Pythagorean Triples

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Today we will consider the diophantine equation $x^2 + y^2 = z^2$.

This is trivial to solve in $\mathbb{Z}$ if any of x, y or z is zero, and we may clearly change the signs of x, y and z at will.

So we may as well assume $x, y, z \in \mathbb{N}$.

In this context we will provide a complete solution to $x^2 + y^2 = z^2$.

Pythagorean Triples

Definition

A *pythagorean triple* is a tuple $(x, y, z) \in \mathbb{N}^3$ satisfying $x^2 + y^2 = z^2$. We say that (x, y, z) is *primitive* if it also satisfies $\gcd(x, y, z) = 1$.

Goal. Describe all pythagorean triples.

Notice that if (x, y, z) is a pythagorean triple and $d = \gcd(x, y, z)$, then

$$x^2+y^2 = d^2\left(\frac{x}{d}\right)^2+d^2\left(\frac{y}{d}\right)^2 = d^2\left(\left(\frac{x}{d}\right)^2+\left(\frac{y}{d}\right)^2\right) = d^2\left(\frac{z}{d}\right)^2.$$

Cancelling d^2 we find that $(x/d, y/d, z/d)$ is also a pythagorean triple, now primitive since $\gcd(x/d, y/d, z/d) = 1$.

Moral. It suffices to describe all primitive pythagorean triples (the rest can be obtained by scaling).

We need a few preparatory lemmas.

Lemma 1

Let (x, y, z) *be a primitive pythagorean triple. Then* $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Proof. Suppose $\gcd(x, y) \neq 1$. Then there is a prime p so that $p \mid \gcd(x, y)$.

Then $p | x^2 + y^2 = z^2$, so that $p | z$ (since p is prime).

But then p is a common divisor of x, y and z, so that $p \mid \gcd(x, y, z)$, contradicting primitivity.

The other two cases are entirely similar. □

Lemma 2

Let (x, y, z) be a primitive pythagorean triple. Then exactly one of x and y is even, and z is odd.

Proof. By Lemma 1, x and y cannot both be even. We need to show that they cannot both be odd either.

Suppose otherwise. Then $x^2 \equiv y^2 \equiv 1 \pmod 4$.

Therefore $z^2 = x^2 + y^2 \equiv 2 \pmod 4$.

But every square is congruent to either 0 or 1 modulo 4, so this is a contradiction.

This establishes that x and y have opposite parity. Therefore their squares do, too.

It follows that $z^2 = x^2 + y^2$ is odd, and hence z is odd as well. $\square$

As a consequence of Lemma 2, we may assume WLOG that if (x, y, z) is a primitive pythagorean triple, then x is even while y and z are odd.

Then $x^2 = z^2 - y^2 = (z - y)(z + y)$, and all three of x, $z - y$ and $z + y$ are even.

Dividing by 4 this becomes

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

Notice that

$$\frac{z-y}{2} + \frac{z+y}{2} = z \quad \text{and} \quad \frac{z+y}{2} - \frac{z-y}{2} = y.$$

Therefore any common divisor $\frac{z-y}{2}$ and $\frac{z+y}{2}$ is a common divisor of y and z.

But $\gcd(y,z) = 1$, so that we must have $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = 1$.

We now need one more lemma.

Lemma 3

Let $a, b, c, n \in \mathbb{N}$. If $\gcd(a,b) = 1$ and $ab = c^n$, then there exist $r, s \in \mathbb{N}$ so that $a = r^n$ and $b = s^n$.

Proof. Because $\gcd(a, b) = 1$, we can appeal to the Fundamental Theorem of Arithmetic to write

$$a = p_1^{e_1} \cdots p_\ell^{e_\ell} \quad \text{and} \quad b = q_1^{f_1} \cdots q_m^{f_m},$$

where $p_1, \ldots, p_\ell, q_1, \ldots, q_m$ are distinct primes.

The Fundamental Theorem then implies that

$$c^n = ab = p_1^{e_1} \cdots p_\ell^{e_\ell} q_1^{f_1} \cdots q_m^{f_m}$$

must be the canonical factorization of c^n.

But if $c = \pi_1^{g_1} \cdots \pi_k^{g_k}$ is the canonical factorization of c, then

$$c^n = \pi_1^{ng_1} \cdots \pi_k^{ng_k}$$

is also the canonical factorization of c^n.

Because canonical forms are unique, it follows that $n|e_i$ and $n|f_j$ for all i, j.
Then $a = r^n$ and $b = s^n$ where

$$r = p_1^{e_1/n} \cdots p_\ell^{e_\ell/n} \quad \text{and} \quad s = q_1^{f_1/n} \cdots q_m^{f_m/n}$$

are both integers. $\square$

Returning to our primitive pythagorean triple, we had

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

with $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = 1$.
By Lemma 3, we conclude that

$$\frac{z-y}{2} = r^2 \quad \text{and} \quad \frac{z+y}{2} = s^2,$$

for some $r, s \in \mathbb{N}$.

Thus

$$z = \frac{z-y}{2} + \frac{z+y}{2} = r^2 + s^2$$

and

$$y = \frac{z+y}{2} - \frac{z-y}{2} = s^2 - r^2.$$

Note that we must have $s > r$ since $y \in \mathbb{N}$.

Moreover

$$\begin{aligned} x^2 = z^2 - y^2 &= (r^2+s^2)^2 - (s^2-r^2)^2 \\ &= (r^4 + 2r^2s^2 + s^4) - (s^4 - 2r^2s^2 + r^4) \\ &= 4r^2s^2, \end{aligned}$$

which implies that $x = 2rs$ (exercise).

Finally, suppose that p is a prime dividing r and s.

Then

$$p | s^2 - r^2 = y \quad \text{and} \quad p | r^2 + s^2 = z,$$

so that $p | \gcd(y, z) = 1$, a contradiction. We conclude that $\gcd(r, s) = 1$.

Moreover, we must have $s \not\equiv r \pmod 2$, otherwise $y \equiv 0 \pmod 2$.

This proves half of our main result.

Theorem 1

The tuple $(x, y, z) \in \mathbb{N}^3$ is a primitive pythagorean triple (with x even) if and only if there exist natural numbers $s > r$ of opposite parity with $\gcd(r, s) = 1$ so that

$$x = 2rs, \;\; y = s^2 - r^2, \;\; z = s^2 + r^2.$$

The Converse

To complete the proof of Theorem 1, suppose that we are given $s > r \geq 1$ of opposite parity with $\gcd(r, s) = 1$, and let

$$x = 2rs, \;\; y = s^2 - r^2, \;\; z = s^2 + r^2.$$

That $x^2 + y^2 = z^2$ is a straightforward algebraic identity.

We only need to show $\gcd(x, y, z) = 1$. Suppose this is not the case. Then there is a prime p so that $p|x$, $p|y$ and $p|z$.

It follows that

$$p|y + z = 2s^2 \quad \text{and} \quad p|z - y = 2r^2.$$

If $p \neq 2$, then $p|s^2$ and $p|r^2$, which implies $p|s$ and $p|r$, which contradicts $\gcd(r, s) = 1$.

So we must have $p = 2$. But then $p|y$ implies

$$s \equiv s^2 \equiv r^2 \equiv r \pmod 2,$$

another contradiction.

This proves the reverse implication of Theorem 1, and therefore completes the proof.

Examples

Here are the first few primitive pythagorean triples.

r	s	x	y	z
1	2	4	3	5
1	4	8	15	17
1	6	12	35	37
2	3	12	5	13
2	7	28	45	53
2	5	20	21	29
3	4	24	7	25
3	8	48	55	73
3	10	60	91	109
4	5	40	9	41
4	7	56	33	65
4	9	72	65	97

A Geometric Approach

There's a variant of the proof of Theorem 1 that is worth mentioning, as it generalizes to arbitrary conic sections.

For now we drop the requirement that $x, y, z \in \mathbb{N}$ and instead allow $x, y, z \in \mathbb{Z}$ with $z \neq 0$.

If (x, y, z) is a pythagorean triple, then $X = \frac{x}{z}$ and $Y = \frac{y}{z}$ are rational numbers satisfying

$$X^2 + Y^2 = 1, \tag{1}$$

i.e. (X, Y) is a rational point on the unit circle.

Conversely, if $X = x/z$ and $Y = y/z$ satisfy (1), then (x, y, z) is a pythagorean triple.

So to determine all of the pythagorean triples it suffices to parametrize the rational points on the unit circle.

We use stereographic projection through the "north pole" $(0,1)$. That is, we consider the line $Y = mX + 1$ of slope m passing through $(0,1)$.

This intersects the unit circle where

$$\begin{aligned} X^2 + (mX+1)^2 = 1 &\Leftrightarrow (m^2+1)X^2 + 2mX = 0 \\ &\Leftrightarrow X((m^2+1)X + 2m) = 0 \\ &\Leftrightarrow X = 0, \frac{-2m}{m^2+1} \Leftrightarrow Y = 1, \frac{1-m^2}{m^2+1}. \end{aligned}$$

The second point

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

is rational if and only if $m \in \mathbb{Q}$ (exercise).

Conversely, if (X_0, Y_0) is a rational point on the unit circle, then the line

$$Y = Y_0 + \frac{Y_0 - 1}{X_0}(X - X_0)$$

has rational slope and passes through $(0, 1)$ and (X_0, Y_0)

Let

$$C(\mathbb{Q}) = \{(X, Y) \,|\, X, Y \in \mathbb{Q}, X^2 + Y^2 = 1\}$$

denote the set of rational points on the unit circle.

The upshot of our reasoning above is that there is a bijection

$$\begin{aligned} \pi : \mathbb{Q} &\to C(\mathbb{Q}), \\ m &\mapsto \left(\frac{-2m}{m^2+1}, \frac{1-m^2}{m^2+1} \right). \end{aligned}$$

Write $m = r/s$. Then we have

$$\pi(r/s) = \left(\frac{-2rs}{r^2+s^2}, \frac{s^2-r^2}{r^2+s^2} \right).$$

With a little more work one can show that if $\gcd(r, s) = 1$, then:

- The coordinates of $\pi(r/s)$ are reduced if $r \not\equiv s \pmod 2$.
- When $r \equiv s \equiv 1 \pmod 2$, then $\pi(r/s) = \left(\frac{v^2-u^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right)$ is in reduced form, with $\gcd(u, v) = 1$ and $u \not\equiv v \pmod 2$.

So, up to interchanging X and Y (and maybe changing a sign), in reduced form we have

$$X = \frac{-2rs}{r^2+s^2} \quad \text{and} \quad Y = \frac{s^2-r^2}{r^2+s^2}$$

for rational points on the unit circle, with $\gcd(r, s) = 1$ and $r \not\equiv s \pmod 2$.

This provides the classification of Theorem 1.

Example

Let's illustrate the case in which $r \equiv s \equiv 1 \pmod 2$.

Take $r = 1$ and $s = 3$. Then

$$\begin{aligned}\pi(1/3) &= \left(\frac{-2\cdot 1\cdot 3}{1^2+3^2}, \frac{3^2-1^2}{1^2+3^2}\right) = \left(\frac{-6}{10}, \frac{8}{10}\right)\\ &= \left(\frac{-3}{5}, \frac{4}{5}\right) = \left(\frac{1^2-2^2}{1^2+2^2}, \frac{2\cdot 1\cdot 2}{2^2+1^2}\right),\end{aligned}$$

which yields the primitive pythagorean triple $(3, 4, 5)$.

The moral is that the function π captures *all* primitive pythagorean triples, without the need to assume x is even.