Version of Proof of the Fermat's Last Theorem

Michael Pogorsky

mpogorsky@yahoo.com

Abstract

This is the shortest and most direct version of proofs of FLT based on deduced for two main cases of the equation $a^n + b^n = c^n$ polynomial expressions $a = uwv + v^n$; $b = uwv + w^n$; $c = uwv + v^n + w^n$. Contradiction revealed in the polynomials prevents them from being integer numbers and proves the Theorem.

Keywords: *Fermat's Last Theorem, Proof, Binomial Theorem, Polynomial, Prime number, Eisenstein's criterion*.

1. Introduction

Though the FLT belongs to the number theory it is taken in this proof rather as a problem of algebra. The proof is based on binomial theorem that allowed to deduce polynomial values of terms *a, b, c* required for them to satisfy as integers equation.

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

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

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

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

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

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

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*.**.

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

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

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

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 integers v, 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)

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

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

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

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

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

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

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 ofthe equation. Now the equation (21) becomes

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

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

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

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

The following analysis is common for both cases. The Case A will be used as more simple.
From expressions (12a), (12b), (12c) and from

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

We obtain

$$uvw = a + b - c \qquad (27a)$$

$$v^n = c - b \qquad (27b)$$

$$w^n = c - a \qquad (27c)$$

Obviously as $(uwv)^n$ is divided by v^n and w^n the $(a + b - c)^n$ is divided by

$$(c-a)(c-b) = c^2 - c(a+b) + ab \qquad (28)$$

Obtained in both cases quotient u^n must be according to expression (10) an integer.

Let us present

$$c^2 - c(a+b) + ab = -[c(a+b) - c^2 - ab] \qquad (29)$$

And

$$(a+b-c)^n = \frac{[c(a+b)-c^2]^n \pm (ab)^n}{c^n} \qquad (30)$$

According to equations (7a), (7b)

$$(ab)^n = (pqvw)^n$$

This means the numerator of the Eq.(30) is divisible by expression (29). We obtain (sign disregarded)

$$u^n = \frac{[c(a+b)-c^2]^{n-1} + [c(a+b)-c^2]^{n-2}ab + \cdots + (ab)^{n-1} + (pq)^n}{c^n} \qquad (31)$$

Each term of the sum in numerator except two last being divided by c^n becomes a fraction

$$Q_i = \frac{(a+b-c)^{n-i}(ab)^{i-1}}{c^i} \qquad (32)$$

with denominator's exponent *i* different in all terms.

Since *ab* and *pq* are coprime with *c* the last two terms result in fraction

$$\frac{(ab)^{n-1}+(pq)^n}{c^n} \qquad (33)$$

Lemma-8 The sum $(ab)^{n-1} + (pq)^n$ is coprime with *c*.

Proof.

$$(ab)^{n-1} + (pq)^n = (pq)^{n-1}[(vw)^{n-1} + pq] \qquad (34)$$

Multiplying sum in brackets by vw with regard to expressions (5a), (5b) we obtain

$$(vw)^n + ab = fk + ab \qquad (35)$$

With regard to Eq.(2)

$$c^2 = (a+k)(b+f) = ab + fk + af + bk \qquad (36)$$

Sum (35) can be divisible by *c* only along with

$$af + bk = f(uvv + f) + k(uwv + k) = uwv(f+k) + (f^2 + k^2) \qquad (37)$$

To be divisible by *c* the right hand part requires term *2fk* coprime with *c*.

Hence sum (35) and (34) with it are coprime with *c*.

The sum of fractions (32), (33) cannot be reduced to common denominator equal 1. Hence u^n in expression (31) as well as *a*, *b*, and *c* in Eq.(1) cannot be integers.

This proves the assumption of existence Eq.(1) with *a, b, c*- integers to be false.

In Case B the Eq.(27a) becomes

$$(n^g uwv)^n = a + b - c \qquad (38)$$

It is divided by $n^{ng-1}w^n = c - a$. So the reasoning stay unchanged, only instead of u^n appears nu^n in Eq.(31). It does not influence obtained conclusions.

3. Conclusion

Thus it is proved 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

$$(a^m)^{n_k} + (b^m)^{n_k} = (c^m)^{n_k} \qquad (39)$$

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 Eq. (26**)** it can be presented as

$$a^{2^{t-1}} = 2^g wv + v^2 \qquad (40)$$

The left hand part of Eq.(40) can be presented as

$$\left(a^{2^{t-2}}\right)^2 = (s+v)^2 = s^2 + 2sv + v^2 \qquad (41)$$

From equations (40) and (41) derives

$$2^g wv = s(s+2v) \qquad (42)$$

This equality definitely requires $s = s_k v$ and the Eq. (42) becomes

$$2^g wv = s_k v^2 (s_k + 2) \qquad (43)$$

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 $n \geq 3$.