much shorter, but it really isn't: With the geometric approach, we proved things about primitive triples that we just used here without reproving them. Moreover, this proof is incomplete because we have not yet proven Theorem 3.

A strange algebraic approach to Pythagorean triples

One last proof. This will be much like the previous one except for one thing: rather than using the integers, we will use something called the **Gaussian integers**. These are numbers of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$. The Gaussian integers, $\{a + bi \,|\, a, b \in Z\}$ are usually denoted $Z[i]$. We now proceed as before: Assume that (x, y, z) is a primitive Pythagorean triple and that y is even. In the previous proof, we rearranged $x^2 + y^2 = z^2$ and used the fact that $z^2 - x^2$ factors. Here, we don't have to rearrange. We have $z^2 = x^2 + y^2 = (x + iy)(x - iy)$, where $x + iy$ and $x - iy$ are Gaussian integers. Now suppose that d is a (Gaussian) integer which divides both $x + iy$ and $x - iy$. Then d is a divisor of their sum, $2x$, and their difference, $2iy$. Since x and y have no common divisors, d must be a divisor of 2. In fact, 2 does have divisors! We have $2 = (1 + i)(1 - i)$, so both $1 + i$ and $1 - i$ are divisors of 2. However, if x is odd, say $x = 2m + 1$, and d is a divisor of both 2 and x, then d is also a divisor of $x - 2m$ but $x - 2m = 1$. This means d is a divisor of 1. The Gaussian divisors of 1 are 1, -1, i, $-i$, so d must be one of these. Divisors of 1 are called **units**. Among the ordinary integers, the units are 1 and -1. Here is an extension of Theorem 3.

Theorem 4 *If u and v are Gaussian integers, uv is a square, and the only common divisors of u and v are units, then u and v must be squares multiplied by units.*

In the case at hand, $z^2 = (x + iy)(x - iy)$ so $x + iy = \text{unit}(p + qi)^2$. It turns out that we can ignore the unit in this case (you might play around to see why) so we can write $x + iy = (p + qi)^2 = p^2 + 2pqi + (qi)^2 = p^2 - q^2 + 2pqi$. Equating real and imaginary parts gives $x = p^2 - q^2$, $y = 2pq$.

Admittedly, we have to take a lot of things on faith in order to use this third approach. However, it has the advantage of being quick, if we assume those things to be true. For example, consider the variation on Pythagorean triples: (x, y, z) for which $x^2 + 2y^2 = z^2$. Suppose we want primitive triples that satisfy this equation. Note that if x is even, then the left hand side would be even, so z^2 would be even forcing z to be even and the triple would not be primitive. So we can assume x and z are both odd. As with the Gaussian integers, we force a factorization:

$$z^2 = x^2 + 2y^2 = (x + \sqrt{-2}y)(x - \sqrt{-2}y).$$

We introduce a new set of "integers," those things of the form $a + b\sqrt{-2}$ where a and b are ordinary integers. This set is usually denoted $Z[\sqrt{-2}]$. More generally, if n is not a perfect square, we let $Z[\sqrt{n}]$ be the set of all numbers of the form $a + b\sqrt{n}$, where a and b are integers. Back to our example, $x^2 + 2y^2 = z^2$. Since x and y are relatively prime, it follows that $x + y\sqrt{-2}$ and $x - y\sqrt{-2}$ will be relatively prime (this takes some effort to justify). As before, the product of relatively prime things equaling a square forces each of them to be squares, so

$$x + y\sqrt{-2} = (p + q\sqrt{-2})^2 = p^2 + 2pq\sqrt{-2} - 2q^2 = p^2 - 2q^2 + 2pq\sqrt{-2}.$$

We have $x = p^2 - 2q^2$ and $y = 2pq$. For z, $z^2 = x^2 + 2y^2 = (p^2 - 2q^2)^2 + 2(2pq)^2$ and I will let you check that we get $z = p^2 + 2q^2$. This means that

$$(x, y, z) = (p^2 - 2q^2, 2pq, p^2 + 2q^2),$$

where p and q are relatively prime and p is odd. One slight correction: since $x^2 = (-x)^2$, it is possible that $p^2 - 2q^2$ could be negative. We should write

$$(x, y, z) = (|p^2 - 2q^2|, 2pq, p^2 + 2q^2).$$

We would have actually seen the absolute value arise if we had been more careful about units. The geometric approach will work on this problem as well. I ask you to use the geometric approach on $x^2 + 2y^2 = z^2$ in the homework.

One final example: Find all primitive triples to $x^2 + 6y^2 = z^2$. Proceeding as before, and skipping most details, $z^2 = x^2 + 6y^2 = (x + y\sqrt{-6})(x - y\sqrt{-6})$. Since x and y are relatively prime, it follows that $x + y\sqrt{-6}$ and $x - y\sqrt{-6}$ will be relatively prime (again, this takes some effort to justify). As before, we have the product of relatively prime things equaling a square so

$$x + y\sqrt{-6} = (p + q\sqrt{-6})^2 = p^2 + 2pq\sqrt{-6} - 6q^2 = p^2 - 6q^2 + 2pq\sqrt{-6}.$$

We have $x = p^2 - 6q^2$, $y = 2pq$, $z = p^2 + 6q^2$, so

$$(x, y, z) = (|p^2 - 6q^2|, 2pq, p^2 + 6q^2).$$

For example, picking $p = 5, q = 2$ we get $x = 25 - 24 = 1$, $y = 2 \times 5 \times 2 = 20$, $z = 25 + 24 = 49$, and indeed $1^2 + 6 \times 20^2 = 2401 = 49^2$. What a great method! Unfortunately, something is definitely wrong here: (1, 2, 5) is a primitive solution to $x^2 + 6y^2 = z^2$ but it does not have the right form. That is, there are no p and q which can give this triple. To try to see what is going on, we can check our calculations with $x = 1$, $y = 2$, $z = 5$. We have $5^2 = (1 + 2\sqrt{-6})(1 - 2\sqrt{-6})$ but it turns out that even though $1 + 2\sqrt{-6}$ and $1 - 2\sqrt{-6}$ are relatively prime, and multiply to a square, neither of them is a perfect square. Let's be ultra careful on these points. First, if $1 + 2\sqrt{-6}$ and $1 - 2\sqrt{-6}$ had a factor in common, it would have to be a divisor of their sum, 2. Can we write $2 = (a + b\sqrt{-6})(c + d\sqrt{-6})$? Here is a great simplifying trick: If a formula holds for complex numbers, then if you take the complex conjugate of everything, you get another formula. That is, since $2 = (a + b\sqrt{-6})(c + d\sqrt{-6})$, we must also have $2 = (a - b\sqrt{-6})(c - d\sqrt{-6})$. Next, if we multiply these two equations together, we get $4 = (a^2 + 6b^2)(c^2 + 6d^2)$. But $a^2 + 6b^2 > 4$ unless $b = 0$. Similarly, we would need $d = 0$, so we want $4 = a^2c^2$, forcing a or c to be a unit. The consequence of this: the only common factors $1 + 2\sqrt{-6}$ and $1 - 2\sqrt{-6}$ can have are ± 1 or ± 2. Since neither is divisible by 2, this leaves only units, so they are relatively prime.

Next, can $1 + 2\sqrt{-6}$ be a square? This would require $1 + 2\sqrt{-6} = (a + b\sqrt{-6})^2 = a^2 - 6b^2 + 2ab\sqrt{-6}$. That is, we need $1 = a^2 - 6b^2$ and $2 = 2ab$. This last equation has only $a = b = 1$ or $a = b = -1$ as solutions, and in each case, $a^2 - 6b^2 = -5 \neq 1$.

Consequently, Theorem 3 might be true for ordinary integers and Theorem 4 might be true for Gaussian integers, but the general statement is not true in all extensions of integers. What goes wrong (or right for the ordinary integers and for Gaussian integers) is a property that systems of integer-like things might have called **Unique Factorization**. We discuss the Unique Factorization Property in the next set of notes.