Subjects: Number theory (math.NT) MSC classes: 11D41 Comments: 16 pages

Did Fermat prove Fermat's Last Theorem?

By Nguyễn Tri Phương

For my parents, HP & KP

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

I. INTRODUCTION

In about 1637, Pierre de Fermat (1601-1665), a French mathematician, annotated the following statement in the margin of his copy of Bachet's translation of Diophantus' Arithmetica

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere: cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

Nowadays, the above comment is comprehended 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, they have not found the trace of his proof of this assertion and despite of many mathematicians' attempts, over 350 years, the problem remained unsolved. Nevertheless, they have still called it Fermat's Last Theorem (FLT), which has become a source of inspiration for progression of mathematics. It was not until in 1994 Professor Andrew John Wiles proved successfully a special case of the Shimura-Taniyama conjecture that implies FLT. Due to complicatedness of Wiles' proof, most people in the world have believed that Fermat had a flaw in his proof. However, with a different viewpoint, we shall present an elegant proof of FLT in this paper.

II. NECESSARY THEOREMS FOR THE PROOF

We shall be using several theorems of elementary number theory as follows:

THEOREM 2.1. If a,b,m and n are integers, and if $c|a$ and $c|b$, then $c|ma+nb$

Nguyễn Tri Phương - phuong.tringuyen@gmail.com
54 Le Dai Hanh street, ward 7, district 11, Ho Chi Minh city, Viet Nam

Proof. Since $c|a$ and $c|b$, there are integers k and l such that $a=kc$ and $b=lc$. Therefore, $ma+nb=mkc+nlc=(mk+nl)c$ i.e. $c|ma+nb$

THEOREM 2.2. If a, b and k are integers, then $GDC(a+kb,b)=GDC(a,b)$

Proof. If m is a common divisor of $a+kb$ and b, by theorem 2.1, m divides $(a+kb)-kb=a$ so that m is a common divisor of a and b. Moreover, if l be a common divisor of a and b, by theorem 2.1, $l|a+kb$ so that l is a common divisor of $a+kb$ and b. Therefore, $GDC(a+kb,b)=GDC(a,b)$.

COROLLARY 2.2.1. If $GDC(a,b)=1$, then $GDC(a+b,b)=GDC(a-b,b)=1$.

THEOREM 2.3. If $GDC(a,b)=1$ and $c|a$, then $GDC(c,b)=1$.

Proof. Let $GDC(c,b)=d$. Then $d|c$, $d|b$, whence, in view of $c|a$, we obtain $d|a$. Consequently, d is a common divisor of a and b. But $GDC(a,b)=1$, thus $d=1$, which proves that $GDC(c,b)=1$.

THEOREM 2.4.. If a,b and c are integers such that $GCD(a,b)=1$ and $a|bc$, then $a|c$.

Proof. Since $GDC(a,b)=1$, there are integers k and l such that $ka+lb=1$. Multiplying both sides of this expression by c, we have $kca+lbc=c$. Since both a and bc are divisible by a, by theorem 2.1, a divides $kca+lbc=c$. Therefore, $a|c$.

THEOREM 2.5. If a,b and c are integers such that $GDC(a,b)=GCD(a,c)=1$, then $GDC(a,bc)=1$.

Proof. Let $d=GDC(a,bc)$ and $d_1=GDC(b,d)$. Then $d|a$, $d|bc$, $d_1|b$ and $d_1|d$, whence, we obtain $d_1|a$. From $d_1|a$, $d_1|b$ and $GDC(a,b)=1$ it follows that $d_1=1$. Thus, $GDC(b,d)=1$. From $d|bc$, by theorem 2.4, we have $d|c$. From $d|a$, $d|c$ and $GDC(a,c)=1$, we conclude that $d=1$ i.e. $GDC(a,bc)=1$.

COROLLARY 2.5.1. If $GDC(a,b)=1$ and n, m are natural numbers, then $GDC(a^n,b^m)=1$.

Proof. By an easy induction.

THEOREM 2.6. If a,b are positive integers such that $a|b$ and $b|a$ then $a=b$.

Proof. Since $a|b$ and $b|a$, there are integers k and l such that $a=kb$ and $b=la$. This implies that $a=kla$ so that $kl=1$. Therefore, either $k=l=1$ or $k=l=-1$. It follows that either $a=b$ or $a=-b$. Since $a,b>0$, we have $a=b$.

Nguyễn Tri Phương - phuong.tringuyen@gmail.com
54 Le Dai Hanh street, ward 7, district 11, Ho Chi Minh city, Viet Nam

THEOREM 2.7. If a,b are of different parity and $GDC(a,b)=1$, then $GDC(a+b,a-b)=1.$

Proof. Let $d=GDC(a+b,a-b)$. Then d is odd and there are integers k and l such that $a+b=kd$, $a-b=ld$, where k,l are both odd and $GDC(k,l)=1$. From here, we get $a=(\frac{k+l}{2})d,\ \ b=(\frac{k-l}{2})d$. This implies that d is a common divisor of a and b. Since $GDC(a,b)=1$, we have $d\,|1$ i.e. $GDC(a+b,a-b)=1.$

THEOREM 2.8. If a,b are both odd and $GDC(a,b)=1$, then $GDC(\frac{a+b}{2},\frac{a-b}{2})=1.$

Proof. Let $d=GDC(\frac{a+b}{2},\frac{a-b}{2})$. Then there are integers k and l such that $\frac{a+b}{2}=kd,$ $\frac{a-b}{2}=ld$, where $GDC(k,l)=1$. From here, we get $a=(k+l)d,\ \ b=(k-l)d$. This implies that d is a common divisor of a and b. Since $GDC(a,b)=1$, we have $d\,|1$ i.e. $GDC(\frac{a+b}{2},\frac{a-b}{2})=1.$

THEOREM 2.9. If a,b are both odd and $GDC(\frac{a+b}{2},\frac{a-b}{2})=1$, then $GDC(a,b)=1.$

Proof. Let $d=GDC(a,b)$. Then d is odd and there are integers k and l such that $a=kd,b=ld$, where k,l are both odd and $GDC(k,l)=1$. From here, we get $\frac{a+b}{2}=(\frac{k+l}{2})d,\ \ \frac{a-b}{2}=(\frac{k-l}{2})d$. This implies that d is a common divisor of $\frac{a+b}{2}$ and $\frac{a-b}{2}$. Since $GDC(\frac{a+b}{2},\frac{a-b}{2})=1$, we have $d\,|1$ i.e. $GDC(a,b)=1.$

THEOREM 2.10. If a,b are both odd and $GDC(a,b)=1$, then $GDC(ab,\frac{a^2+b^2}{2})=1.$

Proof. By theorem 2.8, we have $GDC(\frac{a+b}{2},\frac{a-b}{2})=1$. By corollary 2.5.1, we have $GDC((\frac{a+b}{2})^2,(\frac{a-b}{2})^2)=1$ or $GDC((\frac{\frac{a^2+b^2}{2}+ab}{2}),(\frac{\frac{a^2+b^2}{2}-ab}{2}))=1.$ By theorem 2.9, we conclude that $GDC(ab,\frac{a^2+b^2}{2})=1.$

THEOREM 2.11. If $GCD(a,b)=1$ and n, m are natural numbers, then $GCD((a+b)^n,b^m)=1$ and $GCD((a-b)^n,b^m)=1.$

Proof. It follows directly from corollary 2.2.1 and corollary 2.5.1.

THEOREM 2.12. If a,b are of different parity and $GDC(a,b)=1$ and n is a natural number, then $GDC(a^n+b^n,a^n-b^n)=1.$

Proof. It follows directly from corollary 2.5.1 and theorem 2.7

THEOREM 2.13. If n is an odd natural number and m is a natural number, then a^m+b^m is a divisor of $a^{mn}+b^{mn}$.

Proof. Let k be an arbitrary divisor of a^m+b^m. Then there is an integer l such that $a^m+b^m=lk$ or $a^m=-b^m+lk$. Raising both sides of this expression to the mn^{th} power, we have, by the binomial theorem, $a^{mn}=-b^{mn}+(b^{m(n-1)}l+...-b^m l^{n-1}k^{n-2}+l^n k^{n-1})k$ or $a^{mn}+b^{mn}=(b^{m(n-1)}l+...-b^m l^{n-1}k^{n-2}+l^n k^{n-1})k$. This means k is a divisor of $a^{mn}+b^{mn}$. The theorem is proved.

THEOREM 2.14. If n is an even natural number and m is a natural number, then a^m+b^m is a divisor of $a^{mn}-b^{mn}$.

Proof. as that of theorem 2.13.

THEOREM 2.15. Given equation $a_0x^m+a_1x^{m-1}+...+a_{m-1}x+a_m=0$ (1), where m is a natural number and $a_0,a_1....a_m$ are integers with $a_0\neq 0$ and $a_m\neq 0$.

If $\frac{k}{s}$ is a rational root of equation (1), where s is a natural number, k an integer and $GCD(k,s)=1$ then k and s are respectively divisors of a_m and a_0

Proof. From equation (1), for $x=\frac{k}{s}$, we obtain

$$a_0k^m=-(a_1k^{m-1}+...+a_{m-1}ks^{m-2}+a_ms^{m-1})s$$

$$a_ms^m=-(a_0k^{m-1}+a_1k^{m-2}s+...+a_{m-1}s^{m-1})k$$

The first of these equations proves that s is a divisor of a_0k^m. From $GCD(k,s)=1$, by corollary 2.5.1 and theorem 2.4, we have s is a divisor of a_0. The second shows that k is a divisor of a_ms^m. Similarly, from $GCD(k,s)=1$, we obtain k is a divisor of a_m.

THEOREM 2.16. Given $x^2+y^2+z^2=m^2$ with z odd and $GCD(x,y,z)=1$, there exist integers u,v,w and t such that

$$\begin{aligned} x &= 2(uw - vt) \\ y &= 2(ut + vw) \\ z^2 &= u^2 + v^2 - w^2 - t^2 \\ m^2 &= u^2 + v^2 + w^2 + t^2 \end{aligned} \tag{2.1}$$

Proof. We quote from [2].

Set $x_1 = \frac{x}{2}$ and $y_1 = \frac{y}{2}$. Then

$$x_1^{\,2} + y_1^{\,2} = (\frac{m+z}{2})(\frac{m-z}{2})$$

Set $f = (x_1, y_1)$, $f_1 = (f, \frac{m+z}{2})$ and $f_2 = (f, \frac{m-z}{2})$. By an easy argument one sees that $(f_1, f_2) = 1$, and $f = f_1 f_2$. Set $x_2 = \frac{x_1}{f}$, $y_2 = \frac{y_1}{f}$, $z_1 = \frac{m+z}{2f_1^{\,2}}$ and $z_2 = \frac{m-z}{2f_2^{\,2}}$. Then

$$x_2^{\,2} + y_2^{\,2} = z_1 z_2$$

where $(x_2, y_2) = 1$. Note that z_1 and z_2 are not necessarily relatively prime.

Let

$$x_2 + iy_2 = \prod_{j=1}^{n} X_j$$

be a factorization into Gaussian primes. Note that $x_2 + iy_2$ cannot be divisible by a rational prime p. For if so, then $\frac{(x_2 + iy_2)}{p} = a + ib$, $x_2 = pa$, $y_2 = pb$, a contradiction, as $(x_2, y_2) = 1$. Hence, none of the X_j's is a rational prime $\equiv 3 (\mathrm{mod}\, 4)$.

Now

$$x_2 - iy_2 = \prod_{j=1}^{n} \bar{X}_j$$

and $z_1 z_2 = \prod_{j=1}^{n} (X_j \bar{X}_j)$, $z_1 = \prod_{j=1}^{m} (X_j \bar{X}_j)$, $z_2 = \prod_{j=m+1}^{n} (X_j \bar{X}_j)$

if we write the X_j's in a suitable order. Set

$$u_1 + iv_1 = \prod_{j=1}^{m} X_j, \qquad w_1 + it_1 = \prod_{j=m+1}^{n} X_j$$

Then

$$z_1 = (u_1 + iv_1)(u_1 - iv_1),\ z_2 = (w_1 + it_1)(w_1 - it_1),\ x_2 + iy_2 = (u_1 + iv_1)(w_1 + it_1)$$

Since, given any $\overline{X}_j$ dividing $u_1 - iv_1$, we cannot have $\overline{X}_j(u_1 + iv_1) | (x_2 + iy_2)$,

(for then a rational prime would divide $x_2 + iy_2$), we have $u_1 + iv_1 = GDC(z_1, x_2 + iy_2)$

Similarly, $w_1 + it_1 = GDC(z_2, x_2 + iy_2)$.

Setting $u = f_1 u_1$, $v = f_1 v_1$, $w = f_2 w_1$ and $t = f_2 t_1$, we now easily obtain equations (2.1).

III. RESTATING AND PROVING FLT

Though Fermat stated his theorem in positive integers, we have believed that he constructed it from rational numbers. Therefore, our approach is the curve $x^n + y^n - 1 = 0$ and FLT is restated in the form

THEOREM

There are no nonzero rational points on the curve $x^n + y^n - 1 = 0$ for any integer exponent $n > 2$.

Proof. Obviously, if FLT is true for a particular n, then it is also true for all exponents that are multiples of n. Since every integer n greater than 2 is divisible by either 4 or some odd integer, it shall suffice to demonstrate the validity of the theorem when n is any odd number greater than 2 and when $n = 4$.

We shall use proof by contradiction. That is, we shall assume that there exists a certain nonzero rational point. Then we show that this implies a quadratic equation both roots of which are omitted by their nonsensicality.

Suppose that for any odd number n greater than 2 or $n = 4$, there is a certain nonzero rational point $M_0(x_0, y_0)$ on the curve $(L): x^n + y^n - 1 = 0$ There is no loss of generality in assuming that $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$, where a, b, c are nonzero integers and relatively prime in pairs.

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

Case 1: The numbers a, b are of different parity.

Case 2: The numbers a, b are both odd.

The following remark is worthwhile for case 2.

For any odd number n greater than 2, if $a^n + b^n = c^n$, then we get $a^n = c^n + (-b)^n$. Let $A = c$, $B = -b$, $C = a$. Then $A^n + B^n = C^n$, where A, B are of different parity. This is case 1.

If $a^4 + b^4 = c^4$ then c is even. Let $c = 2u$, where u is a nonzero integer. Then $a^4 + b^4 = (2u)^4$ or $\frac{a^4 + b^4}{2} = 8u^4$. This is impossible because $\frac{a^4 + b^4}{2}$ is odd but $8u^4$ even.

Therefore, we are only concerned case 1. From now on, we assume that the numbers a, b are of different parity and relatively prime.

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

In the plane Oxy, if we call (Δ) the tangent to (L) at $M_0(x_0, y_0)$, (C) the circle with center at the origin and passes through $M_0(x_0, y_0)$, (δ) the tangent to (C) at $M_0(x_0, y_0)$, then the equations of (Δ) and (δ) are respectively $y = -m^{n-1}(x - x_0) + y_0$ and $y = -m(x - x_0) + y_0$. We shall examine the intersection of the straight line (Δ) and the circle (C).

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

$$-m^{n-1} = -m \tag{3.1}$$

or

$$m^{n-2} - 1 = 0 \tag{3.2}$$

By theorem 2.15, the rational solutions of equation (3.2) may be $m = 1$ or $m = -1$, if exist. 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

$$x_1 = \frac{(m^{2n-2} - 1)x_0 + 2m^{n-1}y_0}{m^{2n-2} + 1} \tag{3.3}$$

$$y_1 = \frac{2m^{n-1}x_0 + (1 - m^{2n-2})y_0}{m^{2n-2} + 1} \tag{3.4}$$

From $(3.3), (3.4)$ and $y_0 \neq 0$,

$$\frac{x_1}{y_0} = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \tag{3.5}$$

$$\frac{y_1}{y_0} = \frac{-m^{2n-2} + 2m^n + 1}{m^{2n-2} + 1} \tag{3.6}$$

If $x_1 = 0$, then $m^{2n-2} + 2m^{n-2} - 1 = 0$.

If $y_1 = 0$, then $m^{2n-2} - 2m^n - 1 = 0$.

These equations have no rational solutions. Hence, $x_1 \neq 0$ and $y_1 \neq 0$.

Let $\frac{x_1}{y_0} = \frac{d}{e}$ and $\frac{y_1}{y_0} = \frac{r}{s}$, where d, e, r, s are nonzero integers, $GCD(d,e) = 1$ and $GCD(r,s) = 1$. Then from (3.5) and (3.6), we obtain the following system of equations:

$$em^{2n-1} - dm^{2n-2} + 2em^{n-1} - em - d = 0 \tag{3.7}$$

$$(r+s)m^{2n-2} - 2sm^n + r - s = 0 \tag{3.8}$$

Since $m = \frac{a}{b}$ is a rational solution of equation (3.7), by theorem 2.15, we have $d = pa$ and $e = qb$, where p, q are nonzero integers and $GCD(p,q) = 1$. Thus,

$$\frac{d}{e} = \frac{pa}{qb} = \frac{p}{q}m = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \tag{3.9}$$

Cancelling $m \neq 0$ on both sides of equation (3.9),

$$\frac{p}{q} = \frac{m^{2n-2} + 2m^{n-2} - 1}{m^{2n-2} + 1} \tag{3.10}$$

or

$$(p-q)m^{2n-2} - 2qm^{n-2} + p + q = 0 \tag{3.11}$$

If $r + s = 0$, we get from (3.8)

$$m^n + 1 = 0 \tag{3.12}$$

If $r - s = 0$, we get from (3.8)

$$m^{n-2} - 1 = 0 \tag{3.13}$$

If $p + q = 0$, we get from (3.11)

$$m^n + 1 = 0 \tag{3.14}$$

If $p - q = 0$, we get from (3.11)

$$m^{n-2}-1=0 \tag{3.15}$$

The rational solutions of these four equations may be $m=1$ or $m=-1$, if exist.

Consequently, $r+s,\ r-s,\ p+q$ and $p-q$ are nonzero integers.

From (3.8) and (3.11),

$$2sm^n=(r+s)m^{2n-2}+r-s \tag{3.16}$$

$$2qm^{n-2}=(p-q)m^{2n-2}+p+q \tag{3.17}$$

Multiplying two equations $(3.16),(3.17)$,

$$4sqm^{2n-2}=\left\{(r+s)m^{2n-2}+r-s\right\}\left\{(p-q)m^{2n-2}+p+q\right\} \tag{3.18}$$

Let $m^{2n-2}=t$. Then, by $(p-q)(r+s)\neq 0$, equation (3.18) may be rewritten as a quadratic equation for t

$$(p-q)(r+s)t^2+2(pr-qs)t+(p+q)(r-s)=0 \tag{3.19}$$

Two roots of equation (3.19) are

$$t_1=-1 \tag{3.20}$$

and

$$t_2=\frac{(p+q)(s-r)}{(p-q)(s+r)} \tag{3.21}$$

If $t=t_1$, this implies that $m^{2n-2}+1=0$. Since this equation has no rational solutions, the first root is omitted.

Next, we shall verify that the second root is also omitted by proving that it shall yield the fact that $4a^{n-1}b^{n-1}(a^{n-2}-b^{n-2})(a^n+b^n)$ is not a nonzero integer. Indeed, if $t=t_2$, from (3.16) and (3.17) we deduce

$$m^n=\frac{q(s-r)}{s(p-q)} \tag{3.22}$$

$$m^{n-2}=\frac{s(p+q)}{q(s+r)} \tag{3.23}$$

Dividing two equations $(3.22),(3.23)$,

$$m^2 = \frac{q^2(s^2 - r^2)}{s^2(p^2 - q^2)} \tag{3.24}$$

Raising both sides of equation (3.24) to the $2(n-1)^{th}$ power,

$$m^{2(n-1)} = \frac{q^{2(n-1)}(s+r)^{n-1}(s-r)^{n-1}}{s^{2(n-1)}(p+q)^{n-1}(p-q)^{n-1}} \tag{3.25}$$

From (3.21) and (3.25),

$$\frac{(p+q)(s-r)}{(p-q)(s+r)} = \frac{q^{2(n-1)}(s+r)^{n-1}(s-r)^{n-1}}{s^{2(n-1)}(p+q)^{n-1}(p-q)^{n-1}} \tag{3.26}$$

or

$$s^{2(n-1)}(p+q)^n(p-q)^{n-2} = q^{2(n-1)}(s+r)^n(s-r)^{n-2} \tag{3.27}$$

From $GCD(p,q)=1$, by theorem 2.11, we have $GCD((p+q)^n, q^{2n-2}) = 1$ and $GCD((p-q)^{n-2}, q^{2n-2}) = 1$. Hence, $q^{2(n-1)}$ is a divisor of $s^{2(n-1)}$ in view of theorem 2.4. Moreover, from $GCD(s,r)=1$, we have $s^{2(n-1)}$ is a divisor of $q^{2(n-1)}$ in the same way. From these results, by theorem 2.6, we have $s^{2(n-1)} = q^{2(n-1)}$. Notice that we may always assume that p,r are nonzero integers and q,s positive integers for the fractions $\frac{p}{q}$ and $\frac{r}{s}$ because the role of $-p,-r$ are the same as the role of p,r. Thus, we conclude that $s = q$. Then, (3.21) becomes

$$-a^{2n-2}(p-q)(q+r) + b^{2n-2}(p+q)(q-r) = 0 \tag{3.28}$$

Let $b^{n-1} = a^{n-1} + f$, in which f is a nonzero integer. Then (3.28) becomes

$$(p+q)(q-r)f^2 + 2a^{n-1}(p+q)(q-r)f + a^{2n-2}\{(p+q)(q-r) - (p-q)(q+r)\} = 0 \tag{3.29}$$

Since $(p+q)(q-r) \neq 0$, expression (3.29) may be considered as a quadratic equation for f. Since f is a nonzero integer, the discriminant of equation (3.29) must be a perfect square. This means

$$(p^2 - q^2)(q^2 - r^2) = g^2 \tag{3.30}$$

where g is a certain nonzero integer.

On the other hand, by substituting $m=\frac{a}{b}$ in (3.10) and (3.6), we get

$$\frac{p}{q}=\frac{m^{2n-2}+2m^{n-2}-1}{m^{2n-2}+1}=\frac{a^{2n-2}+2a^{n-2}b^{n}-b^{2n-2}}{a^{2n-2}+b^{2n-2}} \tag{3.31}$$

$$\frac{r}{q}=\frac{-m^{2n-2}+2m^{n}+1}{m^{2n-2}+1}=\frac{-a^{2n-2}+2a^{n}b^{n-2}+b^{2n-2}}{a^{2n-2}+b^{2n-2}} \tag{3.32}$$

Wherefrom follows,

$$p+r=\frac{2a^{n-2}b^{n-2}(a^2+b^2)q}{a^{2n-2}+b^{2n-2}} \tag{3.33}$$

$$p-r=\frac{2(a^{n-2}-b^{n-2})(a^{n}+b^{n})q}{a^{2n-2}+b^{2n-2}} \tag{3.34}$$

It is clear that $p+r$ and $p-r$ are nonzero integers.

For any odd number n greater than 2, since $GCD(a^{2n-2}-b^{2n-2},a^{2n-2}+b^{2n-2})=1$ and, by theorem 2.14, a^2+b^2 is a divisor of $a^{2n-2}-b^{2n-2}$, we have $GCD(a^2+b^2,a^{2n-2}+b^{2n-2})=1$ in view of theorem 2.3. From (3.33) it follows that $a^{2n-2}+b^{2n-2}$ is a divisor of q. Moreover, from (3.31) and $GCD(p,q)=1$ we see q is a divisor of $a^{2n-2}+b^{2n-2}$. Therefore, by theorem 2.6,

$$q=a^{2n-2}+b^{2n-2} \tag{3.35}$$

From (3.33), (3.34) and (3.35) we find

$$p+r=2a^{n-2}b^{n-2}(a^2+b^2) \tag{3.36}$$

$$p-r=2(a^{n-2}-b^{n-2})(a^{n}+b^{n}) \tag{3.37}$$

It is plain that p,q,r and $\frac{p^2+r^2}{2}$ are all odd.

Besides, solving (3.28) and (3.35) as a system of two linear equations in two unknowns a^{2n-2}, b^{2n-2}

$$a^{2n-2}=\frac{(p+q)(q-r)}{2(p-r)} \tag{3.38}$$

$$b^{2n-2} = \frac{(p-q)(q+r)}{2(p-r)} \tag{3.39}$$

Multiplying two expressions $(3.38),(3.39)$,

$$a^{2n-2}b^{2n-2} = \frac{(p^2-q^2)(q^2-r^2)}{4(p-r)^2} \tag{3.40}$$

Multiplying both sides of expression (3.40) by $4(p-r)^2 \neq 0$

$$(p^2-q^2)(q^2-r^2) = \left\{2(p-r)a^{n-1}b^{n-1}\right\}^2 \tag{3.41}$$

Substituting the value of $p-r$ above in (3.41),

$$(p^2-q^2)(q^2-r^2) = \left\{4a^{n-1}b^{n-1}(a^{n-2}-b^{n-2})(a^n+b^n)\right\}^2 \tag{3.42}$$

Now, let us rewrite condition (3.30) as

$$g^2 + (q^2 - \frac{p^2+r^2}{2})^2 + (pr)^2 = (\frac{p^2+r^2}{2})^2 \tag{3.43}$$

If $q^2 - \frac{p^2+r^2}{2} = 0$, it means $p^2-q^2 = q^2-r^2$, then from (3.24) it follows that $m^2 = 1$, which is contrary to the above assumption.

If $q^2 - \frac{p^2+r^2}{2} \neq 0$, then the quadruple $\left[g, q^2 - \frac{p^2+r^2}{2}, pr, \frac{p^2+r^2}{2}\right]$ is an integral solution of the equation $x^2+y^2+z^2 = w^2$.

Since a^2+b^2, $a^{n-2}-b^{n-2}$ are respectively divisors of $a^{2n-4}+b^{2n-4}$, $a^{2n-4}-b^{2n-4}$ and $GCD(a^{2n-4}+b^{2n-4}, a^{2n-4}-b^{2n-4}) = 1$, we have $GCD(a^2+b^2, a^{n-2}-b^{n-2}) = 1$. Moreover, since a^2+b^2, a^n+b^n are respectively divisors of $a^{2n}+b^{2n}$, $a^{2n}-b^{2n}$ and $GCD(a^{2n}+b^{2n}, a^{2n}-b^{2n}) = 1$, we see $GCD(a^2+b^2, a^n+b^n) = 1$. Hence, $GCD(\frac{p+r}{2}, \frac{p-r}{2}) = 1$. This implies $GCD(p,r) = 1$, whence, by theorem 2.10, $GCD(pr, \frac{p^2+r^2}{2}) = 1$. Therefore, by theorem 2.16, there exist integers i, j, k, l such that

$$g = 2(jk+il) \tag{3.44}$$

$$q^2 - \frac{p^2 + r^2}{2} = 2(ik - jl) \tag{3.45}$$

$$pr = i^2 + j^2 - k^2 - l^2 \tag{3.46}$$

$$\frac{p^2 + r^2}{2} = i^2 + j^2 + k^2 + l^2 \tag{3.47}$$

Adding two equations $(3.46), (3.47)$ and then dividing both sides of the result equation by 2,

$$(\frac{p+r}{2})^2 = i^2 + j^2 \tag{3.48}$$

Solving (3.44) and (3.45) as a system of two linear equations in two unknowns k, l

$$k = \frac{\frac{2q^2 - p^2 - r^2}{4} i + \frac{g}{2} j}{i^2 + j^2} \tag{3.49}$$

$$l = \frac{\frac{g}{2} i - \frac{2q^2 - p^2 - r^2}{4} j}{i^2 + j^2} \tag{3.50}$$

From (3.36) and (3.37), we get

$$(\frac{p+r}{2})^2 = a^{2n-4} b^{2n-4} (a^2 + b^2)^2 \tag{3.51}$$

$$\frac{2q^2 - p^2 - r^2}{4} = \frac{2q^2 - \left\{ \frac{(p+r)^2 + (p-r)^2}{2} \right\}}{4} = a^{n-2} b^{n-2} (a^{n-2} - b^{n-2})(a^n + b^n)(a^2 - b^2) \tag{3.52}$$

From (3.30) and (3.42), we deduce

$$\left\{ 4a^{n-1} b^{n-1} (a^{n-2} - b^{n-2})(a^n + b^n) - g \right\} \left\{ 4a^{n-1} b^{n-1} (a^{n-2} - b^{n-2})(a^n + b^n) + g \right\} = 0 \tag{3.53}$$

If $4a^{n-1} b^{n-1} (a^{n-2} - b^{n-2})(a^n + b^n) = g$, then from $(3.48), (3.49), (3.50)$ (3.51) and (3.52) we find

$$k = \frac{(a^{n-2} - b^{n-2})(a^n + b^n) \left\{ (a^2 - b^2) i + 2abj \right\}}{a^{n-2} b^{n-2} (a^2 + b^2)^2} \tag{3.54}$$

$$l=\frac{(a^{n-2}-b^{n-2})(a^n+b^n)\{2abi-(a^2-b^2)j\}}{a^{n-2}b^{n-2}(a^2+b^2)^2} \tag{3.55}$$

Since $GCD((a^{n-2}-b^{n-2})(a^n+b^n),a^{n-2}b^{n-2}(a^2+b^2)^2)=1$, from $(3.54),(3.55)$, by theorem 2.4, we have

$$(a^2-b^2)i+2abj=h_1a^{n-2}b^{n-2}(a^2+b^2)^2 \tag{3.56}$$

$$2abi-(a^2-b^2)j=h_2a^{n-2}b^{n-2}(a^2+b^2)^2 \tag{3.57}$$

where h_1 and h_2 are nonzero integers.

Squaring both sides of expression (3.56),

$$\{(a^2-b^2)i\}^2+2(2abj)\{(a^2-b^2)i\}+(2abj)^2=h_1^2a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.58}$$

Squaring both sides of expression (3.57),

$$(2abi)^2-2(2abi)\{(a^2-b^2)j\}+\{(a^2-b^2)j\}^2=h_2^2a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.59}$$

Adding two expressions $(3.58),(3.59)$,

$$\{(2ab)^2+(a^2-b^2)^2\}(i^2+j^2)=(h_1^2+h_2^2)a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.60}$$

From $(3.48),(3.51)$ and (3.60), it is easily seen that

$$h_1^2+h_2^2=1 \tag{3.61}$$

This is unreasonable.

If $4a^{n-1}b^{n-1}(a^{n-2}-b^{n-2})(a^n+b^n)=-g$, then from $(3.48),(3.49),(3.50)$ (3.51) and (3.52) we find

$$k=\frac{(a^{n-2}-b^{n-2})(a^n+b^n)\{(a^2-b^2)i-2abj\}}{a^{n-2}b^{n-2}(a^2+b^2)^2} \tag{3.62}$$

$$l=\frac{-(a^{n-2}-b^{n-2})(a^n+b^n)\{2abi+(a^2-b^2)j\}}{a^{n-2}b^{n-2}(a^2+b^2)^2} \tag{3.63}$$

Since $GCD((a^{n-2}-b^{n-2})(a^n+b^n),a^{n-2}b^{n-2}(a^2+b^2)^2)=1$, from $(3.62),(3.63)$, by theorem 2.4, we have

$$(a^2-b^2)i-2abj=h_3a^{n-2}b^{n-2}(a^2+b^2)^2 \tag{3.64}$$

$$2abi+(a^2-b^2)j=h_4a^{n-2}b^{n-2}(a^2+b^2)^2 \tag{3.65}$$

where h_3 and h_4 are nonzero integers.

Squaring both sides of expression (3.64),

$$\left\{(a^2-b^2)i\right\}^2-2(2abj)\left\{(a^2-b^2)i\right\}+(2abj)^2=h_3{}^2a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.66}$$

Squaring both sides of expression (3.65),

$$(2abi)^2+2(2abi)\left\{(a^2-b^2)j\right\}+\left\{(a^2-b^2)j\right\}^2=h_4{}^2a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.67}$$

Adding two expressions $(3.66),(3.67)$,

$$\left\{(2ab)^2+(a^2-b^2)^2\right\}(i^2+j^2)=(h_3{}^2+h_4{}^2)a^{2n-4}b^{2n-4}(a^2+b^2)^4 \tag{3.68}$$

From $(3.48),(3.51)$ and (3.68), it is easily seen that

$$h_3{}^2+h_4{}^2=1 \tag{3.69}$$

This is absurd.

For $n=4$, (3.31), (3.33) and (3.34) become,

$$\frac{p}{q}=\frac{a^6+2a^2b^4-b^6}{a^6+b^6} \tag{3.70}$$

$$p+r=\frac{2a^2b^2(a^2+b^2)q}{a^6+b^6} \tag{3.71}$$

$$p-r=\frac{2(a^2-b^2)(a^4+b^4)q}{a^6+b^6} \tag{3.72}$$

Since a^2-b^2 is a divisor of a^6-b^6 and $GCD(a^6-b^6,a^6+b^6)=1$, we have $GCD(a^2-b^2,a^6+b^6)=1$. Furthermore, since a^4+b^4, a^6+b^6 are respectively divisors of $a^{12}+b^{12}$, $a^{12}-b^{12}$ and $GCD(a^{12}-b^{12},a^{12}+b^{12})=1$, we have $GCD(a^4+b^4,a^6+b^6)=1$. From (3.72) it follows that a^6+b^6 is a divisor of q. In addition, from (3.70) and $GCD(p,q)=1$, we see q is a divisor of a^6+b^6. Therefore, by theorem 2.6, we conclude that

$$q=a^6+b^6 \tag{3.73}$$

From (3.71), (3.72) and (3.73) we find

$$p + r = 2a^2b^2(a^2 + b^2) \tag{3.74}$$

$$p - r = 2(a^2 - b^2)(a^4 + b^4) \tag{3.75}$$

It is evident that $GCD(\frac{p+r}{2}, \frac{p-r}{2}) = 1$. This implies $GCD(p, r) = 1$, whence, by theorem 2.10, $GCD(pr, \frac{p^2 + r^2}{2}) = 1$. Similarly, this case also yields a contradiction by the same reasoning used in the proof of the previous case. The theorem has been proved.

References

[1] Sierpinski.Waclaw , Elementary theory of numbers, PWN-Polish Scientific Publishers, Warszawa (1964)

[2] R. Spira, The diophantine equation $x^2 + y^2 + z^2 = m^2$, Amer. Math. Monthly 69 (1962), p 360-361.