Proof of the Fermat’s Last Theorem

Michael Pogorsky

mpogorsky@yahoo.com

Abstract

The Fermat’s Last Theorem is proved by means of general algebra in four major steps. a) The polynomial expressions of type $a = uwv + v^n; b = uwv + w^n; \ \ c = uwv + v^n + w^n$ required for a, b, c to satisfy equation $a^n + b^n = c^n$ are deduced for two main versions of the equation. b) Positive integers u_p and c_p such that $a + b$ is divisible by u_p^n and c is divisible by $c_p u_p$ proved to exist. c) Polynomial $a^n + b^n$ presented through obtained in step (a) expressions for a and b proved to be a sum of three divisible by c polynomials. d) The long division of one of them $w^{n \cdot n} + v^{n \cdot n}$ by either of two other gives remainder not divisible by c. This contradiction proves the Theorem.

Keywords: *Fermat’s Last Theorem, Proof, Binomial Theorem, Polynomial, Prime number, Long division, Remainder*

1. Introduction

According to the Fermat's Last Theorem (FLT) the equation

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

cannot be true when *a*, *b*, *c* and *n* are positive integers and *n>2*

The recognized proof of this statement exists for almost two decades. Nevertheless there is still strong belief that the theorem can be proved in more conventional way. Maybe because the proof Fermat might have in mind (if any) was definitely different from that of Andrew Wiles.

Though the FLT belongs to number theory in this paper it is taken rather as a problem of algebra. The proof is based on binomial theorem that allowed to deduce polynomial values of terms of the equation (1) required to satisfy it. Other tools of basic algebra, such as rules of division of polynomials, helped to reveal the sought contradiction. So, all means used to build this proof are elementary and well known from courses of general algebra. There is no References section at the end of this paper,

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

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

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

Lemma-1. In the expanded by binomial theorem $(\alpha + \beta)^n$ when α and β are integers and n is a prime number all terms between the first and the last ones are divided by *n*.

Proof. After expansion the coefficient at the first term is 1 and at the last – $\frac{n(n-1)(n-2)\ldots 2\cdot 1}{n!}$ i.e. equal 1 too. At the rest of terms all factors of denominators are < *n* and it cannot be reduced in the numerators.

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 *k* in Eq.(4b) and only last terms are not divided respectively by *b* and ***a*****.** In both equations 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-2 The sum $\alpha_1\beta + \alpha_2\beta + \cdots + \alpha_{n-1}\beta + \alpha_n$ with $\alpha_{1,}\alpha_2, \ldots \alpha_n, \beta$ - 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 $\beta[A - (\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1}) = \alpha_n$ with β dividing α_n that contradicts the statement.

Hence the sums in brackets are coprime with *f* in Eq.(4a) and with *k* in Eq.(4b) and are not divided by *n*

Lemma-3. If there are integers *A* and coprime *B* and *C* such that $A^n = BC$ than each *B* and *C* are integers 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}.
Since *B* is coprime with *C* only one of them can be divided by s^{mn} i.e. both *B* and *C* must have all their divisors to the power *n***.**.

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

Proof. 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

$$vp + w^n = wq + v^n \tag{8}$$

After regrouping we obtain

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

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

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

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)

$$vp - v^n = wq - w^n = uwv \tag{11}$$

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

$$a = uwv + v^n; \tag{12a}$$

$$b = uwv + w^n; \tag{12b}$$

$$c = uwv + v^n + w^n. \tag{12c}$$

Now the equation (1) becomes

$$(uwv + v^n)^n + (uwv + w^n)^n = (uwv + v^n + w^n)^n. \tag{13}$$

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

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

.

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

$$k_1 = w^n \tag{15}$$

and

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

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

$$t = gn - 1 \tag{17}$$

Now

$$k = w^n n^{gn-1} \tag{18}$$

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

$$b = n^g wq \tag{19}$$

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

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

After regrouping we obtain

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

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

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

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

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

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

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

and similar to Eq.(13) equation

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

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* 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

$$a + b = 2uwv + v^n + w^n$$

and

$$c = uwv + v^n + w^n$$

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).

Since all considerations of the further discussion are common for both cases the case A will be used as more simple..

The assumption that $a^n + b^n = c^n$ is true leads to the following conclusion.

Lemma-9. In the equation

$$a^n + b^n = 2(uwv)^n + n(uwv)^{n-1}(v^n + w^n) + \cdots + n(uwv)\left(v^{n(n-1)} + w^{n(n-1)}\right) + w^{n \cdot n} + v^{n \cdot n} \qquad (38)$$

where the right hand part is a sum of the polynomials

$$(uwv)^n + n(uwv)^{n-1}v^n + \cdots + n(uwv)v^{n(n-1)} = a^n - v^{n \cdot n} \qquad (39a)$$

$$(uwv)^n + n(uwv)^{n-1}w^n + \cdots + n(uwv)w^{n(n-1)} = b^n - w^{n \cdot n} \qquad (39b)$$

$$w^{n \cdot n} + v^{n \cdot n} \qquad (39c)$$

each of them is divisible by *c*.

Proof. Since

$$a^n = c^n - b^n,$$

$$v^n = c - b,$$

$$w^n = c - a$$

The equation (39a) becomes

$$a^n - v^{n \cdot n} = a^n - (c - b)^n = a^n - (c^n - nc^{n-1}b + \cdots + ncb^{n-1} - b^n) =$$
$$= ncb(c - b)(c^{n-3} - \cdots + b^{n-3}) \qquad (40a)$$

By analogy with it the Eq.(39b) is equal

$$b^n - w^{n \cdot n} = nca(c - a)(c^{n-3} - \cdots + a^{n-3}) \qquad (40b)$$

And

$$w^{n \cdot n} + v^{n \cdot n} = 2c^n - nc^{n-1}(a + b) + \cdots + nc(a^{n-1} + b^{n-1}) - (a^n + b^n) =$$
$$= c^n - nc^{n-1}(a + b) + \cdots + nc(a^{n-1} + b^{n-1}) \qquad (40c)$$

If to divide the polynomial (39c) by either of polynomials (39a) or (39b) the obtained at the end remainder must be divisible by *c*.
To perform the division we present the polynomial (39a) as follows

$$nv^{n(n-1)+1}(uw) + \frac{n(n-1)}{2}v^{n(n-2)+2}(uw)^2 + \frac{n(n-1)(n-2)}{2 \cdot 3}v^{n(n-3)+3}(uw)^3 + \cdots +$$
$$+ nv^{2n-1}(uw)^{n-1} + v^n(uw)^n \qquad (41)$$

Dividing $v^{n \cdot n} + w^{n \cdot n}$ by the first term of the sum (41) we obtain first term of a quotient

$$\frac{v^{n-1}}{n(uw)}$$

Multiplying the rest of terms of expression (41) by it and then subtracting the product from dividend we obtain

$$-\frac{n-1}{2}v^{n(n-1)+1}(uw) - \frac{(n-1)(n-2)}{2 \cdot 3}v^{n(n-2)+2}(uw)^2 - \ldots - v^{3n-2}(uw)^{n-2} - \frac{1}{n}v^{2n-1}(uw)^{n-1} + w^{n \cdot n} \qquad (42)$$

Now we divide the first term of this polynomial by the first term of the sum (41) and obtain the second (the last) term of the quotient

$$-\frac{n-1}{2n}$$

Multiplying the rest of terms of the polynomial (41) by it we obtain

$$-\frac{(n-1)^2}{4}v^{n(n-2)+2}(uw)^2-\cdots-\frac{n-1}{2}v^{2n-1}(uw)^{n-1}-\frac{n-1}{2n}v^n(uw)^n \qquad (43)$$

Subtracting polynomial (43) from the rest of terms of the sum (42) we obtain remainder

$$\frac{n^2-1}{12}v^{n(n-2)+2}(uw)^2+\cdots+\frac{n(n-1)-2}{2n}v^{2n-1}(uw)^{n-1}+\frac{n-1}{2n}v^n(uw)^n+w^{n\cdot n} \qquad (44)$$

To be divisible by *c* the remainder must according to Eq.(34) be divisible by u_p that according to Eq.(32) divides *u*. Since all terms but one of the polynomial (44) contain factor *u* the sum according to Lemma-2 is not divisible by it. So the remainder is not divisible by *c*.
Thus the contradiction with based on the equation (1) Lemma-9 is obtained.

3. Conclusion

Hence the assumption that the equation (1) is true and all following considerations resulted in the revealed contradiction. It proves that the equation

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

is not true when the exponent $n\geq 3$ is a prime number.

If the exponent $n=mn_k$ where $n_k\geq 3$ is a prime number the equation (1) becomes

$$(a^m)^{n_k}+(b^m)^{n_k}=(c^m)^{n_k} \qquad (45)$$

and all foregoing considerations apply.

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

$$a^{2^{t-1}}=2^g wv+v^2 \qquad (46)$$

The left hand part of Eq.(46) can be presented as

$$(a^{2^{t-2}})^2=(s+v)^2=s^2+2sv+v^2 \qquad (47)$$

From equations (46) and (47) derives

$$2^g wv=s(s+2v) \qquad (48)$$

This equality definitely requires $s=s_k$*v* and the Eq. (48) becomes

$$2^g wv=s_k v^2(s_k+2) \qquad (49)$$

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 $n\geq 3.$