Proof of the Fermat's Last Theorem

Michael Pogorsky

mpogorsky@yahoo.com

Abstract

The theorem is proved by means of general algebra. It is based on deduced polynomials $a = uwv + v^n$; $b = uwv + w^n$; $c = uwv + v^n + w^n$ and their modifications required 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 two versions of proof are developed. One of them reveals that after long division of two divisible by *c* polynomials obtained remainder is coprime with it. In another version transformation of $a^n + b^n$ into expression that allows to apply the Eisenstein's criterion reveals a contradiction.

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. 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 $\alpha_1, \alpha_2, \ldots \alpha_n, \beta$ - 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 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

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

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

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

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

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

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

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

$$u=u_pu_s \quad (32)$$

and

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

Then

$$c=u_pc_p \quad (34)$$

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

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

and

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

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

The Eq.(1) can be presented as

$$a^n+b^n=(a+b-uwv)^n$$

In the case A it becomes

$$(a+b)(a^{n-1}-a^{n-2}b+\cdots-ab^{n-2}+b^{n-1})=(a+b)^n-n(a+b)^{n-1}uwv+\frac{n(n-1)}{2}(a+b)^{n-2}(uwv)^2-\cdots-$$
$$-\frac{n(n-1)}{2}(a+b)^2(uwv)^{n-2}+n(a+b)(uwv)^{n-1}-(uwv)^n \quad (38)$$

From it with regard to Eq.(28)

$$\left(u_pu_swv\right)^n=(a+b)[nab(a^{n-3}+\cdots+b^{n-3})-n(a+b)^{n-2}uwv+$$
$$+\frac{n(n-1)}{2}(a+b)^{n-3}(uwv)^2-\cdots-\frac{n(n-1)}{2}(a+b)(uwv)^{n-2}+n(uwv)^{n-1}] \quad (39)$$

Here $a+b$ presents u_p^n and polynomial in brackets - u_s^n and u_s divides $a^{n-3}+\cdots+b^{n-3}$. With factor n at the right hand side n^g may divide either u_p according Eq.(37) or u_s.

The foregoing conclusions open two options to disclose contradictions that prove the Theorem.
Version 1: through remainder that after long division of polynomials is coprime with their common factor.
Version 2: through Eisenstein's criterion
The following discussion is common for both cases. The case A will be used as more simple.

2.3.1. Version 1

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

Lemma-9. In the equation

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

where the right hand part is a sum of the polynomials

$$(uwv)^n + n(uwv)^{n-1}v^n + \cdots + n(uwv)v^{n(n-1)} = a^n - v^{n\cdot n} \quad (41a)$$

$$(uwv)^n + n(uwv)^{n-1}w^n + \cdots + n(uwv)w^{n(n-1)} = b^n - w^{n\cdot n} \quad (41b)$$

$$w^{n\cdot n} + v^{n\cdot n} \quad (41c)$$

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 (41a) becomes

$$a^n - v^{n\cdot n} = a^n - (c-b)^n = a^n - (c^n - nc^{n-1}b + \cdots + ncb^{n-1} - b^n) =$$
$$= ncb(c-b)(c^{n-3} - \cdots + b^{n-3}) \quad (42a)$$

By analogy with it the Eq. (41b) is equal

$$b^n - w^{n\cdot n} = nca(c-a)(c^{n-3} - \cdots + a^{n-3}) \quad (42b)$$

And

$$w^{n\cdot n} + v^{n\cdot n} = 2c^n - nc^{n-1}(a+b) + \cdots + nc(a^{n-1} + b^{n-1}) - (a^n + b^n) =$$
$$= c^n - nc^{n-1}(a+b) + \cdots + nc(a^{n-1} + b^{n-1}) \quad (42c)$$

If to divide the polynomial (41c) by either of polynomials (41a) or (41b) the obtained at the end remainder must be divisible by *c*.

To perform the division we present the polynomial (41a) as follows

$$nv^{n(n-1)+1}(uw) + \frac{n(n-1)}{2}v^{n(n-2)+2}(uw)^2 + \frac{n(n-1)(n-2)}{2\cdot 3}v^{n(n-3)+3}(uw)^3 + \cdots +$$
$$+nv^{2n-1}(uw)^{n-1} + v^n(uw)^n \quad (43)$$

Dividing $v^{n\cdot n} + w^{n\cdot n}$ by the first term of the sum (43) we obtain first term of a quotient

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

Multiplying the rest of terms of expression (43) by it and then subtracting the product from dividend we obtain

$$-\frac{n-1}{2}v^{n(n-1)+1}(uw) - \frac{(n-1)(n-2)}{2\cdot 3}v^{n(n-2)+2}(uw)^2 - \ldots - v^{3n-2}(uw)^{n-2} - \frac{1}{n}v^{2n-1}(uw)^{n-1} + w^{n\cdot n} \quad (44)$$

Now we divide the first term of this polynomial by the first term of the sum (43) and obtain the second (the last) term of the quotient

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

Multiplying the rest of terms of the polynomial (43) by it we obtain

$$-\frac{(n-1)^2}{4}v^{n(n-2)+2}(uw)^2 - \cdots - \frac{n-1}{2}v^{2n-1}(uw)^{n-1} - \frac{n-1}{2n}v^n(uw)^n \quad (45)$$

Subtracting polynomial (45) from the rest of terms of the sum (44) we obtain remainder

$$\frac{n^2-1}{12}v^{n(n-2)+2}(uw)^2+\cdots+\frac{n(n-1)-2}{2n}v^{2n-1}(uw)^{n-1}+\frac{n-1}{2n}v^n(uw)^n+w^{n\cdot n} \quad (46)$$

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 (46) 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.

2.3.2. Version 2

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

$$a=\tfrac{1}{2}(U+f-k) \quad (47a)$$

$$b=\tfrac{1}{2}[U-(f-k)] \quad (47b)$$

$$c=\tfrac{1}{2}(U+f+k) \quad (47c)$$

Then

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

$$+nU(f-k)^{n-1}+(f-k)^n] \quad (48)$$

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

$$+nU(f-k)^{n-1}-(f-k)^n] \quad (49)$$

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

$$+nU(f+k)^{n-1}+(f+k)^n] \quad (50)$$

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

$$2[U^n+\frac{n(n-1)}{2}U^{n-2}(f-k)^2+\cdots+\frac{n(n-1)(n-2)}{2\cdot3}U^3(f-k)^{n-3}+nU(f-k)^{n-1}]=$$

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

$$+nU(f+k)^{n-1}+(f+k)^n] \quad (51)$$

After factorization by *U* the polynomial in brackets becomes

$$U^{n-1}+\frac{n(n-1)}{2}U^{n-3}(f-k)^2+\cdots+\frac{n(n-1)(n-2)}{2\cdot3}U^2(f-k)^{n-3}+n(f-k)^{n-1} \quad (52)$$

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-10. When n^g divides u_s in the case A *n* does not divide $f - k$.

Proof. Assume *n* divides *f - k*
In the Eq.(39) u_s i.e. n^g divide

$$a^{n-3} + \cdots + b^{n-3} = \frac{(a+b)^n - (a^n + b^n)}{nab(a+b)} \qquad (53)$$

From

$$c = c_p u_p = uwv + v^n + w^n = uwv + 2c - (a+b) = u_p u_s wv + 2c_p u_p - u_p^n$$

follows

$$u_s = \frac{u_p^{n-1} - c_p}{wv} \qquad (54)$$

If *n* divides u_s then with regard to Fermat's Little Theorem it divides $c_p - 1$ in the numerator

$$u_p^{n-1} - c_p \pm 1$$

Then *n* divides $c_p^n - 1$ or according Eq.(31)

$$a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1} - 1 \qquad (55)$$

Since *n* divides $b^{n-1} - 1$ it divides the sum of the rest of terms.
To make it demonstrative let us take *n = 5*. Possibility of generalization will be explored later. Then *n* divides

$$a^4 - a^3b + a^2b^2 - ab^3 = a(a-b)(a^2 + b^2) \qquad (56)$$

Either polynomial in parentheses or both of them can be divisible by *n*. We need to assume it divides *a – b = f - k*.
For n = 5 polynomial (53) becomes $a^2 + ab + b^2$. After its division by *a – b* the reminder must be divisible by *n*.
Applying remainder theorem we substitute *a* for *b* and obtain remainder $3b^2$ coprime with *n = 5*.

The conclusion is true for any *n*. The expression (55) without $b^{n-1} - 1$ will always have equal number of positive and negative terms so being divisible by *a – b*. The expression (53) always has *n -2* terms with sum of coefficients coprime with *n*. So will be the remainder after division by *a – b*.
Hence *a – b* is coprime with *n* when n^g divides u_s.
Applied to $f - k$ the contradiction compromises the foregoing assumption and proves the lemma,
So in case A when n^g divides u_s the Eisenstein's criterion can be applied to expression (52).

In case A when $U = a + b$ is supposed according Eq. (37) to be divided by n the difference $f - k = a - b$ being coprime with $a + b$ is not divided by *n*. The Eisenstein's criterion is applicable to polynomial (52) in this case too.

Hence in all examined cases the polynomial (52) is irreducible over rational numbers though must be divisible by $2^{n-1}c_p^n$. Thus the contradiction is obtained for these cases and proves the theorem for all *n* except *n = 3*.
In this case the expression (52) becomes

$$U^2 + 3(f-k)^2 \qquad (57)$$

3. Conclusion

Hence the assumption has been proved wrong that the equation

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

can be true when *a, b, c* are integers and exponents $n \geq 3$ in Version 1 and $n \geq 5$ in Version 2 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

$$(a^m)^{n_k} + (b^m)^{n_k} = (c^m)^{n_k} \quad (58)$$

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

$$a^{2^{t-1}} = 2^g wv + v^2 \quad (59)$$

The left hand part of Eq. (59) can be presented as

$$\left(a^{2^{t-2}}\right)^2 = (s+v)^2 = s^2 + 2sv + v^2 \quad (60)$$

From equations (59) and (60) derives

$$2^g wv = s(s+2v) \quad (61)$$

This equality definitely requires $s = s_k v$ and the Eq. (61) becomes

$$2^g wv = s_k v^2 (s_k + 2) \quad (62)$$

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 $n \geq 3$ ($n \geq 5$) .