Pythagorean Triples

If x and y are the legs of a right triangle and z is the hypotenuse, then Pythagoras' theorem says $x^2 + y^2 = z^2$. A triple of integers $\{x, y, z\}$ is a **Pythagorean triple** if it satisfies $x^2 + y^2 = z^2$. (In what follows, I'll assume that x, y, and z are *positive* integers.)

For example $\{3, 4, 5\}$ is a Pythagorean triple, since $3^2 + 4^2 = 5^2$. $\{6, 8, 10\}$ is also a Pythagorean triple, but there is a sense in which it's "redundant": $2 \cdot \{3, 4, 5\} = \{6, 8, 10\}$. If a Pythagorean triple is not a proper multiple of of another triple, it is said to be **primitive**. Thus, $\{x, y, z\}$ is a primitive Pythagorean triple if $(x, y, z) = 1$.

The result I'll prove will show how you can generate all primitive Pythagorean triples.

Theorem.

(a) Suppose a and b are positive numbers, one is even and the other is odd, $a > b$, and $(a, b) = 1$. Then

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2$$

is a primitive Pythagorean triple.

(b) Suppose $\{x, y, z\}$ is a primitive Pythagorean triple. Then one of x, y is even and the other is odd. If x is even, then there are positive numbers a and b, such that one is even and the other is odd, $a > b$, $(a, b) = 1$, and

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

Proof. (a)

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2.$$

Therefore, $\{x, y, z\}$ is a Pythagorean triple. I have to show it's primitive.

Suppose on the contrary that $p \mid x, y, z$, where p is prime. One of a, b, is even and the other is odd, so y and z must be odd. On the other hand, x is even. Therefore, $p \neq 2$.

Now $p \mid y$ and $p \mid z$ implies $p \mid y + z = 2a^2$. Since $p \neq 2$, $p \mid a^2$. Since p is prime, $p \mid a$.

Likewise, $p \mid y$ and $p \mid z$ implies $p \mid z - y = 2b^2$. Since $p \neq 2$, $p \mid b^2$. Since p is prime, $p \mid b$.

This is a contradiction, because $(a, b) = 1$.

Therefore, $(x, y, z) = 1$, and $\{x, y, z\}$ is a primitive Pythagorean triple.

(b) Suppose $\{x, y, z\}$ is a primitive Pythagorean triple, so $x^2 + y^2 = z^2$ and $(x, y, z) = 1$. First, I'll show that one of x, y must be even and the other odd.

If both x and y are even, then $x^2 + y^2 = z^2$ is even, so z is even. This contradicts $(x, y, z) = 1$.

Suppose both x and y are odd. Note that the square of an odd number is congruent to 1 mod 4:

$$(2m + 1)^2 = 4m^2 + 4m + 1 = 1 \pmod 4.$$

So $z^2 = x^2 + y^2 = 1 + 1 = 2 \pmod 4$. This is impossible, because only 0, 1, and 4 are squares mod 4.

Therefore, one of x, y must be even and the other odd. Suppose x is even and y is odd. Note that $z^2 = x^2 + y^2$ must be odd, so z must be odd. This means that $z - y$ and $z + y$ are even. Then

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

and $\dfrac{x}{2}$, $\dfrac{z - y}{2}$, and $\dfrac{z + y}{2}$ are all *integers*.

Next, I'll show that $\left(\dfrac{z - y}{2}, \dfrac{z + y}{2}\right) = 1$. Suppose p is a prime and $p \mid \dfrac{z - y}{2}, \dfrac{z + y}{2}$. Then

$$p \mid \frac{z - y}{2} + \frac{z + y}{2} = z$$

$$p \mid \frac{z+y}{2} - \frac{z-y}{2} = y$$

$$p \mid \left(\frac{x}{2}\right)^2 \quad \text{so} \quad p \mid \frac{x}{2} \mid x$$

This contradicts $(x, y, z) = 1$. Thus, $\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$.

Now $\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ expresses a product of two relatively prime integers as a perfect square. By the Fundamental Theorem of Arithmetic, each of the numbers on the right must be a perfect square:

$$\frac{z-y}{2} = a^2, \quad \frac{z+y}{2} = b^2.$$

Note that $(a, b) = 1$, for if p is prime and $p \mid a, b$, then $p \mid \frac{z-y}{2}, \frac{z+y}{2}$.

If a and b are both odd or both even, then $z = a^2 + b^2$ and $y = b^2 - a^2$ are both even, contrary to assumption. Hence, one of a, b, is odd and the other is even.

Finally,

$$\left(\frac{x}{2}\right)^2 = a^2 b^2, \quad x^2 = 4a^2 b^2, \quad x = 2ab. \quad \square$$

Example. You can use the theorem to generate all primitive Pythagorean triples. To do this, fix the bigger number a and consider b's less than a. b must be of different parity than a, and relatively prime to a, so many cases are eliminated. The formulas in the theorem give x, y, and z.

a	b	$x = 2ab$	$y = a^2 - b^2$	$z = a^2 + b^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61

For example, consider $a = 6$. b must be less than 6, relatively prime to 6, and odd. Thus, the only possibilities are $b = 1$ and $b = 5$, and these give the last two cases above. $\square$

Example. Let $\{x, y, z\}$ be a Pythagorean triple. Show that one of x, y, z is divisible by 5.

Mod 5 the only squares are 0, 1, and 4.

x	$x^2 \pmod 5$
0	0
1	1
2	4
3	4
4	1

Suppose neither x nor y is divisible by 5. Then x^2 and y^2 can be either 1 or 4 mod 5. Consider the possibilities for $z^2 = x^2 + y^2 \pmod 5$:

$$z^2 = 1 + 1 = 2 \quad \text{is not a square} \pmod 5$$

$$z^2 = 1 + 4 = 0 \quad \text{implies } 5 \mid z$$

$$z^2 = 4 + 1 = 0 \quad \text{implies } 5 \mid z$$

$$z^2 = 4 + 4 = 3 \quad \text{is not a square} \pmod 5$$

In the only cases which are possible, z is divisible by 5.
Thus, one of x, y, z must be divisible by 5. □

The Fermat-Pell Equation

Consider a Diophantine equation of the form

$$x^2 - dy^2 = n.$$

If d is a perfect square, you can solve the equation directly.

Example. $x^2 - 9y^2 = 13$

I can write the equation as

$$(x - 3y)(x + 3y) = 13.$$

This is an equation in integers, and represents a factorization of 13. There are only two ways to factor 13 in positive integers: $1 \cdot 13$ and $13 \cdot 1$. (You can check that the negative factorizations give the same results.)

Suppose $x - 3y = 1$ and $x + 3y = 13$. This is

$$\begin{array}{rcrcl} x & - & 3y & = & 1 \\ x & + & 3y & = & 13 \end{array} \quad \text{or} \quad \begin{bmatrix} 1 & -3 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 13 \end{bmatrix}.$$

So

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{6} \begin{bmatrix} 3 & 3 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 13 \end{bmatrix} = \begin{bmatrix} 7 \\ 2 \end{bmatrix}.$$

$(x, y) = (7, 2)$ is an *integer* solution, so it qualifies as a solution to the original equation. Since x and y appear as x^2 and y^2 in the original equation, $(-7, 2)$, $(7, -2)$, and $(-7, -2)$ also work.

Similarly, $x - 3y = 13$ and $x + 3y = 1$ give $(x, y) = (-7, 2)$ (which I already know).

So the solutions to the Diophantine equation $x^2 - 9y^2 = 13$ are $(7, 2)$, $(-7, 2)$, $(7, -2)$, and $(-7, -2)$.

Now suppose I change the problem to $x^2 - 9y^2 = 10$. Write it as

$$(x - 3y)(x + 3y) = 10.$$

The possible factorizations of 10 are $1 \cdot 10$, $10 \cdot 1$, $2 \cdot 5$, and $5 \cdot 2$.

Try $x - 3y = 1$, $x + 3y = 10$. Then

$$\begin{bmatrix} 1 & -3 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 10 \end{bmatrix}, \quad \text{so} \quad \begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{6} \begin{bmatrix} 3 & 3 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 10 \end{bmatrix} = \begin{bmatrix} 11/2 \\ 9/6 \end{bmatrix}.$$

This is not a solution in integers, so this factorization gives no integer solutions.

You can verify that the other factorizations do not give integer solutions. Hence, $x^2 - 9y^2 = 10$ has no integer solutions. □

Now consider the case where d is not a perfect square. The following fact (which I'll state without proof) relates the solutions to $x^2 - dy^2 = n$ to the continued fraction expansion of $\sqrt{d}$.

Theorem. Suppose $d > 0$, d is not a perfect square, and $|n| < \sqrt{d}$. Any positive solution of $x^2 - dy^2 = n$ with $(x, y) = 1$ satisfies $x = p_n$, $y = q_n$ for some $n > 0$, where $\dfrac{p_n}{q_n}$ is the n-th convergent of the continued fraction expansion of $\sqrt{d}$. □

The theorem doesn't say *which* convergent will give a solution. The special form $x^2 - dy^2 = \pm 1$ is called the **Fermat-Pell equation**. In this case, it's possible to say which convergent will solve the equation. I'll state the following fact without proof, and give some examples.

First, recall from the theory of periodic continued fractions that a **quadratic irrational** — in particular, a number of the form $\sqrt{d}$, where d is not a square — has a *periodic* continued fraction expansion.

Theorem. Suppose $d > 0$ and d is not a perfect square. Any positive solution of $x^2 - dy^2 = \pm 1$ with $(x, y) = 1$ satisfies $x = p_n$, $y = q_n$ for some $n > 0$, where $\dfrac{p_n}{q_n}$ is the n-th convergent of the continued fraction expansion of $\sqrt{d}$.

Let t be the period of the expansion of $\sqrt{d}$.

(a) If t is even, then $x^2 - dy^2 = -1$ has no solutions. $x^2 - dy^2 = 1$ has solutions $x = p_{nt-1}$, $y = q_{nt-1}$, for $n \geq 1$.

(b) If t is odd, then $x^2 - dy^2 = -1$ has solutions $x = p_{nt-1}$, $y = q_{nt-1}$ for $n = 1, 3, 5, \ldots$, and $x^2 - dy^2 = 1$ has solutions $x = p_{nt-1}$, $y = q_{nt-1}$ for $n = 2, 4, 6, \ldots$. □

Example. The continued fraction expansion of $\sqrt{15}$ is $[3; \overline{1, 6}]$. The period is 2, so $x^2 - 15y^2 = -1$ has no solutions.

Consider the equation $x^2 - 15y^2 = 1$.

a_k	p_k	q_k	c_k
3	3	1	3
1	4	1	4
6	27	7	$\frac{27}{7}$
1	31	8	$\frac{31}{8}$
6	213	55	$\frac{213}{55}$

The solutions are $(p_1, q_1) = (4, 1)$, $(p_3, q_3) = (31, 8)$, and so on. You can check by direct computation that $31^2 - 15 \cdot 8^2 = 1$. □

Example. The continued fraction expansion of $\sqrt{1141}$ is

$$[33, 1, 3, 1, 1, 12, 1, 21, 1, 1, 2, 5, 4, 3, 7, 5, 16, 1, 2, 3, 1, 1, 1, 2, 1, 2, 1, 4, 1, 8, 1, 4, 1,$$

$$2, 1, 2, 1, 1, 1, 3, 2, 1, 16, 5, 7, 3, 4, 5, 2, 1, 1, 21, 1, 12, 1, 1, 3, 1, 66];$$

it repeats after that. (*Of course* I figured that out by hand; why do you ask?)

The period is $t = 58$, so $x^2 - 1141y^2 = 1$ has solutions of the form p_{58n-1}, q_{58n-1}. The first is

$$x = 1159808344742542473152089 75, \quad y = 30693385322765657197397208. \text{ □}$$
