Fermat's Last Theorem

T. Muthukumar
tmk@iitk.ac.in

02 Jun 2014

An ancient result states that a triangle with vertices A, B and C with lengths $AB = a$, $BC = b$ and $AC = c$ is right angled at B iff $a^2 + b^2 = c^2$. The fact that $a^2 + b^2 = c^2$ is a necessary condition for the right angle is the famous *Pythagoras theorem*. However, it is also a sufficient condition for the triangle to be a right angle. In fact, it is known that

(i) a triangle is obtuse at B iff $a^2 + b^2 < c^2$;

(ii) a triangle is right angles at B iff $a^2 + b^2 = c^2$;

(iii) a triangle is acute at B iff $a^2 + b^2 > c^2$.

In all the above cases the sufficiency can be proved using the *law of cosines*. An important application of above result is that it can used to construct right angles (say in a construction of a building).

What are all the integer triples $a, b, c \in \mathbb{Z}$ for which $a^2 + b^2 = c^2$? For instance, $(1, 1, 2)$ is not a integer triple that solves $a^2+b^2 = c^2$. Note that if a integer triple (a, b, c) solves $a^2+b^2 = c^2$ then all combinations of $(\pm a, \pm b, \pm c)$ are also integer triple. Therefore, it is enough to look for non-negative integer triples (a, b, c). Further, $(0, 1, 1)$ and $(1, 0, 1)$ is also a trivial integer solution which will not represent a triangle. A positive integer triple (a, b, c) is said to be *Pythagorean triple* if $a^2 + b^2 = c^2$. Note that if (a, b, c) is a Pythagorean triple then $ka, kb, kc)$ is also a Pythagorean triple for all $k \in \mathbb{N}$. For instance, $(3, 4, 5)$ is a Pythagorean triple then $(6, 8, 10)$ (multiplied by 2) is also a Pythagorean triple. This corresponds to the case similar right triangles. A Pythagorean triple (a, b, c) is said to be *primitve* if $\gcd(a, b, c) = 1$, i.e., a, b, c have no common factors, except 1, among them. This is equivalent

to saying that $\gcd(a, b) = 1$ because whatever divides LHS will also divide RHS. For instance, $(3, 4, 5)$ and $(5, 12, 13)$ are both primitive Pythagorean triple (PPT).

As we have already noted, there are integer triples that are not PPT. For instance, $(1, 2, 3)$ is not a PPT. Therefore, two natural questions are:

(i) How many PPT's are there, finite or infinite?

(ii) Is it possible to generate all PPT's?

It turns out that there are infinitely many PPT's and the answer to second question is in affirmative.

Theorem 1. *If (a, b, c) is a PPT then c is always an odd number and, between a and b, one is even and the other odd.*

Proof. Since $\gcd(a, b) = 1$ both cannot be even. Suppose both and a and b are odd, then $a = 2k + 1$ and $b = 2l + 1$. Therefore a^2 and b^2 are also odd because square of an odd number is odd (Use $(2k + 1)^2$)!). Therefore $a^2 + b^2$ is even because sum of odd numbers is even. Thus c^2 is even and, hence c is even. Let $c = 2m$. Then

$$\begin{aligned} 4k^2 + 4k + 1 + 4l^2 + 4l + 1 &= 4m^2 \\ 2(k^2 + l^2 + k + l) + 1 &= 2m^2. \end{aligned}$$

Note that LHS is odd and RHS is even which is a contradiction. Therefore, one of a and b is even and the other odd. This implies c^2 is odd and, hence, c is odd. □

The above result rules out all triples (a, b, c), with c even, as a possible PPT. It is enough to consider c odd. But that still does not say all odd c are allowed. For instance, there is no choice of $(a, b) \in \mathbb{N}$ such that $(a, b, 3)$ is a PPT. In fact, the first PPT is $(3, 4, 5)$.

Also owing to the result above, henceforth in the pair (a, b), we shall always denote the odd number by a and the even number by b. For any PPT (a, b, c), we write $a^2 = c^2 - b^2 = (c + b)(c - b)$. Note that $c - b > 0$.

Theorem 2. *For any PPT (a, b, c), $c + b$ and $c - b$ are relatively prime.*

Proof. Let $x \in \mathbb{N}$ divide both $c+b$ and $c-b$. Then $c+b = kx$ and $c-b = lx$ for some $k, l \in \mathbb{N}$. Then $2c = x(k+l)$ and $2b = x(k-l)$ which means that x divides both $2b$ and $2c$. But $\gcd(b, c) = 1$ and, hence, $x = 1$ or $x = 2$. Since x should also divide a^2, hence a. But a is odd so $x = 1$. □

Above result says that a^2, a perfect square, is product of two relatively prime numbers $c+b$ and $c-b$. Let $c+b = p_1^{x_1} \dots p_k^{x_k}$ and $c-b = q_1^{y_1} \dots q_l^{y_l}$ be the respective unique prime decomposition. Then $a^2 = p_1^{x_1} \dots p_k^{x_k} q_1^{y_1} \dots q_l^{y_l}$. Since $c+b$ and $c-b$ are relatively prime $p_i \neq q_j$ for all i, j. Thus, each x_i and y_j is even. Therefore, $c+b$ and $c-b$ are also perfect squares, say $c+b = m^2$ and $c-b = n^2$, for some $m, n \in \mathbb{N}$ such that $m > n$ and $\gcd(m, n) = 1$. Consequently, $a = mn$ and, since a is odd, both m and n are odd. So, for every choice of odd positive integer m, n such that $m > n$ and $\gcd(m, n) = 1$, we have a PPT (a, b, c) given by $a = mn$, $b = \frac{m^2-n^2}{2}$ and $c = \frac{m^2+n^2}{2}$. The last two equalities are obtained by solving for b and c using $c+b = m^2$ and $c-b = n^2$. Since there are infinitely many choices of m, n satisfying above condition there are infinitely many PPT's.

A generalisation of the Pythagorean triple condition is, for a fixed integer $n > 2$, seeking triples (a, b, c) such that $a^n + b^n = c^n$. Obviously, there are some trivial solution if (a, b, c) is such that $abc = 0$. However, it turns out there are no non-trivial solution, i.e., (a, b, c) with $abc \neq 0$

Theorem 3 (Fermat's Last Theorem)**.** *Given an integer $n > 2$, there are no integer solutions to $a^n + b^n = c^n$ with $abc \neq 0$.*

Suppose $n = kl$. Then if the equation $a^n + b^n = c^n$ has integer solution then, using $(a^k)^l + (b^k)^l = (c^k)^l$, (a^k, b^k, c^k) is a solution corresponding to $n = l$. Therefore, to prove FLT it is enough to prove the result for $l \leq n$. Note that any $n > 2$ is:

1. either $n = 2^m$, for some integer $m > 2$, which is same as $n = 4 \times 2^{k-2}$. Choose $l = 4$ in this case;

2. or an odd prime. Choose $l = n$ in this case;

3. or a muliple of an odd prime. Choose l to be the odd prime.

Thus, it is enough to prove the result for $n = 4$ and odd prime n. If there is an integer solution to $a^4 + b^4 = c^4$ then (a, b, c^2) is an integer solution to $x^4 + y^4 = z^2$. So, to prove FLT for $n = 4$ we show the following theorem:

Theorem 4. *There are no integer solution to $x^4 + y^4 = z^2$ with $xyz \neq 0$.*

Proof. Suppose there is a integer triple (x, y, z) such that $xyz \neq 0$ solving $x^4 + y^4 = z^2$. Without loss of generality, we may assume that x, y, z are all positive, $\gcd(x, y, z) = 1$ and, hence, $\gcd(x, y) = 1$.

(Step 1): Note that (x^2, y^2, z) is a PPT, since $\gcd(x^2, y^2, z) = 1$ (if necessary, we rewrite x and y such that x^2 is odd and y^2 is even). We also know that z is always odd.

(Step 2): There exists odd numbers $m, n \in \mathbb{N}$, such that $m > n$, $\gcd(m, n) = 1$ and

$$x^2 = mn; \quad y^2 = \frac{m^2 - n^2}{2} \text{ and } z = \frac{m^2 + n^2}{2}.$$

Then, $2y^2 = m^2 - n^2 = (m+n)(m-n)$. Since m and n are odd, both $m+n$ and $m-n$ are even and, hence, are not coprime.

(Step 3): Let $d > 1$ divide both $m + n$ and $m - n$. Then $m + n = kd$ and $m - n = ld$ for some $k, l \in \mathbb{N}$. Then $2m = d(k + l)$ and $2n = d(k - l)$ which means that d divides both $2m$ and $2n$. But $\gcd(m, n) = 1$ therefore d divides 2. Therefore, $d = 2$. Hence, $m + n = 2k$, $m - n = 2l$, $m = k + l$ and $n = k - l$. Since $\gcd(m + n, m - n) = 2$, $\gcd(k, l) = 1$.

(Step 4): In fact, using the equation of x^2, we have $x^2 + l^2 = k^2$, i.e., (x, l, k) is a PPT. Therefore, l is even and k is odd. Let $l = 2\ell$. Then $\gcd(k, \ell) = 1$.

(Step 5): Using equation for y^2, we get $2y^2 = 4kl = 8k\ell$, i.e., $y^2 = 4k\ell$. Hence k and ℓ are perfect squares, $k = u^2$ and $\ell = v^2$ and $\gcd(u, v) = 1$. Therefore, $(x, 2v^2, u^2)$ is a PPT.

We repeat Step 2 on $(x, 2v^2, u^2)$. There exists odd numbers $M, N \in \mathbb{N}$, such that $M > N$ and $\gcd(M, N) = 1$ we have

$$x = MN; \quad 2v^2 = \frac{M^2 - N^2}{2} \text{ and } u^2 = \frac{M^2 + N^2}{2}.$$

We repeat Step 3 on $M + N$ and $M - N$ to obtain K and L such that $\gcd(K, L) = 1$, $M + N = 2K$, $M - N = 2L$, $M = K + L$ and $N = K - L$.

We repeat Step 5 on $2v^2$ to conclude that $v^2 = KL$ and, hence, $K = U^2$ and $L = V^2$ and $\gcd(U, V) = 1$.

Using the value of M and N in the equation of u^2, we get

$$u^2 = \frac{M^2 + N^2}{2}$$

$$= \frac{2(K^2+L^2)}{2} = U^4 + V^4.$$

Therefore, (U, V, u) is also a non-trivial integer solution of $x^4 + y^4 = z^2$. Let us compare the two solutions (x, y, z) and (U, V, u). Note that

$$z = \frac{m^2+n^2}{2} = \frac{(u^2+2v^2)^2 + (u^2-2v^2)^2}{2} = u^4 + 4v^4.$$

This implies that $u^4 < z$, hence $u < z$. Thus, when we started with a non-trivial solution (x, y, z) we obtained another non-trivial solution (U, V, u) such that $0 < u < z$. We can repeat the entire proof for again for (U, V, u) playing the role of (x, y, z) above and can obtain another non-trivial solution $U_1, V_1, u_1)$ such that $0 < u_1 < u < z$. This is a contradiction because we cannot carry on infinite number of times as suggested by our proof. Therefore, our assumption on the existence of a non-trivial integer solution is false. □

With all the effort above, it only remains to prove the Fermat's Last theorem for odd primes.

Theorem 5 (Fermat's Last Theorem)**.** *Given an odd prime p, there are no integer solutions to $a^p + b^p = c^p$ with $abc \neq 0$.*

Definition 1. *An odd prime number p is called* regular *if p does not divide the numerator of the Bernoulli number B_k, for all even $k \leq p-3$. Any odd prime which is not regular is called* irregular.

The odd primes $3, 5, 7, \ldots, 31$ are all regular primes. The first irregular prime is 37. It is an open question: are there infinitely many regular primes? However, it is known that there are infinitely many irregular primes.

Theorem 6 (Kummer, 1850)**.** *If p is a regular odd prime then the equation*

$$a^p + b^p = c^p$$

has no solution in $\mathbb{N}$.

Gerhard Frey proved the following result related to FLT:

Theorem 7 (Proved in 1984)**.** *Given a odd prime p if there exists a non-trivial solution to the equation*

$$a^p + b^p = c^p$$

then the following elliptic curve, called Frey's curve*, must exist:*

$$y^2 = x(x - a^p)(x + b^p).$$

So, what is an elliptic curve? Given $a, b, c \in \mathbb{Z}$, consider plane curve of the form $y^2 = x^3 + ax^2 + bx + c$. Let us call it Γ. The discriminant of Γ is defined as

$$\Delta(\Gamma) := -4a^3 + a^2b^2 - 4b^3 - 27c^2 + 18abc.$$

The $\Delta = 0$ relates to the case when the curve self-intersects, called *singular points*. A curve Γ is said to be an *elliptic curve* if $\Delta(\Gamma) \neq 0$. If $\Delta < 0$ the curve will divide the plane in two connected components and if $\Delta > 0$ it divides the plane into more than two connected components. Elliptic curves are symmetrical about x-axis. The points on the elliptic curve form an abelian group under a suitable binary operation $(+)$. An elliptic curve Γ is modular if there exists a L-function of Γ. In 1955, the Taniyama-Shimura-Weil (TSW) conjectured (also called modularity theorem) states that:

Theorem 8 (Later proved in 2001)**.** *Every elliptic curve over the field of rationals is modular.*

This means if Frey's curve existed it must be modular. But, in 1985, Jean-Pierre Serre conjectured (epsilon conjecture) that Frey's curve is not modular which was later proved by Ken Ribet in 1986. Since Frey's curve is an elliptic curve it must be modular assuming TSW conjecture. An elliptic curve is semistable if a prime divides its discriminant and Frey's curve is semistable. In 1994-95 by Andrew Wiles showed that:

Theorem 9 (Proved in 1994)**.** *Every semistable elliptic curve over the field of rationals is modular.*

This means Frey's curve cannot exist and, hence, Fermat's last theorem is true.