The Fermat's Last Theorem and Homothetic Solutions

Radomir Majkic
E-mail: radomirm@hotmail.com

Abstract: The minimal homothetic integer solution of the Fermat equation is zero and the Fermat last theorem is true.

THEOREM: No three positive integers $(\mathrm{X}, \mathrm{Y}, \mathrm{Z})$ satisfy the Fermat equation $\mathrm{X}^n + \mathrm{Y}^n = \mathrm{Z}^n$ for any integer value of n greater than 2.

Introduction

The Fermat Last Theorem has been proven by the great mathematician Andrew Wiles by the use of the powerful tools of the modern mathematics. However, Fermat remarks on margins of his old Greek book live in the minds of many of us the hope that still there is an elegant, simple solution to the problem achievable by the means of the mathematics of the Fermat's XVIl century.

Minimal Setting

No three positive integers $(x, y, z) : (x, y, z) = 1$, $(x, y, z) \neq 0$ *satisfy the Fermat equation* $x^n + y^n = z^n$ *for any odd prime number* $n = p$.

■ The problem does not have solution for $n = 3, 4.5$. If $(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \neq 1$ there is an integer a such that $\mathrm{X} = a\textsc{x}, \mathrm{Y} = a\textsc{y}, \mathrm{Z} = a\textsc{z}$, and if $n = p\textsc{n} > 2$ is composed by a prime p then

$$\mathrm{X}^m + \mathrm{Y}^m = a^m(\textsc{x}^m + \textsc{y}^m) = a^m \textsc{z}^m \quad \Leftrightarrow \quad \textsc{x}^m + \textsc{y}^m = \textsc{z}^m,$$
$$\textsc{x}^m + \textsc{y}^m = \textsc{z}^m = z^p \;\Rightarrow\; (\textsc{x}^{\textsc{n}})^p + (\textsc{y}^{\textsc{n}})^p = (\textsc{z}^{\textsc{n}})^p = x^p + y^p.$$

Thus $(2, x, y, z) = 1$ and only one of the (x, y, z) must be even. If the Fermat equation has a solution for $n = p$ prime it has a solution for all integers which the prime p divides. Hence, the above is the minimal setting of the Fermat Last Theorem problem, and there is no smaller setting than this one. □

The Fermat function or polynomial is the odd prime degree p polynomial $\mathsf{F} = x^p + y^p$ and the equation

$$\mathsf{F} \equiv x^p + y^p = z^p \tag{1}$$

is the Fermat equation. Particular evaluation of the Fermat function is the Fermat number $\textsc{f}$.

Definition: *The minimal solution of the Fermat equation is an integer triple* $(\text{X}, \text{Y}, \text{Z}) : (\text{X}, \text{Y}, \text{Z}) = 1\}$ *satisfying the Fermat equation in its minimal setting. A solution* (x, y, z) *is smaller or below the solution* (x', y', z') *if* $x < x', y < y', z < z'$,

A transformation of the integer solution into a smaller integer solution preserving the Fermat equation is the Fermat descent reduction or the reversed homothety transformation of the solution.

The Fermat Descent Principle

The integer solution set of the Fermat equation, if not empty, is ordered from up to down by the reversed homothetic transformation. The smallest integer solution is the minimal solution and there are no integer solutions below the smallest one.

Corollary 01. *If the Fermat equation lets the reversed homothetic transformation its minimal integer solution is zero, the Fermat equation does not have a non-zero minimal integer solution and the integer solution set of the Fermat equation is empty.*

■ Suppose that $(\text{X}, \text{Y}, \text{Z})$ is the minimal solution and that the Fermat equation lets the reversed homothetic transformation. Then there is a homothetic solution (x, y, z) below the minimal solution, so that (x, y, z) and not $(\text{X}, \text{Y}, \text{Z})$ is the minimal solution. The same applies to the minimal solution (x, y, z) and so on. The reversed homothety is the contraction transformation, and below each new minimal solution, there is a smaller one. Thus, the reversed homothety creates an infinite sequence of the descending integer solutions of the Fermat equation.
However, the lower integer limit of the solution sequence is zero, and the minimal integer solution to the Fermat equation is $(0, 0, 0)$. Clearly, the Fermat equation does not have the positive minimal integer solution and the solution set of the Fermat equation is empty. □

Parametric Solutions

To see if the Fermat equation has solutions it is necessary to show that the Fermat equation lets the homothetic solutions. We will make proof by the explicit construction of a two-parametric solution family.

Corollary 02. *All integer solutions* (x, y, z) *of the Fermat equation are up to common integer factor given by the following two-parametric family*

$$x^p = 2u(u + v) \;\; y^p = v^2 - u^2, \;\; z^p = (u + v)^2, \quad (u, v) = 1. \tag{2}$$

The Fermat number evaluated on the solution set is the perfect square.

■ If (x, y, z) is an integer solution of the Fermat equation $\mathsf{F}(x, y) = z^p$ then the quadratic equation $\mathsf{F}^2(x, y) = z^{2p}$ has the same integer solutions. Thus

$$x^p + y^p = z^p \quad \Leftrightarrow \quad x^{2p} + 2x^p y^p + z^{2p} = z^{2p} \;\Leftrightarrow\; \overline{x}^2 + 2\overline{xy} + \overline{y}^2 = \overline{z}^2.$$

The equation is a special case of the equation $x^2 + qxy + y^2 = z^2$, with $q \in \mathbf{Z}$. see Ref.[1]. All integer solutions up to constant factor and substitution $v \to \pm v$ in a two-parametric representation are

$$\overline{x} = qu^2 + 2uv,\ \ \overline{y} = v^2 - u^2,\ \ \overline{z} = u^2 + quv + v^2, \quad (u, v) = 1.$$

Setting $q = 2$ we get the desired solutions. Notice that the solutions are valid for $q \to \pm q$. The quadratic nature of the z^p as well as $(x^p, y^p, z^p) = u + v$ are the consequences of the specification $q = \pm 2$. Finally, the Fermat number `F` is the perfect square on the all family of the integer solutions. $\square$

Conclusion

No three positive integers (x, y, z) satisfy the Fermat equation $x^n + y^n = z^n$ for $n > 2$.

■ The Fermat equation lets a homothetic transformation.
For, by the assumption, $(u, v) = 1$ and u and v are either of the opposite parities, or both of them are either even or odd.
1. If v and u are of the opposite parity then $v + u$ and $v - u$ are odd and $(v + u, v - u) = 1$. Further $(2, v + u) = 1$, $(u, v + u) = 1$ and $(2u, v + u) = 1$. Hence, there are integers (ξ, η, ζ) such that

$$\begin{aligned}
& y^p = v^2 - u^2 && \Rightarrow\ v - u = \eta^p,\ v + u = \zeta^p, \\
& x^p = 2u(u + v) && \Rightarrow\ 2u = \xi^p, \quad\ v + u = \zeta^p, \\
\therefore\quad & x^p + y^p = \ (\xi^p + \eta^p)\zeta^p = \zeta^{2p} && = z^p, \\
\Rightarrow\quad & \xi^p + \eta^p\ = \zeta^p, \quad (\xi, \eta, \zeta) < (x, y, z).
\end{aligned}$$

2. When both v and u are either even or odd both $v + u$ and $v - u$ are even. Hence $(v + u, v - u) = 2$ and $(2, v + u) = 2$, $(u, v + u) = 1$ so that there are integers (ξ, η, ζ) such that

$$\begin{aligned}
& y^p = v^2 - u^2 && \Rightarrow\ v - u = 2\eta^p, v + u = 2\zeta^p, \\
& x^p = 2u(u + v) && \Rightarrow\ 2u = 2\xi^p, \quad v + u = 2\zeta^p, \\
\therefore\quad & x^p + y^p = \ 4(\xi^p + \eta^p)\zeta^p = 4\zeta^{2p} && = z^p, \\
\Rightarrow\quad & \xi^p + \eta^p\ = \zeta^p, \quad (\xi, \eta, \zeta) < (x, y, z).
\end{aligned}$$

In either case, there is the homothetic transformation of the Fermat equation, and apart from the trivial, the Fermat equation does not have other integer solutions. Consequently, the Fermat Last Theorem is true. $\square$

References

[1] Wiles A. (1995) *Modular Elliptic Curves and Fermat's Last Theorem. Anals of Mathematics, 141, 443-551.*

[2] Andreescu. T. Andrica. D *An Introduction to Diophantine Equations, GIL. Publishing House, 2002*

[3] W. E. Deskins, *Abstract Algebra,* The MacMilan Company, New York,

[4] George E. Andrews, *Number Theory,* Dower Publications, Inc. New York.

[5] Neville Robbins, *Begining Number Theory,* WCB Wm. C Brown Publishers.