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. The proof is based on polynomial expressions deduced through binomial theorem for terms *a, b, c* to satisfy the equation $a^n + b^n = c^n$

The following proof can be outlined as succession of four major steps.

Step 1. Proved that to satisfy equation

$$\mathbf{a^n + b^n = c^n} \qquad \text{(I)}$$

it is required

$$\mathbf{a = uwv + v^n;\ \ b = uwv + w^n;\ \ c = uwv + v^n + w^n;} \qquad \text{(II)}$$

Or

$$\mathbf{a = un^g wv + v^n;\ \ b = un^g wv + n^{gn-1} w^n;\ \ c = un^g wv + v^n + n^{gn-1} w^n;} \qquad \text{(III)}$$

When $\mathbf{n=2}$ the set (III) makes an identity of (I) with $\mathbf{u=1}$ and any $\mathbf{v, w}$.

Step 2. Proved that there must exist integers $\mathbf{u_p}$ and $\mathbf{c_p}$ such that $\mathbf{u = u_p u_s}$ and $\mathbf{a + b = u_p^n}$ or $\mathbf{a + b = n^{gn-1} u_p^n}$; $\mathbf{c = c_p u_p}$ or $\mathbf{c = n^g c_p}$.

Step 3. The left hand part of (I)

$$\mathbf{a^n + b^n = 2(uwv)^n + n(uwv)^{n-1}(v^n + w^n) +}$$
$$\mathbf{+ \frac{n(n-1)}{2}(uwv)^{n-2}(v^{2n} + w^{2n}) + \cdots + nuwv\left(v^{n(n-1)} + w^{n(n-1)}\right) +}$$
$$\mathbf{+(v^{n \cdot n} + w^{n \cdot n})} \qquad \text{(IV)}$$

is a sum of polynomials proved to be divisible by **c**

$$\mathbf{(uwv)^n + n(uwv)^{n-1}v^n + \frac{n(n-1)}{2}(uwv)^{n-2}v^{2n} + \cdots + nuwvv^{n(n-1)}} \qquad \text{(IVa)}$$

$$\mathbf{(uwv)^n + n(uwv)^{n-1}w^n + \frac{n(n-1)}{2}(uwv)^{n-2}w^{2n} + \cdots + nuwvw^{n(n-1)}} \qquad \text{(IVb)}$$

$$\mathbf{v^{n \cdot n} + w^{n \cdot n}} \qquad \text{(IVc)}$$

Step 4. The long division of (IVc) by (IVa) or (IVb) gives a remainder that must be divisible by **c.** The remainder is a sum of terms that all except one ($\mathbf{v^{n \cdot n}}$ or $\mathbf{w^{n \cdot n}}$) contain divisor **u**. Hence the remainder is not divisible by $\mathbf{u_p}$ i.e. by **c.**

The above outline may facilitate reviewing of the following proof

According to the Fermat's Last Theorem the equation

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

cannot be true when $\mathbf{a, b, c,}$ and $\mathbf{n}$ are positive integers and $\mathbf{n > 2}$.

Assume the equation (1) is true.
It is assumed $\mathbf{a,b,c}$ are coprime and $\mathbf{n}$ is a prime.

Let us express

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

Obviously $\mathbf{k}$ and $\mathbf{f}$ are integers. Then

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

After expansion of sums in parentheses by binomial theorem we obtain

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

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

Lemma-1. In the expanded by binomial theorem $\boldsymbol{(\alpha + \beta)^n}$ when $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are integers and $\mathbf{n}$ is a prime number all terms between the first and the last ones are divisible by $\mathbf{n}$.

Proof. After expansion the coefficient at the first term is **1** and at the last – $\mathbf{\frac{n(n-1)(n-2)\ldots 2\cdot 1}{n!}}$ i.e. equal **1** too.
At the rest of terms all factors of denominators are $\mathbf{<n}$ and being reduced leave $\mathbf{n}$ in the numerators.

Since $\mathbf{f}$ divides $\mathbf{a^n}$ and $\mathbf{k}$ divides $\mathbf{b^n}$ they are coprime. Only first terms of the sums in brackets are not divisible by $\mathbf{f}$ in (4a) and $\mathbf{k}$ in (4b) and only last terms are not divisible respectively by $\mathbf{b}$ and $\mathbf{a}$. In both equations last terms have no factor $\mathbf{n}$

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

Case A. Here $\mathbf{n}$ is assumed to be coprime with $\mathbf{f}$ and $\mathbf{k}$.

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

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 a_n contradicting the statement.

Hence the sums in brackets are coprime with f in (4a) and with k in (4b) and are not divisible 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 $C = s^m$ and $m < n$

Then $A^n = Bs^m$.

Since s as a factor of A^n must be to the power n there must be divisor s^{n-m} of B

Since B is coprime with C it cannot be divided by s.

Then $n - m = 0$ and $C = s^n$. A quotient $B = A^n / s^n$ must be to the power n as well.

Lemma-4. There exist positive integers v, p, w, q, such that in (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)

$$f = v^n \quad (5a) \qquad \text{and} \qquad k = w^n \quad (5b)$$

There also must exist positive integers p and q that satisfy in (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

$$a = vp \quad (7a) \qquad b = wq \quad (7b)$$

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

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

.

Proof. With regard to (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 (9) can be rewritten as

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

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

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

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

$$\mathbf{a = uwv + v^n}; \quad \mathbf{b = uwv + w^n}; \quad \mathbf{c = uwv + v^n + w^n}. \qquad (12)$$

Now the equation (1) becomes

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

The equation (13) can be solved for $\mathbf{u}$ when **n=1** and **n=2**.
When **n=1: u=0; a=v; b=w; c=v+w.**
When $\mathbf{n = 2: u = \pm\sqrt{2}}$. Since **v** and **w** are integers **a, b, c** cannot be integers and the case **A** is unacceptable.

<u>Case B</u>. In (4b) **n** is assumed to be factor of **k**.
The expression (7a) deduced for case **A** remains valid: **a=vp**.
<u>Lemma-6</u>. Assume there exist positive integers $\mathbf{k_1}$ and **t** such that $\mathbf{k = k_1 n^t}$ and **n** does not divide $\mathbf{k_1}$.
Then there exist positive integers **q, w, g** such that $\mathbf{b = n^g wq}$.

<u>Proof</u>. Dividing **k** in (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 $\mathbf{k_1}$

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

.

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

$$\mathbf{k_1 = w^n} \qquad (15)$$

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

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

$$\mathbf{t = gn - 1} \qquad (17)$$

Now

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

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

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

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

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

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

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

After regrouping we obtain

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

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

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

Since in both fractions numerators are divisible by denominators $\mathbf{u}$ is an integer. It is a positive integer for the same reason as in (10).

From (22)

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

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

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

and similar to (13) equation

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

As it was with the (13) the (25) can be solved for $\mathbf{u}$ when **n=1** and **n=2.**.

When **n=1: u=0; a=v; b=w; c=v+w.**

When $\mathbf{n = 2}$: $\mathbf{u_{1,2} = \pm 1}$. Substituting these roots for $\mathbf{u}$ in the (25) we obtain an identity

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

This is a universal formula for obtaining equality

$$\mathbf{a^2 + b^2 = c^2}$$

with any three integers taken as **v, w,** and **g.**

The above examination proves that the equation (1) can be true when $n \le 2$, i.e. the first part of the Fermat's theorem

Starting with **n = 3** all **n** are odd numbers

Lemma-8. When $n \ge 3$ there must be positive integers u_p and c_p such that **a+b** is divisible by u_p^n and **c** is divisible by $u_p c_p$.

Proof. Since **n** are odd numbers the left hand part of (1) is

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

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 possibilities: either **a+b** is divisible by **n** or not. The latter is the only possible for case **B** where one of three terms of the sum is coprime with **n.**

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

The polynomial on the left hand side of (28)

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

is not divisible by **a+b** and has no common factors with it unless **a+b** is divisible by **n** since dividing it by **a+b** we obtain a quotient

$$a^{n-2} - 2a^{n-3}b + 3a^{n-4}b^2 - \cdots - (n-1)b^{n-2}$$

and remainder nb^{n-1}.

If **a+b** is not divisible by **n** then according to lemma-3 both sums in parentheses of the right hand side of (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 concluded

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

and

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

Then

$$\mathbf{c = c_p\, u_p} \quad (34)$$

If $\mathbf{n}$ divides $\mathbf{a+b}$ it becomes the only common factor of the left hand parts of (30) and (31). Then according to (28)

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

In this case for being an integer $\mathbf{c}$ requires factor $\mathbf{n}$ and instead of (34) and (30) we have

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

and

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

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 $\mathbf{a^n + b^n = c^n}$ is true leads to the following conclusion.

Lemma-9. In the sum

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

each of the polynomials

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

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

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

must be divisible by $\mathbf{c}$.

Proof. Since

$$\mathbf{a^n = c^n - b^n},$$
$$\mathbf{v^n = c - b},$$
$$\mathbf{w^n = c - a}$$

the (39a) becomes

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

By analogy with it the (39b) is equal

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

And

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

Lemma-10. Lemma-9 is not true.

Proof. If to divide the polynomial (39c) by either (39a) or (39b) there must be a remainder divisible by **c.** To perform the division we present the polynomial (39a) as follows

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

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

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

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

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

The second (the last) term of the quotient

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

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

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

Subtracting (43) from (42) we obtain remainder

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

To be divisible by **c** the remainder must according to (34) be divisible by u_p. Since all terms but one of the (44) contain factor **u** the sum is not divisible by it. So the remainder is not divisible by **c**.
The contradiction proves that the Lemma-9 based on the equation (1) is not true.

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

$$\mathbf{a^n + b^n = c^n}$$

is not true when the exponent **n** is a prime number.

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

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

and all foregoing considerations apply.

The only version of the (1) left to be discussed is the equations with $\mathbf{n = 2^t}$ where $\mathbf{t \geq 2}$
Then according to (24**)**

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

$$\mathbf{b^{2^{t-1}} = 2^g wv + 2^{2g-1} w^2} \qquad (47)$$

$$\mathbf{c^{2^{t-1}} = 2^g wv + v^2 + 2^{2g-1} w^2} \qquad (48)$$

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

$$\mathbf{(a^{2^{t-2}})^2 = (s+v)^2 = s^2 + 2sv + v^2} \qquad (49)$$

From (46) and (49) derives

$$\mathbf{2^g wv = s(s+2v)} \qquad (50)$$

This equality definitely requires $\mathbf{s = s_k v}$ and the (50) becomes

$$\mathbf{2^g wv = s_k v^2 (s_k + 2)} \qquad (51)$$

As **V** cannot be a factor of **W,** this equation cannot be true.

Now the second part of Fermat's theorem is proved: the equation (1) cannot be true when $\mathbf{n \geq 3}$.