

Khusid Mykhaylo,
pensioner,
citizen of Ukraine,
(Independent Researcher
Wetzlar Germany.)
E-mail: michusid@meta.ua

Algebraic solution of Fermat's theorem
(mathematics, number theory)

Abstract: *Fermat's Last Theorem (or Fermat's last theorem) is one of the most popular theorems in mathematics. Formulated in French mathematician Pierre Fermat in 1637. Despite the simplicity of the formulation, literally, at the “school” arithmetic level, proof of the theorem sought by many mathematicians for more than three hundred years. And only in 1994 year the theorem was proven by the English mathematician Andrew Wilson with colleagues; The proof was published in 1995. [1]-[5]*

With this article, the author completes his research on the given topic, makes corrections and eliminates the errors of the previous ones.

Keywords: *Theorem, Fermat, elementary, solution*

Introduction.

$$X^n + Y^n = Z^n \quad (01)$$

where:

n- prime number, $n > 2$; *X, Y, Z* are integers.

The solutions of which can be X, Y, Z - relatively prime numbers.

1. Decomposition of (01) into multipliers.

If n is odd, then (01) will decompose into multipliers:

$$X^n + Y^n = (X + Y)(X^{n-1} - X^{n-2}Y + \dots - XY^{n-2} + Y^{n-1}) \quad (02)$$

where in the second bracket is the geometric progression

first term $a_1 = X^{n-1}$, and a multiplier $q = -\frac{Y}{X}$

The sum of the members of which $S = \frac{a_1(1 - q^n)}{1 - q}$

$$Z^n = Z_{11} Z_{22} \quad (03)$$

where:

$$Z_{11} = X + Y \quad (04)$$

$$Z_{22} = X^{n-1} - X^{n-2}Y + \dots - X Y^{n-1} + Y^{n-1} \quad (05)$$

2. Equivalent representation Z_{22} .

If we sum the equidistant terms from the middle term of the progression Z_{22} in pairs.

of the middle term of the progression in pairs we have:

for degree 3

$$Z_{22} = (X + Y)^2 - 3XY \quad (06)$$

Fifth degree :

$$Z_{22} = \frac{X^5 + Y^5}{X + Y} = X^4 - X^3 Y + X^2 Y^2 - X Y^3 + Y^4 \quad (07)$$

$$X^4 + Y^4 = (X + Y)^4 - 4 X Y (X + Y)^2 + 2 X^2 Y^2 \quad (08)$$

$$-X Y^3 - X^3 Y = -X Y (X^2 + Y^2) = -X Y (X + Y)^2 + 2 X^2 Y^2 \quad (09)$$

$$Z_{225} = (X + Y)^4 - 5(X + Y)^2 + 5 X^2 Y^2 \quad (10)$$

to the 7th degree:

$$Z_{227} = (X + Y)^6 - 7XY(X + Y)^4 + 14X^2Y^2(X + Y)^2 - 7X^3Y^3 \quad (11)$$

degree n :

$$Z_{22N} = \frac{X^n + Y^n}{X + Y} = (X + Y)^{n-1} - K_{n-3}XY(X + Y)^{n-3} + \dots \mp K_2 X^{\frac{n-3}{2}} Y^{\frac{n-3}{2}} (X + Y)^2 \pm nX^{\frac{n-1}{2}} Y^{\frac{n-1}{2}} \quad (12)$$

$$Z_{22N} = (X + Y)^{n-1} - K_{n-3}XY(X + Y)^{n-3} + \dots \mp K_2 X^{\frac{n-3}{2}} Y^{\frac{n-3}{2}} (X + Y)^2 \pm nX^{\frac{n-1}{2}} Y^{\frac{n-1}{2}} \quad (*)$$

where $K_{n-3} \dots K_2$ corresponding coefficients at $(XY) \dots (X + Y) \dots$

equivalent representation Z_{22N} algebraic sum of even powers of

$X + Y$ and the residual term $\pm n X^{\frac{n-1}{2}} Y^{\frac{n-1}{2}}$.

Note that by n we mean in Mathematical deduction1 any odd power, in

Mathematical deduction2 the power of an odd prime number.

Mathematical deduction1.

Suppose that for an n odd number and for the previous $n-2$

an equivalent representation(*) is valid, then for the next $n+2$ it is

(*) is valid.

We show the transition from the two previous odd degrees to the next one

further:

$$Z_n^n = X^n + Y^n \quad (14a)$$

$$(X^{n-2} + Y^{n-2})(X^2 + Y^2) = X^n + Y^n + Y^2 X^{n-2} + X^2 Y^{n-2} \quad (14b)$$

$$Z_n^n = X^n + Y^n = (X^{n-2} + Y^{n-2})(X^2 + Y^2) - X^2 Y^2 (X^{n-4} + Y^{n-4}) \quad (14c)$$

details:

$$\frac{X^{n_1} + Y^{n_1}}{X + Y} \text{ multiply by } (X + Y)^2 - 2XY$$

$$X^{n+2} + Y^{n+2} = (X + Y)[Z_{22N}(X + Y)^2 - 2XYZ_{22N} - X^2 Y^2 (X^{n-2} + Y^{n-2})] \quad (14)$$

$$(X + Y)^{n-1} - K_{n-3}XY(X + Y)^{n-3} + \dots \mp K_2 X^{\frac{n-3}{2}} Y^{\frac{n-3}{2}} (X + Y)^2 \pm nX^{\frac{n-1}{2}} Y^{\frac{n-1}{2}} *$$

$$* (X + Y)^2 = (X + Y)^{n+1} - K_{n-1(01)}XY(X + Y)^{n-1} + \dots \mp K_{4(01)}X^{\frac{n-3}{2}} Y^{\frac{n-3}{2}} \pm nX^{\frac{n-1}{2}} Y^{\frac{n-1}{2}} (X + Y)^2$$

(15)

$$-2XY \left[(X + Y)^{n-1} - K_{n-3}XY(X + Y)^{n-3} + \dots \mp K_2 X^{\frac{n-3}{2}} Y^{\frac{n-3}{2}} (X + Y)^2 \pm nX^{\frac{n-1}{2}} Y^{\frac{n-1}{2}} \right] =$$

$$=$$

$$-2XY(X + Y)^{n-1} - K_{n-3(02)}2X^2Y^2(X + Y)^{n-3} + \dots \mp K_{2(02)}2X^{\frac{n-1}{2}}Y^{\frac{n-1}{2}}(X + Y)^2 \pm 2X^{\frac{n+1}{2}}Y^{\frac{n+1}{2}} \quad n$$

(16)

$$-X^2Y^2(X + Y)^{n-3} + K_{n-3(03)}X^3Y^3(X + Y)^{n-5} + \dots \pm K_{2(03)}X^{\frac{n-1}{2}}Y^{\frac{n-1}{2}}(X + Y)^2 \mp (n-2)X^{\frac{n+1}{2}}Y^{\frac{n+1}{2}}$$

(17)

where $K_{...(01)}$ - corresponding coefficients when multiplied by $(X + Y)^2$,

$K_{...(02)}$ - corresponding coefficients when multiplied by $-2XY$,

$K_{...(03)}$ - corresponding coefficients when multiplied by $-X^2Y^2$

After adding these algebraic terms we again obtain(*)

Mathematical deduction2.

The equivalent representation (*) is valid for any prime n.

By Mathematical deduction1, if the two previous representations of (*) are valid,

of degree 3 and 5, then it is valid for degree 7. Now

taking the previous 5 and 7 degrees we have its validity for the 9th degree, etc,

which means all odd degrees are described by the above formula.

And since it includes odd prime, it is valid for prime n .

Let us represent (1) as according to Newton's binomial:

$$(X+Y)^n - Z^n = nX^{n-1}Y + \frac{n(n-1)}{2}X^{n-2}Y^2 + \dots + \frac{n(n-1)}{2}Y^{n-2}X^2 + nXY^{n-1} =$$

$$= [(X+Y)-Z]^n - n(X+Y)Z^* \dots \quad (18)$$

From (18) it follows that $X+Y - Z$ is divisible by n and further:

$$(X+Y-Z)[(X+Y-Z)^{n-1} - nk_{n-3}(X+Y)Z(X+Y-Z)^{n-3} \pm nk_2(X+Y)^{n-3}Z^{n-3}(X+Y-Z)^2 \mp n(XY)^{\frac{n-1}{2}}]$$

$$= nX^{n-1}Y + \frac{n(n-1)}{2}X^{n-2}Y^2 + \dots + \frac{n(n-1)}{2}Y^{n-2}X^2 + nXY^{n-1} \quad (18a)$$

it follows:

$$(X+Y)[(X+Y)^{n-1} - \dots \mp n(XY)^{\frac{n-1}{2}}] = Z^n \quad (19)$$

$$Z_{11n} = X+Y \quad (20a)$$

$$Z_{22n} = (X+Y)^{n-1} - nk_{n-3}XY(X+Y)^{n-3} + \dots \pm nk_2X^{\frac{n-3}{2}}Y^{\frac{n-3}{2}}(X+Y)^2 \mp nX^{\frac{n-1}{2}}Y^{\frac{n-1}{2}} \quad (20)$$

3. Analysis of Equation (20).

From equation (20) $Z_{11} = X+Y$ and Z_{22} cannot have a common factor for

except for n . Z_{22} consists of members each of which has a factor $X+Y$, with the exception of the last product $nX^{\frac{n-1}{2}}Y^{\frac{n-1}{2}}$, which in the case of a common factor c

$X+Y$ must involve factors of either X and Y , and they are coprime, so (21). From

which the following equalities follow in the absence of n :

$$X+Y = Z_1^n, \quad Z-X = Y_1^n, \quad Z-Y = X_1^n \quad (21)$$

$$Z_{11} = Z_1^n, \quad Z_{22} = Z_2^n, \quad X_{11} = X_1^n, \quad X_{22} = X_2^n, \quad Y_{11} = Y_1^n, \quad Y_{22} = Y_2^n \quad (22)$$

$$X+Y-Z = nX_1Y_1Z_1K_o \quad (23)$$

where

K_o -an integer coprime to the others specified

except n .

$$Z_1^n = X_1^n + Y_1^n + 2 n X_1 Y_1 Z_1 K_o \quad (24)$$

$$X - Y = X_1^n - Y_1^n \quad (25)$$

$$Z_1^n - Z = n X_1 Y_1 Z_1 K_o \quad (26)$$

$$Z_2 = Z_1^{n-1} - n X_1 Y_1 K_o \quad (27)$$

$$X - X_1^n = n X_1 Y_1 Z_1 K_o \quad (28)$$

$$X_2 = X_1^{n-1} + n Z_1 Y_1 K_o \quad (29)$$

$$Y - Y_1^n = n X_1 Y_1 Z_1 K_o \quad (30)$$

$$Y_2 = Y_1^{n-1} + n Z_1 X_1 K_o \quad (31)$$

$$2 X = Z_1^n - Y_1^n + X_1^n \quad (32)$$

$$2 Y = Z_1^n - X_1^n + Y_1^n \quad (33)$$

$$2 Z = Z_1^n + X_1^n + Y_1^n \quad (34)$$

$$Z_1^n - X_1^n - Y_1^n = 2 n X_1 Y_1 Z_1 K_o \quad (35)$$

$$Z_1^n - [(X_1 + Y_1)^n - n X_1^{n-1} Y_1 - \dots - n Y_1^{n-1} X_1] = 2 n X_1 Y_1 Z_1 K_o \quad (36)$$

$$Z_1 - X_1 - Y_1 = n K_n \quad \text{from which it follows} \quad Z_1 > n \quad (37)$$

Note X, Y, Z are coprime numbers, as well as $X_1, X_2, Y_1, Y_2, Z_1, Z_2$.

If the sum or difference of two coprime numbers has a factor n , then

the sum and difference of the n -power of these numbers is divisible by at least n^2 ,

which is obvious from (20), (04).

If in the expansion Z, X, Y has a prime factor n

$$Z_{22} = nZ_2^n, \quad X_{22} = nX_2^n, \quad Y_{22} = nY_2^n \quad (38)$$

and according to formula (20) Z_2 cannot have n available, otherwise

this will lead to the presence of it in X or Y , and vice versa, which is not acceptable.

Z_2, X_2, Y_2 - does not contain the factor n . In this regard, if Z contains a factor n , then

formula (26) has the form, since sum $X_1^n + Y_1^n$ contains a multiplier n^m where natural number; $m \geq 2$ and

Z_2, X_2, Y_2 - does not contain the factor n .

$$n^{nm-1} Z_1^n = X_1^n + Y_1^n + 2n^m X_1 Y_1 Z_1 K. \quad (39)$$

To solve (34) in integers, degree n in $X_1^n + Y_1^n$, should be equal

degree n in the last monomial, that is, minimally n^2 .

similar:

$$n^{nm-1} X_1^n = Z_1^n - Y_1^n - 2n^m X_1 Y_1 Z_1 K \quad (40)$$

$$n^{nm-1} Y_1^n = Z_1^n - X_1^n - 2n^m X_1 Y_1 Z_1 K \quad (41)$$

$$n^{nm-1} Z_1^n - n^m Z_1 Z_2 = n^m X_1 Y_1 Z_1 K, \quad Z = n^m Z_1 Z_2 \quad (42)$$

$$n^m X_1 X_2 - n^{nm-1} X_1^n = n^m X_1 Y_1 Z_1 K, \quad X = n^m X_1 X_2 \quad (43)$$

$$n^m Y_1 Y_2 - n^{nm-1} Y_1^n = n^m X_1 Y_1 Z_1 K, \quad Y = n^m Y_1 Y_2 \quad (44)$$

What follows:

$$Z_2 = n^{nm-m-1} Z_1^{n-1} - X_1 Y_1 K \quad (45)$$

$$X_2 = n^{nm-m-1} X_1^{n-1} + Z_1 Y_1 K \quad (46)$$

$$Y_2 = n^{nm-m-1} Y_1^{n-1} + Z_1 X_1 K \quad (47)$$

If there is n in Z , we assign it to some $Z_1 = n^n Z_1^n$.

Thus

$X+Y-Z=n X_1 Y_1 Z_1 K_o$ universal,

where X_1, Y_1, Z_1, K_o -coprime corresponds to X, Y, Z with and without n . The difference is:

$$K_o = n^{m-1} K \quad (48)$$

It is not necessary to prove that in the presence of n in X or Y or Z there is or is not a solution. It is enough to prove it without its presence since X, Y, Z are coprime numbers and the presence of n in one of them obliges the other two to its absence.

Минимальное значение степени n в (35):

$$(X_1 + Y_1)^n - Z_1^n - nX_1^{n-1}Y_1 + \dots + nY_1^{n-1}X_1 = Z_1^n - X_1^n - Y_1^n$$

$$(X_1 + Y_1)^n - X_1^n - Y_1^n = (X_1 + Y_1 - Z_1 + Z_1)^n$$

4. Degree $n=3$.

According to (28) and Newton's binomial[6]:

$$\begin{aligned} Z_2^3 &= Z_1^6 - 3(X_1^3 + 3 X_1 Y_1 Z_1 K_o)(Y_1^3 + 3 X_1 Y_1 Z_1 K_o) = (Z_1^2 - 3 X_1 Y_1 K_o)^3 = \\ &= Z_1^6 - 9 Z_1^4 X_1 Y_1 K_o + 27 Z_1^2 X_1^2 Y_1^2 K_o^2 - 27 X_1^3 Y_1^3 K_o^3 \end{aligned} \quad (49)$$

On the other side :

$$\begin{aligned} Z_2^3 &= (X+Y)^2 - 3 X Y = \\ &= Z_1^6 - 3 X_1^3 Y_1^3 - 9 X_1^3 X_1 Y_1 Z_1 K_o - 9 Y_1^3 X_1 Y_1 Z_1 K_o - 27 X_1^2 Y_1^2 Z_1^2 K_o^2 \end{aligned} \quad (50)$$

Underlined in (50) according to (35):

$$-3(X_1^3 + Y_1^3 - Z_1^3 + Z_1^3)3 X_1 Y_1 Z_1 K_o = 2*27 X_1^2 Y_1^2 Z_1^2 K_o^2 - 9 X_1 Y_1 Z_1^4 K_o \quad (51)$$

$$9K_o^3 = 1, \quad K_o^3 = \frac{1}{9} \quad (52)$$

There is no solution in whole numbers.

If Z contains n :

$$X + Y = 3^{3m-1} Z_1^3 \quad (53)$$

$$3 Z_2^3 = 3(3^{3m-1} Z_1^2 - 3^m X_1 Y_1 K_o)^3 = 3^{9m-2} Z_1^6 - 3^{6m+1} Z_1^4 X_1 Y_1 K_o + 3^{5m+1} Z_1^2 X_1^2 Y_1^2 K_o^2 - 3^{3m+1} X_1^3 Y_1^3 K_o^3 \quad (54)$$

$$(X + Y)^2 - 3 X Y = 3^{6m-2} Z_1^6 - 3 X Y \quad (55)$$

(54)=(55), when divided by 3^2 there is no solution in integers.

And the next solution option according to (20) the difference:

$$(X + Y)^{n-1} - Z_2^n = Z_1^{(n-1)n} - Z_2^n = (Z_1^{n-1} - Z_2^n) * \\ * [(Z_1^{n-1} - Z_2^n)^{n-1} - \dots \pm n Z_1^{(n-1)(\frac{n-1}{2})} Z_2^{\frac{n-1}{2}}] = n^2 * \dots \quad (56)$$

The difference factor (49) n is minimal to the second power. Applicable for

$n=3$:

$$Z_1^{2*3} - Z_2^3 = 3 X_1 Y_1 K_o (9 X_1^2 Y_1^2 K_o^2 - 3 X Y) \quad (57)$$

According to (01):

$$Z_2^3 = (X + Y)^2 - 3 X Y \quad (58)$$

Hence $3XY$ is divisible by three squared without remainder, and the need

analog X_2 with monomial $3ZY$ or Y_2 $3ZX$ requires that two relatively prime numbers have a factor n , which does not exist. There is no solution in integers.

5. Degree n .

a) Similar to the third degree, for any degree n , where n is prime

odd, the presence of n in one of X, Y, Z will lead to its obligatory presence in

the rest. The confirmation is (20), where in addition to the first polynomial $(X + Y)^{n-1}$

all the rest have a factor of n to the first power, and their sum must contain at least

n^2 according to (56). The remaining members, except for the last one, contain 2

complete ones from X, Y, Z

and one of the elements $X_{11}=Z-Y, Y_{11}=Z-X, Z_{11}=X+Y$ from the missing third. Thus, in total they will give at least n^2 provided that one of them has a factor of n , which will lead to the inevitable presence of a factor of n in the other two, which is also impossible, since X, Y, Z are coprime numbers.

b) It is for this case that we examine the balance of the factor n .

Let us consider equation (01) based on (26), (28), (30):

$$(X_1^n + n X_1 Y_1 Z_1 K_o)^n + (Y_1^n + n X_1 Y_1 Z_1 K_o)^n = (Z_1^n - n X_1 Y_1 Z_1 K_o)^n \quad (59)$$

Let's open the brackets:

$$\begin{aligned} & n X_1 Y_1 Z_1 K_o X_1^{n(n-1)} + n X_1 Y_1 Z_1 K_o Y_1^{n(n-1)} + n X_1 Y_1 Z_1 K_o Z_1^{n(n-1)} + \dots \\ & \dots + 2 \underline{(n X_1 Y_1 Z_1 K_o)^n} + X_1^{nm} + Y_1^{nm} - Z_1^{nm} = 0 \end{aligned} \quad (60)$$

According to (60), the underlined free term is relatively $n X_1 Y_1 Z_1 K_o$

is divisible without remainder by n^{m+1} , where m is the degree taking into account its K_o .

Then we have:

$$Z_1^n - X_1^n - Y_1^n \quad (61)$$

is divisible without remainder by n^m and :

$$Z_1^{nm} - X_1^{nm} - Y_1^{nm} \quad (62)$$

is divisible without remainder by n^{m+1} .

What should we proceed from (20):

$$Z_1^{nm} - X_1^{nm} - Y_1^{nm} = Z_1^{nm} - (X_1^{nm} + Y_1^{nm}) = Z_1^{nm} - (X_1^n + Y_1^n)^n + n(X_1^n + Y_1^n)^{n-2} - \dots \pm n(X_1 Y_1)^{\frac{n-1}{2}} *$$

$$* (X_1^n + Y_1^n) =$$

$$= Z_1^{nm} - (X_1^n + Y_1^n)^n + n X_1^n Y_1^n (X_1^n + Y_1^n)^{n-2} - \dots \pm n (X_1^n Y_1^n)^{\frac{n-1}{2}} (X_1^n + Y_1^n) \quad (63)$$

 where the sum of the underlined terms, referring to (20) contains n^{m+1} .

Further, according to (24):

$$Z_1^{n^2-1} - (Z_1^{n-1} - 2n X_1 Y_1 K_o)(Z_1^n - 2n X_1 Y_1 Z_1 K_o)^{n-1} + (Z_1^{n-1} - 2n X_1 Y_1 K_o) * n^{m+1} \dots \quad (64)$$

and then after opening the brackets (other monomials with a factor n^{m+1}):

$$2n X_1 Y_1 Z_1^{n^2-n} (Z_1^{n-1} - 1) \quad (65)$$

inevitably divides into a simple n . From which it follows according to (27) Z_2^{n-1} also divisible without remainder by prime n .

Similarly:

$$X_1 [(Z_1^m - Y_1^m) - X_1^m] \quad (66)$$

$$\frac{Z_1^n - Y_1^n}{X_1} = \frac{X_1^n + 2n X_1 Y_1 Z_1 K_o}{X_1} = X_1^{n-1} + 2n Z_1 Y_1 K_o \quad (67)$$

$$(X_1^{n-1} + 2n Y_1 Z_1 K_o)(X_1^n + 2n X_1 Y_1 Z_1 K_o)^{n-1} - X_1^{n^2-1} \quad (68)$$

$$X_1^{n-1} - 1, X_2 - X_1^{n-1}, X_2 - 1, X_2^{n-1} - 1 - \text{are divisible by } n \quad (69)$$

$$(X + Y)^{n-1} - 1 = (X_1^n + Y_1^n + 2n X_1 Y_1 Z_1 K_o)^{n-1} - 1 = X_1^{(n-1)n} + \dots + Y_1^{(n-1)n} - 1 \quad (70)$$

Thus, the division of one component is inevitable X_1, Y_1, Z_1

without remainder on n , so that (62) contains n^{m+1} , but there is no solution point 5.a). Otherwise, the free term with respect to p (62) contains a factor n^m and turns into a fraction when reduced in n^{m+1} and there is no solution (01) in integers..

6. Conclusion.

If the degree in (01) is odd, there is no solution. Pharm proved the absence of a

solution for the 4th degree and thereby proved its absence for everyone $n=2^m$, where m is an integer. Fermat's theorem is solvable in the first and second powers!

Literature:

[1]The Moment of Proof: Mathematical Epiphanies.—Oxford University Press, 1999.—ISBN 0-19-513919-4.

[2]Faltings, Gerd(1995).The Proof of Fermat's last theorem by R. Taylor and A. Wiles,Notices of the AMS(42) (7), 743—746.

[3]Daney, Charles(2003).The Mathematics of Fermat's last theorem. Retrieved Aug. 5, 2004.

[4]O'Connor, J. J. & and Robertson, E. F.(1996).Fermat's last theorem. The history of the problem. Retrieved Aug. 5, 2004.

[5]Shay, David (2003).Donald C. Benson.. Retrieved Aug. 5, 2004.

[6]<https://www.britannica.com/science/binomial-theorem>