Diophantus and Fermat

Michael Chmutov

Diophantus "Arithmetic", Book II, Problem 8:

Given a number which is a square, write it as a sum of two other squares.

Find the integer solutions of the equation

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

On the other hand, it is impossible for a cube to be written as the sum of two cubes or a forth power to be written as the sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers.

I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain

Fermat's Last Theorem: *The equation*

$$x^n + y^n = z^n$$

has no (nontrivial) integer solutions for $n \geq 3$.

Fermat: The case $n = 4$.

Pythagorean triples

x, y, z are natural numbers satisfying the relation $x^2 + y^2 = z^2$.

A triple (x, y, z) is called *primitive* if $GCD(x, y, z) = 1$. $\Longrightarrow \begin{cases} GCD(x,y) = 1 \\ GCD(x,z) = 1 \\ GCD(y,z) = 1 \end{cases}$

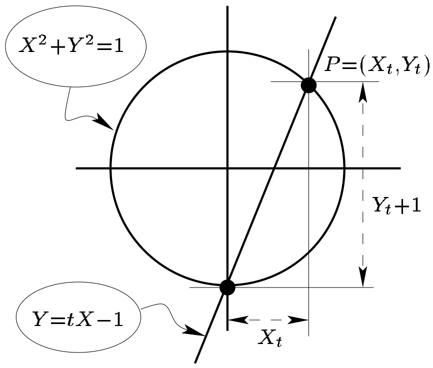
Since $(2n)^2 \equiv 0(mod\ 4)$ and $(2n+1)^2 \equiv 1(mod\ 4)$ the right hand side, z^2, is congruent to to either 1 or 0 modulo 4. Hence precisely one of x or y must be even. Assume that x is even and y is odd.

Proposition 1. *Given any primitive Pythagorean triple* (x, y, z) *there exist relatively prime positive integers* p, q, *such that* $p > q$, p *and* q *have opposite parities, and*

$$\boxed{x = 2pq, \qquad y = p^2 - q^2, \qquad z = p^2 + q^2}$$

Any Pythagorean triple gives a *rational point* $X = \frac{x}{z}$, $Y = \frac{y}{z}$ on the unit circle $X^2 + Y^2 = 1$.

Rational parametrization of the unit circle.



A point $P = (X_t, Y_t)$ on the unit circle determines a number t which is the slope of the line thorugh the points $(0, -1)$ and P. And conversely, a number t determines a point $P = (X_t, Y_t)$ on the unit circle as the second point of the intersection of the slope t stright line thorugh the point $(0, -1)$ with the unit circle. This gives a one-to-one correspondence between points on the unit circle and real numbers t (together with infinity corresponding to the point $(0, 1)$). In formulas it can be written as follows.

- *from point to slope*: $P = (X_t, Y_t) \longrightarrow t = \frac{Y_t+1}{X_t}$.
- *from slope to point*: A stright line with slope t through the point $(0, -1)$ has an equation $Y = tX - 1$. Pluging it into the circle equation we get $(t^2+1)X^2 - 2tX + 1 = 1$, which is equivalent to $X\big((t^2+1)X - 2t\big) = 0$. The solution $X = 0$ corresponds to the point $(0, -1)$. The second solution $X = \frac{2t}{t^2+1}$ gives the X-coordinate of the point P. So the correspondence is
$$t \longrightarrow \left(X_t = \frac{2t}{t^2+1}, Y_t = \frac{t^2-1}{t^2+1}\right) \tag{1}$$

Since the both way correndences are given by rational functions we have a one-to-one correspondence between rational points on the unit circle and rational slopes t.

In particular, for a primitive Pythagorean triple (x, y, z) with even x the corresponding slope will be rational and greater than 1. Write it in lowest terms $t = p/q$. Then p and q are two relatively prime numbers, and $p > q$. Pluging the value $t = p/q$ into equations (1) we obtain
$$\frac{x}{z} = \frac{2pq}{p^2+q^2}, \qquad \frac{y}{z} = \frac{p^2-q^2}{p^2+q^2}$$
Then the primitivity of the triple (x, y, z) implies that
$$x = 2pq, \qquad y = p^2 - q^2, \qquad z = p^2 + q^2$$

The case $n = 4$ of the Last Theorem

Proposition 2. *The equation $x^4 + y^4 = z^2$ has no (nontrivial) integer solutions.*

PROOF. For a contradiction, suppose that there are solutions. Choose a solution (x, y, z) with positive x, y, z, and with the smallest possible value of z. We are going to construct another solution with a smaller value of z. This would be the contradiction with our choice which proves the proposition.

The triple (x^2, y^2, z) is a primitive Pythagorean triple. This follows from the minimality of z. Therefore there exist relatively prime positive integers p, q, such that $p > q$, p and q have opposite parities, and

$$x^2 = 2pq$$
$$y^2 = p^2 - q^2$$
$$z = p^2 + q^2$$

The second of these equations can be written as $y^2 + q^2 = p^2$ and it follows, since p and q are relatively prime, that (y, q, p) is a primitive Pythagorean triple. The number y is odd. Then q is even, and

$$q = 2ab$$
$$y = a^2 - b^2$$
$$p = a^2 + b^2$$

for some relatively prime numbers a, b $(a > b > 0)$ of the opposite parity. Thus

$$x^2 = 2pq = 4ab(a^2 + b^2) .$$

Hence $ab(a^2 + b^2)$ must be a square (of half of the even number x). But the numbers ab and $a^2 + b^2$ are relatively prime because a and b are relatively prime. So ab and $a^2 + b^2$ must both be the squares. But then, since ab is a square and a and b are relatively prime, a and b must both be the squares, say $a = x'^2$ and $b = y'^2$. Therefore $x'^4 + y'^4 = z'^2$, where $z'^2 = a^2 + b^2$. So we've found another solution (x', y', z') of our equation. It is primitive because a, b, and $a^2 + b^2$ are pairwise relatively prime. Moreover,

$$z' < z'^2 = a^2 + b^2 = p < p^2 < p^2 + q^2 = z .$$

This contradicts to the minimality of z.