PYTHAGOREAN TRIPLES

ALEX ROSS

Definition. If x, y, and z are positive integers such that $x^2 + y^2 = z^2$, then $((x, y, z)$ is called a PYTHAGOREAN TRIPLE. Further, if $\gcd(x, y, z) = 1$, then (x, y, z) is called a PRIMITIVE PYTHAGOREAN TRIPLE.

Theorem 1. *If (x, y, z) is a Pythagorean triple, then at least one of x, y, z is even and the other two are either both even or both odd.*

Lemma 1. *If (x, y, z) is a primitive Pythagorean triple, then either x or y is even (inclusive or).*

Proof. Suppose (x, y, z) is a primitive Pythagorean triple with x and y not even (for the sake of contradiction). Then, $x \equiv y \equiv 1 \pmod 2$. Also, $x^2 \equiv y^2 \equiv 1 \pmod 4$. Then, $x^2 + y^2 \equiv z^2 \equiv 2 \pmod 4$. But 2 is *not* a quadratic residue modulo 4. Thus, x and y cannot both be odd. □

Theorem 2. *If (x, y, z) is a Pythagorean triple, one of x, y, z is divisible by 3, one is divisible by 4, and one is divisible by 5.*

Note. This is easy to see for 3, and 5 by contructing the table of sums of squares modulo 3 and 5. It is not so simple for 4. To that end, we need a proof.

Proof. Suppose x, y, z are all even, such that $y \equiv z \equiv 2 \pmod 4$. So, y and z are both equivalent to either 2 or 6 modulo 8. Then $y^2 \equiv z^2 \equiv 4 \pmod 8$. Then, $x^2 + y^2 \equiv z^2 \pmod 8$. So, $x^2 \equiv 0 \pmod 8$. Lo and behold, $x \equiv 0 \pmod 4$. (This is because whatever factors x^2 has, it must have them in pairs. Then, because $2^3 \mid x^2$, certainly $2^4 \mid x^2$, so $2^2 \mid x$.)

Suppose x is even, but y, z are odd. So $x^2 \equiv z^2 - y^2 \equiv 0 \pmod 4$ because $x^2 \equiv 0 \pmod 4$. Now, $y^2 \equiv z^2 \equiv 1 \pmod 4$. Notice also that $y^2 \equiv z^2 \equiv 1 \pmod 8$. So, $x^2 \equiv 0 \pmod 8$, thus $x \equiv 0 \pmod 4$. □

Theorem 3. *If $p, q \in \mathbb{N}$ with $p > q$, then $(2pq, p^2 - q^2, p^2 + q^2)$ is a Pythagorean triple.*

Proof. Let $p, q \in \mathbb{N}$ with $p > q$. Then, $(2pq)^2 + (p^2 - q^2)^2 = 4p^2q^2 + p^4 - 2p^2q^2 + q^4$, and we see that $p^4 + 2p^2q^2 + q^4 = (p^2 + q^2)^2$. Thus,

$$(2pq)^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2.$$

Thus, $(2pq, p^2 - q^2, p^2 + q^2)$ is a Pythagorean triple. □

Note. If p, q are coprime, is $(2pq, p^2 - q^2, p^2 + q^2)$ always primitive? No! Consider $p, q = 5, 3$. Then

$$(2 \cdot 5 \cdot 3, 5^2 - 3^2, 5^2 + 3^2) = (30, 16, 34).$$

Theorem 4. *If (x, y, z) is a primitive Pythagorean triple, then either x or y is even, and if x is even, then $x = 2pq$, $y = p^2 - q^2$, $z = p^2 + q^2$, for some coprime integers p and q.*

Proof. Suppose (x, y, z) is a primitive Pythagorean triple, such that $x \equiv 0 \pmod 2$. Then, $x^2 \equiv 0 \pmod 4$. So $y^2 \equiv z^2 \pmod 4$ so $y \equiv z \pmod 2$. Thus, $y + z \equiv 0 \pmod 2$ and $z - y \equiv 0 \pmod 2$. Then, $\gcd(y + z, z - y) = 2d$. So, $2d \mid (z + y) + (z - y)$, thus $2d \mid 2z$. Thus, $d \mid z$. Similarly, $d \mid y$. But $\gcd(x, y, z)) = 1$, so $d = 1$.

Now, $\gcd(\frac{1}{2}(z + y)), \frac{1}{2}(z - y)) = 1$ and we see that

$$\left[\frac{1}{2}(z + y)\right]\left[\frac{1}{2}(z - y)\right] = \frac{1}{4}(z^2 + y^2) = \left(\frac{1}{2}x\right)^2.$$

Then, both $\frac{1}{2}(z + y)$ and $\frac{1}{2}(z - y)$ must be squares, because

$$\sqrt{\left[\frac{1}{2}(z + y)\right]\left[\frac{1}{2}(z - y)\right]} = \frac{1}{2}x \qquad \text{(Recall, } 2 \mid x.\text{)}$$

Let $p^2 = \frac{1}{2}(z + y)$ and let $q^2 = \frac{1}{2}(z - y)$. Then,

$$x = 2 \cdot \sqrt{\left[\frac{1}{2}(z + y)\right]\left[\frac{1}{2}(z - y)\right]} = 2\sqrt{p^2q^2} = 2pq,$$

and

$$y = \frac{1}{2}(z + y) - \frac{1}{2}(z - y) = p^2 - q^2,$$

and

$$z = \frac{1}{2}(z + y) + \frac{1}{2}(z - y) = p^2 + q^2.$$

To see that p, q are coprime, suppose $d \mid p$ and $d \mid q$. Then, $d^2 \mid 2pq$, so $d \mid x$. Also, $d^2 \mid (p^2 - q^2)$, so $d \mid y$. Also, $d^2 \mid z$. But $\gcd(x, y, z) = 1$, so $d = 1$. Thus, p, q are coprime. □

Note. Just because (x, y, z) is a Pythagorean triple with x even, does not mean there is $p, q \in \mathbb{N}$ such that $(x, y, z) = (2pq, p^2 - q^2, p^2 + q^2)$. Consider:

$$(16, 12, 20) = (2pq, p^2 - q^2, p^2 + q^2).$$

Solving this will result in complex roots!