Proof of the Fermat’s Last Theorem

Michael Pogorsky

mpogorsky@yahoo.com

Abstract

This is one of the versions of proof of the Theorem developed by means of general algebra and based on polynomials $a = uwv + v^n$; $b = uwv + w^n$; $c = uwv + v^n + w^n$ and their modifications. The polynomials are deduced as required for *a, b, c* to satisfy equation $a^n + b^n = c^n$. The equation also requires existence of positive integers u_p and c_p such that $a + b$ is divisible by u_p^n and c is divisible by $c_p u_p$. Based on these conclusions the contradiction in polynomial equation F(u)=0 is revealed. It proves the Theorem

Keywords: *Fermat’s Last Theorem, Proof, Binomial Theorem, Polynomial, Prime number, Polynomial equation.*

1. Introduction

Though the FLT belongs to the number theory it is taken in this proof rather as a problem of algebra. All means used to build this proof are elementary and well known from courses of general algebra. The proof is based on binomial theorem that allowed to deduce polynomial expressions of terms *a*, *b*, *c* required for them to satisfy as integers equation.

$$a^n + b^n = c^n \qquad (1)$$

According to the Fermat's Last Theorem (FLT) it cannot be true when *a, b, c* and *n* are positive integers and *n>2*

Lemma-1. When *n* is a prime number the coefficients at all middle terms of the expanded by binomial theorem $(\alpha + \beta)^n$ are divided by *n*.

Proof. This is well known (see Pascal’s Triangle).

Lemma-2 The sum $\alpha_1\beta + \alpha_2\beta + \cdots + \alpha_{n-1}\beta + \alpha_n$ with $\alpha_1, \alpha_2, \dots \alpha_n, \beta$ - integers and α_n coprime with β is not divisible by β.

Proof. Assume $\alpha_1\beta + \alpha_2\beta + \cdots + \alpha_{n-1}\beta + \alpha_n = A\beta$

Then $\beta[A - (\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1})] = \alpha_n$ i.e β must divide coprime α_n.

Lemma-3. When integers *A* and coprime *B* and *C* are related as $A^n = BC$ then both *B* and *C* are numbers to the power *n*.

Proof. Assume s is a prime and s^m is factor of *A*.

Then A^n is divisible by s^{mn}. Let *mn = p+t* with *p* and *t* coprime with *n*.

Since *B* and *C* are coprime only one of them can be divided by s^{p+t} i.e. it must be to the power *n*. Then both *B* and *C* must have all their divisors to the power *n*..

2. The Proof

It is assumed that *a*, *b*, *c* are coprime integers and n is a prime number.

Assume the equation (1) is true.

Let us express

$$c = a + k = b + f \qquad (2)$$

Obviously *k* and ***f*** are integers. Then

$$a^n + b^n = (a+k)^n = (b+f)^n \qquad (3)$$

After expansion of sums in parentheses by binomial theorem we obtain

$$a^n = f[nb^{n-1} + \frac{1}{2}n(n-1)b^{n-2}f + \cdots + f^{n-1}] \qquad (4a)$$

$$b^n = k[na^{n-1} + \frac{1}{2}n(n-1)a^{n-2}k + \cdots + k^{n-1}] \qquad (4b)$$

Since *f* divides a^n and *k* divides b^n they are coprime. Only first terms of the sums in brackets are not divided by *f* in Eq.(4a) and by *k* in Eq.(4b) and only last terms are not divided respectively by *b* and *a***.**

In both equations (4a) and (4b) last terms have no factor *n***.**

There are two equally possible cases.
A**:** *n* divides neither *f* nor *k*;
B: *n* divides either *f* or *k*. The case B will be discussed separately.

2.1. Case A

Here *n* is assumed to be coprime with *f* and *k*.

Lemma-4. There exist positive integersv, p, w, q, such that in the equation (1) $a = vp$ and $b = wq$

Proof. According to Lemma-2 the sums in brackets are coprime with *f* in Eq.(4a) and with *k* in Eq.(4b) and are not divided by *n*

According to Lemma-3 there must exist positive integers *v* and *w* satisfying in the equations (4a) and (4b)

$$f = v^n \qquad (5a)$$

$$k = w^n \qquad (5b)$$

There also must exist positive integers *p* and *q* that satisfy in equations **(**4a) and **(**4b)

$$p^n = nb^{n-1} + \frac{1}{2}n(n-1)b^{n-2}f + \cdots + f^{n-1} \qquad (6a)$$

$$q^n = na^{n-1} + \frac{1}{2}n(n-1)a^{n-2}k + \cdots + k^{n-1} \qquad (6b)$$

Now the equations **(**4a) and (4b) can be presented as $a^n = v^n p^n$ and $b^n = w^n q^n$
and we obtain

$$a = vp \qquad (7a)$$

$$b = wq \qquad (7b)$$

Lemma-5. For equation (1) with *a* = *vp* and *b* = *wq* there exists a positive integer *u* such that

$$a = uwv + v^n \ ;$$
$$b = uwv + w^n \ ;$$
$$c = uwv + v^n + w^n \ .$$

Proof. With regard to equations (5a), (5b), (7a), and (7b) the expression (2) becomes

$$vp + w^n = wq + v^n \qquad (8)$$

After regrouping we obtain

$$v(p - v^{n-1}) = w(q - w^{n-1}) \qquad (9)$$

Since *v* and w are mutually coprime each of them must divide a polynomial in parentheses on the opposite side of the equation.
Now the equation (9) can be rewritten as

$$\frac{p - v^{n-1}}{w} = \frac{q - w^{n-1}}{v} = u \qquad (10)$$

Since in both fractions numerators are divisible by denominators *u* is an integer.
Since $p^n > f^{n-1} = v^{n(n-1)}$ in Eq.(6a) and $q^n > k^{n-1} = w^{n(n-1)}$ in Eq.(6b) *u* is a positive integer.
From Eq.(10)

$$vp - v^n = wq - w^n = uwv \qquad (11)$$

With regard to equations (7a) and (7b) we obtain

$$a = uwv + v^n; \qquad (12a)$$

$$b = uwv + w^n; \qquad (12b)$$

$$c = uwv + v^n + w^n. \qquad (12c)$$

Now the equation (1) becomes

$$(uwv + v^n)^n + (uwv + w^n)^n = (uwv + v^n + w^n)^n. \qquad (13)$$

The equation (13) can be solved for *u* when $n = 2$: $u = \pm\sqrt{2}$..
Since *v* and *w* are integers *a*, *b*, *c* cannot be integers and the case A is unacceptable for obtaining Pythagorean triples.
The discussion for $n \geq 3$ will be common for both cases A and B.

2.2. Case B

In the equation (4b) n is assumed to be factor of k.
The expression (7a) deduced for case A remains valid: $a = vp$.

Lemma-6. Assume there exist positive integers k_1 and t such that $k = k_1 n^t$ and n does not divide k_1.
Then there exist positive integers q, w, g such that $b = n^g wq$.
Proof. Dividing k in Eq.(4b) n becomes a factor of every term of the sum in brackets. Then n can be factored out leaving the sum in brackets with all terms except the first one divided by k i.e. by n and k_1

$$b^n = k_1 n^{t+1}[a^{n-1} + \tfrac{1}{2}(n-1)a^{n-2}k + \cdots + k_1 n^{t-1} k^{n-2}] \qquad (14) \qquad .$$

According to Lemma-2 the sum in brackets has no factors n and k_1 and according to Lemma-3 there must exist positive integers w and q such that

$$k_1 = w^n \qquad (15)$$

and

$$q^n = a^{n-1} + \tfrac{1}{2}(n-1)a^{n-2}k + \cdots + k_1 n^{t-1} k^{n-2} \qquad (16)$$

For exponent $t + 1$ to be divided by n there must be integer $g \geq 1$ such that

$$t = gn - 1 \qquad (17)$$

Now

$$k = w^n n^{gn-1} \qquad (18)$$

and the Eq.(14) becomes $b^n = w^n n^{gn} q^n$.
Then (with $a = vp$ as in case A)

$$b = n^g wq \qquad (19)$$

Lemma-7. For equation (1) with $a = vp$ and $b = n^g wq$ there exists a positive integer u such that in the Eq.(1)

$$a = n^g uwv + v^n;$$

$$b = n^g uwv + n^{gn-1} w^n;$$

$$c = n^g uwv + v^n + n^{gn-1} w^n.$$

Proof. With regard to equations (5a), (7a), (18), and (19) the expression (2) becomes

$$vp + n^{gn-1}w^n = n^g wq + v^n \qquad (20)$$

After regrouping we obtain

$$v(p - v^{n-1}) = n^g w(q - n^{g(n-1)-1}w^{n-1}) \qquad (21)$$

Since v and $n^g w$ are mutually coprime each of them must divide a polynomial in parentheses on the opposite side of the equation. Now the equation (21) becomes

$$\frac{p - v^{n-1}}{n^g w} = \frac{q - n^{gn-1}w^{n-1}}{v} = u \qquad (22)$$

Since in both fractions numerators are divided by denominators u is an integer.
From expression (22)

$$vp - v^n = n^g wq - n^{gn-1}w^n = n^g uwv \qquad (23)$$

With regard to expressions (7a) and (23) we obtain

$$a = n^g uwv + v^n; \qquad (24a)$$
$$b = n^g uwv + n^{gn-1}w^n; \qquad (24b)$$
$$c = n^g uwv + v^n + n^{gn-1}w^n. \qquad (24c)$$

and similar to Eq.(13) equation

$$(n^g uwv + v^n)^n + (n^g uwv + n^{gn-1}w^n)^n = (n^g uwv + v^n + n^{gn-1}w^n)^n \qquad (25)$$

As it was with the Eq.(13) the Eq.(25) can be solved for u when $n = 2$: $u_{1,2} = \pm 1$.
Substituting these roots for u in the Eq.(25) we obtain an identity

$$(\pm 2^g wv + v^2)^2 + (\pm 2^g wv + 2^{2g-1}w^2)^2 = (\pm 2^g wv + v^2 + 2^{2g-1}w^2)^2 =$$
$$= 2^{2g+1}w^2v^2 \pm 2^{g+1}wv(v^2 + 2^{2g-1}w^2) + v^4 + 2^{2(2g-1)}w^4 \qquad (26)$$

This is a universal formula for obtaining equality

$$a^2 + b^2 = c^2$$

with any three integers taken as $w, v,$ and g.
The polynomial expressions for terms of the Eq.(26) can be transformed into Euclid's formulas for generating Pythagorean triples.

2.3. Common Part

Starting with $n = 3$ all n are odd numbers and the left hand part of the equation (1) becomes

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}) \qquad (27)$$

Obviously c^n must contain all factors of $a + b$ and of

$$a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1} = (a + b)^{n-1} - nab(a^{n-3} + \cdots + b^{n-3}) \qquad (28)$$

There are two possible cases: either $a + b$ is divided by n or not. The latter is the only possible for case B where

$$a + b = 2n^g wv + v^n + n^{ng-1}w^n \qquad (29)$$

Lemma-8. When $n \geq 3$ there must be positive integers u_p and c_p such that $a + b$ is divided by u_p^n and c is divided by $u_p c_p$.
Proof. Division of the left hand part of the expression (28) by $a + b$ leaves remainder nb^{n-1} (or na^{n-1}). It means that

$$a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}$$

is not divisible by $a + b$ and has no common factors with it unless $a + b$ is divisible by n.

If $a + b$ a is not divisible by n then according to Lemma-3 both sums in parentheses of the right hand part of the equation (27) must be integers to the power n and can be expressed as

$$a + b = u_p^n \qquad (30)$$

$$a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1} = c_p^n \qquad (31)$$

If $\quad a + b = 2uwv + v^n + w^n$

and $\quad c = uwv + v^n + w^n$

have common factor it must be a common factor u_p of u and $v^n + w^n$ Then it can be assumed

$$u = u_p u_s \qquad (32)$$

and

$$v^n + w^n = u_p D \qquad (33)$$

Then

$$c = u_p c_p \qquad (34)$$

If in case A n divides $a + b$ it becomes the only common factor of the left hand parts of the equations (30) and (31). Then according to Eq.(28) the Eq.(31) becomes

$$(a + b)^{n-1} - nab(a^{n-3} + \cdots + b^{n-3}) = nc_p^n \qquad (35)$$

In this case for being an integer c requires factor $n^g$with $g \geq 1$ and instead of equations (34) and (30) we have

$$c = n^g u_{pk} c_p \qquad (36)$$

and

$$a + b = n^{gn-1} u_{pk}^n \qquad (37)$$

Thus the Lemma-8 is valid for all possible cases of the equation (1).

The equations (13) and (25) can be transformed into polynomial equations F(u)=0.

The Eq.(13) expanded by binomial theorem

$$2(uwv)^n + n(uwv)^{n-1}(v^n + w^n) + \frac{n(n-1)}{2}(uwv)^{n-2}(v^{n\cdot 2} + w^{n\cdot 2}) + \cdots + nuwv(v^{n(n-1)} + w^{n(n-1)}) +$$
$$+v^{n\cdot n} + w^{n\cdot n} =$$
$$= (uwv)^n + n(uwv)^{n-1}(v^n + w^n) + \frac{n(n-1)}{2}(uwv)^{n-2}(v^n + w^n)^2 + \cdots + nuwv(v^n + w^n)^{n-1} +$$
$$+(v^n + w^n)^n \qquad (38)$$

From it after summarizing the like terms and dividing by $(wv)^n$ we obtain

$$u^n = n(n-1)(uwv)^{n-2} + \frac{n(n-1)(n-2)}{2}(uwv)^{n-3}(v^n + w^n) + \cdots +$$
$$+nuwv\left[(n-1)v^{n(n-3)} + \cdots + (n-1)w^{n(n-3)}\right] + n(v^n + w^n)(v^{n(n-3)} + \cdots + w^{n(n-3)}) \qquad (39)$$

For being more demonstrative it is repeated for n=5

$$2(uwv)^5 + 5(uwv)^4(v^5 + w^5) + 10(uwv)^3(v^{5\cdot 2} + w^{5\cdot 2}) + 10(uwv)^2(v^{5\cdot 3} + w^{5\cdot 3}) + 5uwv(v^{5\cdot 4} + w^{5\cdot 4}) +$$
$$+v^{5\cdot 5} + w^{5\cdot 5} =$$
$$= (uwv)^5 + 5(uwv)^4(v^5 + w^5) + 10(uwv)^3(v^5 + w^5)^2 + 10(uwv)^2(v^5 + w^5)^3 + 5uwv(v^5 + w^5)^4 +$$
$$+(v^5 + w^5)^5 \qquad (40)$$

Or after division by $(wv)^5$ we obtain equation F(u)=0

$$u^5 - 20(uwv)^3 - 30(uwv)^2(v^5 + w^5) - 10uwv(2v^{5\cdot 2} + 3v^5w^5 + 2w^{5\cdot 2}) -$$

$$-5(v^5 + w^5)(v^{5\cdot2} + v^5w^5 + w^{5\cdot2}) = 0 \qquad (41)$$

In the case B we obtain from Eq.(25).

$$u^5 - 4(5^g uwv)^3 - 6(5^g uwv)^2\left(v^5 + 5^{5g-1}w^5\right) - 2\cdot 5^g uwv\left[2v^{5\cdot2} + 3v^5 5^{5g-1}w^5 + 2\left(5^{5g-1}w^5\right)^2\right] -$$
$$-(v^5 + 5^{5g-1}w^5)[v^{5\cdot2} + v^5 5^{5g-1}w^5 + (5^{5g-1}w^5)^2] = 0 \qquad (42)$$

The equations for *n=5* will be used in following discussion. Possibility of generalization will be explored later.

Both polynomial equations (41) and (42) of type

$$\alpha_0 x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_n = 0 \qquad (43)$$

have coefficients $\alpha_0 = 1$ and $\alpha_1 = 0$ and one change of sign. It means according Descartes' rule of signs that there can be only one positive root u_1. As a single one it can be only real. With $\alpha_0 = 1$ it cannot be a fraction.

Lemma-9. The only acceptable root of the equation F(u)=0 is positive root u_1.

Proof. Substitution of any negative root $-u_i$ into $a + b = 2uwv + v^n + w^n$ results in $a + b < c$. If *a, b, c* stay after this positive then

$a^n + b^n < (a + b)^n < c^n$. Otherwise it contradicts initial conditions that all terms are positive. So negative roots are unacceptable.

Since $(uwv)^n = (a + b - c)^n$ the right hand part of Eq.(39) is divided by *a + b* as obtained from

$$c^n - [a^n + b^n - (a + b - c)^n]$$

Then the Eq.(41) can be presented as

$$(u_pu_s)^5 - 5[2uwv + v^5 + w^5][2(uwv)^2 + 2uwv(v^5 + w^5) + v^{5\cdot2} + v^5w^5 + w^{5\cdot2}] = 0 \quad (44)$$

The first polynomial in brackets represents *a + b* according to equations (30) and (37). In the latter case the factor *5* has to be attributed to it making $u_p^5 = (5^g u_{pk})^5$ possible.

Otherwise it has to be attributed to another polynomial in bracket representing u_s^n that in this case must itself be divided by 5^{5g-1}.

The Eq.(43) can be presented by its roots as

$$(x - x_1)(x - x_2)\dots(x - x_n) = 0$$

The coefficient at the term before the last

$$\alpha_{n-1} = x_1x_2\dots x_{n-1} + x_1x_2\dots x_n + \cdots + x_2\dots x_{n-1}x_n \qquad (45)$$

The coefficient at the last (constant) term is product of the roots of equation

$$\alpha_n = x_1x_2\dots x_n \qquad (46)$$

The constant term of the Eq.(41) is a product of the last terms of polynomials for u_p^5 and u_s^5 in Eq.(44)

$$5(v^5 + w^5)(v^{5\cdot2} + v^5w^5 + w^{5\cdot2}) = (u_1u_2\dots u_5) = (u_{p1}u_{p2}\dots u_{p5})(u_{s1}u_{s2}\dots u_{s5}) \qquad (47)$$

The coefficient at the previous term (*u* to the first power) of the Eq.(41)

$$10wv(2v^{5\cdot2} + 3v^5w^5 + 2w^{5\cdot2}) = u_1(u_2u_3u_4 + \cdots + u_3u_4u_5) + u_2u_3u_4u_5 =$$
$$= u_{p1}u_{s1}\left[(u_{p2}u_{p3}u_{p4})(u_{s2}u_{s3}u_{s4}) + \cdots + (u_{p3}u_{p4}u_{p5})(u_{s3}u_{s4}u_{s5})\right] + \left(u_{p2}u_{p3}u_{p4}u_{p5}\right)(u_{s2}u_{s3}u_{s4}u_{s5})$$
$$(48)$$

This coefficient can be obtained from Eq.(44) as sum of coefficients at terms of both polynomials with *u* to the first power multiplied by constant terms of each other. The factor *5* is attributed to $a + b$, so it is included in $u_{p1}u_{p2} \dots u_{p5}$

$$5 \cdot 2wv[v^{5\cdot 2}+v^5w^5 + w^{5\cdot 2} + (v^5 + w^5)^2] = 2wv[5(u_{s1}u_{s2} \dots u_{s5}) + (v^5 + w^5)u_{p1}u_{p2} \dots u_{p5}] =$$
$$= u_{p1}u_{s1}[(u_{p2}u_{p3}u_{p4})(u_{s2}u_{s3}u_{s4}) + \cdots + (u_{p3}u_{p4}u_{p5})(u_{s3}u_{s4}u_{s5})] + (u_{p2}u_{p3}u_{p4}u_{p5})(u_{s2}u_{s3}u_{s4}u_{s5}) \quad (49)$$

With $u_1, u_{p1,}u_{s1}$ assumed to be integers both factors $(u_{p2} \dots u_{p5})$ and $(u_{s2} \dots u_{s5})$ of the last term and polynomial in brackets must be integers too.
Now we regroup the equation so that all terms containing factor u_{p1} to be on the same side and on the opposite - the rest of terms

$$u_{p1}\{2wv(v^5 + w^5)(u_{p2} \dots u_{p5}) - u_{s1}[(u_{p2}u_{p3}u_{p4})(u_{s2}u_{s3}u_{s4}) + \cdots + (u_{p3}u_{p4}u_{p5})(u_{s3}u_{s4}u_{s5})]\} =$$
$$= (u_{s2}u_{s3}u_{s4}u_{s5})(u_{p2}u_{p3}u_{p4}u_{p5} - 5 \cdot 2wvu_{s1}) \quad (50)$$

Lemma-10. The integers u_p and u_s are coprime.
Proof. The remainder after division of $v^{n\cdot(n-3)} + \cdots + w^{n\cdot(n-3)}$ (or $v^{5\cdot 2} + v^5w^5 + w^{5\cdot 2}$ – when *n =5*) with factor u_s by $v^n + w^n$ with factor u_p must contain their common divisor. The remainder obtained according to the Remainder theorem by substitution of $(-w^n)$ for v^n in dividend is always equal $w^{n(n-3)}$ divisible by neither u_p nor u_s.
Hence polynomials have no common divisor i.e. u_p and u_s are coprime.

Then u_{p1} must divide $u_{p2}u_{p3}u_{p4}u_{p5} - 5 \cdot 2wvu_{s1}$ in the right hand part of Eq.(50)

Lemma-11 The polynomial $u_{p2}u_{p3}u_{p4}u_{p5} - 5 \cdot 2wvu_{s1}$ is not divisible by u_{p1}.
Proof. Let us multiply the polynomial by u_{p1} The obtained polynomial must be divisible by u_{p1}^2.

$$u_{p1}u_{p2}u_{p3}u_{p4}u_{p5} - 5 \cdot 2wvu_{s1}u_{p1} = 5(v^5 + w^5) - 5 \cdot 2u_1wv \qquad (51)$$

We subtract it from $5(2u_1wv + v^5 + w^5) = u_{p1}^5$
The obtained difference $10 \cdot 2u_1wv$ is divisible by u_{p1} (to the first power only) what also applies to polynomial (51) creating a contradiction..

If in the Eq.(44) to attribute factor *5* to u_s^5 then we have in the Eq.(49)

$$2wv[(u_{s1}u_{s2} \dots u_{s5}) + 5(v^5 + w^5)u_{p1}u_{p2} \dots u_{p5}]$$

It does not affect the left hand side of Eq.(50).

There is no factor *n* in equation *F(u)=0* in Case B, as it is seen in the Eq.(42).

All foregoing considerations are applicable when *n >5.*
There is always only one term $(u_2u_3u_4 \dots u_n)$ in Eq.(48) without factor u_1.
The constant term of the Eq.(39) is always product of polynomials
$v^n + w^n = u_{p1}u_{p2} \dots u_{pn}$;
$v^{n(n-3)} + \cdots + w^{n(n-3)} = u_{s1}u_{s2} \dots u_{sn}$.

The obtained conclusions are invalid for case *n = 3* when $u_s = 1$.

3. Conclusion

Hence it has been revealed the contradiction of separate conclusions based on the assumption that the equation

$$a^n + b^n = c^n$$

can be true when *a, b, c* are integers and exponents $n \geq 5$ are prime numbers.
This proves the Theorem for discussed cases.

In case of the exponent $n = mn_k$ where n_k is a prime number the equation (1) becomes

$$(a^m)^{n_k} + (b^m)^{n_k} = (c^m)^{n_k} \qquad (52)$$

and all foregoing considerations apply.

The only case left to be discussed is the equation (1) with $n = 2^t$ where $t \geq 2$
Then according to Eq. (26**)** it can be presented as

$$a^{2^{t-1}} = 2^g wv + v^2 \qquad (53)$$

The left hand part of Eq. (53) can be presented as

$$\left(a^{2^{t-2}}\right)^2 = (s + v)^2 = s^2 + 2sv + v^2 \qquad (54)$$

From equations (53) and (54) derives

$$2^g wv = s(s + 2v) \qquad (55)$$

This equality definitely requires $s = s_k v$ and the Eq. (55) becomes

$$2^g wv = s_k v^2 (s_k + 2) \qquad (56)$$

As v cannot be a factor of w**,** this equation cannot be true.

Now all cases of Fermat's theorem are proved: the equation (1) cannot be true when $n \geq 5$.