A Journey into Fermat’s Equation

Mario De Paz and Enzo Bonacci

1. Department of Physics, University of Genoa, Genova I-16146, Italy
2. L.S.S. “G.B. Grassi” of Latina, Latina I-04100, Italy

Received: July 12, 2012 / Accepted: August 21, 2012 / Published: September 25, 2012.

Abstract: As expounded in some recent mathematical conferences, this research on that amazing source of algebraic ideas known as Fermat’s equation is aimed to prove how Fermat triples can be limited until the impossible existence through a criterion of incompatible parities related to unexplored properties of the binomial coefficients. In this paper, the authors use a technique based on the analysis of four numbers and their internal relations with three basic compulsory factors. It leads to the practical impossibility to find any triple of natural numbers candidate to satisfy Fermat’s equation, because when the authors try to meet a condition between parity and range the authors are compelled to violate the other one, so that they are irreducibly alternative. In particular, there is a parity violation when the authors choose all the basic factors in the allowed range and the authors obtain exceeding values of one of the involved variables when the authors try to restore the parity. Since Fermat’s last theorem would consequently be demonstrated, many readers could recall the never found elementary proof of FLT (Fermat’s last theorem) claimed by Pierre de Fermat. The authors are not encouraging such an interpretation because this paper is intended as a journey into Fermat’s equation and the reader’s attitude should be towards the algebraic achievements here proposed, with their possible hidden flaws and future developments, rather than to legendary problems like Fermat’s riddle.

Key words: Fermat’s equation, binomial coefficients, incompatible parities, Fermat’s last theorem, Fermat’s little theorem.

1. Introduction

Among the unexplored properties of the binomial expansion with relevant influences in limiting Fermat triples until an almost impossible condition of existence presented at the 5ecm 2008 [1], the most promising seemed the criterion of incompatible parities elucidated at the VII Iaconu 2009 [2].

Such achievement was improved in the talk at the VIII Iaconu 2011 [3]. As pointed out in the ICMSA 2011 [4] and in the ICA 2012 [5], Fermat’s equation is an amazing source of algebraic ideas all worthy to be illustrated like in a journey.

2. Four Positive Integers in Fermat’s Equation

Let be $a, b, c, k$ four positive integers related by

$$a + b - c = k$$ (1)

with $a, b, c$ relatively primes and $k > 0$ even.

Let us initially suppose that $c$ and $a$ are odd while $b$ is even. The Eq. (1) must be satisfied if

$$a^p + b^p - c^p = 0$$ (2)

with $p > 2$ prime, i.e., in the case of Fermat’s equation at prime indexes. Let us define:

$$x = c - b$$ (3)
$$y = c - a$$ (4)
$$z = a + b$$ (5)

The four initial numbers $a, b, c, k$ are expressed by the following combinations of $x, y, z$:

$$a = \frac{x - y + z}{2}$$ (6)
$$b = \frac{-x + y + z}{2}$$ (7)
$$c = \frac{x + y + z}{2}$$ (8)
$$k = \frac{-x - y + z}{2}$$ (9)

As obvious, $x, y, z$ cannot be chosen at will because $x < z, y < z, x + y < z$ and $z$ cannot be too large with respect to $x + y$ in order to be within the limits imposed by Eq. (2). The authors will meet...
this last limit below. If the Eq.(2) is satisfied by three naturals not containing \( p \) as a factor, it is easily proved (Section 3) that \( x, y, z \) are \( p \)-powers of three basic factors \( f_x, f_y, f_z \) and that \( k \) contains all of them and \( p \) as factors, \( a \) contains \( f_x \) as a factor, \( b \) contains \( f_y \) as a factor, \( c \) contains \( f_z \) as a factor:

\[
\begin{align*}
x &= f_x^p \\
y &= f_y^p \\
z &= f_z^p \\
a &= a_0 f_x \\
b &= b_0 f_y \\
c &= c_0 f_z \\
k &= k_0 f_x f_y f_z
\end{align*}
\]

Let us notice that the Eqs. (10 -- 16) restrict only the Fermat triples, not the Pythagorean triples.

The limits set for \( x, y, z \) in the Eqs. (10 -- 16) restrict the choices of the basic factors \( f_x, f_y, f_z \) which are powered to \( p \); the Eqs. (6 -- 9) become:

\[
\begin{align*}
a &= \frac{f_x^p - f_y^p + f_z^p}{2} = a_0 f_x \\
b &= \frac{-f_x^p + f_y^p + f_z^p}{2} = b_0 f_y \\
c &= \frac{f_x^p + f_y^p + f_z^p}{2} = c_0 f_z \\
k &= \frac{-f_x^p - f_y^p + f_z^p}{2} = k_0 f_x f_y f_z
\end{align*}
\]

It is evident that \( f_x f_z \) must be a multiple of 4 in order to obtain \( a, b, c, k \) with the correct parity. If not so, two out of the three numbers defined by the Eqs. (17 -- 20) would be even, while it is essential that two are odd, e.g.: \( f_x = 1, f_y = 2, f_z = 3, p = 5, \)

\[
a = \frac{1 - 32 + 243}{2} = 106, \quad b = \frac{-1 + 32 + 243}{2} = 137, \quad c = \frac{1 + 32 + 243}{2} = 138.
\]

Moreover, it is possible to satisfy the Eqs. (17 -- 20) by imposing a strict relation among \( f_x, f_y, f_z \); otherwise the variables \( a, b, c \) would not hold the condition of having \( f_x, f_y, f_z \) respectively as factors. First we try with the simplest:

\[
f_x + f_y - f_z = 0
\]

but this choice, even though allowing the Eqs. (17) and (19) to be satisfied, does not allow to satisfy the Eqs. (18) and (20) where \( b \) and \( k \) are only divisible by \( \frac{f_y}{2} \) giving rise to a parity violation.

In fact, both relations require that \( \frac{f_x^p - f_y^p}{f_y} \) is an even number, while from Bonacci’s [6] binomial expansion

\[
f^p_x - f^p_y = (f_x - f_y)^p + p f_x f_y (f_x - f_y) R_p(f_x, f_y)
\]

and by Eq. (21) it is

\[
\frac{f_x^p - f_y^p}{f_y} = (f_x - f_y)^{p-1} + p f_x f_y R_p(f_x, f_y),
\]

i.e., an always odd result from the sum of an even number plus an odd number. If we impose \( f_x + 2f_y - f_z = 0 \) in order to remove such a violation then the Eqs. (17) and (19) are no longer satisfied.

Another possibility is offered by the relation:

\[
f_x^p + f_y^p - f_z = 0
\]

which allows the Eqs. (17 -- 20) for any prime \( p > 2 \).

However, if the Eq. (22) is used then the value of \( f_z \) is always too large and does not allow \( a, b, c \) to be within the limits imposed by Eq. (2), being the three numbers too close to each other even though the parity would be respected. In fact, \( f_x^p \) and \( f_y^p \) are negligible with respect to \( f_z^p \), so \( (f_x^p - f_y^p + f_z^p) + (-f_x^p + f_y^p + f_z^p) \equiv 2(f_z^p) > (f_x^p + f_y^p + f_z^p) \)

and Eq. (2) cannot be satisfied.

For instance, if we put \( f_x = 1, f_y = 4, p = 3 \) we get \( f_z = 1 + 64 = 65 \) which gives rise to the triple \( a = 137281, b = 137344, c = 137345 \) obviously wrong, being the three numbers too close.

With larger values of \( p \) the numbers \( a, b, c \) become closer and closer, excluding the possibility of using the Eq. (22). The choice \( f_x = 5, f_y = 8, p = 3 \) gives \( f_z = 637 \) and even closer \( a = 129237233, b = 129237620, c = 129237683 \). The smallest triple for \( p = 3 \) is \( f_x = 1, f_y = 2, f_z = 1 + 8 = 9, \) still with \( f_z \) too large with respect to \( f_x \) and \( f_y \).

Thus, in case \( p \) is not a factor of \( a, b \) or \( c \), it seems impossible to construct triples of naturals candidate to satisfy Fermat’s equation through the Eqs. (17 -- 20) because if we try to meet the variables’ parity we go out of their range with excessive values and, vice versa, when we keep the
variables in the allowed range then their parity is inevitably violated.

The choice of an even \( c \) and odd \( a, b \) does not appreciably modify the circumstances because the parity violation arises from the presence of 2 both as a divisor and as a factor in the Eqs. (17 – 20). The only significant modification is that the difference between the two odd numbers \( f_y - f_x \) would not be a multiple of 4 but a number like \( n = 4m + 2 \), e.g.:

\[
p = 3, \quad f_x = 1, f_y = 3, f_z = 4, a = \frac{1-27+64}{2} = 19, b = \frac{-1+27+64}{2} = 45, c = \frac{1+27+64}{2} = 46, \text{ not divisible by 4.}
\]

If \( p \) is a factor of one of the three variables \( a, b, c \) then one of the three Eqs. (17 – 19) becomes enormously complicated so that it is no longer possible to contemporarily meet the conditions for odd terms by Eqs. (21) and (22) which should be substituted by a different relation with the indispensable introduction of a factor such as \( p^{-1} \) in the variable, chosen among \( x, y, z \), having \( p \) as a factor. This difficulty is evident for the variable \( k \), which is the weakest point of the problem containing always \( f_x, f_y, f_z \) and \( k_0 \) as factors. In any case, powers of \( f_x \) and \( f_y \) must be involved to obtain the correct factors in \( a, b, c \) giving rise to excessive values of \( f_z \).

For example, the quoted triple \( f_x = 1, f_y = 2, f_z = 1 + 8 = 9 \) applies to the case of \( p = 3 \) factor of \( z \) and \( c \), but we have already established that such a choice leads to the impossibility of the Eq. (2).

Since the dichotomy between parity and range seems unavoidable, it is consequently impossible to find any triple of natural numbers candidate to satisfy Fermat’s equation, which would mean a new algebraic proof for the so-called Fermat’s Last Theorem [7].

3. Even Powers Expansions of \( X, Y, Z \)

Let us suppose that \( A, B, C \) are coprime variables satisfying the Eq. (2). Let us define \( X, Y, Z \):

\[
X = C - B \\
Y = C - A \\
Z = A + B
\]

By expanding the Eq. (2) in terms of the Eqs. (23 – 25):

\[
A^p = C^p - B^p = (C - B)[C^{p-1} + +B^{p-1} + C^{p-2}B + C^{p-3}B^2 + ... + C^2B^{p-3} + CB^{p-2}]
\]

\[
B^p = C^p - A^p = (C - A)[C^{p-1} + +A^{p-1} + C^{p-2}A + C^{p-3}A^2 + ... + C^2A^{p-3} + CA^{p-2}]
\]

\[
C^p = A^p + B^p = (A + B)[A^{p-1} + +B^{p-1} + A^{p-2}B + A^{p-3}B^2 + ... +A^2B^{p-3} + AB^{p-2}]
\]

The factors of \( X = C - B, Y = C - A, Z = A + B \) are in common with \( A^p, B^p, C^p \) respectively.

Let us suppose, by absurd, that \( X, Y, Z \) have common factors and are not necessarily \( p \)-powers.

From the Eq. (28), the variable \( C^p \) has all the factors of \( Z = A + B \), even though they might have different exponents. It follows that \( C \) too has all the factors of \( Z \), no matter with which indexes.

Since \( C \) is coprime with \( A, B \) no factor of \( Z \) can be in common with \( X \) or \( Y \). Similarly, no factor of \( X \) can be found also in \( Y, Z \) and no factor of \( Y \) can be contained in \( X, Z \). The coprimality of \( A, B, C \) implies that \( X, Y, Z \) are coprime as well.

By expanding further and exhaustively the Eqs. (26 – 28):

\[
A^p = C^p - B^p = (C - B)[C^{p-1} + +pCB(C - B)^{p-3} + h_{p-5}C^2B^2(C - B)^{p-5} + +h_{p-7}C^3B^3(C - B)^{p-7} + ...
\]

\[
+ h_2 C \frac{p-3}{2} B \frac{p-3}{2} (C - B)^2 + pC \frac{p-1}{2} B \frac{p-1}{2}
\]

\[
B^p = C^p - A^p = (C - A)[C^{p-1} + +pCA(C - A)^{p-3} + h_{p-5}C^2A^2(C - A)^{p-5} + +h_{p-7}C^3A^3(C - A)^{p-7} + ...
\]

\[
+ h_2 C \frac{p-3}{2} A \frac{p-3}{2} (C - A)^2 + pC \frac{p-1}{2} A \frac{p-1}{2}
\]

\[
C^p = A^p + B^p = (A + B)[(A + B)^{p-1} + -pAB(A + B)^{p-3} + h_{p-5}A^2B^2(A + B)^{p-5} + ...
\]
... - h_{p-7}A^3B^3(A + B)^{p-7} + \cdots \\
\pm h_2 A^{p-3}B^{p-3}(A + B)^2 \pm pC^{p-1}B^{p-1} 

(31)

where in the Eq. (31) the signs of the last terms depend upon the internal parity of \( p \). It is trivial that \( h_{p-1} = 1, h_{p-3} = p, h_0 = p \). For the other coefficients \( h_i \) (all with even indexes), without repeating the equations for \( B^p \) and \( C^p \) in which the coefficients do not change, we analyze the following cases:

\[ A^3 = (C^3 - B^3) = (C - B)((C - B)^2 + 3CB); \]
\[ A^5 = C^5 - B^5 = (C - B)((C - B)^4 + 5CB(C - B)^2 + 5C^2B^2); \]
\[ A^7 = C^7 - B^7 = (C - B)((C - B)^6 + 7CB(C - B)^4 + 14C^22B^2(C - B)^2 + 7C^3B^3); \]
\[ A^9 = C^9 - B^9 = (C - B)((C - B)^8 + 9CB(C - B)^6 + 27C^2B^2(C - B)^4 + 30C^3B^3(C - B)^2 + 9C^4B^4); \]

... 

Due to the last term in the right-hand side of the expansion, the full terms in the square brackets cannot have common factors with the external binomials multipliers if the bases of powers are relatively prime. The only exception is if the factor \( p \) is prime, all coefficients being its multiples.

If \( p \) is not prime then one coefficient may not obey this rule, as the number 30 marked in grey for \( p = 9 \). If \( X, Y, Z \) do not contain \( p \) among their factors they must be pure \( p \)-powers of three basic factors:

\[ X = f_X^p \]
\[ Y = f_Y^p \]
\[ Z = f_Z^p \]

(32)

(33)

(34)

If \( X \) has \( p \) among its factors, the Eqs. (29 – 31) imply that \( X = f_X^p p^{p-1} \) and \( Y, Z \) are pure \( p \)-powers.

For the difference of two powers, we have:

\[ u^n - v^n = (u - v)((u - v)^{n-1} + nuv(u - v)^{n-2} + \cdots + h_1 u^{n-2}v^n) + \cdots + h_2 u^{n-4}v^n + \cdots + h_{n-5} u^2v^n + h_{n-6} u^n) + \cdots + h_{n-3} u^2v^{n-3} + \cdots + h_{n-1} u^{n-2}v \]

and similar relations for sums with alternate signs.

As we have seen in the case \( n = 9 \), where the coefficient 30 hinders the divisibility by \( n \) of the term in square brackets, this term is certainly divisible by \( n \) only if \( n \) is prime.

For \( u = 2, v = 1 \), we get the well-known condition \( 2^n - 2 \) divisible by \( n \) as a not sufficient, but simply necessary, criterion to define prime numbers, \( i.e. \), the Fermat’s Little Theorem for the basis 2.

If we examine the coefficients \( h_i \) in the Eqs. (29 – 31):

\[ n \quad h_0 \quad h_2 \quad h_4 \quad h_6 \quad h_8 \]
\[ 1 \quad 1 \]
\[ 3 \quad 3 \quad 1 \]
\[ 5 \quad 5 \quad 5 \quad 1 \]
\[ 7 \quad 7 \quad 14 \quad 7 \quad 1 \]
\[ 9 \quad 9 \quad 30 \quad 27 \quad 9 \quad 1 \]
\[ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \]

we find out simple rules for deriving a structure similar to the Tartaglia’s triangle [8].

The \( h_0 \) coefficients of terms in \((u \pm v)^0\) are odd growing numbers \( n \).

Each \( h_2 \) coefficient in \((u \pm v)^2\) is the sum of the squares of naturals from \( 1 \) to \( m_2 = \frac{n-1}{2} \), \( i.e. \),

\[ h_2 = \frac{m_2(m_2+1)(2m_2+1)}{6} = \frac{(n^2-1)n}{24} = \frac{n^3-n}{24}: \]

\[ n \quad m_2 \quad h_2 \]
\[ 1 \quad 1 \quad 1 \]
\[ 3 \quad 2 \quad 1+4=5 \]
\[ 7 \quad 3 \quad 1+4+9=14 \]
\[ 9 \quad 4 \quad 1+4+9+16=30 \]
\[ \ldots \quad \ldots \quad \ldots \]

The succeeding upper coefficients of terms in upper even powers always derive from the coefficients of the preceding sequence added starting from top down to \( n-1 \) plus the previous element of the same sequence. This rule applies to each sequence of coefficients as in the following examples.

For the coefficients \( h_4 \) of terms in \((u \pm v)^4\): \( 1+0=1, 1+5+1=7, 1+5+14+7=27 \ldots \)

For the coefficients \( h_6 \) of terms in \((u \pm v)^6\): \( 1+0=1, 1+7+1=9 \ldots \)
A Journey into Fermat’s Equation

So we can expand the list at will, for any \( n \).

If \( n \) is prime, all the coefficients of the \( n^{th} \) row are multiples of \( n \), while if \( n \) is not prime this rule is not necessarily obeyed. It is likely that some multiple will satisfy Little Fermat’s Theorem only for very large values of \( n \) or, at least for the basis 2, will not satisfy it at all. Something more about the expansion is described in Section 4.

**4. Distribution of Coefficients in Even Power Expansions and Following Iterations**

After thorough expansions we have:

\[
a^p - b^p = (a - b)j_{p-1}(a - b)^{p-1} + \]

\[
+ abj_{p-3}(a - b)^{p-3} + \cdots
\]

\[
+ a \frac{p-3}{2} b \frac{p-1}{2} j_2(a - b)^2 + a \frac{p-1}{2} \frac{p-1}{2} j_3(a - b)^3 + \cdots
\]

(35)

\[
a^p + b^p = (a + b)j_{p-1}(a + b)^{p-1} + \\
- abj_{p-3}(a + b)^{p-3} + \cdots
\]

\[
\pm a \frac{p-3}{2} b \frac{p-1}{2} j_2(a + b)^2 \pm a \frac{p-1}{2} \frac{p-1}{2} j_3(a + b)^3 + \cdots
\]

(36)

In Eq. (36) the signs of the last terms depend upon the internal parity of \( p \).

For \( a = 2, b = 1 \) in Eq. (35) we have an interesting expression of Fermat’s Little Theorem, for the basis 2, by observing that \( j_{p-1} = 1 \) and \( a - b = 1 \):

\[2^p - 2 = 2j_{p-3} + 4j_{p-5} + \cdots + 2 \frac{p-3}{2} j_2 + 2 \frac{p-1}{2} j_0.\]

For \( a = 2, b = 1 \) in Eq. (36) we have another expression of Fermat’s Little Theorem, for the basis 2, by observing that \( j_{p-1} = 1 \) and \( a + b = 3 \):

\[2^p - 2 = 3(-1 + 3^{p-1} - 2j_{p-3}3^{p-3} + \cdots \pm 2 \frac{p-3}{2} j_23^2 \pm 2 \frac{p-1}{2} j_0).\]

This last proves that \( 2^p - 2 \) is always a multiple of 3.

The numerical coefficients \( j_i \) in the expansions are:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( j_{p-1} )</th>
<th>( j_{p-3} )</th>
<th>( j_{p-5} )</th>
<th>( j_{p-7} )</th>
<th>( j_{p-9} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td></td>
<td>14</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>9</td>
<td>27</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Hence we may infer the following rules:

Finally, we may build the following pyramid up:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( j_{p-1} )</th>
<th>( j_{p-3} )</th>
<th>( j_{p-5} )</th>
<th>( j_{p-7} )</th>
<th>( j_{p-9} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>p</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>p</td>
<td>p</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>p</td>
<td>2p</td>
<td>p</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>p</td>
<td>3p</td>
<td>3p+3</td>
<td>p</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

From the right external diagonal to the left we find the progressive sequences of the coefficients \( j_i \) whose generation algorithms are described below.

Each \( (a \pm b)^0 \) coefficient in the first sequence is simply the exponent: \( j_0 = p \).

Each \( (a \pm b)^2 \) coefficient in the second sequence is the sum of the squares of the first \( m = \frac{n-1}{2} \) numbers: 1, 1+4=5, 1+4+9=14, 1+4+9+16=30… They are square pyramidal numbers: \( j_2 = \frac{m(m+1)(2m+1)}{6} = \frac{n^3-n}{24} \). Such numbers are multiple of \( n \) if \( m(m+1) \) is divisible by 6 and it happens if \( n \) is prime. If \( n \) is not prime and it is a multiple of 3 then \( j_2 \) is not a multiple of \( n \); this property is the Fermat’s congruence only when \( p = 3 \).

The third sequence refers to \( (a \pm b)^4 \) coefficients and it rises from the sum of numbers whose differences are the square pyramidal numbers of the preceding sequence: 6–1=5, 20–6=14, 50–20=30.

The same thing occurs for the fourth sequence, which refers to \( (a \pm b)^6 \) coefficients and it rises from numbers whose differences are exactly the numbers of the third sequence and so on…

**5. Conclusions**

In this mathematical research on the limits of Fermat’s equation, obtained after a six-year-long cooperation between the authors [8], we use a simple
A Journey into Fermat’s Equation

technique based on the analysis of four numbers and their internal relations with three basic compulsory factors. It leads to:
- a parity violation when we choose all the basic factors in the allowed range;
- exceeding values of one of the involved variables when we try to restore the parity.

It seems thus impossible to find any triple of natural numbers candidate to satisfy Fermat’s equation, because when we try to meet a condition between parity and range we are compelled to violate the other one so that they are irreducibly alternative.

Since Fermat’s Last Theorem would consequently be demonstrated, many readers could think back to the Mirabilis, a never found elementary proof of FLT mentioned in the famous note written down by Pierre de Fermat in 1637.

We are not encouraging such an interpretation because this paper is mainly a journey into Fermat’s equation and, according to our opinion, the reader’s attitude should be towards the algebraic achievements here proposed with their possible hidden flaws and future developments rather than to legendary problems like Fermat’s riddle [9].

Acknowledgments

We thank all the mathematicians who examined our previous versions with genuine interest, providing useful criticism and stimulating suggestions, in particular Professor A. Perelli of the Genoa University and Professor U. Cerruti of the University Turin together with his 2010 PhD research group composed of N. Murru, S. Barbero and M. Abrate.

References