Subjects: Number theory (math.NT) MSC classes: 11D41 Comments: 20 pages

"The margin is too narrow to contain a truly remarkable proof."

Pierre de Fermat

By Nguyễn Tri Phương

For HP & KP

Abstract. The aim of this paper is to try for Fermat's lost proof.

Introduction

In about 1637 Pierre de Fermat, a French mathematician, annotated in his copy of Diophantus' Arithmetica as follows:

There are no nonzero integers a,b,c,n with $n>2$ such that $a^n+b^n=c^n$.

I have discovered a truly remarkable proof of this proposition which the margin is too narrow to contain.

Unfortunately, his proof was lost. Despite of many mathematicians' attempts, it remained unsolved for over 350 years until in 1994 Professor Andrew John Wiles proved successfully a special case of the Shimura-Taniyama conjecture that implies Fermat's Last Theorem (FLT).

Since Wiles' is too long and extremely complicated, it is believed that Fermat had a wrong proof in mind. However, contrary to the standard view, amateur mathematicians still try hard to find an elementary one.

For this purpose, we present here such an elegant proof of FLT that we hope the method used will work effectively for certain plane smooth curves.

1. A short proof of FLT

Our approach is Fermat's curve $x^n+y^n-1=0$. In the proof, we use the method of contradiction by assuming that Fermat's curve has a certain nonzero rational point, we then show that this will lead to the existence of a quadruple being a non-trivial integral solution of the equation $x^2+y^2+z^2=w^2$. On the other hand, we prove that the existence of this quadruple will lead to the contrary of the supposition.

Nguyễn Tri Phương
54 Le Dai Hanh street, ward 7, district 11, Ho Chi Minh city, Viet Nam

Lemma 1

Given a is even and b is odd. If there exist nonzero integers e, f, g, h such that

$$2(fg+eh)=a(a-b)$$

$$2(eg-fh)=ab$$

$$e^2+f^2-g^2-h^2=b(a-b)$$

$$e^2+f^2+g^2+h^2=a^2+b^2-ab$$

Or

$$2(fg+eh)=ab$$

$$2(eg-fh)=a(a-b)$$

$$e^2+f^2-g^2-h^2=b(a-b)$$

$$e^2+f^2+g^2+h^2=a^2+b^2-ab$$

, then there exist two different parity integers i, j and $GCD(i, j)=1$ such that i^2+j^2 is a common divisor of a and b.

Proof

First, let us consider system of equations $(1.1)-(1.4)$.

$$2(fg+eh)=a(a-b) \quad (1.1)$$

$$2(eg-fh)=ab \quad (1.2)$$

$$e^2+f^2-g^2-h^2=b(a-b) \quad (1.3)$$

$$e^2+f^2+g^2+h^2=a^2+b^2-ab \quad (1.4)$$

Adding equations $(1.3)\,\&\,(1.4)$ term by term,

$$2(e^2+f^2)=a^2 \quad (1.5)$$

Nguyễn Tri Phương
54 Le Dai Hanh street, ward 7, district 11, Ho Chi Minh city, Viet Nam

Or

$$(e+f)^2+(e-f)^2=a^2 \tag{1.6}$$

Solving equation (1.6),

$$e+f=k(i^2-j^2) \tag{1.7}$$

$$e-f=k(2ij) \tag{1.8}$$

$$a=k(i^2+j^2) \tag{1.9}$$

where i, j are two different parity integers , $GCD(i, j)=1$ and $k=GCD(e+f, e-f)$.

It follows that

$$e=\frac{k}{2}(i^2-j^2+2ij) \tag{1.10}$$

$$f=\frac{k}{2}(i^2-j^2-2ij) \tag{1.11}$$

Adding equations $(1.1)\,\&\,(1.2)$ term by term,

$$2(e+f)g+2(e-f)h=a^2 \tag{1.12}$$

Wherefrom follows

$$h=\frac{a^2-2(e+f)g}{2(e-f)} \tag{1.13}$$

Replacing the values of $e+f, e-f$ and a from $(1.7),(1.8)$ and (1.9) into (1.13),

$$h=\frac{k(i^2+j^2)^2+2(j^2-i^2)g}{4ij} \tag{1.14}$$

From (1.2),

$$b=\frac{2(eg-fh)}{a} \tag{1.15}$$

Replacing the values of e, f, a and h from $(1.10),(1.11),(1.9)$ and (1.14) into (1.15),

$$b = \frac{(i^2 + j^2)(kj^2 + 2kij - ki^2 + 2g)}{4ij} \tag{1.16}$$

Since $GCD(i, j) = 1$ and i, j are two different parity integers, we have $GCD(i^2 + j^2, 4ij) = 1$. It follows that $kj^2 + 2kij - ki^2 + 2g = l(4ij)$, where l is a nonzero integer.

Then

$$b = l(i^2 + j^2) \tag{1.17}$$

From (1.9) and (1.17), it follows that $i^2 + j^2$ is a common divisor of a and b.

Next, considering the following system of equations will lead to the same result.

$$2(fg + eh) = ab$$

$$2(eg - fh) = a(a - b)$$

$$e^2 + f^2 - g^2 - h^2 = b(a - b)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab$$

Hence, lemma 1 is proved.

Theorem

For any integer n greater than 2, there are no nonzero rational points on the curve $x^n + y^n - 1 = 0$.

Proof

It is clear that we are only necessary to prove the theorem for two cases:

Case 1: n is an odd number greater than 2.

Case 2: $n = 4$.

Suppose that for any odd number n greater than 2 or equal to 4, the curve $(L): x^n + y^n - 1 = 0$ has a certain nonzero rational point $M_0(x_0, y_0)$. Without loss of

generality, assume that $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$, where a, b, c are nonzero integers and relatively prime in pairs.

Let $m = \frac{x_0}{y_0} = \frac{a}{b}$. It is easy to see that $m \neq 0, m \neq 1$ and $m \neq -1$.

In the plane Oxy, we introduce the circle (C) with center at the origin and passing through the point $M_0(x_0, y_0)$. Then, the equation of the tangent (δ) to the circle (C) at the point $M_0(x_0, y_0)$ is $y = -m(x - x_0) + y_0$. Moreover, the equation of the tangent (Δ) to the curve (L) at the point $M_0(x_0, y_0)$ is $y = -m^{n-1}(x - x_0) + y_0$.

If the straight line (Δ) coincides with the straight line (δ), then

$$-m^{n-1} = -m \tag{1.18}$$

Or

$$m^{n-2} - 1 = 0 \tag{1.19}$$

The rational roots of equation (1.19) may be $m = 1$ or $m = -1$, if exist. (see reference [2]). For this reason, the straight line (Δ) intersects the circle (C) at two distinct points $M_0(x_0, y_0)$ and $M_1(x_1, y_1)$ such that

$$x_1 = \frac{(m^{2n-2} - 1)x_0 + 2m^{n-1}y_0}{m^{2n-2} + 1} \tag{1.20}$$

$$y_1 = \frac{2m^{n-1}x_0 + (1 - m^{2n-2})y_0}{m^{2n-2} + 1} \tag{1.21}$$

From (1.20) & (1.21) and $y_0 \neq 0$,

$$\frac{x_1}{y_0} = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \tag{1.22}$$

$$\frac{y_1}{y_0} = \frac{-m^{2n-2} + 2m^n + 1}{m^{2n-2} + 1} \tag{1.23}$$

If $x_1 = 0$, then $m^{2n-2} + 2m^{n-2} - 1 = 0$. This equation has no rational roots.

If $y_1 = 0$, then $m^{2n-2} - 2m^n - 1 = 0$. This equation has no rational roots.

Therefore, $x_1 \neq 0$ and $y_1 \neq 0$.

Replacing $m = \frac{a}{b}$ into equations $(1.22)\,\&\,(1.23)$,

$$\frac{x_1}{y_0} = \frac{a(a^{2n-2} + 2a^{n-2}b^n - b^{2n-2})}{b(a^{2n-2} + b^{2n-2})} \tag{1.24}$$

$$\frac{y_1}{y_0} = \frac{-a^{2n-2} + 2a^n b^{n-2} + b^{2n-2}}{a^{2n-2} + b^{2n-2}} \tag{1.25}$$

Since $M_0(x_0, y_0)$ and $M_1(x_1, y_1)$ are on the circle (C), we have

$$x_1^{\,2} + y_1^{\,2} = x_0^{\,2} + y_0^{\,2} \tag{1.26}$$

Dividing both members of equation (1.26) by $y_0^{\,2} \neq 0$,

$$(\frac{x_1}{y_0})^2 + (\frac{y_1}{y_0})^2 = (\frac{x_0}{y_0})^2 + 1 \tag{1.27}$$

Replacing the values of $\frac{x_1}{y_0}$ and $\frac{y_1}{y_0}$ from (1.24) and (1.25) into equation (1.27),

$$(\frac{ap}{bq})^2 + (\frac{r}{q})^2 = (\frac{a}{b})^2 + 1 \tag{1.28}$$

where $p = a^{2n-2} + 2a^{n-2}b^n - b^{2n-2}$, $q = a^{2n-2} + b^{2n-2}$ and $r = -a^{2n-2} + 2a^n b^{n-2} + b^{2n-2}$ are nonzero integers. (It is easy to see this).

Since $(bq)^2 \neq 0$, from (1.28) it follows that

$$(ap)^2 + (br)^2 = (a^2 + b^2)q^2 \tag{1.29}$$

Multiplying both members of equation (1.29) by $a^2 + b^2 \neq 0$,

$$(a^2 + b^2)\left\{(ap)^2 + (br)^2\right\} = \left\{(a^2 + b^2)q\right\}^2 \tag{1.30}$$

Then, adding both members of equation (1.30) to $-2ab\left\{(ap)^2+(br)^2\right\}$

$$(a^2+b^2-2ab)\left\{(ap)^2+(br)^2\right\}=\left\{(a^2+b^2)q\right\}^2-2ab\left\{(ap)^2+(br)^2\right\} \tag{1.31}$$

From $(1.29)\,\&\,(1.31)$,

$$(a-b)^2\left\{(a^2+b^2)q^2\right\}=\left\{(a^2+b^2)q\right\}^2-2ab\left\{(a^2+b^2)q^2\right\} \tag{1.32}$$

Or

$$(a-b)^2(a^2+b^2)q^2=\left\{(a^2+b^2-ab)q\right\}^2-(ab)^2q^2 \tag{1.33}$$

Since $q^2\neq 0$, from (1.33) we find

$$\left\{a(a-b)\right\}^2+(ab)^2+\left\{b(a-b)\right\}^2=(a^2+b^2-ab)^2 \tag{1.34}$$

Since $GCD(a,b)=1$, there only exist the two following cases:

Case a: The numbers a,b are of different parity (one is odd, one is even).

Case b: The numbers a,b are both odd.

In case a, for any odd number n greater than 2 or equal to 4, without loss of generality, assume that a is even and b is odd. Then $a(a-b)$, ab are even and $b(a-b), a^2+b^2-ab$ are odd. Thus, from (1.34), it is clear that the quadruple $\left[a(a-b),ab,b(a-b),a^2+b^2-ab\right]$ is a non-trivial integral solution of the equation $x^2+y^2+z^2=w^2$. Moreover, since $GCD(b(a-b),a^2+b^2-ab)=1$, the quadruple $\left[a(a-b),ab,b(a-b),a^2+b^2-ab\right]$ is a primitive integral solution of the equation $x^2+y^2+z^2=w^2$. As known, if the quadruple $\left[a(a-b),b(a-b),ab,a^2+b^2-ab\right]$ is a primitive integral solution of the equation $x^2+y^2+z^2=w^2$, then there exist nonzero integers e,f,g,h such that (see reference [1]).

$$2(fg+eh)=a(a-b) \tag{1.35}$$

$$2(eg-fh)=ab \tag{1.36}$$

$$e^2+f^2-g^2-h^2=b(a-b) \tag{1.37}$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab \tag{1.38}$$

Or

$$2(fg + eh) = ab \tag{1.39}$$

$$2(eg - fh) = a(a-b) \tag{1.40}$$

$$e^2 + f^2 - g^2 - h^2 = b(a-b) \tag{1.41}$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab \tag{1.42}$$

On the other hand, by lemma 1, from this fact it follows that there exist two different parity integers i, j and $GCD(i, j) = 1$ such that $i^2 + j^2$ is a common divisor of a and b. This is contrary to the above supposition $GCD(a,b) = 1$.

In case b, if n is an odd number greater than 2, then from $a^n + b^n = c^n$ we have $a^n = c^n + (-b)^n$. Let $A = c$, $B = -b$, $C = a$. Then $A^n + B^n = C^n$, where the integers A, B are of different parity. This contradicts case a.

In case b, if $n = 4$, then from $a^4 + b^4 = c^4$ we have $c = 2l$, where l is a nonzero integer. From here it follows that $\frac{a^4 + b^4}{2} = 8l^4$. This is a contradiction because $\frac{a^4 + b^4}{2}$ is odd and $8l^4$ is even.

In short, there are no nonzero rational points on the curve (L). The theorem is proved.

2. Generalization for a plane smooth curve

One question arises from the above proof naturally. To which curve can the above method be applied when determining whether any rational point on it ? To answer a little about this question, we will show that a plane smooth curve has always a specific equation the form of which is $x^2 + y^2 + z^2 = w^2$.

Lemma 2.1

Given in the plane Oxy a circle $(C): x^2 + y^2 - r^2 = 0$. Suppose that the circle (C) has two distinct nonzero points $M_0(x_0, y_0), M_1(x_1, y_1)$ such that

1) $x_0 + x_1 \neq 0$

2) $x_0 - x_1 \neq 0$

3) $y_0 - y_1 \neq 0$

Then

$$\{x_0(y_0 - y_1)\}^2 + \{y_0(y_0 - y_1)\}^2 + (x_0x_1)^2 = (x_0^2 + y_0^2 - y_0y_1)^2$$

Proof

Let M_2 be the symmetric point of M_1 through the axis Oy and k, l be the slopes of the straight lines M_0M_1, M_0M_2. Then

$$k = \frac{y_0 - y_1}{x_0 - x_1} \neq 0 \tag{2.1}$$

$$l = \frac{y_0 - y_1}{x_0 + x_1} \neq 0 \tag{2.2}$$

Let the circle (C) intersect the axis Oy at $A(0, \sqrt{x_0^2 + y_0^2})$ and $B(0, -\sqrt{x_0^2 + y_0^2})$. Then the point M_0 is either on the arc M_1AM_2 or on the arc M_1BM_2 and the slopes of the straight lines M_0A, M_0B are, respectively

$$h = \frac{y_0 - \sqrt{x_0^2 + y_0^2}}{x_0} \tag{2.3}$$

$$g = \frac{y_0 + \sqrt{x_0^2 + y_0^2}}{x_0} \tag{2.4}$$

We start with the case the point M_0 is on the arc M_1BM_2. From the supposition, it follows that the point M_0 does not coincide with the points M_1, M_2, A.
If $1 + kh = 0$, i.e. the straight line M_0A is perpendicular to the straight line M_0M_1, then the point M_1 coincides with the point $B(0, -\sqrt{x_0^2 + y_0^2})$ and $x_1 = 0$. This is contrary to the supposition. Hence, $1 + kh \neq 0$.

If $1+lh=0$, i.e. the straight line M_0A is perpendicular to the straight line M_0M_2, then the point M_2 coincides with the point $B(0,-\sqrt{x_0^2+y_0^2})$ and $x_1=0$. This is contrary to the supposition. Hence, $1+lh\neq 0$.

Since $1+kh\neq 0, 1+lh\neq 0$ and the arc M_1A equals to the arc AM_2, we find

$$\frac{h-l}{1+hl}=\frac{k-h}{1+kh} \tag{2.5}$$

Or

$$(k+l)h^2+2(1-kl)h-(k+l)=0 \tag{2.6}$$

Let us consider (2.6) as a quadratic equation for h. Since $k+l=\frac{2x_0(y_0-y_1)}{x_0^2-x_1^2}\neq 0$, we get

$$h_{1,2}=\frac{kl-1+/-\sqrt{(k^2+1)(l^2+1)}}{k+l} \tag{2.7}$$

Or

$$h_{1,2}=\frac{y_0(y_0-y_1)+/-\sqrt{(x_0^2+y_0^2-y_0y_1)^2-(x_0x_1)^2}}{x_0(y_0-y_1)} \tag{2.8}$$

From $(2.3)\&(2.8)$, if $h=h_1$, then

$$\frac{y_0-\sqrt{x_0^2+y_0^2}}{x_0}=\frac{y_0(y_0-y_1)+\sqrt{(x_0^2+y_0^2-y_0y_1)^2-(x_0x_1)^2}}{x_0(y_0-y_1)} \tag{2.9}$$

Or

$$-(y_0-y_1)\sqrt{x_0^2+y_0^2}=\sqrt{(x_0^2+y_0^2-y_0y_1)^2-(x_0x_1)^2} \tag{2.10}$$

Squaring both members of (2.10) and rearranging,

$$\{x_0(y_0-y_1)\}^2+\{y_0(y_0-y_1)\}^2+(x_0x_1)^2=(x_0^2+y_0^2-y_0y_1)^2 \tag{2.11}$$

From $(2.3)\&(2.8)$, if $h=h_2$, then

$$\frac{y_0-\sqrt{{x_0}^2+{y_0}^2}}{x_0}=\frac{y_0(y_0-y_1)-\sqrt{({x_0}^2+{y_0}^2-y_0y_1)^2-(x_0x_1)^2}}{x_0(y_0-y_1)} \tag{2.12}$$

Or

$$-(y_0-y_1)\sqrt{{x_0}^2+{y_0}^2}=-\sqrt{({x_0}^2+{y_0}^2-y_0y_1)^2-(x_0x_1)^2} \tag{2.13}$$

Wherefrom follows equality (2.11).

In the case the point M_0 is on the arc M_1AM_2, by symmetry of A,B and h,g we easily obtain equality (2.11). Hence, lemma 2.1 is proved.

Theorem 2.1

Given in the plane Oxy a smooth curve (L): $f(x,y)=0$. Suppose that the curve (L) has a certain nonzero rational point $M_0(x_0,y_0)$ such that

1) $-\dfrac{f'_x(x_0,y_0)}{f'_y(x_0,y_0)}=k$ is a nonzero rational number.

2) $(k^2-1)x_0-2ky_0\neq 0$

3) $-2kx_0+(1-k^2)y_0\neq 0$

4) $kx_0-y_0\neq 0$

5) $x_0+ky_0\neq 0$

Then

$$\{2kx_0(x_0+ky_0)\}^2+\{2ky_0(x_0+ky_0)\}^2+\{(k^2-1){x_0}^2-2kx_0y_0\}^2=\{(k^2+1){x_0}^2+2kx_0y_0+2k^2{y_0}^2\}^2$$

Proof

In the plane Oxy, we introduce the circle (C) with center at the origin and passing through the point $M_0(x_0,y_0)$. Then, the equation of the tangent (δ) to the circle (C) at

the point $M_0(x_0, y_0)$ is $y = -\frac{x_0}{y_0}(x - x_0) + y_0$. Moreover, the equation of the tangent (Δ) to the curve (L) at the point $M_0(x_0, y_0)$ is $y = k(x - x_0) + y_0$, where k is its slope.

If the straight line (Δ) coincides with the straight line (δ), then $k = -\frac{x_0}{y_0}$. This is contrary to the supposition. For this reason, the straight line (Δ) intersects the circle (C) at two distinct points $M_0(x_0, y_0)$ and $M_1(x_1, y_1)$ such that

$$x_1 = \frac{(k^2 - 1)x_0 - 2ky_0}{k^2 + 1} \neq 0$$

$$y_1 = \frac{-2kx_0 + (1 - k^2)y_0}{k^2 + 1} \neq 0$$

From these equalities, we find

$$x_0 + x_1 = \frac{2k(kx_0 - y_0)}{k^2 + 1} \neq 0$$

$$x_0 - x_1 = \frac{2(x_0 + ky_0)}{k^2 + 1} \neq 0$$

$$y_0 - y_1 = \frac{2k(x_0 + ky_0)}{k^2 + 1} \neq 0$$

$$x_0 x_1 = \frac{(k^2 - 1){x_0}^2 - 2kx_0 y_0}{k^2 + 1}$$

$${x_0}^2 + {y_0}^2 - y_0 y_1 = \frac{(k^2 + 1){x_0}^2 + 2kx_0 y_0 + 2k^2 {y_0}^2}{k^2 + 1}$$

Then, we hold theorem 2.1 by lemma 2.1

Analogously, considering M_2 as the symmetric point of M_1 through the axis Ox will yield the following lemma and theorem.

Lemma 2.2

Given in the plane Oxy a circle $(C): x^2 + y^2 - r^2 = 0$. Suppose that the circle (C) has two distinct nonzero points $M_0(x_0, y_0), M_1(x_1, y_1)$ such that

1) $y_0 + y_1 \neq 0$

2) $x_0 - x_1 \neq 0$

3) $y_0 - y_1 \neq 0$

Then

$$\{x_0(x_0 - x_1)\}^2 + \{y_0(x_0 - x_1)\}^2 + (y_0 y_1)^2 = ({x_0}^2 + {y_0}^2 - x_0 x_1)^2$$

Theorem 2.2

Given in the plane Oxy a smooth curve $(L): f(x, y) = 0$. Suppose that the curve (L) has a certain nonzero rational point $M_0(x_0, y_0)$ such that

1) $-\dfrac{f'_x(x_0, y_0)}{f'_y(x_0, y_0)} = k$ is a nonzero rational number.

2) $(k^2 - 1)x_0 - 2ky_0 \neq 0$

3) $-2kx_0 + (1 - k^2)y_0 \neq 0$

4) $kx_0 - y_0 \neq 0$

5) $x_0 + ky_0 \neq 0$

Then

$$\{2x_0(x_0 + ky_0)\}^2 + \{2y_0(x_0 + ky_0)\}^2 + \{-2kx_0y_0 + (1 - k^2){y_0}^2\}^2 = \{2{x_0}^2 + 2kx_0y_0 + (k^2 + 1){y_0}^2\}^2$$

3. Application

To be continued, we will apply theorem 2.1 to prove FLT again. To do this, we obviously need another lemma.

Lemma 3.1

Given two different parity integers a,b. If $GCD(a,b)=1$, then there do not exist nonzero integers d,e,f,g,h with d odd such that

$$d(fg+eh)=a^{n-1}b(a^{n-2}-b^{n-2})$$

$$d(eg-fh)=a^{n-2}b^2(a^{n-2}-b^{n-2})$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2}$$

Or

$$d(fg+eh)=a^{n-2}b^2(a^{n-2}-b^{n-2})$$

$$d(eg-fh)=a^{n-1}b(a^{n-2}-b^{n-2})$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2}$$

where n is odd greater than 2 or equal to 4.

Proof

Assuming that there exist nonzero integers d,e,f,g,h with d odd such that

$$d(fg+eh)=u \tag{3.1}$$

$$d(eg-fh)=v \tag{3.2}$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2} \tag{3.3}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2} \tag{3.4}$$

where $u=a^{n-1}b(a^{n-2}-b^{n-2})$, $v=a^{n-2}b^2(a^{n-2}-b^{n-2})$.

Adding equations $(3.3)\&(3.4)$ term by term,

$$d(e^2+f^2)=a^{2n-4}(a^2+b^2)\neq 0 \tag{3.5}$$

It is clear that d is a positive integer.

Let us consider $(3.1)\&(3.2)$ as a system of two linear equations in two unknowns g,h and solve it

$$g=\frac{ev+fu}{d(e^2+f^2)}=\frac{b(a^{n-2}-b^{n-2})(eb+fa)}{a^{n-2}(a^2+b^2)} \tag{3.6}$$

$$h=\frac{eu-fv}{d(e^2+f^2)}=\frac{b(a^{n-2}-b^{n-2})(ea-fb)}{a^{n-2}(a^2+b^2)} \tag{3.7}$$

In the case n is odd greater than 2, since $GCD(a^{2n-4}-b^{2n-4},a^{2n-4}+b^{2n-4})=1$, a^2+b^2 is a divisor of $a^{2n-4}+b^{2n-4}$ and $a^{n-2}-b^{n-2}$ is a divisor of $a^{2n-4}-b^{2n-4}$, we have $GCD(a^2+b^2,a^{n-2}-b^{n-2})=1$, then $GCD(a^{n-2}(a^2+b^2),b(a^{n-2}-b^{n-2}))=1$. From $(3.6),(3.7)$, it follows that

$$eb+fa=i_1a^{n-2}(a^2+b^2) \tag{3.8}$$

$$ea-fb=i_2a^{n-2}(a^2+b^2) \tag{3.9}$$

where i_1,i_2 are nonzero integers.

Squaring both members of equation (3.8),

$$(eb)^2+2ebfa+(fa)^2=i_1^{\,2}a^{2n-4}(a^2+b^2)^2 \tag{3.10}$$

Squaring both members of equation (3.9),

$$(ea)^2-2eafb+(fb)^2=i_2^{\,2}a^{2n-4}(a^2+b^2)^2 \tag{3.11}$$

Adding equations $(3.10)\&(3.11)$ term by term,

$$(a^2+b^2)(e^2+f^2)=(i_1^{\,2}+i_2^{\,2})a^{2n-4}(a^2+b^2)^2 \tag{3.12}$$

From equations $(3.5)\&(3.12)$, we get

$$i_1^{\,2}+i_2^{\,2}=\frac{1}{d} \tag{3.13}$$

This is a contradiction.

In the case $n=4$, $(3.6)\&(3.7)$ become

$$g=\frac{ev+fu}{d(e^2+f^2)}=\frac{b(a^2-b^2)(eb+fa)}{a^2(a^2+b^2)} \tag{3.14}$$

$$h=\frac{eu-fv}{d(e^2+f^2)}=\frac{b(a^2-b^2)(ea-fb)}{a^2(a^2+b^2)} \tag{3.15}$$

Since $GCD(a^2-b^2,a^2+b^2)=1$, from $(3.14),(3.15)$ it follows that

$$eb+fa=j_1a^2(a^2+b^2) \tag{3.16}$$

$$ea-fb=j_2a^2(a^2+b^2) \tag{3.17}$$

where j_1, j_2 are nonzero integers. It is clear that this case also leads to a contradiction.

Next, considering the following system of equations in the same way will also lead to a contradiction.

$$d(fg+eh)=v$$

$$d(eg-fh)=u$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2}$$

Hence, lemma 3.1 is proved.

Theorem

For any integer n greater than 2, there are no nonzero rational points on the curve $x^n+y^n-1=0$.

Proof

It is clear that we are only necessary to prove the theorem for two cases:

Case 1: n is an odd number greater than 2.

Case 2: $n=4$.

Suppose that for any odd number n greater than 2 or equal to 4, the curve $(L): x^n + y^n - 1 = 0$ has a certain nonzero rational point $M_0(x_0, y_0)$. Without loss of generality, assume that $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$, where a, b, c are nonzero integers and relatively prime in pairs.

Let $m = \frac{x_0}{y_0} = \frac{a}{b}$. It is easy to see that $m \neq 0, m \neq 1$ and $m \neq -1$.

The slope of the tangent (Δ) to the curve (L) at the point $M_0(x_0, y_0)$ is $k = -m^{n-1} \neq 0$.

We have

$$(k^2 - 1)x_0 - 2ky_0 = (m^{2n-2} - 1)x_0 + 2m^{n-1}y_0 \tag{3.18}$$

If $(m^{2n-2} - 1)x_0 + 2m^{n-1}y_0 = 0$, then $(m^{2n-2} - 1)\frac{x_0}{y_0} + 2m^{n-1} = 0$ or

$$m^{2n-2} + 2m^{n-2} - 1 = 0 \tag{3.19}$$

The rational roots of equation (3.19) may be $m = 1$ or $m = -1$, if exist.

$$-2kx_0 + (1 - k^2)y_0 = 2m^{n-1}x_0 + (1 - m^{2n-2})y_0 \tag{3.20}$$

If $2m^{n-1}x_0 + (1 - m^{2n-2})y_0 = 0$, then $2m^{n-1}\frac{x_0}{y_0} + (1 - m^{2n-2}) = 0$ or

$$m^{2n-2} - 2m^n - 1 = 0 \tag{3.21}$$

The rational roots of equation (3.21) may be $m = 1$ or $m = -1$, if exist.

$$kx_0 - y_0 = -m^{n-1}x_0 - y_0 \tag{3.22}$$

If $-m^{n-1}x_0 - y_0 = 0$, then $-m^{n-1}\frac{x_0}{y_0} - 1 = 0$ or

$$m^n + 1 = 0 \tag{3.23}$$

The rational roots of equation (3.23) may be $m = 1$ or $m = -1$, if exist.

Nguyễn Tri Phương
54 Le Dai Hanh street, ward 7, district 11, Ho Chi Minh city, Viet Nam

$$ky_0 + x_0 = -m^{n-1}y_0 + x_0 \tag{3.24}$$

If $-m^{n-1}y_0 + x_0 = 0$, then $-m^{n-1} + \frac{x_0}{y_0} = 0$ or

$$m^{n-2} - 1 = 0 \tag{3.25}$$

The rational roots of equation (3.25) may be $m = 1$ or $m = -1$, if exist.

Therefore, by theorem 2.1

$$\{2kx_0(x_0 + ky_0)\}^2 + \{2ky_0(x_0 + ky_0)\}^2 + \{(k^2-1)x_0^{\,2} - 2kx_0y_0\}^2 = \{(k^2+1)x_0^{\,2} + 2kx_0y_0 + 2k^2y_0^{\,2}\}^2 \tag{3.26}$$

Or

$$y_0^{\,4}\left\{2k\frac{x_0}{y_0}(\frac{x_0}{y_0}+k)\right\}^2 + y_0^{\,4}\left\{2k(\frac{x_0}{y_0}+k)\right\}^2 + y_0^{\,4}\left\{(k^2-1)\frac{x_0^{\,2}}{y_0^{\,2}} - 2k\frac{x_0}{y_0}\right\}^2 = y_0^{\,4}\left\{(k^2+1)\frac{x_0^{\,2}}{y_0^{\,2}} + 2k\frac{x_0}{y_0} + 2k^2\right\}^2 \tag{3.27}$$

Since $y_0^{\,4} \neq 0$ and $m = \frac{x_0}{y_0}$, from (3.27) we find

$$m^4\{2m^{n-1}(m^{n-2}-1)\}^2 + m^4\{2m^{n-2}(m^{n-2}-1)\}^2 + m^4\{m^{2n-2} + 2m^{n-2} - 1\}^2 = m^4\{m^{2n-2} + 2m^{2n-4} - 2m^{n-2} + 1\}^2 \tag{3.28}$$

Since $m^4 \neq 0$, from (3.28) we have

$$\{2m^{n-1}(m^{n-2}-1)\}^2 + \{2m^{n-2}(m^{n-2}-1)\}^2 + \{m^{2n-2} + 2m^{n-2} - 1\}^2 = \{m^{2n-2} + 2m^{2n-4} - 2m^{n-2} + 1\}^2 \tag{3.29}$$

Replacing $m = \frac{a}{b}$ into (3.29) and simplifying,

$$\{2a^{n-1}b(a^{n-2}-b^{n-2})\}^2 + \{2a^{n-2}b^2(a^{n-2}-b^{n-2})\}^2 + \{a^{2n-2} + 2a^{n-2}b^n - b^{2n-2}\}^2 = \{a^{2n-2} + 2a^{2n-4}b^2 - 2a^{n-2}b^n + b^{2n-2}\}^2 \tag{3.30}$$

Since $GCD(a,b) = 1$, there only exist the two following cases:

Case a: The numbers a,b are of different parity (one is odd, one is even).

Case b: The numbers a,b are both odd.

In case a, for any odd number n greater than 2 or equal to 4, $2a^{n-1}b(a^{n-2}-b^{n-2})$, $2a^{n-2}b^2(a^{n-2}-b^{n-2})$ are even and $a^{2n-2}+2a^{n-2}b^n-b^{2n-2}$, $a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2}$ are odd. Thus, from (3.30), it is clear that the quadruple $\left[2a^{n-1}b(a^{n-2}-b^{n-2}), 2a^{n-2}b^2(a^{n-2}-b^{n-2}), a^{2n-2}+2a^{n-2}b^n-b^{2n-2}, a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2}\right]$ is a non-trivial integral solution of the equation $x^2+y^2+z^2=w^2$. As known, if so, then there exist nonzero integers d, e, f, g, h with d odd such that (see reference [1]).

$$2d(fg+eh)=2a^{n-1}b(a^{n-2}-b^{n-2}) \tag{3.31}$$

$$2d(eg-fh)=2a^{n-2}b^2(a^{n-2}-b^{n-2}) \tag{3.32}$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2} \tag{3.33}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2} \tag{3.34}$$

Or

$$2d(fg+eh)=2a^{n-2}b^2(a^{n-2}-b^{n-2}) \tag{3.35}$$

$$2d(eg-fh)=2a^{n-1}b(a^{n-2}-b^{n-2}) \tag{3.36}$$

$$d(e^2+f^2-g^2-h^2)=a^{2n-2}+2a^{n-2}b^n-b^{2n-2} \tag{3.37}$$

$$d(e^2+f^2+g^2+h^2)=a^{2n-2}+2a^{2n-4}b^2-2a^{n-2}b^n+b^{2n-2} \tag{3.38}$$

On the other hand, by lemma 3.1, from this fact it follows that $GCD(a,b)\neq 1$. This is contrary to the above supposition $GCD(a,b)=1$.

In case b, if n is an odd number greater than 2, then from $a^n+b^n=c^n$ we have $a^n=c^n+(-b)^n$. Let $A=c$, $B=-b$, $C=a$. Then $A^n+B^n=C^n$, where the integers A, B are of different parity. This contradicts case a.

In case b, if $n=4$, then from $a^4+b^4=c^4$ we have $c=2l$, where l is a nonzero integer. From here it follows that $\frac{a^4+b^4}{2}=8l^4$. This is a contradiction because $\frac{a^4+b^4}{2}$ is odd and $8l^4$ is even.

In short, there are no nonzero rational points on the curve (L). The theorem is proved.

References

[1] R.D. Carmichael, Diophantine analysis, Dover Publications Inc, New York (1959), p 28-34

[2] Sierpinski.Waclaw , Elementary theory of numbers, PWN-Polish Scientific Publishers, Warszawa (1964), p 35-36