International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, December 2012)

The Truly Marvellous Proof

Leszek Włodzimierz Guła

***Abstract*- The elementary proof of the Fermat's Last Theorem.**

***Keywords*— Greatest Common Divisor, Indirect Proof, Newton Binomial Formula, Pythagorean Theorem, Square Trinomial.**

I. Introduction

Problem II.8 of the Diophantus' Arithmetica asks how a given square number is split into two other squares. Diophantus' shows how to solve this sum-of-squares problem for $k = 4$ and $u = 2$, inasmuch as for all $k,u \in Z$:

$$k^2 = [2ku/(u^2 + 1)]^2 + [k(u^2 - 1)/(u^2 + 1)]^2. \qquad (1)$$

Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the Arithmetica next to Diophantus' sum-of-squares problem: it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

From *(1)* it implies that for all relatively prime numbers $u > v$ such that $u - v$ is odd:

$$(u^2 + v^2)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = (u^2 - v^2)^2 + (2uv)^2.$$

Thus for some $x,y,z \in N_1$ we get a primitive Pythagorean triple $(x,y,z) = (u^2 - v^2, 2uv, u^2 + v^2)$ - the primitive because $gcd(x,y,z) = 1$.

II. The Fermat's Last Theorem

Theorem 1. *For all* $n \in N_3$ *and for all* $X,Y,Z \in N_1$:

$$X^n + Y^n \neq Z^n.$$

Proof. Let for some $n \in N_3$ and for some $X,Y,Z \in N_1$, with $gcd(X,Y,Z) = 1$:

$$X^n + Y^n = Z^n. \qquad (2)$$

From *(2)* it follows that

$$X + Y > Z \wedge X^2 + Y^2 > Z^2 \wedge X^{n-1} + Y^{n-1} > Z^{n-1}, \qquad (3)$$

Otherwise $X^n + Y^n < Z^n$, which is obviously.

From *(2)* and *(3)* it implies that only one number out of (X,Y,Z) is even and the even number $X + Y - Z > 0$ and if n is even, then Z is odd – which is obviously.

We assume that $X, Z - Y$ are odd and that for some relatively prime numbers $u > v$ such that $u - v \in \{3,5,7,...\}$:

$2v(u - v) = X + Y - Z$ and $(u - v)^n + 2v(u - v) = X$ because for $(u - v)^2 + 2v(u - v) = X$ we get

$X + Z - X - (u - v)^2 = Y \wedge X^2 + [X + Z - X - (u - v)^2]^2 - (Z - X + X)^2 > 0 \wedge X^2 - 2(u - v)^2X - 2(Z - X)(u - v)^2 + (u - v)^4 > 0 \wedge 2v^2 = Z - X \wedge \sqrt{\Delta} = 4v(u - v)$

And consequently a false sentences

$$X < X_1 = (u - v)^2 - 2(u - v) \vee (u - v)^2 + 2(u - v) = X_2 < X.$$

Hence, with $gcd(u,v,c) = 1$ it must be

$$1 < c = u - v \wedge c^n + 2vc = X \wedge c^n = Z - Y \wedge Z - X + 2vc = Y \wedge c^n + Y = Z \wedge (c^n + 2vc)^n = (c^n + Y)^n - Y^n \wedge (Z - X + 2vc)^n = (Z - X + X)^n - X^n.$$

Thus

$$c^{n(n-2)}2vc + (n - 1)c^{n(n-3)}(2vc)^2/2 + ... + (2vc)^{n-1} + (2v)^n/n = Y[c^{n(n-2)} + (n - 1)c^{n(n-3)}Y/2 + ... + Y^{n-2}] \wedge$$

$$(Z - X)^{n-2}2vc + (n - 1)(Z - X)^{n-3}(2vc)^2/2 + ... + (2vc)^{n-1} + (2vc)^n/(n(Z - X)) = X[(Z - X)^{n-2} + (n - 1)(Z - X)^{n-3}X/2 + ... + X^{n-2}].$$

Therefore for some $n \in N_3$ and for some $v,c \in \{3,5,7,...\}$:

$$c^n + 2vc = X \wedge [odd\ gcd(n,Y) > 1 \vee odd\ gcd(n,Z) > 1] \wedge gcd(n,c) = 1 \wedge Z - X + 2vc = Y \wedge c^n + Z - X + 2vc = Z.$$

Moreover for $n \in \{3,5,7,...\}$:

$$[X + Y + (-Y)]^n + Y^n = [X + Y + (-2vc)]^n \Rightarrow$$

$$[(X + Y)^{n-2}(- Y) + (n - 1)(X + Y)^{n-3}(- Y)^2/2 + ... + (- Y)^{n-1} = (X + Y)^{n-2}(- 2vc) + (n - 1)(X + Y)^{n-3}(- 2vc)^2/2 + ... + (- 2vc)^{n-1} - (2vc)^n/(n(X + Y)) \wedge (n|Y \vee n|X + Y, Z) \wedge n|v].$$

A. The Proof for Odd n, $Z - X$, Y

From the above we get - for some $n,m,c \in \{3,5,7,...\}$ and for some $h \in \{1,3,5,...\}$, with $gcd(n,m,c,h) = 1$:

$$nmh = v \wedge c^n + 2nmch = X \wedge \{[n|Y \wedge n^{n-1}h^n + 2nmch = Y \wedge 2^nm^n = X + Y = c^n + n^{n-1}h^n + 4nmch \wedge n^{n-1}h^n + X = Z] \vee [n|X + Y, Z \wedge h^n + 2nmch = Y \wedge 2^nn^{n-1}m^n = X + Y = c^n + h^n + 4nmch \wedge h^n + X = Z]\}.$$

Thus for some $n,m,c \in \{3,5,7,...\}$ and for some $h \in \{1,3,5,...\}$, with $gcd(n,m,c,h) = 1$:

$$\{[(2m)^n - c^n = n^{n-1}h^n + 4nmch \wedge n|2m - c] \vee [2^nn^{n-1}m^n = c^n + h^n + 4nmch \wedge n|c + h]\} \Rightarrow$$

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, December 2012)

$\{[n^2 \mid (2m)^n - c^n \wedge ((2m)^n - c^n)/n^2 = n^{n-3}h^n + 4mch/n \wedge gcd(n,m,c,h) = 1] \vee [n^2 \mid c^n + h^n \wedge gcd(n,m,c,h) = 1 \wedge 2^n n^{n-3}m^n = (c^n + h^n)/n^2 + 4mch/n]\} \Rightarrow$

$mch/n \notin \{3,5,7,...\}$. ♣

B. The Proof for Odd n and Even Z – X, Y

From the above we get - for some $n,m,c \in \{3,5,7,...\}$ and for some $h \in \{1,3,5,...\}$, with $gcd(n,m,c,h) = 1$:

$nmh = v \wedge c^n + 2nmch = X \wedge \{[n|Y \wedge 2^n n^{n-1}h^n + 2nmch = Y \wedge m^n = X + Y = c^n + 2^n n^{n-1}h^n + 4nmch \wedge 2^n n^{n-1}h^n + X = Z] \vee [n| X + Y, Z \wedge 2^n h^n + 2nmch = Y \wedge n^{n-1}m^n = X + Y = c^n + (2h)^n + 4nmch \wedge 2^n h^n + X = Z]\}$.

Thus for some $n,m,c \in \{3,5,7,...\}$ and for some $h \in \{1,3,5,...\}$, with $gcd(n,m,c,h) = 1$:

$\{[m^n - c^n = 2^n n^{n-1}h^n + 4nmch \wedge n \mid m - c] \vee [n^{n-1}m^n = c^n + (2h)^n + 4nmch \wedge n \mid c + 2h]\} \Rightarrow$

$\{[n^2 \mid m^n - c^n \wedge (m^n - c^n)/n^2 = 2^n n^{n-3}h^n + 4mch/n \wedge gcd(n,m,c,h) = 1] \vee [n^2 \mid c^n + (2h)^n \wedge gcd(n,m,c,h) = 1 \wedge n^{n-3}m^n = (c^n + (2h)^n)/n^2 + 4mch/n]\} \Rightarrow$

$mch/n \notin \{3,5,7,...\}$. ♣

C. The Proof for Even n

From the above it follows that for some $a \in \{2,3,4,...\}$ and for some $v, c, X, Z \in \{3,5,7,...\}$

And for some $Y \in \{6,10,14,...\}$ and for some relatively prime numbers $U > V$ such that $U - V \in \{3,5,7,...\}$, with $gcd(a,c) = 1$ and $gcd(v,c) = 1$:

$\{[2a = n \wedge (c^{2a} + 2vc)^{2a} = X^{2a} = Z^{2a} - Y^{2a} \wedge X^a = U^2 - V^2 \wedge Z^a = U^2 + V^2 \wedge Y^a = 2UV \wedge (c^{2a-1} + 2v)^{2a} = Z^a + Y^a = (U + V)^2 \wedge c^{2a} = (U - V)^2 = Z^a - Y^a = Z - Y \equiv 0 \wedge (U + V, U - V) = ((c^{2a-1} + 2v)^a, c^a) \wedge gcd(U + V, U - V) = gcd((c^{2a-1} + 2v)^a, c^a) = 1] \equiv 0\}$.

This is the proof. ♣

REFERENCES

[1] Gładki,P., http://www.math.us.edu.pl/~pgladki/faq/node135.html
[2] http://en.wikipedia.org/wiki/Fermat's_Last_Theorem