Proof by Infinite descent...!

Sachin Kumar
University of Waterloo, Faculty of Mathematics

In this essay, I would like to discuss, not-so-common by extremely powerful non-trivial proof technique called infinite descent. This method was developed by Pierre de Fermat, when he was proving the case $n = 4$ of the Fermat's Last theorem (a famous conjecture on a special class of diophantine equation, that was proved by Andrew Wiles). At an overview, it has some abstract similarities with mathematical induction.

The method of infinite descent is a proof technique that uses the fact that there are a finite number of positive integers less than any given positive integer. The method relies on the fact that the set of non-negative integers follows the well-ordering principle, so only a finite number of non-negative integers are smaller than any given one. In other words, there is no infinite sequence of strictly decreasing non-negative integers. This intuition can lead to the solution of a lot of challenging problems, particularly in Diophantine equations.

Although Euclid makes use of it in his Elements, the method of infinite descent is attributed to Pierre de Fermat for stating it explicitly. In a letter to Christian Huygens, Fermat claimed infinite descent as his own: "I have finally organized this according to my method and shown that if a given number is not of this nature there will be a smaller number which also is not, then a third less than the second, etc., to infinity, from which one infers that all numbers are of this nature."

Fermat's method of infinite descent is an offshoot of mathematical induction that can be used to disprove statements. In the metaphor of climbing down a ladder, if a higher rung cannot be reached without first reaching a lower rung coupled with the notion that no lowest rung exists, then no rung can ever be reached.

Definition. Let $m \in \mathbb{Z}_+$. Suppose that whenever $P(m)$ holds for some $m > k$, there exists a $j \in \mathbb{Z}_+$ such that $m > j > k$ and $P(j)$ holds. Then $P(n)$ is false, for all $n \in \mathbb{Z}_+$.

Intuition. If there exists an n for which $P(n)$ was true, one could construct a sequence $n > n_1 > n_2 > \cdots$ all of which would be greater than k but for the non-negative integers; no such infinite descending sequence exists. The method of descent has two variants that can be useful especially in the solution of Diophantine equations.

1. There is no sequence of non-negative integers.

2. If the sequence of non-negative integers n_i with $1 \leq i$ satisfies the inequalities $n_1 \geq n_2 \geq \cdots$, then there exists i such that $n_i = n_{i+1} = \ldots$.

If you are interested on how it works, you can read an article that, where I proved that general result that $\sqrt[n]{p} \notin \mathbb{Q}$ (Click here!).

Why is this technique so big of a deal? If you looked it at a more abstract sense, we can understand that given a Diophantine equation, we can prove whether it has solutions or not in a given algebraically closed field, (where $F = \mathbb{Q}$ or $\mathbb{C}$, not $\mathbb{R}$ obviously), if it does how many and what are they? We will now prove a special generalized case of Fermat's last theorem, where $n = 4k$, which is kind of amazing!

Theorem. $x^4 + y^4 = z^2$ has no integer solutions when $xyz \neq 0$.

Proof. Assume such a solution exists, i.e, triplets. We can further assume that $\gcd(x^2, y^2, z) = 1$ (if they are not, then cancelling the common factors leaves us with a coprime triplet). Note that $x^4 + y^4 = z^2 \implies (x^2)^2 + (y^2)^2 = z^2$ and by pythogoras theorem, we know that x^2, y^2 and z are a pythogorian triplet. There exist coprime p, q of opposite parity such that,

$$\begin{aligned} x^2 &= 2pq \\ y^2 &= p^2 - q^2 \\ z &= p^2 + q^2 \end{aligned}$$

Note that the equation, $y^2 = p^2 - q^2$ gives rise to another Pythagorean triplet and hence,

$$\begin{aligned} q &= 2ab \\ y &= a^2 - b^2 \\ p &= a^2 + b^2 \end{aligned}$$

with the same restrictions on a, b as p, q. Substituting, we get $x^2 = 2pq = 4ab(a^2 + b^2)$. Note that if $p \mid a$ or $p \mid b$, then it cannot divide $a^2 + b^2$ since $\gcd(a, b) = 1$. Hence, ab and $a^2 + b^2$ are all perfect squares. Since ab is a perfect square, and a, b are relatively prime, both a and b are perfect squares, i.e., $a = A^2$, $b = B^2$. As $a^2 + b^2$ is a perfect square,

$$P^2 = a^2 + b^2 = A^4 + B^4$$

Recall that $P^2 = a^2 + b^2 = p < p^2 + q^2 = z$ and hence $P < z$, and it is evident that an infinite descent has occured. □

Corollary. Fermat's last theorem for $n = 4k$.

References

1. Fermat's Method of Infinite Descent. Brilliant.org. Retrieved 15:24, August 17, 2023, from https://brilliant.org/wiki/general-diophantine-equations-fermats-method-of/

2. Proof by infinite descent. Wikipedia.org. August 17, 2023.