Geometric Note to the Last Fermat's Theorem

Timotej Sumny

Department of Mathematics, Faculty of Natural Science, Constantine the Philosopher in Nitra, Nitra, Slovakia

Email address:

Timotej.sumny@ukf.sk

Abstract: In this paper, we concerned with geometrical interpretation of tangent line to the curve and grid points which can be used to some illustration of Fermat's last theorem. With tangent line we find segment at axis *x, y*. With using this segments we make a ratio to find condition to grid point at the curve from equation of Last Fermat's theorem.

Keywords: Tangent Line, Grid Point, Elliptic Curve

1. Introduction

French lawyer Pier Fermat is one of the world's most renowned mathematicians. He dealt with mathematics in his free time and was very successful in this field. His ''little,, theorem is well known in the theory of numbers.

For any integer number a and p is primary number, the number $a^p - a$ is an integer multiple of p

The proof is possible to find in [1]. So called Fermat's last theorem was not proved in the field of maths for a long time. It was proved in 1994 by a British mathematician Andrew Wiles in his work called Modular elliptic curves and Last Fermat's theorem, which had more than a 100 pages [4]. Fermat's last theorem can be proved as follows:

No three positive integers x, y, and z can satisfy the equation for any integer value of n greater than two.

$$x^n + y^n = z^n, n > 2 \qquad (1)$$

In this paper, we look at the geometric interpretation of Fermat's last theorem.

Firstly, we use the curves which are represented with equations from Fermat's theorem.

Secondly, we use the tangent line. We need ordinates of tangent point, because numbers of ordinates are numbers of solution Fermat's equation for Real number.

2. The Meaning of The Last Fermat's Theorem

The base of modern proof was on the Taniyama-Shimura-Weil's conjecture. This conjecture connecting topology and number theory. It is focused to connect between elliptic curve and modular forms. That is means that every elliptic curve at form $y^2 = ax^3 + bx^2 + cx + d$ defined over the rational numbers is a modular form in disguise. This conjecture is important to elliptic curves that are used on the cryptography. At 1982 Gerhard Frey made elliptic curve at form $y^2 = x(x - a^l)(x + b^l)$ which is connected with the Last Fermat Theorem at form $a^l + b^l = c^l$ where l is primes. At 1985 Jaean - Pierre Serre shown that Frey curve could not be modular. And definite connect between Taniyama-Shimura-Weil's conjecture and the Last Fermat Theorem made Ken Ribet at 1990 with epsilon conjecture. And finally after 358 years of history was definite proof by Andrew Wiles. How we can see, this proof made new mathematic method and connect and connect different parts of mathematics.

3. Diophantine Equations

Diophantic equations are indefinite polynomial equations, whose solutions are only integers numbers. History about Diophantine equation began about 3. century with work Hellenistic mathematics Diophantus from Alexandria with Aritmetica. His work was inspirited by special problems from real life. Now the Diophantine problems are difficult part of number theory and it is a reason for their interest history.

Diophantine equations have a form:

$$f(x_1, \dots x_j, \dots x_n) = 0$$

The f is polynomial equations with variables $x_1, \dots x_j, \dots x_n$ and integers coeficients solutions is arranged sets $[a_1, \dots, a_j, \dots, a_n]$ for $f(a_1, \dots, a_j, \dots, a_n) = 0$.

4. Geometric Number Theory

The Diophantine equations are difficult problem and this is a reason why mathematicians use geometry method to solve a problems task. The most works about geometry number theory made Herman Minkowski. He studied n- dimensional space with integer vector. This space is symmetry to rotations and translations.

5. Grid Point at E_2

We use Cartesian coordinate system $\langle O, x, y \rangle$. For integer we use unit scale at axis x, y. Now every point at this plane is with integers coordinate $A[x_0, y_0]$, $y \in Z$, and these point are from the grid. Each grid point can be connect by the line. Let we use grid points $O[0,0]$ and $A[x_0, y_0]$.

The line has equation

$$y = \frac{y_0}{x_0} . x$$

Let $(x_0, y_0) = 1$, then $\frac{y_0}{x_0} = q$

$$y = q . x$$

With using tangent line, we have point that is crossing tangent line whit axis x, y. For this point is possibility using affine transformation.

Let

$$F(x, y) = c$$

For tangent line we use form

$$(O - A). grad(F[A]) = b$$

Let

$$s. grad(F[A]) = 0$$

Next we connect last forms

$$-s. grad(F[A]) + (A - O). grad(F[A]) = b$$

Next, we use

$$\left(s + (A - O)\right). grad(F[A]) = b$$

Let $s = \left(S_j - A\right)$, $j = x, y$ and exist invers vector $grad(F[A])^{-1}$ at E_2

$$-\left(A - S_j + O - A\right). grad(F[A]). grad(F[A])^{-1}$$
$$= b. grad(F[A])^{-1}$$

$$-\left(A - S_j + O - A\right). 1 = b. grad(F[A])^{-1}$$

Now we find point $S_x[s_x, 0]$, $1_x = (1,0)$

$$(O - S_x). 1_x = b. grad(F[A])^{-1}. 1_x$$

$$-s_y = b. 1_y. grad(F[A])^{-1}$$

Note

$$grad(F[A])^{-1} = \frac{grad(F[A])^T}{\sqrt{grad(F[A]). grad(F[A])}}$$

For Diophantine equation is useful if $s_y \in Z$, but it is not necessary, other useful information is if

$$\frac{(O - A)}{grad(F[A])} = (u, v) ; u, v \in Q$$

6. Using Geometry to Last Fermat Theorem

In E2 is function represented the last Fermat theorem is curve $f(x, y) = z^2$. We can use a tangent line in the point $X[x_0, y_0]$. Now we can write a equation for tangent line:

$$x_0^n + y_0^n = x_0^{n-1}x + y_0^{n-1}y \qquad (2)$$

We use substitution $\frac{y_0}{x_0} = q$

$$1 + q^n = \frac{x}{x_0} + q^n \frac{y}{y_0}$$

$$q^n \left(1 - \frac{y}{y_0}\right) = \frac{x}{x_0} - 1$$

$$q^{n-1} = \frac{x - x_0}{y_0 - y}$$

$$q = \sqrt[n-1]{-\frac{\Delta X}{\Delta Y}}$$

Last equation is relationship between the angle tangent line and the angle vector *(O-X)*. Tangent line intersect axis x in point $S_x \left[\frac{z^n}{x_0^{n-1}}, 0\right]$. Because $\frac{z^n}{x_0^{n-1}}$ is rational number we expect that $k = \frac{x_0}{(\Delta X)^{\frac{1}{n-1}}}$ is rational number too.

Now, we can compute

$$k = \frac{x_0^2}{y_0^{\frac{n}{n-1}}}$$

$$k = x_0^2 y_0^{\frac{n}{n-1}}$$

On the other side, we can use $r \in Q$, $r = \frac{x_0}{(y_0 - y)^{\frac{1}{n-1}}}$

$$r = \frac{x_0 y_0}{x_0^{\frac{n}{n-1}}}$$

$$r = x_0^{\frac{-1}{n-1}} y_0$$

Now we can see condition from numbers k and r. Next we use condition for rational number.

$$y_0^n = A^{n-1}, x_0^n = b^{n-1}, x_0 = c^{n-1} ; A, b, c, x_0, y_0 \in N \ (3)$$

Let

$$x_0 = b.\alpha \; ; \; x_0 = c.\beta, \alpha, \beta \in Q \qquad (4)$$

$$x_0^n = b^n.\alpha^n => b^{n-1} = b^n.\alpha^n$$

$$b = \alpha^{-n}$$

$$x_0 = \alpha^{1-n} \qquad (5)$$

$$x_0 = \beta.c => c^{n-2} = \beta$$

From (b) and (c) we have

$$\alpha^{1-n} = c.\beta$$

$$\alpha^{1-n} = c^{n-1} \qquad (6)$$

Now, we use (d):

$$\alpha = c^{-1} \qquad (7)$$

$$x_0^2 = b.\beta$$

$$x_0^2 = \beta.c^n$$

$$0 = \beta(b - c^n) \qquad (8)$$

$$x_0^2 = b.\alpha.c^{n-1}$$

$$x_0^2 = b.\beta$$

$$x_0^{n-2} = b^{n-2}.\beta \qquad (9)$$

Connect (a) and (e):

$$c^{-n}.b^{n-1} = \beta^n$$

$$b^{n-2} = \beta^n$$

$$a^{2-n} = \beta \qquad (10)$$

$$\beta^{n+1} = (b.c)^{n-2}$$

$$c^2.b^{-1}.\beta = 1 \qquad (11)$$

$$(b.c)^{\frac{n-2}{n+1}} = \beta \qquad (12)$$

From (e), (g) and (h):

$$(b.c)^{n-2} = x_0^{n-2} \qquad (13)$$

$$b.c \neq x_0 \; ; \; n = 2 \qquad (14)$$

From the lasts conditions (11) and (13) and (14) we can see only one possibility for $\alpha, \beta \in Q$ and $A, b, c, x_0, y_0 \in N$ is only for $n = 2$ and $\beta = 1$.

7. Conclusion

We used the geometric character curve for the last Fermat theorem. The tangent line determinate specific ratio on axis x. Next we use elementary knowledge from number theory for integer's number. At last point we found form between parameters $a, b, c \in N$ and, $\beta \in Q$. Last forms are true only for $n = 2$.

References

[1] Veselý, F: *O dělitelnostičíselcelých*. Mladafronta, Praha 1966.

[2] Vít, P: *Řeťazovézlomky*. Mladáfronta, Praha 1982.

[3] KluvánekI.-Mišík L. Švec M. *Matematika 1*. Slovenské vydavateľstvo technickej literatúry Bratislava 1959.

[4] Wiles, A. "Modular Elliptic-Curves and Fermat's Last Theorem." *Ann. Math.* 141, 443-551, 1995. http://math.stanford.edu/~lekheng/flt/wiles.pdf

[5] STEWART, Ian; TALL, David. *Algebraic number theory and Fermat's last theorem*. CRC Press, 2015.

[6] DI GREGORIO, Leandro Torres. Proof for the Beal conjecture and a new proof for Fermat's last theorem. *Int. J. of Pure and Applied Mathematics*, 2013, 2.5: 149-155.

[7] ARBARELLO, Enrico, et al. *Geometry of algebraic curves*. Springer Science & Business Media, 2013.

[8] NEUKIRCH, Jürgen. *Algebraic number theory*. Springer Science & Business Media, 2013.

[9] DICKSON, Leonard Eugene. *History of the theory of numbers: Diophantine Analysis*. Courier Corporation, 2013.

[10] http://mathworld.wolfram.com/FermatsLastTheorem.html

[11] LEKKERKERKER, Cornelis Gerrit. *Geometry of numbers*. Elsevier, 2014.