Pythagorean triples

A **Pythagorean triple** is a set of three integers a, b, c which are pairwise relatively prime such that

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

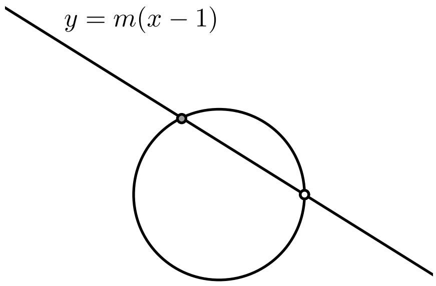
Bot the Babylonian and Greek mathematicians knew how to find them. I'll explain here what I think is the simplest modern way to do this. There are two stages to this.

Stage 1.

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

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

so that $(a/c, b/c)$ lies on the circle $x^2 + y^2 = 1$.



It also works the other way. If (x, y) is a point on the unit circle with rational coordinates, then it turns out that we can write $x = a/c$, $y = b/c$ in reduced form. The point is that they have the same denominator in reduced form.

Exercise. *Prove that if $x = a/c$ is in reduced form and $y = b/c$ with $x^2 + y^2 = 1$, tehn b/c is also in reduced form.*

Stage 2.

Suppose x and y are fractions with $x^2+y^2 = 1$. Because the coordinates of $x, y)$ are rational, we can connect it by a straight line with rational slope m to the point $(1, 0)$. Explicitly, he slope is $m = y/(x - 1)$.

The equation of this line is $y = m(x - 1)$. Conversely, any line $y = m(x - 1)$ intersects the circle in two points, and since on of them, namely $(1, 0)$, has rational coordinates so has the other. We can solve explicitly for x and y given m.

$$\begin{aligned} x^2 + y^2 &= 1 \\ &= x^2 + m^2(x - 1)^2 \\ &= x^2(1 + m^2) - 2m^2x + m^2 \\ x^2 - 2\frac{m^2}{m^2+1}x + \frac{m^2-1}{m^2+1} &= 0 \\ (x - 1)\left(x - \frac{m^2-1}{m^2+1}\right) &= 0 \end{aligned}$$

so that

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

As m varies from $-\infty$ to ∞ the point (x, y) traverses the whole circle except the point $(1, 0)$. Thsi is the point of stage 2: the Pythagoraen triples correspond to slopes m in the range $m < -1$. We haven't seen the exact path backwards yet, though.

We want to use this construction to generate Pythagorean triples. First of all, we want x and y positive, which means $m < -1$. We want m rational, so set

$$m = \frac{-p}{q}$$

with $p > q$, and p and q relatively prime. Then

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

This suggests that, to get Pythagorean triples, set

$$a = p^2 - q^2, \quad b = 2pq, \quad c = p^2 - q^2 .$$

Here's a few examples:

p	q	$p^2 - q^2$	$2pq$	$p^2 + q^2$
2	1	3	4	5
3	1	8	6	10
3	2	5	12	13

We see that the case $(3, 1)$ doesn't work, and if you think about it you realize two odd numbers can't ever work, because $p^2 - q^2$ and $p^2 + q^2$ will both be even. So we can restrict ourselves to the case where one is even, one odd.

Exercise 1. *Make up a table of all triples with $8 \geq p > q > 0$, one odd and one even.*

Exercise 2. *Prove that if $p > q$ are relatively prime with one odd and one even, then $a = 2pq$, $b = p^2 - q^2$, and $c = p^2 + q^2$ are a Pythagorean triple.*

Exercise 3. *If p and q are both odd, you can get a good triple by dividing $p^2 - q^2$, $p^2 + q^2$, and $2pq$ all by 2. Prove that. Calculate all of these with $5 \geq p$. You don't really get anything new. Why is that?*

Exercise 4. *Swapping a and b doesn't really give you a new triple. What does this swap mean in terms of m?*