Pythagorean triple

Created by Mr. Francis Hung Last updated: 22 April 2011

Solve $x^2 + y^2 = z^2$ for integral solution.

The triple (x, y, z) is called Pythagorean's Triple.

Clearly (0,0,0) is a trivial solution.

If (x, y, z) is a solution, then (kx, ky, kz) are solution for any integer k.

If (x, y, z) is a solution, then $(-x, -y, -z)$ is also a solution.

If (x, y, z) is a solution and (x, y, z) are relatively prime, then the solution is called primitive root.

Let (x, y, z) be a positive primitive root.

Theorem 1 At least one of x, y is even.

Proof: If both x and y are odd, let $x = 2m + 1$, $y = 2n + 1$; where n, m are integers.

then $z^2 = x^2 + y^2$

$= 4(m^2 + m + n^2 + n) + 2$

RHS is even $\Rightarrow z^2$ is even

$\Rightarrow z$ is even

Let $z = 2k$; where k is an integer.

$4k^2 = 4(m^2 + m + n^2 + n) + 2$

LHS is divisible by 4 but RHS is not !!! (which is a contradiction)

$\therefore$ At least one of x and y is even.

WLOG let $y = 2a$

Theorem 2 If $(x, y) = c > 1$, then c divides z.

Proof: Let $x = cx_1$, $y = cy_1$

$x^2 + y^2 = z^2 \Rightarrow c^2(x_1^2 + y_1^2) = z^2$

c^2 divides z^2

c divides z ($\because c > 0$)

Since (x, y, z) is a prime solution, therefore x and y are relatively prime. Let y be even.

Theorem 3 x and z are both odd and x and z are relatively prime.

Proof: $\because$ x and y are relatively prime and y is even.

x must be odd (otherwise 2 is a common factor)

x^2 is odd and y^2 is even.

$x^2 + y^2$ is odd

$\therefore$ z is odd

$\therefore$ z is odd

Suppose $(x, z) = c > 1$

Let $x = cx_1$, $z = cz_1$

Then $y^2 = z^2 - x^2$

$= (cz_1)^2 - (cx_1)^2$

$= c^2(z_1^2 - x_1^2)$

$\Rightarrow c^2$ divides y^2

$\Rightarrow c$ divides y

$\Rightarrow c$ divides y and c divides x

$\therefore c$ divides $(x, y) = 1$ (given)

$\Rightarrow c = 1$

Since x and z are both odd, so $z + x$ and $z - x$ are even.

Theorem 4 $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$

Proof: $\because$ Both x and z are odd

$\therefore \frac{z+x}{2}, \frac{z-x}{2}$ are integers.

Let $\frac{z+x}{2} = a, \frac{z-x}{2} = b$

$\because x$ and z are relatively prime (by theorem 3)

There exists integers m, n such that $mz + nx = 1$ ....(1)

$(m+n)\left(\frac{z+x}{2}\right) + (m-n)\left(\frac{z-x}{2}\right)$

$= \frac{1}{2}(mz + nz + mx + nx + mz - nz - mx + nx)$

$= \frac{1}{2}(2mz + 2nx)$

$= mz + nx = 1$ (by (1))

Therefore $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$

Now $y^2 = z^2 - x^2$

$= 4\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$ and $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$

Let $\frac{z+x}{2} = u^2$, $\frac{z-x}{2} = v^2$; where u and v are integers.

$\Rightarrow u$ and v are relatively prime.

So $\begin{cases} y^2 = 4u^2v^2 \\ z = u^2 + v^2 \\ x = u^2 - v^2 \end{cases} \Rightarrow \begin{cases} y = 2uv \\ z = u^2 + v^2 \\ x = u^2 - v^2 \end{cases}$

u	v	x	y	z
2	1	3	4	5
3	1	8	6	10
3	2	5	12	13

Method 2

$x^2 + y^2 = z^2 \Rightarrow y^2 = z^2 - x^2 \Rightarrow y^2 = (z + x)(z - x) \Rightarrow \dfrac{y}{z - x} = \dfrac{z + x}{y} = u$

Let $y = u(z - x)$ ....(1); $z + x = uy$ ....(2)

Sub (1) into (2) $z + x = u^2z - u^2x$

$(u^2 + 1)x = (u^2 - 1)z$

Let $x = (u^2 - 1)v$, $z = (u^2 + 1)v \Rightarrow y = u[(u^2 + 1)v - (u^2 - 1)v] = 2uv$

u	v	x	y	z
2	1	3	4	5
3	1	8	6	10
4	1	15	8	17
5	1	24	10	26

Note that we cannot find the primitive root (5, 12, 13) unless

$uv = 6$............. (3)

$6u - v = 5$ ...... (4)

From (4), $v = 6u - 5$

sub. into (3)

$u(6u - 5) = 6$

$6u^2 - 5u - 6 = 0$

$u = \dfrac{3}{2}$ or $u = -\dfrac{2}{3}$

$v = 4$ or -9

$x = 5, y = 12, z = 13$

which means that u and v may not be an integer.