

Pythagorean Triples

Many people know that $3^2 + 4^2 = 5^2$. Less commonly known are $5^2 + 12^2 = 13^2$ or $7^2 + 24^2 = 25^2$. Such a set of integers is called a Pythagorean Triple. The reason for this is because of its 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, 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 type. 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 that $x^2 = 4y + 4$. We can rewrite this: $y = \frac{x^2 - 4}{4}$. I will let you show the following: $x^2 - 4$ is divisible by 4 if and only if x is even. Letting $x = 2k$, this gives a triple: (2k, $k^2 - 1$, $k^2 + 1$). For example, when $k = 4$, we get the triple (8, 15, 17), and $8^2 + 15^2 = 64 + 225 = 289 = 17^2$.

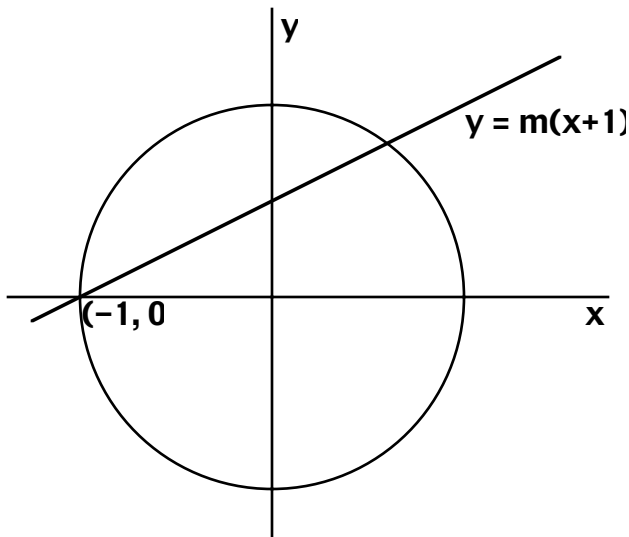
Is it possible to find a simple way to describe **all** Pythagorean triples? In fact, we **can** find all such triples, and we can use several methods to do so. In this set of notes, I will give both geometric and an algebraic approaches.

Geometric approach:

If $x^2 + y^2 = z^2$, then dividing by z^2 gives $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$, or $a^2 + b^2 = 1$,

where a and b are rational numbers (instead of integers). Similarly, if $a^2 + b^2 = 1$ where a and b are rational numbers and z is the least common

multiple of the denominators of a and b , then $(za)^2 + (zy)^2 = z^2$ and za and zb will be integers. Thus, finding integer solutions to $x^2 + y^2 = z^2$ is equivalent to finding rational solutions to $x^2 + y^2 = 1$. This may not look like progress, but there is a simple geometrical idea for getting all rational points on this curve (the curve is the unit circle, of course). Consider the following figure of the unit circle and a line passing through $(-1, 0)$:



This line will intersect the circle in another point, call it (a, b) . To find this point, we solve the equations $x^2 + y^2 = 1$ 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 $x = -1$ is known to be a solution to this equation, the other solution can be found by dividing by

$x + 1$. We have, after the division: $(m^2 + 1)x + m^2 - 1 = 0$. Thus, 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 $y =$

$$m\left(\frac{1 - m^2}{m^2 + 1} + 1\right) = m \frac{2}{m^2 + 1} = \frac{2m}{m^2 + 1}. \quad \text{The point } (a, b) \text{ is } \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{m^2 + 1}\right).$$

We are only interested in points (a, b) which, as in the diagram, are in the first quadrant. To insure this, the slope, m , of the line should satisfy $0 < m < 1$.

Some comments on this: First, if m is a rational number, then by the form above for a and b , we have that a and b are rational. The converse is also true: if a and b are rational, then so is m : the slope of the line containing

$(-1, 0)$ and (a, b) is $m = \frac{b}{a + 1}$. Thus, if a and b are rational, then m is the

quotient of rational numbers, so m is rational. Now since m is rational,

suppose that $m = \frac{q}{p}$ where p and q are integers. If $0 < m < 1$, then it must be

that $p > q > 0$. We have

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

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 discovered this pattern, it can now be checked easily:

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

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 Pythagorean triples can be formed in this way, however! Here are two examples: $(x, y, z) = (4, 3, 5)$ cannot occur since $y = 2pq$ implies that y is even. Similarly, $(x, y, z) = (15, 20, 25)$ cannot occur. In this case, we would need $20 = 2pq$, or $pq = 10$, with $p > q > 0$. The only possibilities for p and q are 10 and 1 or 5 and 2. Neither of these pairs gives rise to $(15, 20, 25)$.

How can this be? Every rational solution to $a^2 + b^2 = 1$ can be obtained by the procedure outlined above. In this case, the triple $(15, 20, 25)$ corresponds to the rational solutions $a = \frac{15}{25}$, $b = \frac{20}{25}$. But $\frac{15}{25} = \frac{3}{5}$ and $\frac{20}{25} = \frac{4}{5}$. So we see that many different Pythagorean triples can 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) .

Theorem 1. Every Pythagorean triple has the form

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

where $p > q > 0$, p, q are integers, and d is a positive **rational number** such that the triple has all integer entries.

It is customary to modify the problem of finding all Pythagorean triples as follows: Suppose any two of x, y, z are divisible by some **integer** d . Then it is easy to see that the third one is also divisible by d . In this case, if we write $x = dx_1, y = dy_1, z = dz_1$, then $x^2 + y^2 = z^2 \Rightarrow d^2x_1^2 + d^2y_1^2 = d^2z_1^2$, or $x_1^2 + y_1^2 = z_1^2$. Based on this, we usually only look for Pythagorean triples in which no two numbers have any factors in common. If two numbers do not have any common factors, we call the numbers **relatively prime**. If (x, y, z) is a Pythagorean triple with x, y, z pairwise relatively prime, we say (x, y, z) is **primitive**. Our discussion above shows that every Pythagorean triple has the form (dx, dy, dz) where (x, y, z) is a primitive triple.

Suppose that (x, y, z) is a primitive triple. Then exactly one of x, y, z must be even. In fact, it must be that z is odd: if x and y are both odd, and z is even, let $x = 2m + 1, y = 2n + 1, z = 2p$. Then we have $(2m + 1)^2 + (2n + 1)^2 = (2p)^2$, or $4m^2 + 4m + 4n^2 + 4n + 2 = 4p^2$. Dividing by 2 gives $2(m^2 + m + n^2 + n) + 1 = 2p^2$, which says that a certain number is both even and odd. Since this cannot happen, we rule out the case where x and y are both odd. Since exactly one of x and y must be even, we will arbitrarily decide to only look at triples in which x is odd and y is even. So $(3, 4, 5)$ is ok, but we will ignore $(4, 3, 5)$.

Theorem 2. Every primitive Pythagorean triple (x, y, z) in which y is even is of the form $(p^2 - q^2, 2pq, p^2 + q^2)$ where $p > q > 0$ are integers, p and q are relatively prime and one of p or q is even. Conversely, if $p > q > 0$, p and q are relatively prime and exactly one of them is even, then $(p^2 - q^2, 2pq, p^2 + q^2)$ is a primitive Pythagorean triple.

Proof: Let (x, y, z) be a primitive Pythagorean triple in which y is even. As before, there must be integers $p > q > 0$ such that $\frac{x}{z} = \frac{p^2 - q^2}{p^2 + q^2}$ and $\frac{y}{z} = \frac{2pq}{p^2 + q^2}$.

We may pick p and q to be relatively prime, since if $p = dp_1$ and $q = dq_1$, then

$$\frac{p^2 - q^2}{p^2 + q^2} = \frac{d^2p_1^2 - d^2q_1^2}{d^2p_1^2 + d^2q_1^2} = \frac{p_1^2 - q_1^2}{p_1^2 + q_1^2}$$

and

$$\frac{2pq}{p^2 + q^2} = \frac{2d^2p_1q_1}{d^2p_1^2 + d^2q_1^2} = \frac{2p_1q_1}{p_1^2 + q_1^2},$$

so we could have used p_1 and q_1 instead of p and q . If both p and q are odd, say $p = 2n + 1$, $q = 2m + 1$ then

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

From this, it follows that x must be even (the numerator is divisible by 4 but the denominator is divisible by only 2.) This contradicts x being odd. Thus it cannot be that p and q are both odd, so one must be even and the other odd.

Conversely, if $p > q > 0$, p and q are relatively prime, and one of them is even, then let d be a common divisor of $p^2 - q^2$ and $p^2 + q^2$. Any number which divides two numbers must divide both their sum and difference as well. Thus, d will be a divisor of $(p^2 + q^2) + (p^2 - q^2) = 2p^2$ and $(p^2 + q^2) - (p^2 - q^2) = 2q^2$. Since d is odd (this follows because exactly one of p and q is even so $p^2 + q^2$ is odd and d is a divisor of $p^2 + q^2$), it must be that d is a common divisor of p^2 and q^2 , from which we conclude that p and q are not relatively prime. That is, p and q are not relatively prime unless d , the common divisor of $p^2 - q^2$ and $p^2 + q^2$, is only 1. This means that $p^2 - q^2$ and $p^2 + q^2$ are relatively prime, and $2pq$ is prime to both of them. Thus, $(p^2 - q^2, 2pq, p^2 + q^2)$ is a primitive triple. This concludes the proof.

Pythagorean triples from an algebraic approach:

Everything above was based on the geometric idea that rational solutions to the equation $x^2 + y^2 = 1$ can be found by considering lines of rational slope passing through $(-1, 0)$. We now look at things purely algebraically. Again, we will restrict our attention to primitive Pythagorean triples. Suppose (x, y, z) is a

primitive triple and that y is even. We have:

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

If we write $y = 2y_1$, then $4y_1^2 = 4 \left(\frac{z + x}{2} \right) \left(\frac{z - x}{2} \right)$ or $y_1^2 = \left(\frac{z + x}{2} \right) \left(\frac{z - x}{2} \right)$. If

$u = \frac{z + x}{2}$ and $v = \frac{z - x}{2}$, then $z = u + v$ and $x = u - v$. From this it follows

that u and v are relatively prime. (Any common factor of u and v will be a common factor of their sum and difference. Since x and z are relatively prime, so are u and v .) We now state a result to be proved at a later point:

Theorem 3. If the product of two relatively prime positive integers is a square, then both integers must themselves be squares.

So, for example, $6^2 = 4 \cdot 9$, which are both squares. However, $6^2 = 2 \cdot 18$, but this does not contradict the theorem because 2 and 18 are not relatively prime.

Now, since $uv = y_1^2$ and u and v are relatively prime, it must be that u and v are both squares, say $u = p^2$ and $v = q^2$. From this, we have $x = u - v = p^2 - q^2$, $z = u + v = p^2 + q^2$ and $y^2 = 4y_1^2 = 4uv = 4p^2q^2$, so $y = 2pq$. Consequently, we again have $(x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2)$.

This approach may seem much shorter than the geometric approach. However, remember, we had all the discussion on primitive triples in that section. Moreover, there is still Theorem 3 to prove.

A strange algebraic approach to Pythagorean triples:

This approach will be much like the previous one except for one thing: we are going to expand what we call integers: the **Gaussian integers** are all expressions of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$. We now proceed as before: we assume that (x, y, z) is a primitive triple and that y is even. This time, we use a different factorization: $z^2 = x^2 + y^2 = (x + iy)(x - iy)$, where $x + iy$ and $x - iy$ are not ordinary integers, but Gaussian integers instead. Now suppose that d is a (Gaussian) integer which divides both $x + iy$ and $x - iy$.

Then d is a common divisor of $2x = (x + iy) + (x - iy)$ and $2iy = (x + iy) - (x - iy)$. Since x and y have no common divisor, d must be a divisor of 2. (2 actually has a lot of divisors: besides 1 and 2, there are $1 + i$, $1 - i$, $-1 + i$ and $-1 - i$.)

However, if x is odd, say $x = 2m + 1$, and d is a divisor of both 2 and x , then d will be a divisor of $x - 2m$, which is to say, d must be 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**.) Here is an extension to theorem 3:

Theorem 3' 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, we have $z^2 = (x + iy)(x - iy)$ so $x + iy$ must be a square times a unit, say $x + iy = (\text{unit})(p + qi)^2$. It turns out that we can ignore the unit in this case (you might try playing around with using units to see why), so $x + iy = (p + qi)^2$. This means that $x + iy = p^2 + 2ipq + q^2i^2 = p^2 - q^2 + i(2pq)$, so $x = p^2 - q^2$ and $y = 2pq$.

Admittedly, this third approach has lots of gaps in it: we have to take a lot of things on faith in order to use it. However, it has the advantage of being quick, once these things are assumed to be true. For example, consider the equation

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

and suppose we ask for all primitive triples that make this equation true. Note the following: if x is even, then the left hand side of the expression will be even, so z^2 must be even. From this, it follows that z is even. Since we want primitive solutions, we don't allow this. So x and z must both be odd. As before, we force a factorization:

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

We next introduce a new set of "integers": all things having the form $a + \sqrt{-2}b$, where a and b are integers. Since x and y are relatively prime, it follows that $x + \sqrt{-2}y$ and $x - \sqrt{-2}y$ will be relatively prime (this takes a little work to justify). As before, since the product of relatively prime things is a square, each of them must be a square, so

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

and we have $x = p^2 - 2q^2$, $y = 2pq$, $z^2 = x^2 + 2y^2 = (p^2 - 2q^2)^2 + 2(2pq)^2$
 from which it follows that $z = p^2 + 2q^2$. Thus,

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

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 really 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 do that in the exercises.

One final example: Find all primitive triples to $x^2 + 6y^2 = z^2$. Proceeding as before, $z^2 = x^2 + 6y^2 = (x + \sqrt{-6}y)(x - \sqrt{-6}y)$. If x and y are relatively prime, then so are $x + \sqrt{-6}y$ and $x - \sqrt{-6}y$, so as before we have that $x + \sqrt{-6}y$ is a square, $x + \sqrt{-6}y = (p + \sqrt{-6}q)^2 = p^2 - 6q^2 + \sqrt{-6}2pq$, and we get $(x, y, z) = (p^2 - 6q^2, 2pq, p^2 + 6q^2)$, or more precisely,
 $(|p^2 - 6q^2|, 2pq, p^2 + 6q^2)$.

This time, the gaps in our proof are too big: $(1, 2, 5)$ is a primitive triple satisfying $x^2 + 6y^2 = z^2$, but there is no way to get $(1, 2, 5)$ from p and q above. To see what is going wrong, we can substitute $x = 1, y = 2, z = 5$ in for the above calculations: $5^2 = 1^2 + 6(2)^2$ is certainly true, as is $5^2 = (1 + 2\sqrt{-6})(1 - 2\sqrt{-6})$ but it turns out that $1 + 2\sqrt{-6}$ is not a perfect square after all. If we try to solve $1 + 2\sqrt{-6} = \pm(p + \sqrt{-6}q)^2$ we may use the following trick: take the absolute value of each side: $|1 + 2\sqrt{-6}| = |p + \sqrt{-6}q|^2$, which becomes $\sqrt{25} = p^2 + 6q^2$, or $p^2 + 6q^2 = 5$. But this equation has no integer solutions (p, q) , so something is wrong with Theorem 3'.

What goes wrong is something called **Unique Factorization**. The next set of notes discusses the Unique Factorization property.