University Cosmopolitan

Nil sine studio.

Lecture by Dr. Enzo Bonacci on Unexplored Properties of Binomial Expansion in Mathematics

Enzo Bonacci was born in Brescia (Italy) in 1972 and spent there his childhood.

At the end of the 70's his family moved to Latina, city where he still lives and works; his school marks were so excellent to deserve the City Medal conferred by the Mayor.

During his scientific high school he received a prize that used to study in Cambridge (UK), where he was extremely impressed with Newton's manuscripts on maths and physics.

After graduating in Chemical Engineering from "La Sapienza" University of Rome, he spent his university prize to travel the world and to achieve diplomas in numerous foreign languages.

He was chosen to do his national service at the office of the Under Secretary of Defence. In spite of his scientific education he has never neglected his artistic side, writing poems and novels selected by international literary contests and becoming a columnist for some newspapers.

Member of the *ODI* (Italian Order of Engineers) since 2001, he has become technical-scientific consultant for important boards.

After qualifying in *mathematics* and *physics*, he has been teaching at Scientific High School since 2001, holding several posts like *Responsible for Public Relations* and *Secretary of the School Council*.

In November 2003 he became responsible for the scientific project *Evolution of Rational Thinking and Epistemological Problems*. During 2004 he became responsible for the IFTS project *Transformation of Agroindustrial Products*. In January 2005 he was elected *Secretary of AEDE-Latina* (European Association of Teachers).

In October 2007 he got the cover of BLU magazine about his effort to extend Relativity and became member of the *IOP* (MInstP).

In 2008 he was selected among the 280 CBEL mathematicians and he was awarded with the Honorary Ph.D. in Theoretical Physics by the Cosmopolitan University.

CONSEQUENCES OF BINOMIAL EXPANSION’S UNEXPLORED PROPERTIES ON FERMAT’S TRIPLES[*]

Abstract

There are some unexplored properties of the binomial expansion with relevant influences on Fermat’s equation. The lecture consists of two steps:

1) Proving unexplored properties of Pascal’s triangle;
2) Analysing the consequences of some binomial properties in limiting Fermat’s triple until an almost impossible condition of existence.

Classifications

5ecm Congress Code: 2-Algebra

AMS(2000): 11B65-Binomial coefficients, 11D41-Fermat’s equation.

Explanations

There are some mathematical definitions worthy to be explained.

“GCF(a,b,c)” means *greatest common factor*, *i.e.*, the greatest factor that divides a,b and c.

“$b|a$” and the equivalent “a=0 (mod$b$)” mean that b divides a, *i.e.*, b is a factor of a.

“a≠0 (mod$b$)” means that b does not exactly divide a, *i.e.*, b is not a factor of a.

“a is coprime to b” means that a and b do not share common factors, *i.e.*, GCF(a,b)=1.

“a and b are relatively prime” means that a and b are coprime.

“a,b,c are pairwise coprime” when GCF(a,b)=GCF(a,c)=GCF(b,c)=1.

“a,b,c is a primitive triple” when a, b and c are pairwise coprime.

“a is not coprime to b” means that a and b have common factors, *i.e.*, GCF(a,b)>1.

“a=q (mod$p$)” and the equivalent “a–q=0 (mod$p$)” mean that p divides a–q, *i.e.*, p is a factor of a–q.

“$C_{a,b}$” means *binomial coefficient* or *combination without repetition* of b objects out of a.

“FLT” means *Fermat’s Last Theorem*.

“$\wedge$” represents the English conjunction *and*, *i.e.*, the intersection between different propositions.

“$\vee$” represents the Latin conjunction *vel* and the English *or*, *i.e.*, the union between different propositions.

“$\underline{\vee}$” represents the Latin adversative conjunction *aut*, *i.e.*, the alternative between different propositions.

([*]) From an algebraic research presented at the Fifth European Mathematical Congress (2008) in Amsterdam by Professor Mario De Paz (University of Genoa) and Mr. Enzo Bonacci (Ph.D. Honoris Causa in Theoretical Physics by Cosmopolitan University).

PASCAL'S TRIANGLE AND BINOMIAL EXPANSIONS

1.1 ***Pascal's triangle.***

$$\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
1 \quad 9 \quad 36 \quad 84 \quad 126 \quad 126 \quad 84 \quad 36 \quad 9 \quad 1 \\
1 \quad 10 \quad 45 \quad 120 \quad 210 \quad 252 \quad 210 \quad 120 \quad 45 \quad 10 \quad 1 \\
\dots
\end{array}$$

1.2 ***Binomial coefficients.***

$$\begin{array}{c}
C_{0,0}=1 \\
C_{1,0}=1 \;\; C_{1,1}=1 \\
C_{2,0}=1 \;\; C_{2,1}=2 \;\; C_{2,2}=1 \\
C_{3,0}=1 \;\; C_{3,1}=3 \;\; C_{3,2}=3 \;\; C_{3,3}=1 \\
C_{4,0}=1 \;\; C_{4,1}=4 \;\; C_{4,2}=6 \;\; C_{4,3}=4 \;\; C_{4,4}=1 \\
C_{5,0}=1 \;\; C_{5,1}=5 \;\; C_{5,2}=10 \;\; C_{5,3}=10 \;\; C_{5,4}=5 \;\; C_{5,5}=1 \\
C_{6,0}=1 \;\; C_{6,1}=6 \;\; C_{6,2}=15 \;\; C_{6,3}=20 \;\; C_{6,4}=15 \;\; C_{6,5}=6 \;\; C_{6,6}=1 \\
C_{7,0}=1 \;\; C_{7,1}=7 \;\; C_{7,2}=21 \;\; C_{7,3}=35 \;\; C_{7,4}=35 \;\; C_{7,5}=21 \;\; C_{7,6}=7 \;\; C_{7,7}=1 \\
C_{8,0}=1 \;\; C_{8,1}=8 \;\; C_{8,2}=28 \;\; C_{8,3}=56 \;\; C_{8,4}=70 \;\; C_{8,5}=56 \;\; C_{8,6}=28 \;\; C_{8,7}=8 \;\; C_{8,8}=1 \\
C_{9,0}=1 \;\; C_{9,1}=9 \;\; C_{9,2}=36 \;\; C_{9,3}=84 \;\; C_{9,4}=126 \;\; C_{9,5}=126 \;\; C_{9,6}=84 \;\; C_{9,7}=36 \;\; C_{9,8}=9 \;\; C_{9,9}=1 \\
C_{10,0}=1 \;\; C_{10,1}=10 \;\; C_{10,2}=45 \;\; C_{10,3}=120 \;\; C_{10,4}=210 \;\; C_{10,5}=252 \;\; C_{10,6}=210 \;\; C_{10,7}=120 \;\; C_{10,8}=45 \;\; C_{10,9}=10 \;\; C_{10,10}=1 \\
\dots
\end{array}$$

1.3 ***$\forall p>2$ prime, $\exists k\in[1,p-2]\subset Z$: $1+(-1)^{k+1}C_{p-1,k}\equiv 0$ (modp).***

The above property is explained as follows:

$$\begin{array}{c}
C_{0,0}=1 \\
C_{1,0}=1 \;\; C_{1,1}=1 \\
C_{2,0}=1 \; \boxed{\mathbf{C_{2,1}=2}} \; C_{2,2}=1 \\
C_{3,0}=1 \;\; C_{3,1}=3 \;\; C_{3,2}=3 \;\; C_{3,3}=1 \\
C_{4,0}=1 \; \boxed{\mathbf{C_{4,1}=4 \;\; C_{4,2}=6 \;\; C_{4,3}=4}} \; C_{4,4}=1 \\
C_{5,0}=1 \;\; C_{5,1}=5 \;\; C_{5,2}=10 \;\; C_{5,3}=10 \;\; C_{5,4}=5 \;\; C_{5,5}=1 \\
C_{6,0}=1 \; \boxed{\mathbf{C_{6,1}=6 \;\; C_{6,2}=15 \;\; C_{6,3}=20 \;\; C_{6,4}=15 \;\; C_{6,5}=6}} \; C_{6,6}=1 \\
C_{7,0}=1 \;\; C_{7,1}=7 \;\; C_{7,2}=21 \;\; C_{7,3}=35 \;\; C_{7,4}=35 \;\; C_{7,5}=21 \;\; C_{7,6}=7 \;\; C_{7,7}=1 \\
C_{8,0}=1 \;\; C_{8,1}=8 \;\; C_{8,2}=28 \;\; C_{8,3}=56 \;\; C_{8,4}=70 \;\; C_{8,5}=56 \;\; C_{8,6}=28 \;\; C_{8,7}=8 \;\; C_{8,8}=1 \\
C_{9,0}=1 \;\; C_{9,1}=9 \;\; C_{9,2}=36 \;\; C_{9,3}=84 \;\; C_{9,4}=126 \;\; C_{9,5}=126 \;\; C_{9,6}=84 \;\; C_{9,7}=36 \;\; C_{9,8}=9 \;\; C_{9,9}=1 \\
C_{10,0}=1 \; \boxed{\mathbf{C_{10,1}=10 \;\; C_{10,2}=45 \;\; C_{10,3}=120 \;\; C_{10,4}=210 \;\; C_{10,5}=252 \;\; C_{10,6}=210 \;\; C_{10,7}=120 \;\; C_{10,8}=45 \;\; C_{10,9}=10}} \; C_{10,10}=1 \\
\dots
\end{array}$$

P=3, k=1: $1+(-1)^2C_{2,1}=1+2=3\equiv 0$ (mod3)

P=5, k=1: $1+(-1)^2C_{4,1}=1+4=5\equiv 0$ (mod5)
P=5, k=2: $1+(-1)^3C_{4,2}=1-6=-5\equiv 0$ (mod5)
P=5, k=3: $1+(-1)^4C_{4,3}=1+4=5\equiv 0$ (mod5)

P=7, k=1: $1+(-1)^2C_{6,1}=1+6=7\equiv 0$ (mod7)
P=7, k=2: $1+(-1)^3C_{6,2}=1-15=-14\equiv 0$ (mod7)
P=7, k=3: $1+(-1)^4C_{6,3}=1+20=21\equiv 0$ (mod7)
P=7, k=4: $1+(-1)^5C_{6,4}=1-15=-14\equiv 0$ (mod7)
P=7, k=5: $1+(-1)^6C_{6,5}=1+6=7\equiv 0$ (mod7)

P=11, k=1: $1+(-1)^2C_{10,1}=1+10=11\equiv 0$ (mod11)
P=11, k=2: $1+(-1)^3C_{10,2}=1-45=-44\equiv 0$ (mod11)
P=11, k=3: $1+(-1)^4C_{10,3}=1+120=121\equiv 0$ (mod11)
P=11, k=4: $1+(-1)^5C_{10,4}=1-210=-209\equiv 0$ (mod11)
P=11, k=5: $1+(-1)^6C_{10,5}=1+252=253\equiv 0$ (mod11)
P=11, k=6: $1+(-1)^7C_{10,6}=1-210=-209\equiv 0$ (mod11)
P=11, k=7: $1+(-1)^8C_{10,7}=1+120=121\equiv 0$ (mod11)
P=11, k=8: $1+(-1)^9C_{10,8}=1-45=-44\equiv 0$ (mod11)
P=11, k=9: $1+(-1)^{10}C_{10,9}=1+10=11\equiv 0$ (mod11)

1.4 $k\in[1,(p-5)/2]\subset Z$: $n_k=[1+(-1)^{k+2}C_{p-1,k+1}]/p+(-1)^{k+1}C_{p-3,k}+(-1)^{k}n_1C_{p-5,k-1}+(-1)^{k-1}n_2C_{p-7,k-2}+\cdots+n_{k-1}C_{k+1,1}$.

The above binomial iterative formula is explained as follows:

$n_1=(1-C_{p-1,2})/p+C_{p-3,1}$

$n_2=(1+C_{p-1,3})/p-C_{p-3,2}+n_1C_{p-5,1}$

$n_3=(1-C_{p-1,4})/p+C_{p-3,3}-n_1C_{p-5,2}+n_2C_{p-7,1}$

…

$j\in[3,(p-5)/2]\subset Z$: $n_j=[1+(-1)^{j+2}C_{p-1,j+1}]/p+(-1)^{j+1}C_{p-3,j}+(-1)^{j}n_1C_{p-5,j-1}+(-1)^{j-1}n_2C_{p-7,j-2}+\cdots+n_{j-1}C_{j+1,1}$

…

$n_{(p-5)/2}=[1+(-1)^{(p-1)/2}C_{p-1,(p-3)/2}]/p+(-1)^{(p-3)/2}C_{p-3,(p-5)/2}+(-1)^{(p-5)/2}n_1C_{p-5,(p-7)/2}+(-1)^{(p-7)/2}n_2C_{p-7,(p-9)/2}+\cdots+n_{(p-7)/2}C_{(p-3)/2,1}$

1.5 *Prime useful properties.*

1.5.1 $\forall p$ prime: $a=0\ (\mathrm{mod}\,p)\Leftrightarrow a^p=0\ (\mathrm{mod}\,p^p)$.

1.5.2 The sum and the difference among pairwise coprimes is coprime to each term.

1.5.3 $\forall p$ prime, $s,t\in N$, $s<t$: $p^s|a\wedge a\neq0\ (\mathrm{mod}\,p^{s+1})\wedge p^t|b\Rightarrow a\pm b=0\ (\mathrm{mod}\,p^s)\wedge a\pm b\neq0\ (\mathrm{mod}\,p^{s+1})$.

1.6 *Binomial expansion $a^p\pm b^p$, with $a,b,p\in N$ and $3\leq p\leq7$ prime.*

1.6.1 $a^3\pm b^3=(a\pm b)^3-[\pm3ab(a\pm b)]$.

1.6.2 $a^5\pm b^5=(a\pm b)^5-\{\pm5ab(a\pm b)[(a\pm b)^2-(\pm ab)]\}$.

1.6.3 $a^7\pm b^7=(a\pm b)^7-\{\pm7ab(a\pm b)[(a\pm b)^2-(\pm ab)]^2\}$.

Let us resume the above properties as follows:

1.6.4 $a^p\pm b^p=(a\pm b)^p-\{\pm pab(a\pm b)[(a\pm b)^2-(\pm ab)]^{(p-3)/2}\}$.

1.7 ***Binomial expansion $a^p\pm b^p$, with $a,b,p\in N$ and $p>2$ prime.***

Proof. By the binomial Property 1.3 $k\in[1,p-2]\subset Z:1+(-1)^{k+1}C_{p-1,k}\equiv 0\ (modp)$, we have:

$a^p-b^p=(a-b)^p+$

$+pab(a-b)^{p-2}+$

$+(ab)^2(a-b)^{p-4}(1-C_{p-1,2}+pC_{p-3,1})+$

$+(ab)^3(a-b)^{p-6}[1+C_{p-1,3}-pC_{p-3,2}+(1-C_{p-1,2}+pC_{p-3,1})C_{p-5,1}]+$

$+(ab)^4(a-b)^{p-8}\{1-C_{p-1,4}+pC_{p-3,3}-(1-C_{p-1,2}+pC_{p-3,1})C_{p-5,2}+[1+C_{p-1,3}-pC_{p-3,2}+(1-C_{p-1,2}+pC_{p-3,1})C_{p-5,1}]C_{p-7,1}\}+$

$+\ \cdots\ +$

$+(ab)^{(p-3)/2}(a-b)^3\{1+(-1)^{(p-1)/2}C_{p-1,(p-3)/2}+$

$\qquad +(-1)^{(p-3)/2}pC_{p-3,(p-5)/2}+$

$\qquad +(-1)^{(p-5)/2}(1-C_{p-1,2}+pC_{p-3,1})C_{p-5,(p-7)/2}+$

$\qquad +(-1)^{(p-7)/2}[1+C_{p-1,3}-pC_{p-3,2}+(1-C_{p-1,2}+pC_{p-3,1})C_{p-5,1}]C_{p-7,(p-9)/2}+$

$\qquad +\ \cdots\ +$

$\qquad +[1+(-1)^{(p-3)/2}C_{p-1,(p-5)/2}+p(-1)^{(p-5)/2}C_{p-3,(p-7)/2}+p(-1)^{(p-7)/2}n_1C_{p-5,(p-9)/2}+$

$\qquad +\ \cdots\ +pn_{(p-9)/2}C_{(p-5)/2,1}]C_{(p-3)/2,1}\}+$

$+(ab)^{(p-1)/2}(a-b)p.$

By introducing ***a-b=t***, and according to Definition 1.4:

$n_k=[1+(-1)^{k+2}C_{p-1,k+1}]/p+(-1)^{k+1}C_{p-3,k}+(-1)^k n_1C_{p-5,k-1}+(-1)^{k-1}n_2C_{p-7,k-2}+\ \cdots\ +n_{k-1}C_{k+1,1}$,

we have:

$a^p-b^p=t^p+$

$+(ab)t^{p-2}p+$

$+(ab)^2t^{p-4}pn_1+$

$+(ab)^3t^{p-6}(1+C_{p-1,3}-pC_{p-3,2}+pn_1C_{p-5,1})+$

$+(ab)^4t^{p-8}(1-C_{p-1,4}+pC_{p-3,3}-pn_1C_{p-5,2}+pn_2C_{p-7,1})+$

$+\ \cdots\ +$

$+(ab)^{(p-3)/2}t^3[1+(-1)^{(p-1)/2}C_{p-1,(p-3)/2}+(-1)^{(p-3)/2}pC_{p-3,(p-5)/2}+(-1)^{(p-5)/2}pn_1C_{p-5,(p-7)/2}+(-1)^{(p-7)/2}pn_2C_{p-7,(p-9)/2}+$

$\qquad +\ \cdots\ +pn_{(p-7)/2}C_{(p-3)/2,1}]+$

$+(ab)^{(p-1)/2}tp.$

Further:

$a^p-b^p=t^p+$

$+pabt^{p-2}+$

$+pn_1(ab)^2t^{p-4}+$

$+pn_2(ab)^3t^{p-6}+$

$+pn_3(ab)^4t^{p-8}+$

$+\ \cdots\ +$

$+pn_{(p-5)/2}(ab)^{(p-3)/2}t^3+$

$+p(ab)^{(p-1)/2}t.$

Therefore:

$a^p-b^p=t^p+pabt^{p-2}+pn_1(ab)^2t^{p-4}+pn_2(ab)^3t^{p-6}+\ \cdots\ +pn_{(p-5)/2}\ (ab)^{(p-3)/2}t^3+p(ab)^{(p-1)/2}t=$

$=t[t^{p-1}+pabt^{p-3}+pn_1(ab)^2t^{p-5}+pn_2(ab)^3t^{p-7}+\ \cdots\ +pn_{(p-5)/2}\ (ab)^{(p-5)/2}t^2+p(ab)^{(p-3)/2}]=$

$=t\{t^{p-1}+pab[t^{p-3}+n_1abt^{p-5}+n_2(ab)^2t^{p-7}+\ \cdots\ +n_{(p-5)/2}\ (ab)^{(p-7)/2}t^2+(ab)^{(p-5)/2}]\}=$

$=t\{t^{p-1}+pab[t^{p-3}+ab[n_1t^{p-5}+n_2abt^{p-7}+\ \cdots\ +n_{(p-5)/2}\ (ab)^{(p-9)/2}t^2+(ab)^{(p-7)/2}]]\}=$

$=t\{t^{p-1}+pab[t^{p-3}+ab[n_1t^{p-5}+ab[n_2t^{p-7}+\ \cdots\ +n_{(p-5)/2}\ (ab)^{(p-11)/2}t^2+(ab)^{(p-9)/2}]]]\}=$

$=\ \ldots\ =$

$=t\{t^{p-1}+pab[t^{p-3}+ab[n_1t^{p-5}+ab[n_2t^{p-7}+\ \cdots\ +ab(n_{(p-5)/2}t^2+ab)\ \cdots\ ]]]\}.$

By substituting back $a-b=t$:

1.7.1 $\boldsymbol{a^p-b^p=(a-b)^p+pab(a-b)\{(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\cdots+ab[n_{(p-5)/2}(a-b)^2+ab]\cdots]]\}.}$

Similarly to the above proof:

1.7.2 $\boldsymbol{a^p+b^p=(a+b)^p-pab(a+b)\{(a+b)^{p-3}-ab[n_1(a+b)^{p-5}-ab[n_2(a+b)^{p-7}+\cdots-ab[n_{(p-5)/2}(a+b)^2-ab]\cdots]]\}.}$

Let us resume the above Properties 1.7.1 and 1.7.2 as follows:

1.7.3 $\boldsymbol{a^p\pm b^p=(a\pm b)^p-(\pm pab)(a\pm b)\{(a\pm b)^{p-3}-(\pm ab)[n_1(a\pm b)^{p-5}-(\pm ab)[n_2(a\pm b)^{p-7}+\ \cdots}$

$\qquad\boldsymbol{\cdots\ -(\pm ab)[n_{(p-5)/2}(a\pm b)^2-(\pm ab)]\cdots]]\}.}$

1.8 ***$\forall a,b,p\in N$, $p>2$ prime: $(a\pm b)^p=a^p\pm b^p$ (modpab).***

Proof. By the binomial expansion 1.7.3:

$$a^p\pm b^p=(a\pm b)^p-(\pm pab)(a\pm b)\{(a\pm b)^{p-3}-(\pm ab)[n_1(a\pm b)^{p-5}-(\pm ab)[n_2(a\pm b)^{p-7}+\cdots$$
$$\cdots-(\pm ab)[n_{(p-5)/2}(a\pm b)^2-(\pm ab)]\cdots]]\};$$
$$(a\pm b)^p-(a^p\pm b^p)=\pm pab(a\pm b)\{(a\pm b)^{p-3}-(\pm ab)[n_1(a\pm b)^{p-5}-(\pm ab)[n_2(a\pm b)^{p-7}+\cdots$$
$$\cdots-(\pm ab)[n_{(p-5)/2}(a\pm b)^2-(\pm ab)]\cdots]]\}.$$

Therefore $(a\pm b)^p-(a^p\pm b^p)=0\ (modpab)$.

1.9 ***$\forall a,b,p\in N$, $p>2$ prime: $a^p\pm b^p=0$ (modp) $\Leftrightarrow$ $a\pm b=0$ (modp).***

Proof. By the binomial expansion 1.7.3:

$a^p\pm b^p=0\ (modp)$;

$$(a\pm b)^p-\underbrace{\underbrace{(\pm pab)}_{=0\ (modp)}(a\pm b)\{(a\pm b)^{p-3}-(\pm ab)[n_1(a\pm b)^{p-5}-(\pm ab)[n_2(a\pm b)^{p-7}+\cdots-(\pm ab)[n_{(p-5)/2}(a\pm b)^2-(\pm ab)]\cdots]]\}}_{=0\ (modp)}=0\ (modp).$$

Therefore $(a\pm b)^p=0\ (modp)$.

1.10 ***$\forall a,b,p\in N$, $p>2$ prime: $a^p\pm b^p=0$ (modp) $\Rightarrow$ $a^p\pm b^p=0$ (modp^2).***

Proof. By binomial Property 1.9 $a^p\pm b^p=0\ (modp)\ \Leftrightarrow\ a\pm b=0\ (modp)$:

$$\underbrace{(a\pm b)}_{=0\ (modp^p)}{}^p-\underbrace{\underbrace{(\pm pab)}\,\underbrace{(a\pm b)}\{\underbrace{(a\pm b)}^{p-3}-(\pm ab)[n_1\underbrace{(a\pm b)}^{p-5}-(\pm ab)[n_2\underbrace{(a\pm b)}^{p-7}+\cdots-(\pm ab)[n_{(p-5)/2}\underbrace{(a\pm b)}^2-(\pm ab)]\cdots]]\}}_{=0\ (modp^2)}=0\ (modp^2).$$

According to prime Property 1.5.3, since $p>2$: $a^p\pm b^p=0\ (modp^2)$.

1.11 ***$\forall a,b,q\in N$, a coprime to b, $q\geq 2$, $p>2$ prime: $a^p\pm b^p=0$ (modp^q) $\Leftrightarrow$ $a\pm b=0$ (modp^{q-1}).***

Proof. Let us assume $a^p-b^p=0\ (modp^q)$; by Properties 1.9 and 1.10 $a^p-b^p=0\ (modp)$ implies:
1.11.1 $a-b=0\ (modp)$;
1.11.2 $a^p-b^p=0\ (modp^2)$, *i.e.*, $q\geq 2$.
By Property 1.5.2 $(a-b)$ is coprime to ab, so that $ab\neq 0\ (modp)$.
As a consequence of 1.11.1 and 1.11.2, since p is prime:
$n_{(p-5)/2}(a-b)^2+ab\neq 0\ (modp)$;
$ab(n_{(p-5)/2}(a-b)^2+ab)\neq 0\ (modp)$;
$ab[n_2(a-b)^{p-7}+\ \cdots\ +ab(n_{(p-5)/2}(a-b)^2+ab)\ \cdots\ ]\neq 0\ (modp)$;
1.11.3 $(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\ \cdots\ +ab(n_{(p-5)/2}(a-b)^2+ab)\ \cdots\ ]]]\neq 0\ (modp)$.
By comparing the Property 1.11.2 $a^p=x^p\ (modp^2)$ to the binomial expansion 1.7.1:
$a^p-b^p=(a-b)^p+pab(a-b)\{(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\cdots+ab[n_{(p-5)/2}(a-b)^2+ab]\cdots]]\}=0\ (modp^q)$;
$pab(a-b)\{(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\ \cdots\ +ab(n_{(p-5)/2}(a-b)^2+ab)\ \cdots\ ]]\}=0\ (modp^q)$;

$$\underbrace{ab}_{\neq 0\ (modp)}*(a-b)*\{\underbrace{(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\ \cdots\ +ab(n_{(p-5)/2}(a-b)^2+ab)}_{\neq 0\ (modp)\ \text{according to Property 1.11.3}}\ \cdots\ ]]\}=0\ (modp^{q-1}).$$

Necessarily $a-b=0\ (modp^{q-1})$.
Analogously, if $a^p+b^p=0\ (modp^q)$ then $a+b=0\ (modp^{q-1})$.

1.12 ***$\forall a,b\in N$, a coprime to b, $p>2$ prime: $(a^p\pm b^p)/(a\pm b)$ is coprime to $a\pm b \Leftrightarrow a\pm b\neq 0\ (modp)$***

Proof. By Property 1.5.2 $(a+b)$ is coprime to ab because a and b are relatively prime.
By expansion 1.7.1:

$$a^p+b^p=(a+b)^p-pab(a+b)\{(a+b)^{p-3}-ab[n_1(a+b)^{p-5}-ab[n_2(a+b)^{p-7}+\cdots-ab[n_{(p-5)/2}(a+b)^2-ab]\cdots]]\};$$

$$(a^p+b^p)/(a+b)=\underbrace{(a+b)^{p-1}-pab\{\underbrace{(a+b)^{p-3}-\underbrace{ab[n_1(a+b)^{p-5}-\underbrace{ab[n_2(a+b)^{p-7}+\cdots-\underbrace{ab[n_{(p-5)/2}(a+b)^2-ab]}_{\text{coprime to } (a+b)}\cdots]}_{\text{coprime to } (a+b)}]}_{\text{coprime to } (a+b)}\}}_{\text{coprime to } (a+b)\ \Leftrightarrow\ a+b\neq 0\ (modp)}}_{\text{coprime to } (a+b)\ \Leftrightarrow\ a+b\neq 0\ (modp)}.$$

Therefore $(a^p+b^p)/(a+b)$ is coprime to $(a+b)$ if and only if $a+b\neq 0\ (modp)$.
Analogously, $(a^p-b^p)/(a-b)$ is coprime to $(a-b)$ if and only if $a-b\neq 0\ (modp)$.

1.13 ***$\forall a,b,q\in N$, a coprime to b, $p>2$ prime: $a^p\pm b^p=0\ (mod2^q) \Leftrightarrow a\pm b=0\ (mod2^q)$.***

Proof. If $a^p-b^p=0\ (mod2)$, necessarily:
1.13.1 $ab\neq 0\ (mod2)$, because a and b are both odd as coprime;
1.13.2 $a-b=0\ (mod2)$.
By 1.13.1 and 1.13.2 we have:

$$a^p-c^p=\underbrace{(a-b)\{(a-b)^{p-1}+\underbrace{pab[(a-b)^{p-3}+\underbrace{ab[n_1(a-b)^{p-5}+\underbrace{ab[n_2(a-b)^{p-7}+\cdots+\underbrace{ab(n_{(p-5)/2}(a-b)^2+ab)}_{\neq 0\ (mod2)}\cdots]}_{\neq 0\ (mod2)}]}_{\neq 0\ (mod2)}]}_{\neq 0\ (mod2)}\}}_{\neq 0\ (mod2)}=0\ \ (mod2^q).$$

Therefore $a-b=0\ (mod2^q)$.
Analogously, if $a^p+b^p=0\ (mod2^q)$ then $a+b=0\ (mod2^q)$.

1.14 ***$\forall a,b,q\in N$, a coprime to b, $p>2$ prime: $a^p\pm b^p\neq 2^q$.***

Proof. By Property 1.13, if $a^p-b^p=2^q$, necessarily: $a-b=2^q$;

$$a^p-c^p=\underbrace{(a-b)}_{=0\ (mod2^q)}\underbrace{\{(a-b)^{p-1}+pab[(a-b)^{p-3}+ab[n_1(a-b)^{p-5}+ab[n_2(a-b)^{p-7}+\cdots+ab(n_{(p-5)/2}(a-b)^2+ab)\cdots]]]\}}_{\neq 0\ (mod2)}=2^q*r.$$

$\exists r\in N$, $r>1$ coprime to 2: $a^p\pm b^p=2^q*r$.
Analogously, if $a^p+b^p=2^q$ then $a^p+b^p=2^q*r$.

1.15 ***$A,B,C,n\in N$, $A\leq B\leq C$: $n^A+n^B=n^C \Leftrightarrow n=2$, $A=B$, $C=B+1$.***

Proof. It is a *reductio ad absurdum*. Let us assume valid $n^A+n^B=n^C$:
$n^A(1+n^{B-A})=n^C$
$1+n^{B-A}=n^{C-A}$
$1=n^{C-A}-n^{B-A}$
$1=n^{B-A}(n^{C-B}-1)$
If $n=1$ then $1=0$ impossible.
If $n=2$ then $A=B$ and $C-B=1$.
If $n>2$ then $n^{B-A}(n^{C-B}-1)>2$, *i.e.*, $1>2$ impossible.

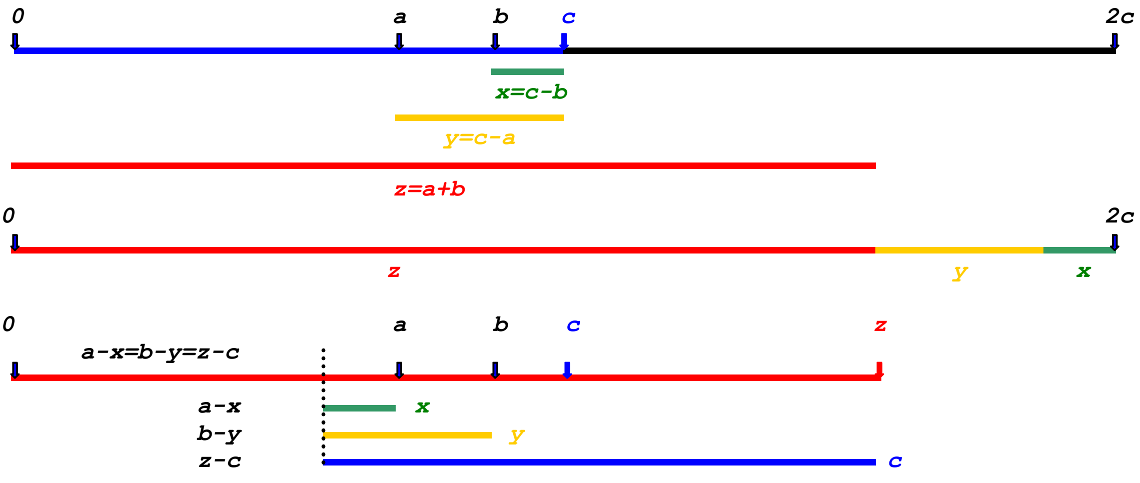
ANALYSIS OF FERMAT’S EQUATIONS THROUGH THE BINOMIAL PROPERTIES

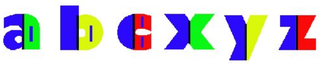
2.1 ABSTRACT

We find some remarkable differences between Fermat’s triples and Pythagoras’ after combining the coprimality properties with the following binomial expansion:
$a^p \pm b^p = (a\pm b)^p - (\pm abc)(a\pm b)\{(a\pm b)^{p-3} - (\pm ab)[n_1(a\pm b)^{p-5} - (\pm ab)[n_2(a\pm b)^{p-7} + \cdots - (\pm ab)[n_{(p-5)/2}(a\pm b)^2 - (\pm ab]\cdots]]\}$;
being $n_k=[1+(-1)^{k+2}C_{p-1,k+1}]/p+(-1)^{k+1}C_{p-3,k}+(-1)^k n_1C_{p-5,k-1}+(-1)^{k-1}n_2C_{p-7,k-2}+ \cdots +n_{k-1}C_{k+1,1}$.
For example the simplest Pythagorean triple ($3^2+4^2=5^2$) it contains a mere power of 2 ($4=2^2$) that is also the index, cases both excluded for Fermat triples; furthermore each number 3, 4 and 5 has only one prime factor so that a Pythagorean triple can be formed by combining just three primes, case precluded to Fermat triples which need at least five different primes.
We also find several limitations on Fermat’s triples upon which we try an elementary attempt of proving Fermat’s Last Theorem *by absurd* based also on the Rational Root Theorem.
According to our calculations Fermat triples could be hindered by the impossibility to reduce them to the primitive form, *i.e.*, with pairwise coprime elements.

2.2 DEFINITIONS

2.2.1 Let $a,b,c\in$N be pairwise coprime, with $a<b<c$.
2.2.2 Let $c^p=a^p+b^p$ be a primitive Fermat’s equation, with $p>2$ prime.
2.2.3 Denote $x=c-b$, with x,b,c pairwise coprime and $0<x<a$ by construction.
2.2.4 Denote $y=c-a$, with y,a,c pairwise coprime and $x<y<b$ by construction.
2.2.5 Denote $z=a+b$, with z,a,b pairwise coprime and $b<c<z$ by construction.
2.2.6 Denote $d=x\hat{}(1/p)$, denote $\varphi_x=a^p/x\in$N; denote $g=\varphi_x\hat{}(1/p)$.
2.2.7 Denote $e=y\hat{}(1/p)$, denote $\varphi_y=b^p/y\in$N; denote $h=\varphi_y\hat{}(1/p)$.
2.2.8 Denote $f=z\hat{}(1/p)$, denote $\varphi_z=c^p/z\in$N; denote $i=\varphi_z\hat{}(1/p)$.
2.2.9 $n_k=[1+(-1)^{k+2}C_{p-1,k+1}]/p+(-1)^{k+1}C_{p-3,k}+(-1)^k n_1C_{p-5,k-1}+(-1)^{k-1}n_2C_{p-7,k-2}+ \cdots +n_{k-1}C_{k+1,1}$.
2.2.10 $a^p=c^p-b^p=x\{x^{p-1}+pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+ \cdots +bc(n_{(p-5)/2}x^2+bc) \cdots]]]\}=x*\varphi_x$.
2.2.11 $b^p=c^p-a^p=y\{y^{p-1}+pac[y^{p-3}+ac[n_1y^{p-5}+ac[n_2y^{p-7}+ \cdots +ac(n_{(p-5)/2}y^2+ac) \cdots]]]\}=y*\varphi_y$.
2.2.12 $c^p=a^p+b^p=z\{z^{p-1}-pab[z^{p-3}-ab[n_1z^{p-5}-ab[n_2z^{p-7}+ \cdots -ab[n_{(p-5)/2}z^2-ab] \cdots]]]\}=z*\varphi_z$.
2.2.13 $a^p-x^p=(a-x)\{(a-x)^{p-1}+pax[(a-x)^{p-3}+ax[n_1(a-x)^{p-5}+ax[n_2(a-x)^{p-7}+\cdots+ax(n_{(p-5)/2}(a-x)^2+ax)\cdots]]]\}$.
2.2.14 $b^p-y^p=(b-y)\{(b-y)^{p-1}+pby[(b-y)^{p-3}+by[n_1(b-y)^{p-5}+by[n_2(b-y)^{p-7}+\cdots+by(n_{(p-5)/2}(b-y)^2+by)\cdots]]]\}$.
2.2.15 $z^p-c^p=(z-c)\{(z-c)^{p-1}+pzc[(z-c)^{p-3}+zc[n_1(z-c)^{p-5}+zc[n_2(z-c)^{p-7}+\cdots+zc(n_{(p-5)/2}(z-c)^2+zc)\cdots]]]\}$.
2.2.16 The *qualitative* relationships among a,b,c,x,y,z are represented as follows:





2.3 PROPOSITIONS

2.3.1 ***$1\leq x<y<z$; $\varphi_x>x^{p-1}$, $\varphi_y>y^{p-1}$, $c^{p-1}/2<\varphi_z<z^{p-1}$.***
Proof. By Definition 2.2.1 $a<b<c$, therefore $1\leq c-b<c-a<c$.
By Def. 2.2.2 $c^p=a^p+b^p$, thus $z=a+b>c>y>x\geq 1$.
Since $x=c-b<a$ then $\varphi_x=a^p/x>a^{p-1}>x^{p-1}$.
Since $y=c-a<b$ then $\varphi_y=b^p/y>b^{p-1}>y^{p-1}$.
Since $c<z<2c$ then $c^{p-1}/2<\varphi_z=c^p/z<c^{p-1}<z^{p-1}$.

2.3.2 ***bc is coprime to x, ac is coprime to y, ab is coprime to z.***
Proof. By Def. 2.2.3 x,b,c are pairwise coprime; by Def. 2.2.4 y,a,c are pairwise coprime; by Def. 2.2.5 z,a,b are pairwise coprime.

2.3.3 ***Each prime factor of x is factor of a too, not vice versa.***
Proof. By Def. 2.2.10:
$a^p=c^p-b^p=x\{x^{p-1}+pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\cdots+bc(n_{(p-5)/2}x^2+bc)\cdots]]]\}$, *i.e.*, $a^p=0\ (modx)$.
$\forall q>1$ prime, if $q|x$ then $q|a^p$, *i.e.*, $q^p|a^p$.

2.3.4 ***Each prime factor of y is factor of b too, not vice versa.***
Proof. Analogously to Proposition 2.3.3.

2.3.5 ***Each prime factor of z is factor of c too, not vice versa.***
Proof. Analogously to Prop. 2.3.3.

2.3.6 ***$a=0\ (modp)$ if and only if $x=0\ (modp^{p-1})$ and $\varphi_x=0\ (modp)$ but $\varphi_x\neq 0\ (modp^2)$.***
Proof. Since p is prime, $a=0\ (modp)$ implies $a^p=0\ (modp^p)$.
According to Definition 2.2.10:

$$a^p=c^p-b^p=x\{x^{p-1}+\underbrace{pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\ \cdots\ +bc(n_{(p-5)/2}x^2+bc)\ \cdots\ ]]]}_{=0\ (modp)}\}=0\ (modp^p).$$

Necessarily $x=0\ (modp)$.
By Prop. 2.3.2 bc and x are relatively prime, therefore:

$$a^p=c^p-b^p=x\{\underbrace{x^{p-1}+\underbrace{p\underbrace{bc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\ \cdots\ +bc(n_{(p-5)/2}x^2+bc)\ \cdots\ ]]]}_{\neq 0\ (modp)\text{ because coprime to }x}}_{=0\ (modp)\text{ but }\neq 0\ (modp^2)}}_{=0\ (modp)\text{ but }\neq 0\ (modp^2)\text{ by Property 1.5.3}}\}=0\ (modp^p).$$

Necessarily $x=0\ (modp^{p-1})$. Since $p>2$, $p-1>1$:

$$\varphi_x = a^p/x = \underbrace{\underbrace{x^{p-1}}_{=0\ (modp^{p-1})} + \underbrace{pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\ \cdots\ +bc(n_{(p-5)/2}x^2+bc)\ \cdots\ ]]]}_{=0\ (modp)\text{ but }\neq 0\ (modp^2)}}_{\varphi_x=0\ (modp)\text{ but }\varphi_x\neq 0\ (modp^2)\text{ by Property 1.5.3}}=0\ (modp^p).$$

Necessarily $\varphi_x=0\ (modp)$ but $\varphi_x\neq 0\ (modp^2)$.

2.3.7 ***$b=0\ (modp)$ if and only if $y=0\ (modp^{p-1})$ and $\varphi_y=0\ (modp)$ but $\varphi_y\neq 0\ (modp^2)$.***
Proof. Analogously to Prop. 2.3.6.

2.3.8 ***$c=0\ (modp)$ if and only if $z=0\ (modp^{p-1})$ and $\varphi_z=0\ (modp)$ but $\varphi_z\neq 0\ (modp^2)$.***
Proof. Analogously to Prop. 2.3.6.

2.3.9 ***If $x>1$ then x and φ_x can share the unique factor p, if and only if $p=GCF(x,\varphi_x)$, otherwise they are coprime.***

Proof. By Prop. 2.3.2 bc and x are relatively prime, therefore:

$$\varphi_x=a^p/x=\underbrace{x^{p-1}+\underbrace{pbc\underbrace{[x^{p-3}+bc\underbrace{[n_1x^{p-5}+bc\underbrace{[n_2x^{p-7}+\cdots+\underbrace{bc(n_{(p-5)/2}x^2+bc)}_{\text{coprime to } x}\cdots]}_{\text{coprime to } x}]}_{\text{coprime to } x}]}_{\text{coprime to } x}}_{\text{coprime to } x \text{ but } p}}_{\text{coprime to } x \text{ but } p}=0 \pmod{p^p}.$$

Necessarily x and φ_x can share the unique factor p. By Prop. 2.3.6, $a=0\ (mod p)$ if and only if $x=0\ (mod p^{p-1})$, $\varphi_x=0\ (mod p)$ and $\varphi_x\neq 0\ (mod p^2)$, *i.e.*, $GCF(x,\varphi_x)=p$.

2.3.10 ***Y and φ_y can share the unique factor p, if and only if $p=GCF(y,\varphi_y)$, otherwise they are coprime.***

Proof. Analogously to Prop. 2.3.9.

2.3.11 ***Z and φ_z can share the unique factor p, if and only if $p=GCF(z,\varphi_z)$, otherwise they are coprime.***

Proof. Analogously to Prop. 2.3.9.

2.3.12 ***If $x>1$ then a has at least one factor more than x and coprime to it.***

Proof. By Prop. 2.3.6, if $a=0\ (mod p)$ then $\varphi_x=0\ (mod p)$ and $\varphi_x\neq 0\ (mod p^2)$; hence:

$\varphi_x/p=a^p/px=\{x^{p-1}+pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\cdots+bc(n_{(p-5)/2}x^2+bc)\cdots]]]\}/p\neq 0\ (mod p)$.

Denote $q=\varphi_x/p$, it is $q>1$ by construction and q coprime to x by Prop. 2.3.9.

If $a\neq 0\ (mod p)$ then $a=(x*\varphi_x)^{1/p}=d*g$.

Since x is coprime to φ_x then $d=x^{1/p}\in$N is coprime to $g=\varphi_x{}^{1/p}\in$N.

2.3.13 ***b has always at least one factor more than y and coprime to it.***

Proof. Analogously to Prop. 2.3.12; furthermore $y>1$ by Prop. 2.3.1.

2.3.14 ***c has always at least one factor more than z and coprime to it.***

Proof. Analogously to Prop. 2.3.12; furthermore $z>2$ by Prop. 2.3.1.

2.3.15 ***$a\neq 0\ (mod p) \Leftrightarrow x\neq 0\ (mod p) \wedge a^{p-1}=1\ (mod p)$.***

Proof. By Prop. 2.3.3, if p does not divide a then does not divide x.
By Prop. 2.3.6, p divides a if and only if the $p-1$ power of p divides x.
By Fermat's Little Theorem, $a^p-a=a(a^{p-1}-1)=0\ (mod p)$.
Since $a\neq 0\ (mod p)$ necessarily $a^{p-1}-1=0\ mod p$.

2.3.16 ***$b\neq 0\ (mod p) \Leftrightarrow y\neq 0\ (mod p) \wedge b^{p-1}=1\ (mod p)$.***

Proof. Analogously to Prop. 2.3.15.

2.3.17 ***$c\neq 0\ (mod p) \Leftrightarrow z\neq 0\ (mod p) \wedge c^{p-1}=1\ (mod p)$.***

Proof. Analogously to Prop. 2.3.15.

2.3.18 ***If $x=1 \Leftrightarrow p\mid(a^{p-1}-1)$***

Proof. Since $x\neq 0\ (mod p)$, by Prop. 2.3.15 we have $a\neq 0\ (mod p)$, *i.e.*, $a^{p-1}-1=0\ (mod p)$ according to Fermat's Little Theorem.

2.3.19 $\boldsymbol{x\neq0\ (mod p)\ \wedge\ x>1\ \Leftrightarrow\ p\,|\,(x^{p-1}-1)\ \wedge\ p\,|\,(\varphi_x-1).}$

Proof. By Fermat’s Little Theorem $x^p-x=x(x^{p-1}-1)=0\ (mod p)$.
Since x≠0 (modp) we have $x^{p-1}-1=0\ (mod p)$. By Def. 2.2.6:
$\varphi_x=a^p/x=x^{p-1}+pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\cdots+bc(n_{(p-5)/2}x^2+bc)\cdots]]]$;

$$\varphi_x-1=\underbrace{x^{p-1}-1}_{=0\ (mod p)}+\underbrace{pbc[x^{p-3}+bc[n_1x^{p-5}+bc[n_2x^{p-7}+\cdots+bc(n_{(p-5)/2}x^2+bc)\cdots]]]}_{=0\ (mod p)}.$$

Necessarily $\varphi_x-1=0\ (mod p)$.

2.3.20 $\boldsymbol{y\neq0\ (mod p)\ \Leftrightarrow\ p\,|\,(y^{p-1}-1)\ \wedge\ p\,|\,(\varphi_y-1).}$

Proof. Analogously to Prop. 2.3.19; furthermore $y>1$ by Prop. 2.3.1.

2.3.21 $\boldsymbol{z\neq0\ (mod p)\ \Leftrightarrow\ p\,|\,(z^{p-1}-1)\ \wedge\ p\,|\,(\varphi_z-1).}$

Proof. Analogously to Prop. 2.3.19; furthermore $z>2$ by Prop. 2.3.1.

2.3.22 $\boldsymbol{x\neq0\ (mod p)\ \Leftrightarrow\ \exists d,g\in Z^+}$ ***relatively prime:*** $\boldsymbol{a=dg;\ x=d^p\ \wedge\ \varphi_x=g^p;}$
besides $\boldsymbol{p\,|\,(g^{p-1}-1)\ \wedge\ p\,|\,(g-1);}$ ***if*** $\boldsymbol{d>1}$ ***then*** $\boldsymbol{p\,|\,(d^{p-1}-1).}$

Proof. If $x\neq0\ (mod p)$ then x and φ_x are coprime according to Prop. 2.3.9.
Since $a^p=x*\varphi_x$ and $GCF(x,\varphi_x)=1$, necessarily $x=d^p$ and $\varphi_x=g^p$.
By Fermat’s Little Theorem, if $d>1$ then $d^p-d=d(d^{p-1}-1)=0\ (mod p)$.
Since $d^p=x\neq0\ (mod p)$, *i.e.*, $d\neq0\ (mod p)$, we have $d^{p-1}-1=0\ (mod p)$.
By LFT: $g^p-g=g(g^{p-1}-1)=0\ (mod p)$.
By Prop. 2.3.5 $x\neq0\ (mod p)\ \Leftrightarrow\ a\neq0\ (mod p)$, *i.e.*, $g\neq0\ (mod p)$ hence $g^{p-1}-1=0\ (mod p)$.
By $\varphi_x=g^p\in N$ and according to Prop. 2.3.19 $p\,|\,(\varphi_x-1)$, we have $p\,|\,(g^p-1)$, that implies $p\,|\,(g-1)$ according to Property 1.9.

2.3.23 $\boldsymbol{y\neq0\ (mod p)\ \Leftrightarrow\ \exists e,h\in Z^+}$ ***relatively prime:*** $\boldsymbol{b=eh;\ y=e^p\ \wedge\ \varphi_y=h^p;}$
besides $\boldsymbol{p\,|\,(e^{p-1}-1)\ \wedge\ p\,|\,(h^{p-1}-1)\ \wedge\ p\,|\,(h-1).}$

Proof. Analogously to Prop. 2.3.22, furthermore $y>1$ by Prop. 2.3.1.

2.3.24 $\boldsymbol{z\neq0\ (mod p)\ \Leftrightarrow\ \exists f,i\in Z^+}$ ***relatively prime:*** $\boldsymbol{c=fi;\ z=f^p\ \wedge\ \varphi_z=i^p;}$
besides $\boldsymbol{p\,|\,(f^{p-1}-1)\ \wedge\ p\,|\,(i^{p-1}-1)\ \wedge\ p\,|\,(i-1).}$

Proof. Analogously to Prop. 2.3.22, furthermore $z>2$ by Prop. 2.3.1.

2.3.25 $\boldsymbol{a-x=b-y=z-c=0\ (mod2p).}$

Proof. By Def. 2.2.1 $c^p=a^p+b^p$ we have:
$(a^p-a)+(b^p-b)-(c^p-c)+a+b-c=0$; therefore:
$a+b-c=(c^p-c)-(a^p-a)-(b^p-b)=0\ (mod p)$ by Little Fermat’s Theorem; hence:
$a+b-c=0\ (mod p)$; by Defs. 2.2.3÷2.2.5 we have $(a+b)-c=a-(c-b)=b-(c-a)$, thus:
$z-c=a-x=b-y=0\ (mod p)$.
If c is even then $z=a+b$ is even too because a and b are odd; on the contrary, if c is odd then $z=a+b$ is odd too because a and b are one odd and the other even; anyway:
$z-c=0\ (mod2)$, therefore:
$z-c=a-x=b-y=0\ (mod2)$.
We may resume the above results as follows: $z-c=a-x=b-y=0\ (mod2p)$.

2.3.26 $\boldsymbol{x\neq0\ (mod p)\ \Leftrightarrow\ p\,|\,(a-d).}$

Proof. By Prop. 2.3.25 $p\,|\,(a-x)$ and according to LFT $p\,|\,(a^p-a)$, we have $p\,|\,(a^p-x)$.
By Prop. 2.3.22 $x=d^p$, hence $p\,|\,(a^p-d^p)$; by Property 1.9 we have $p\,|\,(a-d)$.
By Prop. 2.3.22 $a=dg$, we have $p\,|\,(dg-d)$, *i.e.*, $p\,|\,d(g-1)$.
Since $d\neq0\ (mod p)$, we have $p\,|\,(g-1)$, confirming Prop. 2.3.22.

2.3.27 $\boldsymbol{y\neq0\ (mod p)\ \Leftrightarrow\ p\,|\,(b-e).}$

Proof. Analogously to Prop. 2.3.26.

2.3.28 $\boldsymbol{z\neq0\ (mod p)\ \Leftrightarrow\ p\,|\,(c-f).}$

Proof. Analogously to Prop. 2.3.26.

2.3.29 $\boldsymbol{z^p-c^p=0\ (mod2pabz);\ a^p-x^p=0\ (mod2pbcx);\ b^p-y^p=0\ (mod2pacy).}$

Proof. By Def. 2.2.12:

$c^p=a^p+b^p=z\{z^{p-1}-pab[z^{p-3}-ab[n_1z^{p-5}-ab[n_2z^{p-7}+\cdots-ab(n_{(p-5)/2}z^2-ab)\cdots]]]\}$;

$c^p=z^p-pabz[z^{p-3}-ab[n_1z^{p-5}-ab[n_2z^{p-7}+\cdots-ab(n_{(p-5)/2}z^2-ab)\cdots]]]\}$;

$z^p-c^p=pabz[z^{p-3}-ab[n_1z^{p-5}-ab[n_2z^{p-7}+\cdots-ab(n_{(p-5)/2}z^2-ab)\cdots]]]\}$;

$z^p-c^p=0\ (mod2pabz)$.

Analogously by Defs. 2.2.10, 2.2.11: $a^p-x^p=0\ (mod2pbcx)$, $b^p-y^p=0\ (mod2pacy)$.

2.3.30
$$\begin{aligned}
\boldsymbol{z^p-c^p} &\boldsymbol{=(z-c)\{(z-c)^{p-1}+pzc[(z-c)^{p-3}+zc[n_1(z-c)^{p-5}+zc[n_2(z-c)^{p-7}+\cdots+zc[n_{(p-5)/2}(z-c)^2+zc]\cdots]]]\};}\\
&\boldsymbol{=(a-x)\{(a-x)^{p-1}+pzc[(a-x)^{p-3}+zc[n_1(a-x)^{p-5}+zc[n_2(a-x)^{p-7}+\cdots+zc[n_{(p-5)/2}(a-x)^2+zc]\cdots]]]\};}\\
&\boldsymbol{=(b-y)\{(b-y)^{p-1}+pzc[(b-y)^{p-3}+zc[n_1(b-y)^{p-5}+zc[n_2(b-y)^{p-7}+\cdots+zc[n_{(p-5)/2}(b-y)^2+zc]\cdots]]]\}.}\\
\boldsymbol{a^p-x^p} &\boldsymbol{=(a-x)\{(a-x)^{p-1}+pax[(a-x)^{p-3}+ax[n_1(a-x)^{p-5}+ax[n_2(a-x)^{p-7}+\cdots+ax(n_{(p-5)/2}(a-x)^2+ax)\cdots]]]\};}\\
&\boldsymbol{=(b-y)\{(b-y)^{p-1}+pax[(b-y)^{p-3}+ax[n_1(b-y)^{p-5}+ax[n_2(b-y)^{p-7}+\cdots+ax(n_{(p-5)/2}(b-y)^2+ax)\cdots]]]\};}\\
&\boldsymbol{=(z-c)\{(z-c)^{p-1}+pax[(z-c)^{p-3}+ax[n_1(z-c)^{p-5}+ax[n_2(z-c)^{p-7}+\cdots+ax(n_{(p-5)/2}(z-c)^2+ax)\cdots]]]\}.}\\
\boldsymbol{b^p-y^p} &\boldsymbol{=(b-y)\{(b-y)^{p-1}+pby[(b-y)^{p-3}+by[n_1(b-y)^{p-5}+by[n_2(b-y)^{p-7}+\cdots+by(n_{(p-5)/2}(b-y)^2+by)\cdots]]]\};}\\
&\boldsymbol{=(a-x)\{(a-x)^{p-1}+pby[(a-x)^{p-3}+by[n_1(a-x)^{p-5}+by[n_2(a-x)^{p-7}+\cdots+by(n_{(p-5)/2}(a-x)^2+by)\cdots]]]\};}\\
&\boldsymbol{=(z-c)\{(z-c)^{p-1}+pby[(z-c)^{p-3}+by[n_1(z-c)^{p-5}+by[n_2(z-c)^{p-7}+\cdots+by(n_{(p-5)/2}(z-c)^2+by)\cdots]]]\}.}
\end{aligned}$$

Proof. By Defs. 2.2.13÷2.2.15 and according to Prop. 2.3.25 $a-x=b-y=z-c$.

2.3.31 $\boldsymbol{a=0\ (mod2)\ \Leftrightarrow\ x=0\ (mod2^p).}$

Proof. Let us assume $a=0\ (mod2)$, by Property 1.5.1 $a^p=0\ (mod2^p)$.

If $x\neq0\ (mod2)$:

$$a^p=c^p-b^p=\underbrace{x\{\underbrace{x^{p-1}+pbc[\underbrace{x^{p-3}+bc[\underbrace{n_1x^{p-5}+bc[\underbrace{n_2x^{p-7}+\ \cdots\ +bc(\underbrace{n_{(p-5)/2}x^2+bc}_{=0\ \ (mod2)})\ \cdots}_{=0\ \ (mod2)}\ ]]}_{=0\ \ (mod2)}]}_{=0\ \ (mod2)}}_{\neq0\ \ (mod2)}\}}_{\neq0\ \ (mod2)}.$$

It means $a^p\neq0\ (mod2)$ inconsistent with the assumption; hence $x=0\ (mod2)$.

Since $a^p=0\ (mod2^p)$ and $x=0\ (mod2)$ we have:

$$a^p=c^p-b^p=x\{\underbrace{x^{p-1}+pbc[\underbrace{x^{p-3}+bc[\underbrace{n_1x^{p-5}+bc[\underbrace{n_2x^{p-7}+\cdots+bc(\underbrace{n_{(p-5)/2}x^2+bc}_{\neq0\ \ (mod2)})\cdots}_{\neq0\ \ (mod2)}]]}_{\neq0\ \ (mod2)}]}_{\neq0\ \ (mod2)}}_{\neq0\ \ (mod2)}\}=0\ \ (mod2^p).$$

Thus necessarily $x=0\ (mod2^p)$.

2.3.32 $\boldsymbol{b=0\ (mod2)\ \Leftrightarrow\ y=0\ (mod2^p).}$

Proof. Analogously to Prop. 2.3.31.

2.3.33 $\boldsymbol{c=0\ (mod2)\ \Leftrightarrow\ z=0\ (mod2^p).}$

Proof. Analogously to Prop. 2.3.31.

2.4 THEOREMS

2.4.1 $c^2=a^2+b^2 \Leftrightarrow a\veebar b=0\ (mod2) \wedge c\neq 0\ (mod2)$.

Proof. In Pythagoras' primitive triple $a^2+b^2=c^2$ there are two odds and one even; anyway $a+b-c=0\ (mod2)$, *i.e.*, $z-c=0\ (mod2)$.
By expanding $c=z-(z-c)$, we have:
$c=a+b-(z-c)$;
$c^2=[a+b-(z-c)]^2$;
$c^2=a^2+b^2+2ab+(z-c)^2-2(a+b)(z-c)$;
$c^2-(a^2+b^2)=2ab+(z-c)^2-2(a+b)(z-c)$;
$0=2ab+(z-c)^2-2(a+b)(z-c)$;

$$\underbrace{\underbrace{2(a+b)(z-c)}_{=0\ (mod2^2)}-\underbrace{(z-c)^2}_{=0\ (mod2^2)}}_{=0\ (mod2^2)}=2ab;$$

$2ab=0\ (mod2^2)$;
$ab=0\ (mod2)$;
$a\veebar b=0\ (mod2)$.
Since a,b,c are pairwise coprime: $c\neq 0\ (mod2)$.

2.4.2 $c^3=a^3+b^3 \Leftrightarrow a\veebar b\veebar c=0\ (mod3)$.

Proof. By Prop. 2.3.25, when $p=3$: $z-c=0\ (mod3)$.
By expanding $c=z-(z-c)$, we have:
$c=a+b-(z-c)$;
$c^3=[a+b-(z-c)]^3$;
$c^3=a^3+b^3+3a^2b+3ab^2+(z-c)^3-3(a+b)^2(z-c)-3(z-c)^2(a+b)$;
$c^3-(a^3+b^3)=3abz+(z-c)^3-3z^2(z-c)-3(z-c)^2z$;
$0=3abz+(z-c)^3-3z^2(z-c)-3(z-c)^2z$;

$$\underbrace{\underbrace{3z^2(z-c)}_{=0\ (mod3^2)}+\underbrace{3(z-c)^2z}_{=0\ (mod3^3)}-\underbrace{(z-c)^3}_{}}_{=0\ (mod3^2)\text{ according to Property 1.5.3}}=3abz;$$

$3abz=0\ (mod3^2)$;
$abz=0\ (mod3)$;
$a\veebar b\veebar z=0\ (mod3)$.
By Prop. 2.3.5, $3|z$ implies $3|c$, thus: $a\veebar b\veebar c=0\ (mod3)$.

2.4.3 ***If*** $a,b,c\neq 0\ (modp)$ ***then*** $2c=d^p+e^p+f^p,\ b-a=e^p-d^p,\ b+c=e^p+f^p,\ a+c=d^p+f^p$.

Proof. By Props. 2.3.22÷2.3.25.

2.4.4 ***There must be least two p-power of integers in the triple x,y,z.***

Proof. Since x,y,z are pairwise coprime, only one can be divisible by p.
If $x,y,z\neq 0\ (modp)$ then $x=d^p$, $y=e^p$, $z=f^p$ according to Props. 2.3.22÷2.3.24.
If $x=0\ (modp)$ then $y,z\neq 0\ (modp)$, *i.e.*, $y=e^p$, $z=f^p$.
If $y=0\ (modp)$ then $x,z\neq 0\ (modp)$, *i.e.*, $x=d^p$, $z=f^p$.
If $z=0\ (modp)$ then $x,y\neq 0\ (modp)$, *i.e.*, $x=d^p$, $y=e^p$.
Therefore $x=d^p\wedge y=e^p\wedge z=f^p\ \veebar\ x=d^p\wedge y=e^p\ \veebar\ x=d^p\wedge z=f^p\ \veebar\ y=e^p\wedge z=f^p$.

2.4.5 ***There must only one number divisible by*** 2^p ***in the triple x,y,z.***

Proof. In $a^p+b^p=c^p$ only one out of a,b,c must be even.
If $a=0\ (mod2)$ then $x=0\ (mod2^p)$, according to Prop. 2.3.31.
If $b=0\ (mod2)$ then $y=0\ (mod2^p)$, according to Prop. 2.3.32.
If $c=0\ (mod2)$ then $z=0\ (mod2^p)$, according to Prop. 2.3.33.
Therefore $2^p|x\ \veebar\ 2^p|y\ \veebar\ 2^p|z$.

2.4.6 ***There must only one number divisible by 2 in the triple d,e,f.***

Proof. By Theorem 2.4.5 only one out of x,y,z must be divisible by 2^p.
If $x=0\ (mod2^p)$ then $d=0\ (mod2)$, according to Def. 2.2.6.
If $y=0\ (mod2^p)$ then $e=0\ (mod2)$, according to Def. 2.2.7.
If $z=0\ (mod2^p)$ then $f=0\ (mod2)$, according to Def. 2.2.8.
Therefore $2|d\ \veebar\ 2|e\ \veebar\ 2|f$.

2.4.7 ***If $a,b,c\neq 0\ (mod p)$ then $c^p=a^p+b^p$ is $(f*i)^p=(d*g)^p+(e*h)^p$; with d,e,f,g,h,i pairwise coprime and $d\geq 1$.***
Proof. By Props. 2.3.22÷2.3.24.

2.4.8 ***If $a=0\ (mod p)$ then $c^p=a^p+b^p$ is $(f*i)^p=(p*j)^p+(e*h)^p$; with p,e,f,j,h,i pairwise coprime.***
Proof. By Props. 2.3.6, 2.3.23 and 2.3.24.

2.4.9 ***If $b=0\ (mod p)$ then $c^p=a^p+b^p$ is $(f*i)^p=(d*g)^p+(p*l)^p$; with d,p,f,g,l,i pairwise coprime and $d\geq 1$.***
Proof. By Props. 2.3.7, 2.3.22 and 2.3.24.

2.4.10 ***If $c=0\ (mod p)$ then $c^p=a^p+b^p$ is $(p*m)^p=(d*g)^p+(e*h)^p$; with d,e,f,g,p,m pairwise coprime and $d\geq 1$.***
Proof. By Props. 2.3.8, 2.3.22 and 2.3.23.

2.5 COROLLARIES

2.5.1 ***A primitive Fermat's equation $c^p=a^p+b^p$ can be only:***

I) $(dg)^p+(eh)^p=(fi)^p \Leftrightarrow a,b,c\neq 0\ (mod p)$, with d,e,f,g,h,i pairwise coprime, $d\geq 1$;
besides $x=d^p$, $y=e^p$, $z=f^p$ with $2|d \veebar 2|e \veebar 2|f$.

II) $(pj)^p+(eh)^p=(fi)^p \Leftrightarrow a=0\ (mod p)$, with p,e,f,j,h,i pairwise coprime, $j>1$;
besides $y=e^p$, $z=f^p$ with $2|j \veebar 2|e \veebar 2|f$.

III) $(dg)^p+(pl)^p=(fi)^p \Leftrightarrow b=0\ (mod p)$, with d,p,f,g,l,i pairwise coprime, $l>1$, $d\geq 1$;
besides $x=d^p$, $z=f^p$ with $2|d \veebar 2|l \veebar 2|f$.

IV) $(dg)^p+(eh)^p=(pm)^p \Leftrightarrow c=0\ (mod p)$, with d,e,f,g,p,m pairwise coprime, $d\geq 1$;
besides $x=d^p$, $y=e^p$ with $2|d \veebar 2|e \veebar 2|m$.

Proof. By Theorems 2.4.6÷2.4.10.

2.5.2 ***In a primitive Fermat's equation $c^p=a^p+b^p$:***

I) there cannot be a mere power of 2;
II) there cannot be a mere power of the index p;
III) a can be a mere power of an odd $q\neq p$ if and only if $x=1$;
IV) if $x>1$ then a has at least two relatively prime factors;
V) b has at least two relatively prime factors;
VI) c has at least two relatively prime factors;

Proof. By Corollary 2.5.1.

2.5.3 ***A primitive Fermat triple a,b,c can be formed only by combining at least five different primes, if $x=1$; otherwise it takes minimum six primes.***
Proof. By Corollary 2.5.2 if the coprime factors forming a,b,c are all primes.

2.5.4 ***$\neg\exists a,b,c,x,y,z\in N$: $z-c=a-x=b-y$, on the basis of the Rational Root Theorem.***
Proof. The equality condition $z-c=a-x=b-y$ is at odds with the constraints imposed by Propositions 2.3.3÷2.3.5 and 2.3.12÷2.3.14, *i.e.*, it is impossible that all differences can be obtained from two variables one of which has all the factors of the other plus at least an additional factor coprime to the other. Actually, the mere non-coprimality on the differences $a-x$, $b-y$, $z-c$ it is not enough to contradict Fermat. For example if $p=3$ at least in a case out of around 10^9 combinations of factors chosen among the first 50 prime numbers, we find the possible integers $a=22038731=11*13*229*673$; $b=19945108=47*2^2*277*383$; $c=22869315=3^2*5*79*7*919$; $x=2924207=11^3*13^3$; $y=830584=47^3*2^3$; $z=41983839=79*3^{12}$.
The restriction $z-c=a-x=b-y$ becomes impossibility only when combined with the conditions $x|a^n$, $x|b^n$, $z|c^n$. In fact we should find a combination of two relatively prime factors $u>v$ such as $2c>z>c$, which also satisfy the above mentioned conditions. Let us imagine the *simplest possible combination*. Let $z=u^2$ and $c=uv$, we have: $z-c=u^2-uv=u(u-v)$; with $u>1$ coprime to $v>1$, since φ_z (if $z\neq 0\ (mod p)$) or φ_z/p (if $z=0\ (mod p)$) are larger than 1 and coprime to z. Similarly, to represent $b-y$ we chose the relatively prime factors $s<t$, such as $y=s^2$ and $b=st$, we have: $b-y=st-s^2=s(t-s)=u(u-v)$, with $s>1$ coprime to $t>1$, since φ_y (if $y\neq 0\ (mod p)$) or φ_y/p (if $y=0\ (mod p)$) are larger than 1 and coprime to y. Obviously s,t,u,v are pairwise coprime by construction. Finally we chose the factors $1\leq q<r$, relatively prime if $q>1$, such as $x=q^2$ and $c=qr$, we have: $a-x=qr-q^2=q(r-q)=u(u-v)=s(t-s)$. If $x>1$ then $q>1$ is coprime to $r>1$, since φ_x (if $x\neq 0\ (mod p)$) or φ_y/p (if $y=0\ (mod p)$) are lager than 1 and coprime to x. In this case, obviously q,r,s,t,u,v are pairwise coprime by construction, otherwise if $x=q=1$ only r,s,t,u,v are pairwise coprime.
According to Proposition 2.3.25 $a-x=b-y=z-c$, that is: $q(r-q)=s(t-s)=u(u-v)=kqsu$, with $k\in Z^+$ by construction. Since every difference between coprimes is coprime in turn to both terms of the difference, we have:

I) $r-q=ksu$, with s,u,r pairwise coprime, and this holds also for k and q if they are larger than 1;

II) $t-s=kqu$, with s,u,t pairwise coprime, and this holds also for k and q if they are larger than 1;

III) $u-v=kqs$, with s,u,v pairwise coprime, and this holds also for k and q if they are larger than 1.

Extracting one variable at will, for instance s, as a function of the others:

IV) $s_1=(r-q)/ku$;

V) $s_2=t-kqu$;

VI) $s_3=(u-v)/kq$;

The relations $s_1(k)$, $s_2(k)$ and $s_3(k)$ are not compatible with k integer.

In fact, from $s_1=s_2$ we have: $(r-q)/ku=t-kqu$, *i.e.*, $q=(k^2u^2-1)/(kut-r)$.

Substituting in $s_3=(u-v)/kq$:

$s=(u-v)/k[(k^2u^2-1)/(kut-r)]=[(u-v)(kut-r)]/[k[(k^2u^2-1)]$;

$s=[kqs(kut-r)]/[k[(k^2u^2-1)]$;

$1=[kq(kut-r)]/[k[(k^2u^2-1)]$;

$1=(kqut-rq)/(k^3u^2-k)$;

$kqut-rq=k^3u^2-k$;

$k^3u^2-k-kqut+rq=0$;

$\wp(\mathbf{k})=\mathbf{k}^3u^2-\mathbf{k}(1+qut)+rq=0$.

$\wp(\mathbf{k})=\mathbf{k}^3z-\mathbf{k}(1+qut)+a=0$.

According to the *Rational Root Theorem*, the eventually integer solutions of the polynomial $\wp(k)$ are to be searched for among the fractions $k=k_n/k_d$ having as numerator a factor of the constant term $k_n|a$ and as denominator a factor of the main coefficient $k_d|z$.

The case $k_n=k_d=k=1$ is impossible, because it leads to the absurd: $z+a=1+qut$.

The case $k_d=1$ and $k_n>1$ is impossible, because it implies $k|a$, *i.e.*, that k is equal to a factor of a, or to a itself, both cases being excluded by the coprimality of r and q with k.

The case $k_d>1$ and $k_n>1$ implies, finally, that k is an irreducible fraction to any integer since no common factor exists between z and a, owing to the fact that all factors of z are factors of c too and c is coprime to a.

Thus the equation $\wp(\mathbf{k})=0$ admits exclusively fractional roots $k\notin$N, in contradiction with the hypothesis $k\in$Z$^+$.

With any other more complicated combination of numbers with respect to the one introduced by q,r,s,t,u,v, the situation does not change:

$\wp(k)=0 \Leftrightarrow k\notin$N, in contradiction with $k\in$Z$^+$.

In fact in any polynomial obtained by eliminating a variable from $a-x=b-y=z-c$:

$\wp(k)=a_nk^n+a_{n-1}k^{n-1}+\cdots+a_2k^2+a_1k+a_0=0$;

the eventual roots $k\in$N cannot be coprime to a,b or c, as required by the definition of k, because the constant term a_0 and the leading coefficient a_n are formed *only* by the factors constituting a, b or c. Those factors are never linked in manners different from the mere *product* among them, so that there are not additional factors neither in a_0 nor in a_n (*e.g.*, there are not linear or higher degree combinations among coprimes to generate additional factors).

Furthermore, the factors from the variables a, b or c contained in the coefficients a_n and a_0 are always *crossed*, so that the fraction a_n/a_0 is anyway *irreducible*.

2.5.5 ***Corollary 2.5.4 is inconsistent with Proposition 2.3.25.***

Proof. The thesis of Corollary 2.5.4 denies the thesis of Proposition 2.3.25.

2.5.6 ***$\neg\exists a,b,c\in N$: $c^p=a^p+b^p$, i.e., primitive Fermat triples with prime exponent $p>2$ cannot exist.***

Proof. According to Corollary 2.5.5, the hypothesis of a valid triple $c^p=a^p+b^p$ generates a contradiction.

2.5.7 ***$\neg\exists n\in N$, $n>2$: $c^n=a^n+b^n$, i.e., no primitive Fermat triples with natural exponent $n>2$.***

Proof. If $p|n$, then we have an obvious consequence of Corollary 2.5.6, because triples with odd non prime powers like $c^{\gamma p}=a^{\alpha p}+b^{\beta p}$ can be easily transformed into triples with prime p exponent $(c^\gamma)^p=(a^\alpha)^p+(b^\beta)^p$.

Otherwise n is a power of 2, i.e., $4|n$, case excluded by a known Fermat’s proof.

2.5.8 ***$\neg\exists n,A,B,C\in N$, $n>2$: $C^n=A^n+B^n$, i.e., Fermat’s Last Theorem.***

Proof. By Corollary 2.5.7, since any natural triple A,B,C can be reduced to its primitive a,b,c dividing it by the greatest common factor $m=GCF(A,B,C)$: $a=A/m$, $b=B/m$ and $c=C/m$.

2.5.9 ***$\exists A,B,C\in N$: $C^2=A^2+B^2$, i.e., Pythagoras’ Theorem.***

Proof. For $p=2$ the mixed product of variables is $2ab$ and it does not imply common factors among the three differences $z-c=a-x=b-y$.

CONCLUSIONS

After having examined my paper *New Ideas on Number Theory* (2006) and having corrected some flaws there present, Professor De Paz noticed how for p=2 the mixed product of variables is 2ab and it does not imply the existence of common factors in the differences $(a+b)-c=a-(c-b)=b-(c-a)$ which instead is proved for p>2 thanks to the binomial expansion I had proposed as elementary key to solve FLT; therefore he contacted me proposing a cooperation on Fermat's Last Theorem.

After some full-working months, having assumed the completeness of possibilities against and having demonstrated that such hypothesis is contradictory with the premises, we supplied the elementary attempt of proof called *Six moves to checkmate Fermat?* (2007).

The genesis of this first demonstration of ours saw four crucial events:

1. My discovery of the consequences of his binomial expansion on Fermat's equation, namely on prime and non prime factors in the variables implied;
2. The intuition by Mario about the impossibility of $(a+b)-c=a-(c-b)=b-(c-a)$ in those factorial conditions;
3. The method of minimum couples to be used when looking for eventual contradiction, developed by De Paz;
4. My intuition about the *Rational Root Theorem* for the final step of confutation.

It was thus a perfectly balanced group work between the authors, each one providing, when needed, either a strategic intuition or a key operative instrument, faithfully reported in papers 1-13 of our 5ecm Poster 2.21.

The approach of this paper allows to extend to any prime *p>2* the properties of power p=3 for which the proof has been given since Euler's age by the method of infinite descent, different from the one presented here but coincident with the fact that for indexes p>2 it is not possible to find coprime triples satisfying the primitive Fermat's equation.

After Fermat himself proved how to exclude all the exponents multiple of *four,* it could be the final step to complete the elementary proof of FLT.

I will always be grateful to my great friend Mario De Paz for a huge list of reasons. To those who do not have the privilege of knowing him I can just say that he is one of the brightest exponent of the Italian academic world, pleasantly smart, always curious, never banal, an incredibly skilled researcher with a commendable humble attitude.

Without his help I would have given up studying mathematics two years ago and I could not grow as a person in the way it happened.

REFERENCES

[1] Bonacci, E., *New Ideas on Number Theory*, Carta e Penna Publisher, Turin, 2006

[2] Bonacci, E., *Six moves to checkmate Fermat?*, Carta e Penna Publisher, Turin, 2007

[3] Bonacci, E., De Paz, M., “Consequences of binomial expansion’s unexplored properties on Fermat’s triples and Cosine Law,” Amsterdam (2008), *5ecm-Programme and Abstracts*, p. 85

[4] Bonacci, E., De Paz, M., *Consequences of binomial expansion’s unexplored properties on Fermat’s triples and Cosine Law at the 5ecm in Amsterdam*, Aracne Sec. A1 N° 121, Rome, 2008