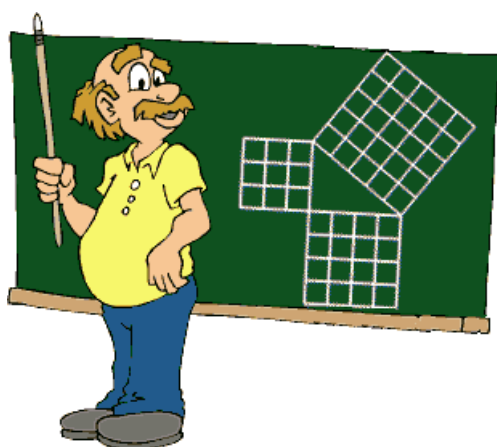


# Rational Unit Circle Points/Pythagorean Triples

Karl Hahn

© 2004



This is a topic that has fascinated me since I was 12 years old...

As you know, the functions that form the unit circle are:

$$y = \sqrt{1 - x^2} \text{ and } y = -\sqrt{1 - x^2}$$

You might have noticed that for many rational values of  $x$  that you can put into these functions (and we will be concerned primarily with the first one, and only in the domain of  $0 \leq x \leq 1$  – that is the first quad-

rant), you often get irrational values for  $y$ . For example, if you put in  $x = \frac{1}{2}$ , you get out  $y = \frac{\sqrt{3}}{2}$ , and if you put in  $x = \frac{2}{3}$ , you get out  $y = \frac{\sqrt{5}}{3}$ . But for certain special rational values of  $x$  you also get rational values for  $y$ . For example, if you put in  $x = \frac{3}{5}$ , you get out  $y = \frac{4}{5}$ , and if you put in  $x = \frac{5}{13}$ , you get out  $y = \frac{12}{13}$ .

The question to be explored now is, how frequently do such “nice” points occur on the unit circle? In particular, if you take any interval of the unit circle, no matter how small, can you always find a point on the unit circle in that interval where both  $x$  and  $y$  are rational numbers?

To answer this, you first must see the relationship between rational unit circle points and so called Pythagorean triples. If  $x$  and  $y$  are both rational numbers and  $(x, y)$  is on the unit circle, we can find the least common denominator of the two fractions that form  $x$  and  $y$ . Call that common denominator,  $c$ , which is a positive integer. So

$$x = \frac{b}{c}$$

and

$$y = \frac{a}{c}$$

where  $a$  and  $b$  are also positive integers. Putting these into the unit circle equation,  $x^2 + y^2 = 1$ , you have

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

or equivalently,  $a^2 + b^2 = c^2$ , where  $a$ ,  $b$ , and  $c$  are all positive integers. Such triples of integers are known as *Pythagorean triples* or sometimes as *Pythagorean triplets*.

To find the answer to the original question posed here, we look at how we find Pythagorean triples. First, you should observe that if  $(a, b, c)$  is a Pythagorean triple, then so is  $(ka, kb, kc)$ , for any positive integer multiplier,  $k$ , you might choose. But notice that if you have two Pythagorean triples, and one is multiple of the other, then they both correspond to the same unit circle point. So we will be concerned here primarily with Pythagorean triples in which  $a$ ,  $b$ , and  $c$  have no factors in common other than 1. You should be able to see that each distinct such Pythagorean triple (that is each triple with no common factors) corresponds to a unique point on the unit circle.

Just choosing random numbers for  $a$  and  $b$  then adding their squares does not usually give you a perfect square. But for  $a$  and  $b$  to be elements of a Pythagorean triple, that is the property we need to have. So how do we choose  $a$  and  $b$  to guarantee that the sum of their squares will be a perfect square,  $c^2$ ? First observe that  $a$ ,  $b$ , and  $c$  cannot all be even numbers because we have already stipulated that we do not want all three to have any common factors – including a common factor of 2. They cannot all be odd either, because the square of an odd number is also odd, and the sum of two odd numbers is even. It turns out also that  $c$  cannot be even. So  $c$  must be odd, and either  $a$  is even and  $b$  odd, or vice versa. Without loss of generality we can explore only the case where  $a$  is even and  $b$  is odd.

Since  $c$  and  $b$  are both odd and  $c > b$ , both the sum,  $c + b$ , and the difference,  $c - b$ , are positive even integers. The problem of finding Pythagorean triples becomes much easier at this point if you do a change in variables. Let  $m$  be the mean of  $c$  and  $b$  (that is half of their sum) and  $n$  be half of their difference. We know that both  $m$  and  $n$

are positive integers. Then  $c = m + n$ , and  $b = m - n$ . Using that substitution, the equation for the Pythagorean triple becomes

$$\begin{aligned} a^2 + (m - n)^2 &= (m + n)^2 \\ a^2 + m^2 - 2mn + n^2 &= m^2 + 2mn + n^2 \end{aligned}$$

Taking the cancellation and moving all the remaining  $mn$  terms to the right of the equal, we have

$$a^2 = 4mn$$

Consequently, all we have to do to form a Pythagorean triple is to choose  $m$  and  $n$  such that  $4mn$  is a perfect square, which is equivalent to  $mn$  being a perfect square (because 4 is a perfect square itself). Before we see how to do that, remember that the Pythagorean triple must have no common factors. Observe that this implies that  $m$  and  $n$  must have no common factors.

For a number,  $s$ , to be a perfect square, it is necessary and sufficient that each prime in its prime factorization occur an even number of times. To factor a perfect square into  $m$  and  $n$ , then, you would have to partition the prime factors in  $s$  between  $m$  and  $n$ . But if  $m$  and  $n$  are to have no common factors, then each prime that occurs in the prime factorization of  $s$  must have all its occurrences partitioned entirely into  $m$  or entirely into  $n$ . So each prime partitioned into  $m$  must occur an even number of times in  $m$ , and each prime partitioned into  $n$  must occur an even number of times in  $n$ . Hence  $m$  and  $n$  must both, themselves, be perfect squares.

### Why $c$ Can't be Even

If  $c$  were even, then  $c^2$  would necessarily be a multiple of 4. Since  $a$ ,  $b$ , and  $c$  cannot all be even, then if  $c$  is even,  $a$  and  $b$  must both be odd. So it must be true that  $a = 2i + 1$  and  $b = 2j + 1$  for some positive integers,  $i$  and  $j$ . But if you take the sum of the squares of those two expressions, you get:

$$c^2 = (2i + 1)^2 + (2j + 1)^2 = 4i^2 + 4i + 1 + 4j^2 + 4j + 1$$

All the terms in the right-hand side of the above are multiples of 4 except the two 1's. So this sum *cannot* be a multiple of 4. But if  $c$  is even, its square, and hence this sum, *must* be a multiple of 4, which is the contradiction that proves that  $c$  must be odd whenever the Pythagorean triple has no common factors. Consequently  $a$  and  $b$  must differ their parity – that is  $a$  must be even and  $b$  odd, or vice versa.

So how do we find  $m$  and  $n$  that are both square and have no common factors? Easy. Choose two numbers,  $u$  and  $v$ , that have no common factors and square them both. The recipe, then, to create a Pythagorean triple,  $(a, b, c)$ , is:

1. Choose two positive integers,  $u$  and  $v$ , that have no common factors. One of them must be greater than the other, so let  $u > v$ .
2. Set  $a = 2uv$ ,  $b = u^2 - v^2$ , and  $c = u^2 + v^2$ .

For example, if  $u = 8$  and  $v = 3$ , then  $a = 48$ ,  $b = 55$ , and  $c = 73$  is a Pythagorean triple.

Now let's get back to the question of how frequently rational points occur on the unit circle. When you state that every interval of the unit circle, no matter how small, always contains a rational point, you are saying, in the equivalent mathspeak, that the rational points are *dense* on the unit circle. And that is what we will now prove.

The proof involves the recipe we just derived for Pythagorean triples. Remember that each Pythagorean triple maps to a rational point on the unit circle. So if you use the recipe, choosing  $u$  and  $v$ , then the rational point on the unit circle that the triple maps to is:

$$x = \frac{u^2 - v^2}{u^2 + v^2} \qquad y = \frac{2uv}{u^2 + v^2}$$

Each point on the unit circle can be identified by an angle,  $\theta$ . If a point,  $(x, y)$ , is on the unit circle, then

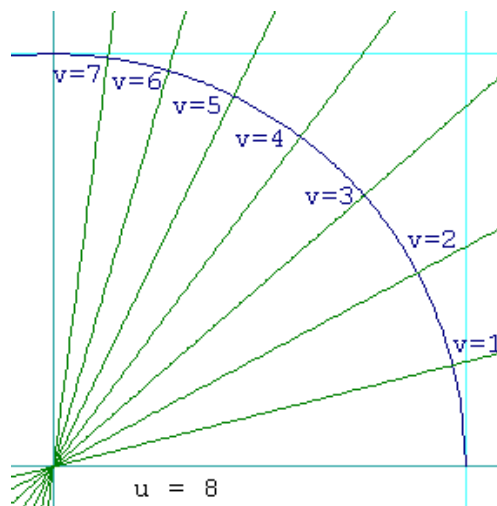
$$\frac{y}{x} = \tan \theta$$

or equivalently

$$\arctan\left(\frac{y}{x}\right) = \theta$$

If you can choose positive integers,  $u$  and  $v$ , to make the corresponding  $\theta$  angles as close together as you like, then you've proved the theorem. So, from the last few equations you have:

$$\arctan\left(\frac{2uv}{u^2 - v^2}\right) = \theta$$



Here you can see the points where the green lines intersect the blue circular arc. These are unit circle rational points you get with  $u = 8$  and  $v$  counting from 1 to 7

If you choose  $u$  as large as you like, then  $v$  can count from zero to  $u$ , where  $v = 0$  corresponds to the point,  $(1, 0)$ , and  $v = u$  corresponds to  $(0, 1)$  on the unit circle. All the  $v$ 's in between will correspond to first-quadrant points on the unit circle. But how close together are they? We find this by taking the derivative of the equation for  $\theta$  with respect to  $v$ . You have to use the chain rule and the quotient rule. We treat  $u$  as a constant. Recall that  $\frac{d}{dx} \arctan(x) = \frac{1}{1+x^2}$ . So

$$\frac{d\theta}{dv} = \frac{1}{1 + \frac{4u^2v^2}{(u^2-v^2)^2}} \frac{(u^2 - v^2)(2u) - (-2v)(2uv)}{(u^2 - v^2)^2}$$

You get some glorious simplifications of this nasty thing. In the right-hand factor's numerator,  $(u^2 - v^2)(2u) - (-2v)(2uv)$ , do the following:

1. Factor out the common  $2u$ ;
2. Observe that  $-v^2 - (-2v)(v) = v^2$ ;
3. That entire numerator becomes  $(2u)(u^2 + v^2)$ .

Now multiply the right-hand factor's denominator by the left-hand factor's denominator. You get  $(u^2 - v^2)^2 + 4u^2v^2$  as the product. Now square out the  $(u^2 - v^2)^2$  and add the  $4u^2v^2$  to the result. What you end up with is a perfect square, and is, in fact,  $(u^2 + v^2)^2$ . So far we have simplified this to

$$\frac{d\theta}{dv} = \frac{(2u)(u^2 + v^2)}{(u^2 + v^2)^2} = \frac{2u}{u^2 + v^2}$$

The right-hand expression is a measure of how close the points are on the unit circle if you choose an arbitrary value of  $u$  and allow  $v$  to count from zero to  $u$ . Observe that this expression is largest when  $v = 0$ . At that point, the spacing reduces to  $\frac{2}{u}$ . Since you can choose  $u$  as large as you like, you can make  $\frac{2}{u}$ , and hence the largest spacing between rational points, as small as you like. And that completes the proof, because if you can choose rational points as close together as you like anywhere on the unit circle, then every interval, no matter how small, must contain one. Simply choose  $u$  to make  $\frac{2}{u}$  smaller than the length of the  $\theta$ -interval in question.

Here's another way to prove the same thing. If you have a point on the unit circle whose angle is  $\theta$ , then let  $r$  be  $\tan \theta$ . If you had to choose a  $u$  and  $v$  (not necessarily integers) to use in the recipe, then

$$r = \frac{2uv}{u^2 - v^2}$$

Now choose  $u$  arbitrarily and solve for  $v$

$$\begin{aligned} ru^2 - rv^2 &= 2uv \\ 0 &= rv^2 + 2uv + ru^2 \end{aligned}$$

which is a quadratic in  $v$ , so we apply the quadratic formula:

$$v = \frac{-2u \pm \sqrt{4u^2 + 4r^2u^2}}{2r} = u \frac{-1 \pm \sqrt{1+r^2}}{r}$$

Since we want  $v$  to be positive, we choose the “plus” from the  $\pm$ . So

$$\frac{u}{v} = \frac{\sqrt{1+r^2} - 1}{r}$$

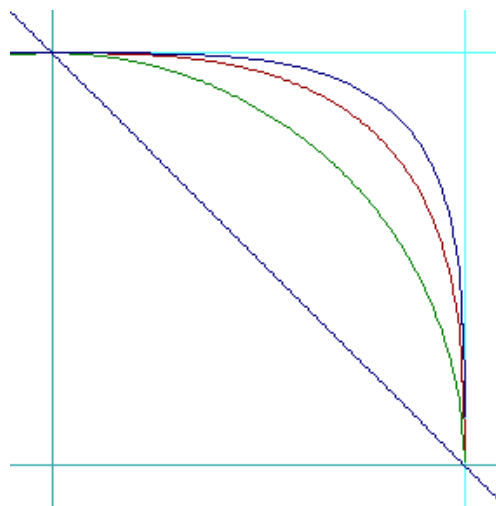
This last equation tells the whole tale. No matter what positive value  $r$  is, you can always find positive integers,  $u$  and  $v$ , so that  $\frac{v}{u}$  comes as close as you like to  $\frac{\sqrt{1+r^2}-1}{r}$ . So for example, if I want to choose  $u$  and  $v$  where  $\frac{v}{u}$  comes within 0.001 of  $\sqrt{2} - 1$  (to approximate the case where  $\theta = \frac{\pi}{4}$  and  $\tan(\theta) = r = 1$ ), I could choose  $u = 70$  and  $v = 29$ . When you use the recipe to form the Pythagorean triple from these you get  $a = 4060$ ,  $b = 4059$ , and  $c = 5741$  (if you want to see how I came up with the smallest  $u$  and  $v$  whose ratio approximates  $\sqrt{2} - 1$  to within 0.001, search the web for continued fractions). See for yourself how close to  $\frac{\sqrt{2}}{2}$  both  $\frac{a}{c}$  and  $\frac{b}{c}$  are. And while you have the calculator out, you can confirm for yourself that this  $(a, b, c)$  is indeed a Pythagorean triple.

In 1995, Andrew Wiles proved Fermat’s Last Theorem, which asserts that the equation,

$$a^n + b^n = c^n$$

has integer solutions for  $a$ ,  $b$ , and  $c$  only for  $n = 1$  and  $n = 2$ . For all higher values of  $n$ , no integer solutions to this equation can possibly exist. The world had waited over 300 years for such a proof. Each positive integer,  $n$ , defines a “Fermat function,” as shown in the figure to the right. We define the Fermat function of degree  $n$  to be

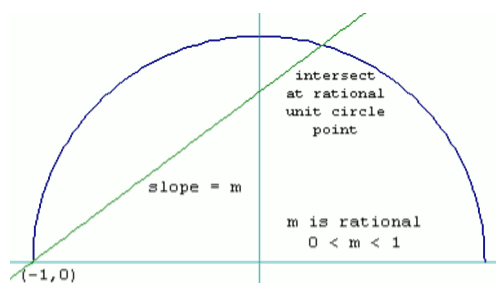
$$y = (1 - x^n)^{\frac{1}{n}}$$



**Plots of Fermat functions for  $n = 1$ ,  $n = 2$ ,  $n = 3$ , and  $n = 4$ .**

For  $n = 1$  and  $n = 2$ , the curves pass through rational points in every interval. But for the curves where  $n = 3$  and  $n = 4$ , as well as all higher values of  $n$ , a most amazing thing happens. All of these higher-degree Fermat curves snake their way through the plane, which is densely packed with an infinitude of rational points, but besides  $(1, 0)$  and  $(0, 1)$ , these functions avoid absolutely all of them. See if you can understand why Fermat's Last Theorem implies this.

**Exercise:** See if you can prove the following: If a line passes through the point  $(-1, 0)$  and has a slope that is both rational and between 0 and 1, then that line intersects the unit circle in the first quadrant at a rational point. Start out with the equation of the line,



$$y = m(x + 1)$$

Since  $m$  is rational, you can assume that there are two positive integers,  $u$  and  $v$ , where  $m = \frac{v}{u}$ . Since  $m < 1$ , you can assume that  $v < u$ . Recall that the equation for the unit circle is

$$x^2 + y^2 = 1$$

or equivalently

$$y^2 = 1 - x^2$$

Now square both sides of the equation for the line, then subtract the resulting equation from the equation for a circle. That will eliminate  $y$ , and you will be able to solve for  $x$  using the quadratic formula. You will get two solutions, but one of them will be  $x = -1$ , and you already knew that the circle and the line intersected at that  $x$ . So the interesting solution is the other one. Back-substitute that solution to find  $y$ . You should be able to see how both  $x$  and  $y$  turn out to be rational numbers whenever  $m$  is rational. Try it. And then try substituting  $\frac{v}{u}$  for  $m$  in the solution to see how this solution relates back to the original recipe we derived for finding Pythagorean triples.