Version of the Proof of the Fermat's Last Theorem

Michael Pogorsky

mpogorsky@yahoo.com

Abstract

As my previous Proof of the FLT (vixra.org/pdf/1209.0099v2.pdf) this Version is based on polynomial expressions $a = uwv + v^n$; $b = uwv + w^n$; $c = uwv + v^n + w^n$ deduced for two main cases of the equation $a^n + b^n = c^n$. Another way has been found to prove the Theorem by transforming this equation into expression that allows applying of the Eisenstein's criterion to reveal a contradiction.

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

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. 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.

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 $\alpha_1, \alpha_2, \ldots \alpha_n, \beta$ - 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 $\beta[A - (\alpha_1 + \alpha_2 + \cdots + \alpha_{n-1})] = \alpha_n$ 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 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* and *C* are coprime only one of them can be divided by s^m i.e. it must be to the power *n* to be divided by s^{mn}. Then both *B* and *C* must have all their divisors to the power *n*..

Assume the equation (1) is true.
Let us express

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

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

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

After expansion of sums in parentheses by binomial theorem we obtain

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

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

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)

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

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

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

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

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

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

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

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

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

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

After regrouping we obtain

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

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

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

.
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 of the 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

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

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

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

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

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

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

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

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

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

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

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

and

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

Then

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

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

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

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

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

and

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

In this case $v^n + w^n$ becomes divisible by $n^g u_{pk}$.

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

The following discussion is common for both cases the case A will be used as more simple.

From the expression $a + b = 2uwv + v^n + w^n$

$$uwv = \frac{1}{2}[a + b - (v^n + w^n)]$$

Denoting $a + b = U;\ v^n = f;\ w^n = k$ we can express equations (12a), (12b), and (12c) as

$$a = \frac{1}{2}(U + f - k) \qquad (38a)$$

$$b = \frac{1}{2}[U - (f - k)] \qquad (38b)$$

$$c = \frac{1}{2}(U + f + k) \qquad (38c)$$

Then

$$a^n = \frac{1}{2^n}[U^n + nU^{n-1}(f-k) + \frac{n(n-1)}{2}U^{n-2}(f-k)^2 + \cdots + \frac{n(n-1)}{2}U^2(f-k)^{n-2} +$$

$$+nU(f-k)^{n-1} + (f-k)^n] \qquad (39)$$

$$b^n = \frac{1}{2^n}[U^n - nU^{n-1}(f-k) + \frac{n(n-1)}{2}U^{n-2}(f-k)^2 - \cdots - \frac{n(n-1)}{2}U^2(f-k)^{n-2} +$$

$$+nU(f-k)^{n-1} - (f-k)^n] \qquad (40)$$

$$c^n = \frac{1}{2^n}[U^n + nU^{n-1}(f+k) + \frac{n(n-1)}{2}U^{n-2}(f+k)^2 + \cdots + \frac{n(n-1)}{2}U^2(f+k)^{n-2} +$$

$$+nU(f+k)^{n-1} + (f+k)^n] \qquad (41)$$

Now the Eq. (13) becomes after multiplication of both hand sides by 2^n

$$2[U^n + \frac{n(n-1)}{2}U^{n-2}(f-k)^2 + \cdots + \frac{n(n-1)(n-2)}{2\cdot 3}U^3(f-k)^{n-3} + nU(f-k)^{n-1}] =$$

$$= U^n + nU^{n-1}(f+k) + \frac{n(n-1)}{2}U^{n-2}(f+k)^2 + \cdots + \frac{n(n-1)}{2}U^2(f+k)^{n-2} +$$

$$+nU(f+k)^{n-1} + (f+k)^n] \qquad (42)$$

After factorization by *U* the polynomial in brackets becomes

$$U^{n-1} + \frac{n(n-1)}{2}U^{n-3}(f-k)^2 + \cdots + \frac{n(n-1)(n-2)}{2\cdot 3}U^2(f-k)^{n-3} + n(f-k)^{n-1} \qquad (43)$$

The coefficients at all terms of the polynomial except the first one contain factor *n* to the power 1. The Eisenstein's criterion can be applied unless $f - k$ is divisible by *n*.

In the case B

$$f - k = v^n - n^{ng-1}w^n$$

Here $f - k$ is obviously coprime with *n*.

Lemma-9. In the case A when *n* does not divide $a + b$ it does not divide $f - k$.

Proof. When n does not divide $a + b$ according Eq.(30)

$$u_s = n^g u_{sk} \qquad (44)$$

Assume that $f - k$ is divisible by n^g. Then n divides $v - w$ in

$$f - k = (v - w)[(v - w)^{n-1} - nvw(v^{n-3} - \cdots + w^{n-3})]$$

and $g \geq 2$.

Subtracting $2U^n$ from both hands sides of the Eq.(42)

$$2\left[\frac{n(n-1)}{2}U^{n-2}(f-k)^2+\cdots+\frac{n(n-1)(n-2)}{2\cdot 3}U^3(f-k)^{n-3}+nU(f-k)^{n-1}\right]=$$

$$=nU^{n-1}(f+k)+\frac{n(n-1)}{2}U^{n-2}(f+k)^2+\cdots+\frac{n(n-1)}{2}U^2(f+k)^{n-2}+nU(f+k)^{n-1}+$$

$$+(f+k)^n-U^n \qquad (45)$$

On the left hand side the lowest possible power of n is n^5.
On the right hand side the last three terms

$$nU(f+k)^{n-1}-[U^n-(f+k)^n]=n(2uwv+f+k)(f+k)^{n-1}+(f+k)^n-$$

$$-\left[(2uwv)^n+n(2uwv)^{n-1}(f+k)+\cdots+\frac{n(n-1)}{2}(2uwv)^2(f+k)^{n-2}+n\cdot 2uwv(f+k)^{n-1}+(f+k)^n\right]=$$

$$=n(f+k)^n-[(2uwv)^n+n(2uwv)^{n-1}(f+k)+\cdots+\frac{n(n-1)}{2}(2uwv)^2(f+k)^{n-2}] \qquad (46)$$

Here on the right hand side two last terms of the expanded U^n are canceled. The rest of its terms except $(2uwv)^n$ can be canceled too after expansion of all *U*-s on the right hand side of Eq.(45). Then the lowest power of n on that side will be at $n(f+k)^n$ i.e. equal 1.
The contradiction proves the assumption that n^g divides $f-k$ to be wrong.

Thus when in case A n does not divide $a+b$ the Eisenstein's Criterion can be applied to expression (43). It proves the latter as well as in case B is irreducible over rational numbers. But with $U=u_p^n$ we conclude from Eq. (42) that the polynomial must be equal $2^{n-1}c_p^n$.
The contradiction proves the Theorem for discussed cases.

In case A when $a+b=U$ is divided by n according Eq. (37) the polynomial (43) must be equal $2^{n-1}nc_p^n$.
With $a+b$ divided by n and *a*, *b* - coprime with it $a-b=f-k$ is coprime with n and the polynomial (43) is irreducible over rational numbers in this case too.
The foregoing considerations are not valid when $n=3$ and polynomial (43) becomes

$$U^2+3(f-k)^2 \qquad (47)$$

3. Conclusion

Hence when the exponent $n\geq 5$ is a prime number the assumption that the equation

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

is true and all following considerations resulted in the revealed contradiction that proves the assumption of being wrong. That proves the Theorem for discussed cases.

If the exponent $n=mn_k$ where $n_k\geq 5$ is a prime number the equation (1) become

$$(a^m)^{n_k}+(b^m)^{n_k}=(c^m)^{n_k} \qquad (48)$$

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

$$a^{2^{t-1}}=2^g wv+v^2 \qquad (49)$$

The left hand part of Eq.(49) can be presented as

$$\left(a^{2^{z-z}}\right)^2 = (s+v)^2 = s^2 + 2sv + v^2 \qquad (50)$$

From equations (49) and (50) derives

$$2^g wv = s(s+2v) \qquad (51)$$

This equality definitely requires $s = s_k v$ and the Eq. (51) becomes

$$2^g wv = s_k v^2 (s_k + 2) \qquad (52)$$

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 $n \geq 5$.