8-13-2006

Pythagorean Triples

- A triple of integers $\{x, y, z\}$ is a **Pythagorean triple** if $x^2 + y^2 = z^2$.
- A Pythagorean triple $\{x, y, z\}$ is **primitive** if $(x, y, z) = 1$.
- There is an algorithm for generating all primitive 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

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

A similar statement holds if y is even.

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

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

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, $\left(\dfrac{z-y}{2}, \dfrac{z+y}{2}\right) = 1$.

Now $\left(\dfrac{x}{2}\right)^2 = \left(\dfrac{z-y}{2}\right)\left(\dfrac{z+y}{2}\right)$ 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 $p \mid \dfrac{z-y}{2}, \dfrac{z+y}{2}$.

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,

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

Example. Take $a = 21$. Choose a number b that is less than 21, such that b has different parity than 21 (so b is even), and such that $(a, b) = 1$. For example, let $b = 16$. Then

$$a^2 - b^2 = 185, \quad 2ab = 672, \quad a^2 + b^2 = 697.$$

Since

$$185^2 + 672^2 = 485809 = 697^2,$$

$\{185, 672, 697\}$ is a primitive Pythagorean triple. $\square$

Example. You can use the theorem to generate all primitive Pythagorean triples. To do this, fix the bigger number a. Then consider b's less than a such that b is of different parity than a and such that $(a, b) = 1$. These requirements on b eliminate many possibilities. For each pair of numbers a and b, the formulas in the

theorem give the elements x, y, and z of the triple.

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 $a = 6$. Then 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. □

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. □

Primitive Pythagorean Triples

a	b	$a^2 - b^2$	$2ab$	$a^2 + b^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65
7	6	13	84	85
8	1	63	16	65
8	3	55	48	73
8	5	39	80	89
8	7	15	112	113
9	2	77	36	85
9	4	65	72	97
9	8	17	144	145
10	1	99	20	101
10	3	91	60	109
10	7	51	140	149
10	9	19	180	181