Lecture 2 - Pythagorean Triples

Before getting into Pythagorean triples, let's recall some vocabulary from last time and also introduce a new category of numbers.

- A natural number is a positive whole number. The set of all natural numbers is denoted $\mathbb{N}$:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

- We say a natural number n is square if there exists a natural number m such that $n = m^2$. E.g., $1, 4, 9, 16, 25, \ldots$ are square numbers
- We'll say that $d \in \mathbb{N}$ divides $n \in \mathbb{N}$ if there exists a $m \in \mathbb{N}$ such that

$$n = md$$

If d divides n, we'll write $d|n$. For example, $2|12$, $7|21$, and $13|78$: ($12 = 6 \cdot 2$, $21 = 3 \cdot 7$, and $78 = 6 \cdot 13$).

- We'll say d is a common factor of m and n if $d|m$ and $d|n$. For instance, 15 is a common factor of 45 and 90. Notice a single pair of numbers can have several common factors: 45, 15, 9, 5, and 3 are all common factors of 45 and 90.
- A rational number is a fraction of two integers (whole numbers) where the denominator is not zero. E.g., $\frac{3}{7}$, $-\frac{22}{3}$, and $\frac{14}{1,927}$ are rational numbers. The collection of all rational numbers is denoted $\mathbb{Q}$.

As we saw last time, the sum of two squares is sometimes a square,

$$9+16=25$$
$$3^2+4^2=5^2$$

and sometimes it's not:

$$16+25=41$$
$$4^2+5^2 = \text{non-square}$$

If a, b, and c are natural numbers satisfying $a^2+b^2=c^2$, then we call (a,b,c) a Pythagorean triple. Here are a few Pythagorean triples:

$(3,4,5)$	$3^2+4^2=9+16=25=5^2$
$(5,12,13)$	$5^2+12^2=25+144=169=13^2$
$(8,15,17)$	$8^2+15^2=64+225=289=17^2$
$(9,12,15)$	$9^2+12^2=81+144=225=15^2$

Maybe the most obvious question to ask about Pythagorean triples is how many are there? Are there only finitely-many or are there infinitely-many?

It's not too hard to show that there must be infinitely-many Pythagorean triples:

Lemma

If (a,b,c) is a Pythagorean triple and $d \in \mathbb{N}$ is any natural number, then (da, db, dc) is also a Pythagorean triple

Pf

We need to show $(da)^2+(db)^2=(dc)^2$, and we already know $a^2+b^2=c^2$, so let's just try to start with $(da)^2+(db)^2$

and see if we can rewrite it as $(dc)^2$.

$$\begin{aligned}(da)^2 + (db)^2 &= d^2a^2 + d^2b^2 \\ &= d^2(a^2+b^2) \\ &= d^2c^2 \\ &= (dc)^2\end{aligned}$$

□

As a consequence of this simple result, there must be infinitely-many Pythagorean triples: take any one of them and continue to multiply its values by larger and larger values of d:

$(3,4,5)$, $(6,8,10)$, $(9,12,15)$, $(12,16,20)$, ...

Notice that this list, even though it's infinitely long, will never contain the Pythagorean triples $(5,12,13)$ or $(8,15,17)$.

So now we have another question: is there any way of producing a list containing <u>all</u> Pythagorean triples?

There is in fact a way of producing such a list which utilizes an idea which is commonly attributed to Euclid.

Let's first notice that is (a,b,c) is a Pythagorean triple, so

$$a^2+b^2=c^2$$

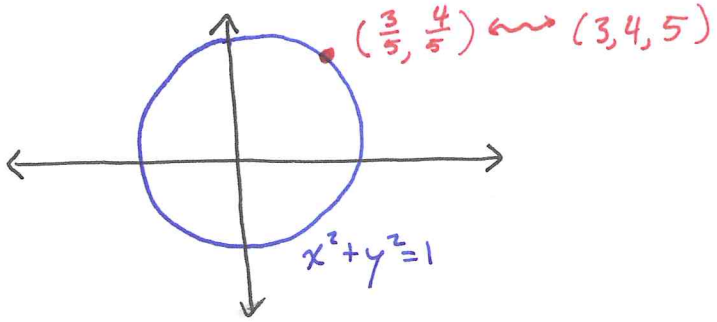
Then dividing both sides of the equation by c^2 yields

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

or

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

That is, the point $(x,y) = \left(\frac{a}{c}, \frac{b}{c}\right)$ is a solution to the equation $x^2+y^2=1$. Thus every Pythagorean triple (a,b,c) determines a point on the unit circle with rational coordinates — i.e., an (x,y)-pair solving $x^2+y^2=1$ with x and y both rational numbers.



Furthermore, if we have a point on the circle with rational coordinates — say

$$\left(\frac{\alpha}{\beta}, \frac{\gamma}{\delta}\right)$$

then we can associate to this point a Pythagorean triple:

$$\left(\frac{\alpha}{\beta}\right)^2 + \left(\frac{\gamma}{\delta}\right)^2 = 1$$

$$\Rightarrow \frac{\alpha^2}{\beta^2} + \frac{\gamma^2}{\delta^2} = 1$$

$$\Rightarrow \frac{\alpha^2\delta^2}{\beta^2\delta^2} + \frac{\gamma^2\beta^2}{\beta^2\delta^2} = 1$$

$$\Rightarrow (\alpha\delta)^2 + (\gamma\beta)^2 = (\beta\delta)^2$$

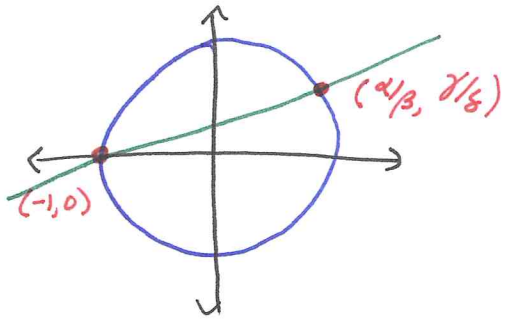
We'd like to say $(\alpha\delta, \gamma\beta, \beta\delta)$ is a Pythagorean triple, but we need to be slightly careful: α, β, γ, or δ could be negative. So, really, if $\left(\frac{\alpha}{\beta}, \frac{\gamma}{\delta}\right)$ is on the unit circle, the corresponding Pythagorean triple should be $(|\alpha\delta|, |\beta\gamma|, |\beta\delta|)$.

Regardless, we now have a new tool we can use to find Pythagorean triples, and are lead to

the question of finding points on the unit circle with rational coordinates.

That is, we can re-interpret the question "How do you produce a list of all Pythagorean triples?" as "How do you produce a list of all points on the unit circle with rational coordinates?"

To answer this question we can use some simple geometry. Take any rational point $(\alpha/\beta, \gamma/\delta)$ on the unit circle, and draw the line which goes through that point and the point $(-1,0)$. Notice the slope of this line must be rational.



$$m = \frac{\gamma/\delta - 0}{\alpha/\beta - (-1)}$$

$$= \frac{\gamma}{\delta \cdot (\alpha/\beta + \beta/\beta)}$$

$$= \frac{\beta\gamma}{\alpha\delta}$$

Now say we draw a line through $(-1,0)$ with some rational slope $m = \frac{u}{v}$. Is it guaranteed that this line will intersect the circle at a rational point?

The equation of the line is

$$y - 0 = m(x - (-1))$$
$$\Rightarrow y = mx + m$$

So the points on this line have the form $(x, mx+m)$. If such a point lives on the unit circle, then

$$x^2 + (mx+m)^2 = 1$$
$$\Rightarrow x^2 + m^2x^2 + 2m^2x + m^2 = 1$$
$$\Rightarrow (1+m^2)x^2 + (2m^2)x + m^2 - 1 = 0$$

Applying the quadratic formula gives

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

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

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

$$= \frac{-(m^2+1)}{m^2+1} \quad \text{or} \quad \frac{1-m^2}{1+m^2}$$

The solution $x = \frac{-(m^2+1)}{m^2+1} = -1$ corresponds to $(-1, 0)$, but the other solution gives us the rational point on the circle

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

Plugging in $m = \frac{u}{v}$, we have

$$\frac{1-\left(\frac{u}{v}\right)^2}{1+\left(\frac{u}{v}\right)^2} = \frac{\left(\frac{v^2-u^2}{v^2}\right)}{\left(\frac{v^2+u^2}{v^2}\right)} = \frac{v^2-u^2}{v^2+u^2}$$

$$\frac{2\left(\frac{u}{v}\right)}{1+\left(\frac{u}{v}\right)^2} = \frac{\left(\frac{2u}{v}\right)}{\left(\frac{v^2+u^2}{v^2}\right)} = \frac{2uv}{v^2+u^2}$$

Putting all of this together, given a rational number $\frac{u}{v}$, we associate a rational point on the unit circle,

$$\left(\frac{v^2-u^2}{v^2+u^2}, \frac{2uv}{v^2+u^2}\right)$$

and to this point we may associate a Pythagorean triple:

$$\left[\frac{v^2-u^2}{v^2+u^2}\right]^2 + \left[\frac{2uv}{v^2+u^2}\right]^2 = 1$$

$$\Rightarrow (v^2-u^2)^2 + (2uv)^2 = (v^2+u^2)^2$$

and so the triple is $(v^2-u^2, 2uv, v^2+u^2)$, assuming $v^2 > u^2$. So if we can produce a list of all rational numbers (which is easy to do — use Cantor's "zig-zag" trick), then we can produce a list of all the Pythagorean triples (there is one caveat: our list of rationals should include all the ways a rational number may be written — e.g., we want $1/2$, $2/4$, $3/6$, ... to each appear in our list).

Notice that multiple Pythagorean triples may get associated to the same point on the unit circle. Both $(3,4,5)$ and $(6,8,10)$ get associated to the same point as

$$(3/5, 4/5) = (6/10, 8/10).$$

Just as we can generate infinitely-many Pythagorean triples from a given Pythagorean triple, we have infinitely-many Pythagorean triples associated to each rational point on the unit circle.

All of the Pythagorean triples associated to a rational point on the unit circle are multiples of a particular Pythagorean triple associated to that rational point, which is called a primitive Pythagorean triple.

We say a Pythagorean triple (a,b,c) is **primitive** if a, b, and c have no common factors: that is, there is no number d which divides a, b, and c.

Pythagorean Triple	Primitive?
$(3,4,5)$	Yes
$(5,12,13)$	Yes
$(16,30,34)$	No – 2 is a common factor
$(8,15,17)$	Yes
$(21,72,75)$	No – 3 is a common factor
$(7,24,25)$	Yes

If we use a computer to generate a list of Pythagorean triples as indicated above, and then throw out the ones which are <u>not</u> primitive. (so, only leaving primitive ones in our list), we may notice some patterns

$(3,4,5)$
$(5,12,13)$
$(8,15,17)$
$(7,24,25)$
$(20,21,29)$
$(12,35,37)$
$(9,40,41)$
$(28,45,53)$
$(11,60,61)$
$(16,63,65)$
$(33,56,65)$
$(48,55,73)$
$(13,84,85)$
$(36,77,85)$
$\vdots$

You may notice that c appears to always be odd, and that one of a or b is always odd and the other one is even. Both of these phenomena are easy to explain.

Recall that a natural number n is **even** if there exists a natural number m such that $n = 2m$. We say n is **odd** if there exists a natural number m so that $n = 2m-1$. A few basic facts, which you should try to prove as an exercise are

- the square of an even number is even
- the square of an odd number is odd
- the sum of two even numbers is even
- the sum of two odd numbers is even
- the sum of an odd and an even number is odd.

Using the facts above, suppose a and b were both even. Then a^2 and b^2 would be even, but then $c^2 = a^2 + b^2$ would also be even. If each of a, b, and c is even, then (a, b, c) can not be primitive because two would be a common factor.

Now suppose a and b are both odd. Then a^2 and b^2 are odd, so $c^2 = a^2 + b^2$ must be even. As the square of an odd number is odd, this means c is even as well. Hence we can find $x, y, z \in \mathbb{N}$ such that $a = 2x-1$, $b = 2y-1$, and $c = 2z$. Plugging these into $a^2 + b^2 = c^2$ gives

$$(2x-1)^2 + (2y-1)^2 = (2z)^2$$
$$\Rightarrow 4x^2 - 4x + 1 + 4y^2 - 4y + 1 = 4z^2$$
$$\Rightarrow 4x^2 - 4x + 4y^2 - 4y + 2 = 4z^2$$
$$\Rightarrow 2x^2 - 2x + 2y^2 - 2y + 1 = 2z^2$$

However, this is impossible because $2x^2-2x+2y^2-2y+1$ is odd while $2z^2$ is even. Thus it must be that a and b can't both be odd.

So, in any Pythagorean triple, one of a or b must be even. However, they can't both be even. So one of a or b is even, the other is odd, and this implies that c must be odd. We will always suppose, for a primitive Pythagorean triple (a,b,c), that a is odd and b is even.

So, if we are to find all primitive Pythagorean triples, we want to find all natural numbers a, b, and c such that

- a is odd,
- b is even,
- a, b, and c have no common factors, and
- $a^2+b^2=c^2$

Notice if $a^2+b^2=c^2$, then $a^2=c^2-b^2=(c-b)(c+b)$ Is this a helpful observation? Well, let's take some of our primitive Pythagorean triples and see what $c-b$ and $c+b$ look like

(a,b,c)	c^2-b^2	$c-b$	$c+b$
$(3,4,5)$	5^2-4^2	1	9
$(5,12,13)$	13^2-12^2	1	25
$(5,8,17)$	17^2-15^2	9	25
$(7,24,25)$	25^2-24^2	1	49
$(35,12,37)$	37^2-12^2	25	49

Notice that $c-b$ and $c+b$ always seem to be squares, and $c-b$ and $c+b$ never seem to have a common factor. Can we explain why this is?

Suppose d was a common factor of both $c-b$ and $c+b$. Say

$$c-b = md$$
$$c+b = nd$$

Notice

$$d(n+m) = dn + dm = c+b+c-b = 2c$$
$$d(n-m) = dn - dm = c+b-(c-b) = 2b$$

Thus d is also a common divisor of $2b$ and $2c$ — but b and c have no common divisors: as the only value dividing b and c is 1, the only values dividing $2b$ and $2c$ are 1 and 2. Hence $d=1$ or $d=2$. However,

$$\begin{aligned} a^2 &= c^2 - b^2 \\ &= (c-b)(c+b) \\ &= md \cdot nd \\ &= (mnd)d \end{aligned}$$

So d must divide a^2 as well. Since a^2 is odd, we must have $d=1$. That is, $c-b$ and $c+b$ have no common factors. Since $(c-b)(c+b)$ equals a square, but $c-b$ and $c+b$ have no common factors, $c-b$ and $c+b$ must also be squares.

(Question for students: if x and y have no common divisors but $xy = z^2$, then x and y are squares. Why?)

Since $c+b$ and $c-b$ are squares, we can write $c+b=s^2$, $c-b=t^2$. Furthermore, as a is odd, $c+b$ and $c-b$ are odd, so s and t must be odd. Notice that $c+b > c-b$, so $s^2 > t^2$ and $s > t$ (if we take s and t to be positive) Furthermore, since $c+b$ and $c-b$ have no common factors, then s and t have no common factors.

Notice

$$(c+b)+(c-b) = 2c$$
$$\Rightarrow \quad s^2+t^2 = 2c$$
$$\Rightarrow \quad c = \frac{s^2+t^2}{2}$$

and

$$(c+b)-(c-b) = 2b$$
$$\Rightarrow \quad s^2-t^2 = 2b$$
$$\Rightarrow \quad b = \frac{s^2-t^2}{2}$$

As $a^2 = (c+b)(c-b)$,

$$a = \sqrt{(c+b)(c-b)}$$
$$= \sqrt{s^2 \cdot t^2}$$
$$= st.$$

What we've shown is that every primitive Pythagorean triple (a,b,c) can be written as

$$a = st$$
$$b = \frac{s^2-t^2}{2}$$
$$c = \frac{s^2+t^2}{2}$$

where s and t are odd integers with no common factors and $s > t$.

Furthermore it turns out that if s and t satisfy the properties above, then

$$\left(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}\right)$$

will be a <u>primitive</u> Pythagorean triple. Checking that it's a Pythagorean triple is easy, showing it's primitive is hard and will have to wait until we discuss prime number.

Homework

Due Thurs., Jan. 15

- Create an account on http://cloud.sagemath.org using your @clemson.edu email address.

Due Tues., Jan 20

- From Silverman 1.1, 1.5, 1.6
  2.1, 2.7, 2.8 ← Hard!
  3.2, 3.3, 3.5★