Pythagorean triples and Fermat's theorem n = 4

Rolando Zucchini

Independent math researcher Italy
author of :
SCQ - Syracuse Conjecture Quadrature © – viXra 2305.0029
A theorem on the Golden Section and Fibonacci numbers © – viXra 2310.0020

ABSTRACT

This article contains a theorem to build the Primitive Pythagorean triples and the proof of the last Fermat's Theorem for n = 4.

CONTENTS

Introduction

The last Fermat's theorem states :

The equation $x^n + y^n = z^n$ has not integer solutions for $n > 2$

It's the generalization of the equation of Diaphanous :

$$x^2 + y^2 = z^2$$

on the Pythagorean triples. That is, three positive integers (x; y; z) which satisfy Pythagoras's theorem. Already at that time many Pythagorean triples were know : (3;4;5); (6;8;10); (5;12;13); (15;20;25); … …
We can observe that once a primitive triple is know, we can obtain infinite ones from it by multiplying its three terms by any natural number *m*. In fact, assuming that (a; b; c) is a Pythagorean triple : $a^2 + b^2 = c^2$; multiplying the three numbers by a generic $m > 0$, we obtain the triple (ma; mb; mc), and it turns out $(ma)^2 + (mb)^2 = (mc)^2 = m^2 \cdot (a^2 + b^2) = m^2c^2 \rightarrow a^2 + b^2 = c^2$.

Co-prime numbers

Two positive (natural) integers are co-prime (or relatively prime) if and only if they do not have a divisor in common except 1, or how to say : GCD(a; b) = 1. A simple method to establish whether two natural numbers are co-prime, without resorting to their factorization, is the so-called Euclid algorithm. It's the oldest algorithm and is reported in Euclid's famous book *Elements*. It was probably already know by Eudoxus of Cnidus (390 – 337 (?) B.C.) and it is mentioned in the writings of Aristotle. Using he methodology of modular arithmetic (see historical note 1) Euclid's algorithm is summarized in the following procedure :

a / b = q + r = a **mod**b
If r = 0 → GCD(a; b) = b
If r ≠ 0, we pose a = b ∧ b = r → b / r = $q_1 + r_1$ = b **mod**r
If $r_1 = 0$ → GCD(a; b) = r
If $r_1 \neq 0$, we pose b = r ∧ r = r_1 → r / r_1 = $q_2 + r_2$ = r **mod**r_1
… …

Example: GCD(76; 16) : 76/16 = 4 + r = 12 = 76 **mod**16 → 16/12 = 1 + r = 4 = 16 **mod**12 → 12/4 = 3 + r = 0 = 12 **mod**4 → GCD(76;16) = 4.

Co-prime numbers have the following properties:

1) If *a* and *b* are co-prime and *a* divides the product *bc*, then *a* divides *c*.
2) The natural numbers *a* e *b* are co-prime if and only if there exist two natural integers *x* and *y* such that $a \cdot x + b \cdot y = 1$.
3) If *a* and *b* are co-prime then the numbers $2^a - 1 \wedge 2^b - 1$ they are also co-prime.
4) If *a* and *b* are co-prime, then in the Cartesian plane the point *P*(*a;b*) is visible from the origin. That is, no other points with entire coordinates lie on the segment *OP* of the straight line *r*(*OP*).

Remark

Two co-prime numbers they are said of opposite parity if one is even and the other is odd.

The infinite descent

The infinite descent is a demonstrative method by contradiction, used in number theory and applicable to the properties of integer natural number. It allows us to state if a certain property is satisfied by a positive integer, it cannot be satisfied by a smaller integer. In fact, assuming that they are valid for any number they should be valid for smaller numbers, for even smaller numbers, and so on up to infinite. But this process cannot be applied to integers because they cannot decrease through an infinite number of steps. In brief: if we want to demonstrate that a proposition *p* is false, it is assumed that it's true for a certain integer *n*, and if it is also valid for $m < n$, then *p* is always false; in fact, repeating the reasoning, there would exist another number $k < m < n$ for which *p* would be true. But this is absurd and therefore the proposition *p* is false. This type of reasoning was invented by Pierre de Fermat to demonstrate the particular case $n = 4$ of his famous theorem (§ 5.).

An example of application infinite descent

Theorem : *The Diophantine equation* $x^2 + y^2 = 3(z^2 + w^2)$ *does not admit integer solutions, excluding the trivial solution* $x = y = z = w = 0$.

Demonstration:

Using the terminology of modular arithmetic, if there were a quadruple $(x_0;y_0;z_0;w_0)$ solution of the equation, we would have : $x_0^2 + y_0^2 \equiv 0 \bmod 3$. But this is only possible if x_0 and y_0 are divisible by 3. Putting $x_0 = 3x_1 \wedge y_0 = 3y_1$ and replacing them in the initial equation we have :

$(3x_1)^2 + (3y_1)^2 = 3(z_0^2 + w_0^2) \rightarrow 9(x_1^2 + y_1^2) = 3(z_0^2 + w_0^2) \rightarrow 3(x_1^2 + y_1^2) = z_0^2 + w_0^2$

Also in this case z_0 and w_0 are multiples of 3, therefore : $x_1^2 + y_1^2 = 3(z_1^2 + w_1^2) \rightarrow (x_1;y_1;z_1;w_1)$ is solution of the equation with $x_1 < x_0$, $y_1 < y_0$, $z_1 < z_0$, $w_1 < w_0$. For the infinite descent it follow that the Diophantine equation $x^2 + y^2 = 3(z^2 + w^2)$ does not admit integer solutions.

The Pythagorean triples

Theorem : *If* $x, y, z \in N : x^2 + y^2 = z^2$ *then there exist two integer numbers* $p \wedge q$ $(p > q)$ *such that :*

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases}$$

Demonstration :

If x, y, z constitute a Pythagorean triple then they are mutually co-prime
If two of them had a common divisor, then it should also be common at the third. Hence :
$x = d \cdot x_1$, $y = d \cdot y_1$, $z = d \cdot z_1$; substituting into Pythagorean triple we have :

$x^2 + y^2 = z^2 \rightarrow (d \cdot x_1)^2 + (d \cdot y_1)^2 = (d \cdot z_1)^2 \rightarrow d^2 \cdot x_1^2 + d^2 \cdot y_1^2 = d^2 \cdot z_1^2 \rightarrow x_1^2 + y_1^2 = z_1^2$

then $x_1 = x/d$, $y_1 = y/d$, $z_1 = z/d$ constitute a primitive Pythagorean triple.

$(8;6;10) \rightarrow (8/2;6/2;10/2) \rightarrow (4;3;5)$ primitive
$(20;15;25) \rightarrow (20/5;15/5;25/5) \rightarrow (4;3;5)$ primitive

… .

It follows that x, y, z cannot be even numbers, because they would be divisible by 2; x, y, z cannot be three odd numbers, because the square of an odd number is still odd and the sum of two odd numbers result an even number; hence z cannot be odd. If x, y are two odd numbers, z cannot be an even number, because if this happens we have : $z = 2k \rightarrow x^2 + y^2 = z^2 = 4k^2$. If we pose $x = 2m+1 \wedge y = 2n+1$ we would have : $(2m+1)^2+(2n+1)^2 = (2k)^2 \rightarrow 4m^2+4m+1+4n^2+4n+1 = 4k^2 \rightarrow 4m^2+4n^2+4m+4n+2 = 4k^2 \rightarrow 4m^2+4n^2+4m+4n = 4k^2-2 \rightarrow 4(m^2+n^2+m+n) = 2(2n^2-1) \rightarrow 2(m^2+n^2+m+n) = 2n^2-1$ which is impossible. In short, z^2 is a doubly even number (divisible by 4) and cannot be the sum of the squares of two odd numbers, because this sum is simply even.

Examples :

$1^2 + 3^2 = 1 + 9 = 10$ simply even
$3^2 + 5^2 = 9 + 25 = 34$ simply even
$5^2 + 7^2 = 25 + 49 = 74$ simply even
$7^2 + 9^2 = 49 + 81 = 130$ simply even
$3^2 + 7^2 = 9 + 49 = 58$ simply even
$5^2 + 9^2 = 25 + 81 = 106$ simply even
… …

In general, if we choose two generic odd numbers we will have :
$(2m+1)^2 + (2n+1)^2 = 4m^2+4m+1 + 4n^2+4n+1 = 4(m^2+n^2)+4(m+n)+2$ simply even.

We can therefore conclude that in Pythagorean triples (x, y, z) : $x^2 + y^2 = z^2$, $x \wedge y$ must be two primes numbers of opposite parity and z must be an odd number

If $x^2 + y^2 = z^2 \rightarrow x^2 = z^2 – y^2 = (z + y)(z – y)$, setting x even and y odd, being z odd, it follow that z+y and z-y they are even being the addition and subtraction of two odd ones. From this, there will exist u, v, w, such that $x = 2u$; $z + y = 2v$; $z - y = 2w$. Then :

$(2u)^2 = (2v)\cdot(2w) \rightarrow 4u^2 = 4vw \rightarrow u^2 = vw$

Combining the two equalities by addition and subtraction $\begin{cases} z + y = 2v \\ z - y = 2w \end{cases}$
We have :

$2z = 2v + 2w \rightarrow z = v + w$
$2y = 2v – 2w \rightarrow y = v – w$

Hence, being $y \vee z$ odd, $v \wedge w$ they must necessarily be co-prime of opposite parity. If this were not the case, any common factor between them would also divide $z \wedge y$, but this, as assumed, is impossible. Furthermore $u^2 = vw$ in only make sense if $u \wedge v$ are two squares. So, there exist $p \wedge q$ such that $v = p^2 \wedge w = q^2$ and GCD(p; q) = GCD(u; v) = 1.

Substituting we have :

$z = v + w = p^2 + q^2$
$y = v – w = p^2 – q^2$ $(p > q)$

Then : $x^2 = z^2 – y^2 = (z + y)(z – y) = 2v\cdot2w = 4vw = 4p^2q^2 \rightarrow x = 2pq$

We can therefore conclude that :

$$\begin{cases} x = 2pq \\ y = p^2 - q^2 \\ z = p^2 + q^2 \end{cases} \qquad \rightarrow \text{ Q.E.D.}$$

Examples :

(4;3;5) : p = 2 ∧ q = 1
(12;5;13) : p = 3 ∧ q = 2.

If we choose p = 6 ∧ q = 5 we have the primitive Pythagorean triple (60;11;61).
… …

If we choose p = 21 ∧ q = 16 we have the primitive Pythagorean triple (672;185;697).
… …
… …

Whit such a procedure it is possible to build infinite primitive Pythagorean triples.

Last Fermat's theorem for n = 4

Statement :

The equation $x^4 + y^4 = z^4$ does not admit positive integer solutions if $xyz \neq 0$ ($x, y, z \neq 0$).

Demonstration :

Let's consider the case $x^4 + y^4 = z^2$ because $z^4 = (z^2)^2$. As seen previously x, y, z are co-prime and therefore are also co-prime x^2, y^2, z^2; furthermore, being Pythagorean triple it turns out :

$$\begin{cases} x^2 = 2pq \\ y^2 = p^2 - q^2 \\ z^2 = p^2 + q^2 \end{cases}$$

With p ∧ q co-prime of opposite parity and p > q > 0.

From $y^2 = p^2 - q^2 \rightarrow q^2 + y^2 = p^2$; q, y, p they are still Pythagorean triples with p odd and q even being of opposite parity. Then :

$$\begin{cases} q = 2ab \\ y = a^2 - b^2 \\ p = a^2 + b^2 \end{cases}$$

With a, b co-prime of opposite parity : a > b > 0.

From $x^2 = 2pq \rightarrow x^2 = 2(a^2+b^2)\cdot 2ab = 4ab(a^2+b^2)$ in which ab is a square and [ab; (a^2+b^2)] are co-prime. In fact if a certain h divided ab then it would have to divide a or b, but not both because a, b are co-prime. It follows that h cannot divide (a^2+b^2). Since ab and (a^2+b^2) are squares, and a, b co-primes, a and b are also squares.

Setting $a = X^2$ and $b = Y^2$ from $p = a^2 + b^2$ we obtain :

$$X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 \rightarrow X^4 + Y^4 < z^4 = x^4 + y^4.$$

Iterating the procedure two new solutions will be found $X_1 < X \wedge Y_1 < Y$ such that $X_1^2 + Y_1^2 < z^4$. Thus proceeding ad infinitum. But the infinite descent is not applicable to positive integer numbers (natural numbers); hence, since the sum of two fourth powers cannot be a square, it cannot be a fourth power either.

Remark :

From the theorem above it follows that the equation $x^{4m} + y^{4m} = z^{4m}$ does not admit integer solution. In fact, if we put $X = x^m$, $Y = y^m$, $Z = z^m \rightarrow X^4 + Y^4 = Z^4$, which, as demonstrated before, does not have integer solutions. We can conclude that the equation :

$$x^n + y^n = z^n$$

does not admit positive integer solutions if n is divisible by 4; i.e. : $x^8 + y^8 = z^8$; $x^{12} + y^{12} = z^{12}$; … .

In addition : if $n > 2$ is not divisible by 4 and is not power of 2, it will be divided by a certain prime number $p \neq 2$. So, if we pose $n = pm$; for to prove that $x^n + y^n = z^n$ have not integer solutions it will be enough to prove that $x^p + y^p = z^p$ does not have integers solutions. Hence the proof of the last Fermat's theorem for $n = 4$ allows us to reduce the general case to the case in which $n > 2$ is a prime number.

Historical notes

1) The modular arithmetic, also known as clock arithmetic because is based on the calculation of hours in cycles of 12 or 24, is an important mathematical technique in integer number theory, with many applications in arithmetic and algebra. It was introduced by C. F. Kauss (Carl Friedrich Gauss; Braunschweig 1777 – Gottinga 1855) in the treatise *Disquisitiones Arithmeticae* published in 1801.

2) Fermat (Pierre de Fermat; Beaumont de Lomagne 1601– Castres 1665) was a mathematician and magistrate. He enjoyed reading classical Greek texts on geometry and arithmetic. He leaves many hypotheses or conjectures to posterity. Also the so-called last Fermat's theorem, formulated by him in 1637, it was nothing more than a conjecture. It was called theorem because he declared that he had demonstrated it in an annotation in the margins of Diaphanous book, in which it was written *"I have a wonderful demonstration of this theorem with cannot be contained in the too narrow margin of the page*". But, evidently, this was not the case. As we saw, he proves the theorem only for $n = 4$.

3) Euler (Leonhard Euler 1707 – 1783) proved the case $n = 3$.
Marie-Sophie Germain (Paris 1776 – 1831) argued that Fermat's theorem was probably true for an *n* equal to a particular prime number *p* such that $p = 2n+1$ was also prime.
The case $n = 5$ was demonstrated by Adrien-Marie Legendre (Paris 1752 – 1833).
The case $n = 7$ was proved, in 1839, by Gabriel Lamè (1796 – 1870).

The general proof of the last Fermat's theorem was given by Andrew John Wiles (Cambridge 1953 – Princeton 2015).

References – **Bybliography**

Wikipedia (wiki) : Teorema di Fermat
www.unica.it : Teorema di Fermat n = 4
www.uniroma3 : Teorema di Fermat Cenni Storici
Il quinto postulato : Zucchini R., Mnamon Milano 2012
Gli incommensurabili : Zucchini R., Mnamon Milano 2013