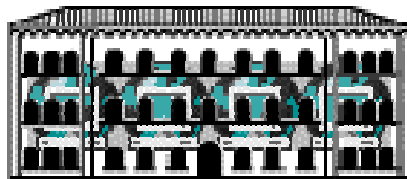




**Research paper by
Dr. Enzo Bonacci
about New Ideas on
Number Theory**

**Cosmopolitan
University**



Courses & Research



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.

New Ideas on Number Theory

*Mr. Enzo Bonacci (Italy), Honorary Doctor**

INDEX

<i>Consequences of binomial expansion's unexplored properties on Fermat's triples and Cosine Law</i>	Page 4
Abstract	Page 4
Classifications	Page 4
Explanations	Page 4
Pascal's triangle and binomial expansions	Page 5
Analysis of Fermat's equations through the binomial properties	Page 10
Multidimensional extension of the Cosine Law on synclastic surfaces	Page 18
<i>An old elementary attempt at proving Fermat's Last Theorem</i>	Page 21
Introduction	Page 21
Definitions	Page 21
Propositions	Page 21
Theorems	Page 23
Corollaries	Page 25
<i>Simplification of Goldbach's conjecture and its negative twin</i>	Page 26
Introduction	Page 26
Definitions	Page 26
Propositions	Page 26
Conjectures	Page 27
Theorems	Page 27
Corollaries	Page 28
References	Page 29

(*) Ph.D. Honoris Causa in Theoretical Physics by 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

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

Explanations

There are some mathematical definitions worthy to be explained.

" $\text{GCF}(a,b,c)$ " means *greatest common factor*, *i.e.*, the greatest factor that divides a,b and c .

" $b|a$ " and the equivalent " $a=0 \pmod{b}$ " mean that b divides a , *i.e.*, b is a factor of a .

" $a \not\equiv 0 \pmod{b}$ " 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.*, $\text{GCF}(a,b)=1$.

" a and b are relatively prime" means that a and b are coprime.

" a,b,c are pairwise coprime" when $\text{GCF}(a,b)=\text{GCF}(a,c)=\text{GCF}(b,c)=1$.

" 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.*, $\text{GCF}(a,b)>1$.

" $a=q \pmod{p}$ " and the equivalent " $a-q=0 \pmod{p}$ " 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).

1.8 Binomial expansion $a^p - b^p$, with $a, b, p \in \mathbb{N}$ and $p > 2$ prime.

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

$$\begin{aligned} a^p - b^p &= (a-b)^p + \\ &+ pab(a-b)^{p-2} + \\ &+ (ab)^2(a-b)^{p-4} (1 - C_{p-1, 2} + pC_{p-3, 1}) + \\ &+ (ab)^3(a-b)^{p-6} [1 + C_{p-1, 3} - pC_{p-3, 2} + (1 - C_{p-1, 2} + pC_{p-3, 1}) C_{p-5, 1}] + \\ &+ (ab)^4(a-b)^{p-8} \{1 - C_{p-1, 4} + pC_{p-3, 3} - (1 - C_{p-1, 2} + pC_{p-3, 1}) C_{p-5, 2} + [1 + C_{p-1, 3} - pC_{p-3, 2} + (1 - C_{p-1, 2} + pC_{p-3, 1}) C_{p-5, 1}] C_{p-7, 1}\} + \\ &+ \dots + \\ &+ (ab)^{(p-3)/2} (a-b)^3 \{1 + (-1)^{(p-1)/2} C_{p-1, (p-3)/2} + \\ &\quad + (-1)^{(p-3)/2} pC_{p-3, (p-5)/2} + \\ &\quad + (-1)^{(p-5)/2} (1 - C_{p-1, 2} + pC_{p-3, 1}) C_{p-5, (p-7)/2} + \\ &\quad + (-1)^{(p-7)/2} [1 + C_{p-1, 3} - pC_{p-3, 2} + (1 - C_{p-1, 2} + pC_{p-3, 1}) C_{p-5, 1}] C_{p-7, (p-9)/2} + \\ &\quad + \dots + \\ &\quad + [1 + (-1)^{(p-3)/2} C_{p-1, (p-5)/2} + p(-1)^{(p-5)/2} C_{p-3, (p-7)/2} + p(-1)^{(p-7)/2} n_1 C_{p-5, (p-9)/2} + \\ &\quad + \dots + pn_{(p-9)/2} C_{(p-5)/2, 1}] C_{(p-3)/2, 1}\} + \\ &+ (ab)^{(p-1)/2} (a-b)p. \end{aligned}$$

By introducing $a-b=t$, and according to Definition 1.5:

$$n_k = [1 + (-1)^{k+2} C_{p-1, k+1}] / p + (-1)^{k+1} C_{p-3, k} + (-1)^k n_1 C_{p-5, k-1} + (-1)^{k-1} n_2 C_{p-7, k-2} + \dots + n_{k-1} C_{k+1, 1},$$

we have:

$$\begin{aligned} a^p - b^p &= t^p + \\ &+ (ab) t^{p-2} p + \\ &+ (ab)^2 t^{p-4} pn_1 + \\ &+ (ab)^3 t^{p-6} (1 + C_{p-1, 3} - pC_{p-3, 2} + pn_1 C_{p-5, 1}) + \\ &+ (ab)^4 t^{p-8} (1 - C_{p-1, 4} + pC_{p-3, 3} - pn_1 C_{p-5, 2} + pn_2 C_{p-7, 1}) + \\ &+ \dots + \\ &+ (ab)^{(p-3)/2} t^3 [1 + (-1)^{(p-1)/2} C_{p-1, (p-3)/2} + (-1)^{(p-3)/2} pC_{p-3, (p-5)/2} + (-1)^{(p-5)/2} pn_1 C_{p-5, (p-7)/2} + (-1)^{(p-7)/2} pn_2 C_{p-7, (p-9)/2} + \\ &\quad + \dots + pn_{(p-7)/2} C_{(p-3)/2, 1}] + \\ &+ (ab)^{(p-1)/2} tp. \end{aligned}$$

Further:

$$\begin{aligned} a^p - b^p &= t^p + \\ &+ pabt^{p-2} + \\ &+ pn_1 (ab)^2 t^{p-4} + \\ &+ pn_2 (ab)^3 t^{p-6} + \\ &+ pn_3 (ab)^4 t^{p-8} + \\ &+ \dots + \\ &+ pn_{(p-5)/2} (ab)^{(p-3)/2} t^3 + \\ &+ p(ab)^{(p-1)/2} t. \end{aligned}$$

Therefore:

$$\begin{aligned} a^p - b^p &= t^p + pabt^{p-2} + pn_1 (ab)^2 t^{p-4} + pn_2 (ab)^3 t^{p-6} + \dots + pn_{(p-5)/2} (ab)^{(p-3)/2} t^3 + p(ab)^{(p-1)/2} t = \\ &= t [t^{p-1} + pabt^{p-3} + pn_1 (ab)^2 t^{p-5} + pn_2 (ab)^3 t^{p-7} + \dots + pn_{(p-5)/2} (ab)^{(p-5)/2} t^2 + p(ab)^{(p-3)/2}] = \\ &= t \{t^{p-1} + pab[t^{p-3} + n_1 abt^{p-5} + n_2 (ab)^2 t^{p-7} + \dots + n_{(p-5)/2} (ab)^{(p-7)/2} t^2 + (ab)^{(p-5)/2}]\} = \\ &= t \{t^{p-1} + pab[t^{p-3} + ab[n_1 t^{p-5} + n_2 abt^{p-7} + \dots + n_{(p-5)/2} (ab)^{(p-9)/2} t^2 + (ab)^{(p-7)/2}]]\} = \\ &= t \{t^{p-1} + pab[t^{p-3} + ab[n_1 t^{p-5} + ab[n_2 t^{p-7} + \dots + n_{(p-5)/2} (ab)^{(p-11)/2} t^2 + (ab)^{(p-9)/2}]]]\} = \\ &= \dots = \\ &= t \{t^{p-1} + pab[t^{p-3} + ab[n_1 t^{p-5} + ab[n_2 t^{p-7} + \dots + ab(n_{(p-5)/2} t^2 + ab) \dots]]]\}. \end{aligned}$$

By substituting back $a-b=t$:

$$\mathbf{1.8.1} \quad a^p - b^p = (a-b)^p + pab(a-b) \{ (a-b)^{p-3} + ab[n_1 (a-b)^{p-5} + ab[n_2 (a-b)^{p-7} + \dots + ab[n_{(p-5)/2} (a-b)^2 + ab] \dots] \}.$$

Similarly to the above proof:

$$\mathbf{1.8.2} \quad a^p + b^p = (a+b)^p - pab(a+b) \{ (a+b)^{p-3} - ab[n_1 (a+b)^{p-5} - ab[n_2 (a+b)^{p-7} + \dots - ab[n_{(p-5)/2} (a+b)^2 - ab] \dots] \}.$$

Let us resume the above Properties 1.8.1 and 1.8.2 as follows:

$$\mathbf{1.8.3} \quad a^p \pm b^p = (a \pm b)^p - (\mp pab) (a \pm b) \{ (a \pm b)^{p-3} - (\mp ab) [n_1 (a \pm b)^{p-5} - (\mp ab) [n_2 (a \pm b)^{p-7} + \dots - (\mp ab) [n_{(p-5)/2} (a \pm b)^2 - (\mp ab) \dots]] \}.$$

1.9 $\forall a, b, p \in \mathbb{N}, p > 2$ prime: $(a \pm b)^p = a^p \pm b^p \pmod{pab}$.

Proof. By the binomial expansion 1.8.3:

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

Therefore $(a \pm b)^p - (a^p \pm b^p) = 0 \pmod{pab}$.

1.10 $\forall a, b, p \in \mathbb{N}, p > 2$ prime: $a^p \pm b^p = 0 \pmod{p} \Leftrightarrow a \pm b = 0 \pmod{p}$.

Proof. By the binomial expansion 1.8.3:

$$\begin{aligned} a^p \pm b^p &= 0 \pmod{p}; \\ (a \pm b)^p - (\pm pab) (a \pm b) \{ (a \pm b)^{p-3} - (\pm ab) [n_1 (a \pm b)^{p-5} - (\pm ab) [n_2 (a \pm b)^{p-7} + \dots - (\pm ab) [n_{(p-5)/2} (a \pm b)^2 - (\pm ab) \dots] \dots] \} &= 0 \pmod{p}. \\ &\underbrace{\hspace{15em}}_{=0 \pmod{p}} \\ &= 0 \pmod{p} \end{aligned}$$

Therefore $(a \pm b)^p = 0 \pmod{p}$.

1.11 $\forall a, b, p \in \mathbb{N}, p > 2$ prime: $a^p \pm b^p = 0 \pmod{p} \Rightarrow a^p \pm b^p = 0 \pmod{p^2}$.

Proof. By binomial Property 1.10 $a^p \pm b^p = 0 \pmod{p} \Leftrightarrow a \pm b = 0 \pmod{p}$:

$$\begin{aligned} (a \pm b)^p - (\pm pab) (a \pm b) \{ (a \pm b)^{p-3} - (\pm ab) [n_1 (a \pm b)^{p-5} - (\pm ab) [n_2 (a \pm b)^{p-7} + \dots - (\pm ab) [n_{(p-5)/2} (a \pm b)^2 - (\pm ab) \dots] \dots] \} &= 0 \pmod{p^2}. \\ = 0 \pmod{p^2} &\underbrace{\hspace{15em}}_{=0 \pmod{p^2}} \end{aligned}$$

According to prime Property 1.6.3, since $p > 2$: $a^p \pm b^p = 0 \pmod{p^2}$.

1.12 $\forall a, b, q \in \mathbb{N}, a$ coprime to $b, q \geq 2, p > 2$ prime: $a^p \pm b^p = 0 \pmod{p^q} \Leftrightarrow a \pm b = 0 \pmod{p^{q-1}}$.

Proof. Let us assume $a^p - b^p = 0 \pmod{p^q}$; by Properties 1.10 and 1.11 $a^p - b^p = 0 \pmod{p}$ implies:

1.12.1 $a - b = 0 \pmod{p}$;

1.12.2 $a^p - b^p = 0 \pmod{p^2}$, i.e., $q \geq 2$.

By Property 1.6.2 $(a - b)$ is coprime to ab , so that $ab \neq 0 \pmod{p}$.

As a consequence of 1.12.1 and 1.12.2, since p is prime:

$$n_{(p-5)/2} (a - b)^2 + ab \neq 0 \pmod{p};$$

$$ab (n_{(p-5)/2} (a - b)^2 + ab) \neq 0 \pmod{p};$$

$$ab [n_2 (a - b)^{p-7} + \dots + ab (n_{(p-5)/2} (a - b)^2 + ab) \dots] \neq 0 \pmod{p};$$

$$1.12.3 (a - b)^{p-3} + ab [n_1 (a - b)^{p-5} + ab [n_2 (a - b)^{p-7} + \dots + ab (n_{(p-5)/2} (a - b)^2 + ab) \dots] \neq 0 \pmod{p}.$$

By comparing the Property 1.12.2 $a^p = b^p \pmod{p^2}$ to the binomial expansion 1.8.1:

$$a^p - b^p = (a - b)^p + pab (a - b) \{ (a - b)^{p-3} + ab [n_1 (a - b)^{p-5} + ab [n_2 (a - b)^{p-7} + \dots + ab [n_{(p-5)/2} (a - b)^2 + ab] \dots] \} = 0 \pmod{p^q};$$

$$pab (a - b) \{ (a - b)^{p-3} + ab [n_1 (a - b)^{p-5} + ab [n_2 (a - b)^{p-7} + \dots + ab (n_{(p-5)/2} (a - b)^2 + ab) \dots] \} = 0 \pmod{p^q};$$

$$ab * (a - b) * \{ (a - b)^{p-3} + ab [n_1 (a - b)^{p-5} + ab [n_2 (a - b)^{p-7} + \dots + ab (n_{(p-5)/2} (a - b)^2 + ab) \dots] \} = 0 \pmod{p^{q-1}}.$$

$$\underbrace{\hspace{15em}}_{\neq 0 \pmod{p}} \quad \underbrace{\hspace{15em}}_{\neq 0 \pmod{p} \text{ according to Property 1.12.3}}$$

Necessarily $a - b = 0 \pmod{p^{q-1}}$.

Analogously, if $a^p + b^p = 0 \pmod{p^q}$ then $a + b = 0 \pmod{p^{q-1}}$.

1.13 $\forall a, b \in \mathbb{N}$, a coprime to b , $p > 2$ prime: $(a^p + b^p)/(a+b)$ is coprime to $a+b \Leftrightarrow a+b \neq 0 \pmod{p}$

Proof. By Property 1.6.2 $(a+b)$ is coprime to ab because a and b are relatively prime. By expansion 1.8.1:

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

$$(a^p + b^p)/(a+b) = (a+b)^{p-1} - pab \{ (a+b)^{p-3} - ab[n_1(a+b)^{p-5} - ab[n_2(a+b)^{p-7} + \dots - ab[n_{(p-5)/2}(a+b)^2 - ab] \dots] \}.$$

$\underbrace{\hspace{15em}}_{\text{coprime to } (a+b)}$
 $\underbrace{\hspace{10em}}_{\text{coprime to } (a+b)}$
 $\underbrace{\hspace{10em}}_{\text{coprime to } (a+b)}$
 $\underbrace{\hspace{15em}}_{\text{coprime to } (a+b) \Leftrightarrow a+b \neq 0 \pmod{p}}$
 $\text{coprime to } (a+b) \Leftrightarrow a+b \neq 0 \pmod{p}$

Therefore $(a^p + b^p)/(a+b)$ is coprime to $(a+b)$ if and only if $a+b \neq 0 \pmod{p}$.

Analogously, $(a^p - b^p)/(a-b)$ is coprime to $(a-b)$ if and only if $a-b \neq 0 \pmod{p}$.

1.14 $\forall a, b, q \in \mathbb{N}$, a coprime to b , $p > 2$ prime: $a^p + b^p = 0 \pmod{2^q} \Leftrightarrow a+b = 0 \pmod{2^q}$.

Proof. If $a^p + b^p = 0 \pmod{2}$, necessarily:

1.14.1 $ab \neq 0 \pmod{2}$, because a and b are both odd as coprime;

1.14.2 $a-b = 0 \pmod{2}$.

By 1.14.1 and 1.14.2 we have:

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

$\underbrace{\hspace{15em}}_{\neq 0 \pmod{2}}$
 $\underbrace{\hspace{10em}}_{\neq 0 \pmod{2}}$
 $\underbrace{\hspace{10em}}_{\neq 0 \pmod{2}}$
 $\underbrace{\hspace{15em}}_{\neq 0 \pmod{2}}$
 $\neq 0 \pmod{2}$

Therefore $a-b = 0 \pmod{2^q}$.

Analogously, if $a^p + b^p = 0 \pmod{2^q}$ then $a+b = 0 \pmod{2^q}$.

1.15 $\forall a, b, q \in \mathbb{N}$, a coprime to b , $p > 2$ prime: $a^p + b^p \neq 2^q$.

Proof. By Property 1.14, if $a^p + b^p = 2^q$, necessarily: $a-b = 2^q$;

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

$\underbrace{\hspace{15em}}_{=0 \pmod{2^q}} \quad \underbrace{\hspace{15em}}_{\neq 0 \pmod{2}}$

$\exists r \in \mathbb{N}$, $r > 1$ coprime to 2: $a^p + b^p = 2^q * r$.

Analogously, if $a^p + b^p = 2^q$ then $a^p + b^p = 2^q * r$.

1.16 $A, B, C, n \in \mathbb{N}$, $A \leq B \leq C$: $n^A + n^B = n^C \Leftrightarrow n=2, A=B, C=B+1$.

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:

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

being $n_k = [1 + (-1)^{k+2} C_{p-1, k+1}] / p + (-1)^{k+1} C_{p-3, k} + (-1)^k n_1 C_{p-5, k-1} + (-1)^{k-1} n_2 C_{p-7, k-2} + \dots + n_{k-1} C_{k+1, 1}$.

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 $a, b, c \in \mathbb{N}$ 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 $d = x^{1/p}$, denote $\varphi_x = a^p / x \in \mathbb{N}$; denote $g = \varphi_x^{1/p}$.

2.2.7 Denote $e = y^{1/p}$, denote $\varphi_y = b^p / y \in \mathbb{N}$; denote $h = \varphi_y^{1/p}$.

2.2.8 Denote $f = z^{1/p}$, denote $\varphi_z = c^p / z \in \mathbb{N}$; denote $i = \varphi_z^{1/p}$.

2.2.9 $n_k = [1 + (-1)^{k+2} C_{p-1, k+1}] / p + (-1)^{k+1} C_{p-3, k} + (-1)^k n_1 C_{p-5, k-1} + (-1)^{k-1} n_2 C_{p-7, k-2} + \dots + n_{k-1} C_{k+1, 1}$.

2.2.10 $a^p = c^p - b^p = x \{ x^{p-1} + pbc [x^{p-3} + bc [n_1 x^{p-5} + bc [n_2 x^{p-7} + \dots + bc (n_{(p-5)/2} x^2 + bc) \dots]]] \} = x^* \varphi_x$.

2.2.11 $b^p = c^p - a^p = y \{ y^{p-1} + pac [y^{p-3} + ac [n_1 y^{p-5} + ac [n_2 y^{p-7} + \dots + ac (n_{(p-5)/2} y^2 + ac) \dots]]] \} = y^* \varphi_y$.

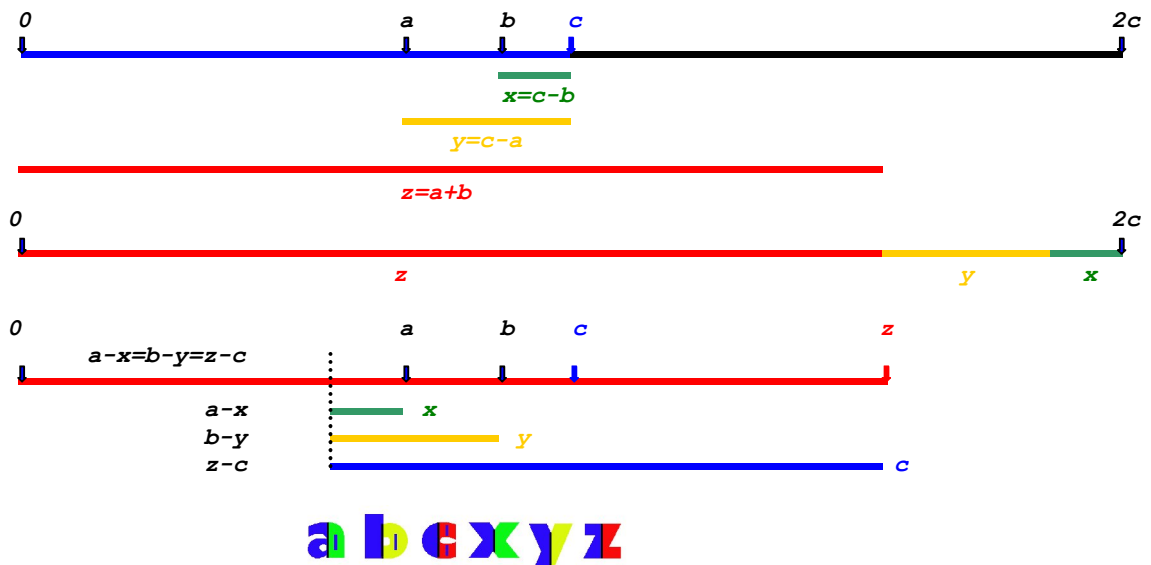
2.2.12 $c^p = a^p + b^p = z \{ z^{p-1} - pab [z^{p-3} - ab [n_1 z^{p-5} - ab [n_2 z^{p-7} + \dots - ab (n_{(p-5)/2} z^2 - ab) \dots]]] \} = z^* \varphi_z$.

2.2.13 $a^p - x^p = (a-x) \{ (a-x)^{p-1} + pax [(a-x)^{p-3} + ax [n_1 (a-x)^{p-5} + ax [n_2 (a-x)^{p-7} + \dots + ax (n_{(p-5)/2} (a-x)^2 + ax) \dots]]] \}$.

2.2.14 $b^p - y^p = (b-y) \{ (b-y)^{p-1} + pby [(b-y)^{p-3} + by [n_1 (b-y)^{p-5} + by [n_2 (b-y)^{p-7} + \dots + by (n_{(p-5)/2} (b-y)^2 + by) \dots]]] \}$.

2.2.15 $z^p - c^p = (z-c) \{ (z-c)^{p-1} + pzc [(z-c)^{p-3} + zc [n_1 (z-c)^{p-5} + zc [n_2 (z-c)^{p-7} + \dots + zc (n_{(p-5)/2} (z-c)^2 + zc) \dots]]] \}$.

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:

$a^p = c^p - b^p = x \{ x^{p-1} + pbc[x^{p-3} + bc[n_1x^{p-5} + bc[n_2x^{p-7} + \dots + bc(n_{(p-5)/2}x^2 + bc) \dots]]] \}$, i.e., $a^p = 0 \pmod{x}$.

$\forall q > 1$ 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 $a = 0 \pmod{p}$ if and only if $x = 0 \pmod{p^{p-1}}$ and $\varphi_x = 0 \pmod{p}$ but $\varphi_x \neq 0 \pmod{p^2}$.

Proof. Since p is prime, $a = 0 \pmod{p}$ implies $a^p = 0 \pmod{p^p}$.

According to Definition 2.2.10:

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

Necessarily $x = 0 \pmod{p}$.

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

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

$$\underbrace{\hspace{15em}}_{=0 \pmod{p} \text{ but } \neq 0 \pmod{p^2}}$$

$$= 0 \pmod{p} \text{ but } \neq 0 \pmod{p^2} \text{ by Property 1.6.3}$$

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

$$\varphi_x = a^p/x = \underbrace{x^{p-1}}_{=0 \pmod{p^{p-1}}} + \underbrace{pbc[x^{p-3} + bc[n_1x^{p-5} + bc[n_2x^{p-7} + \dots + bc(n_{(p-5)/2}x^2 + bc) \dots]]}_{=0 \pmod{p} \text{ but } \neq 0 \pmod{p^2}} = 0 \pmod{p} \text{ but } \varphi_x \neq 0 \pmod{p^2} \text{ by Property 1.6.3}$$

Necessarily $\varphi_x = 0 \pmod{p}$ but $\varphi_x \neq 0 \pmod{p^2}$.

2.3.7 $b = 0 \pmod{p}$ if and only if $y = 0 \pmod{p^{p-1}}$ and $\varphi_y = 0 \pmod{p}$ but $\varphi_y \neq 0 \pmod{p^2}$.

Proof. Analogously to Prop. 2.3.6.

2.3.8 $c = 0 \pmod{p}$ if and only if $z = 0 \pmod{p^{p-1}}$ and $\varphi_z = 0 \pmod{p}$ but $\varphi_z \neq 0 \pmod{p^2}$.

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 $p = \text{GCF}(x, \varphi_x)$, otherwise they are coprime.

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

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

$$\begin{array}{c} \underbrace{\hspace{10em}}_{\text{coprime to } x} \\ \underbrace{\hspace{8em}}_{\text{coprime to } x} \\ \underbrace{\hspace{6em}}_{\text{coprime to } x} \\ \underbrace{\hspace{4em}}_{\text{coprime to } x} \\ \underbrace{\hspace{2em}}_{\text{coprime to } x \text{ but } p} \\ \underbrace{\hspace{1em}}_{\text{coprime to } x \text{ but } p} \end{array}$$

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

2.3.10 Y and φ_y can share the unique factor p , if and only if $p = \text{GCF}(y, \varphi_y)$, 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 $p = \text{GCF}(z, \varphi_z)$, 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 $a = 0 \pmod{p}$ then $\varphi_x = 0 \pmod{p}$ and $\varphi_x \neq 0 \pmod{p^2}$; hence:

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

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

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

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

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 $a \neq 0 \pmod{p} \Leftrightarrow x \neq 0 \pmod{p} \wedge a^{p-1} = 1 \pmod{p}$.

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, $a^p - a = a(a^{p-1} - 1) = 0 \pmod{p}$.

Since $a \neq 0 \pmod{p}$ necessarily $a^{p-1} - 1 = 0 \pmod{p}$.

2.3.16 $b \neq 0 \pmod{p} \Leftrightarrow y \neq 0 \pmod{p} \wedge b^{p-1} = 1 \pmod{p}$.

Proof. Analogously to Prop. 2.3.15.

2.3.17 $c \neq 0 \pmod{p} \Leftrightarrow z \neq 0 \pmod{p} \wedge c^{p-1} = 1 \pmod{p}$.

Proof. Analogously to Prop. 2.3.15.

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

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

2.3.19 $x \neq 0 \pmod{p} \wedge x > 1 \Leftrightarrow p \mid (x^{p-1} - 1) \wedge p \mid (\varphi_x - 1)$.

Proof. By Fermat's Little Theorem $x^p - x = x(x^{p-1} - 1) = 0 \pmod{p}$.
 Since $x \neq 0 \pmod{p}$ we have $x^{p-1} - 1 = 0 \pmod{p}$. By Def. 2.2.6:
 $\varphi_x = a^p/x = x^{p-1} + pbc[x^{p-3} + bc[n_1x^{p-5} + bc[n_2x^{p-7} + \dots + bc(n_{(p-5)/2}x^2 + bc) \dots]]]$;
 $\varphi_x - 1 = \underbrace{x^{p-1} - 1}_{=0 \pmod{p}} + \underbrace{pbc[x^{p-3} + bc[n_1x^{p-5} + bc[n_2x^{p-7} + \dots + bc(n_{(p-5)/2}x^2 + bc) \dots]]]}_{=0 \pmod{p}}$.

Necessarily $\varphi_x - 1 = 0 \pmod{p}$.

2.3.20 $y \neq 0 \pmod{p} \Leftrightarrow p \mid (y^{p-1} - 1) \wedge p \mid (\varphi_y - 1)$.

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

2.3.21 $z \neq 0 \pmod{p} \Leftrightarrow p \mid (z^{p-1} - 1) \wedge p \mid (\varphi_z - 1)$.

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

2.3.22 $x \neq 0 \pmod{p} \Leftrightarrow \exists d, g \in \mathbb{Z}^+$ relatively prime: $a = dg$; $x = d^p \wedge \varphi_x = g^p$;
 besides $p \mid (g^{p-1} - 1) \wedge p \mid (g - 1)$; if $d > 1$ then $p \mid (d^{p-1} - 1)$.

Proof. If $x \neq 0 \pmod{p}$ 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 $d^p - d = d(d^{p-1} - 1) = 0 \pmod{p}$.

Since $d^p = x \neq 0 \pmod{p}$, i.e., $d \neq 0 \pmod{p}$, we have $d^{p-1} - 1 = 0 \pmod{p}$.

By LFT: $g^p - g = g(g^{p-1} - 1) = 0 \pmod{p}$.

By Prop. 2.3.5 $x \neq 0 \pmod{p} \Leftrightarrow a \neq 0 \pmod{p}$, i.e., $g \neq 0 \pmod{p}$ hence $g^{p-1} - 1 = 0 \pmod{p}$.

By $\varphi_x = g^p \in \mathbb{N}$ and according to Prop. 2.3.19 $p \mid (\varphi_x - 1)$, we have $p \mid (g^p - 1)$, that implies $p \mid (g - 1)$ according to Property 1.10.

2.3.23 $y \neq 0 \pmod{p} \Leftrightarrow \exists e, h \in \mathbb{Z}^+$ relatively prime: $b = eh$; $y = e^p \wedge \varphi_y = h^p$;
 besides $p \mid (e^{p-1} - 1) \wedge p \mid (h^{p-1} - 1) \wedge p \mid (h - 1)$.

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

2.3.24 $z \neq 0 \pmod{p} \Leftrightarrow \exists f, i \in \mathbb{Z}^+$ relatively prime: $c = fi$; $z = f^p \wedge \varphi_z = i^p$;
 besides $p \mid (f^{p-1} - 1) \wedge p \mid (i^{p-1} - 1) \wedge p \mid (i - 1)$.

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

2.3.25 $a - x = b - y = z - c = 0 \pmod{2p}$.

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:

$a + b - c = (c^p - c) - (a^p - a) - (b^p - b) = 0 \pmod{p}$ by Little Fermat's Theorem; hence:

$a + b - c = 0 \pmod{p}$; by Defs. 2.2.3 ÷ 2.2.5 we have $(a + b) - c = a - (c - b) = b - (c - a)$, thus:

$z - c = a - x = b - y = 0 \pmod{p}$.

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:

$z - c = 0 \pmod{2}$, therefore:

$z - c = a - x = b - y = 0 \pmod{2}$.

We may resume the above results as follows: $z - c = a - x = b - y = 0 \pmod{2p}$.

2.3.26 $x \neq 0 \pmod{p} \Leftrightarrow p \mid (a - d)$.

Proof. By Prop. 2.3.25 $p \mid (a - x)$ and according to LFT $p \mid (a^p - a)$, we have $p \mid (a^p - x)$.

By Prop. 2.3.22 $x = d^p$, hence $p \mid (a^p - d^p)$; by Property 1.10 we have $p \mid (a - d)$.

By Prop. 2.3.22 $a = dg$, we have $p \mid (dg - d)$, i.e., $p \mid d(g - 1)$.

Since $d \neq 0 \pmod{p}$, we have $p \mid (g - 1)$, confirming Prop. 2.3.22.

2.3.27 $y \neq 0 \pmod{p} \Leftrightarrow p \mid (b - e)$.

Proof. Analogously to Prop. 2.3.26.

2.3.28 $z \neq 0 \pmod{p} \Leftrightarrow p \mid (c - f)$.

Proof. Analogously to Prop. 2.3.26.

2.4 THEOREMS

2.4.1 $c^2=a^2+b^2 \Leftrightarrow a \vee b=0 \pmod{2} \wedge c \neq 0 \pmod{2}$.

Proof. In Pythagoras' primitive triple $a^2+b^2=c^2$ there are two odds and one even; anyway $a+b-c=0 \pmod{2}$, i.e., $z-c=0 \pmod{2}$.

By expanding $c=z-(z-c)$, we have:

$$\begin{aligned} c &= a+b-(z-c); \\ c^2 &= [a+b-(z-c)]^2; \\ c^2 &= a^2+b^2+2ab+(z-c)^2-2(a+b)(z-c); \\ c^2-(a^2+b^2) &= 2ab+(z-c)^2-2(a+b)(z-c); \\ 0 &= 2ab+(z-c)^2-2(a+b)(z-c); \\ \underbrace{2(a+b)(z-c)}_{=0 \pmod{2^2}} - \underbrace{(z-c)^2}_{=0 \pmod{2^2}} &= 2ab; \\ &= 0 \pmod{2^2} \end{aligned}$$

$$2ab=0 \pmod{2^2};$$

$$ab=0 \pmod{2};$$

$$a \vee b=0 \pmod{2}.$$

Since a, b, c are pairwise coprime: $c \neq 0 \pmod{2}$.

2.4.2 $c^3=a^3+b^3 \Leftrightarrow a \vee b \vee c=0 \pmod{3}$.

Proof. By Prop. 2.3.25, when $p=3$: $z-c=0 \pmod{3}$.

By expanding $c=z-(z-c)$, we have:

$$\begin{aligned} c &= a+b-(z-c); \\ c^3 &= [a+b-(z-c)]^3; \\ c^3 &= a^3+b^3+3a^2b+3ab^2+(z-c)^3-3(a+b)^2(z-c)-3(z-c)^2(a+b); \\ c^3-(a^3+b^3) &= 3abz+(z-c)^3-3z^2(z-c)-3(z-c)^2z; \\ 0 &= 3abz+(z-c)^3-3z^2(z-c)-3(z-c)^2z; \\ \underbrace{3z^2(z-c)}_{=0 \pmod{3^2}} + \underbrace{3(z-c)^2z}_{=0 \pmod{3^3}} - \underbrace{(z-c)^3}_{=0 \pmod{3^3}} &= 3abz; \\ &= 0 \pmod{3^2} \text{ according to Property 1.6.3} \end{aligned}$$

$$3abz=0 \pmod{3^2};$$

$$abz=0 \pmod{3};$$

$$a \vee b \vee z=0 \pmod{3}.$$

By Prop. 2.3.5, $3|z$ implies $3|c$, thus: $a \vee b \vee c=0 \pmod{3}$.

2.4.3 If $a, b, c \neq 0 \pmod{p}$ 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 $x, y, z \neq 0 \pmod{p}$ then $x=d^p$, $y=e^p$, $z=f^p$ according to Props. 2.3.22+2.3.24.

If $x=0 \pmod{p}$ then $y, z \neq 0 \pmod{p}$, i.e., $y=e^p$, $z=f^p$.

If $y=0 \pmod{p}$ then $x, z \neq 0 \pmod{p}$, i.e., $x=d^p$, $z=f^p$.

If $z=0 \pmod{p}$ then $x, y \neq 0 \pmod{p}$, i.e., $x=d^p$, $y=e^p$.

Therefore $x=d^p \wedge y=e^p \wedge z=f^p \vee x=d^p \wedge y=e^p \vee x=d^p \wedge z=f^p \vee y=e^p \wedge z=f^p$.

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 $a=0 \pmod{2}$ then $x=0 \pmod{2^p}$, according to Prop. 2.3.31.

If $b=0 \pmod{2}$ then $y=0 \pmod{2^p}$, according to Prop. 2.3.32.

If $c=0 \pmod{2}$ then $z=0 \pmod{2^p}$, according to Prop. 2.3.33.

Therefore $2^p|x \vee 2^p|y \vee 2^p|z$.

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 $x=0 \pmod{2^p}$ then $d=0 \pmod{2}$, according to Def. 2.2.6.

If $y=0 \pmod{2^p}$ then $e=0 \pmod{2}$, according to Def. 2.2.7.

If $z=0 \pmod{2^p}$ then $f=0 \pmod{2}$, according to Def. 2.2.8.

Therefore $2|d \vee 2|e \vee 2|f$.

2.4.7 If $a, b, c \neq 0 \pmod{p}$ then $c^p = a^p + b^p$ is $(f \cdot i)^p = (d \cdot g)^p + (e \cdot h)^p$; 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 $a = 0 \pmod{p}$ then $c^p = a^p + b^p$ is $(f \cdot i)^p = (p \cdot j)^p + (e \cdot h)^p$; 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 $b = 0 \pmod{p}$ then $c^p = a^p + b^p$ is $(f \cdot i)^p = (d \cdot g)^p + (p \cdot l)^p$; 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 $c = 0 \pmod{p}$ then $c^p = a^p + b^p$ is $(p \cdot m)^p = (d \cdot g)^p + (e \cdot h)^p$; 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) $(dg)^p + (eh)^p = (fi)^p \Leftrightarrow a, b, c \neq 0 \pmod{p}$, with d, e, f, g, h, i pairwise coprime, $d \geq 1$; besides $x = d^p$, $y = e^p$, $z = f^p$ with $2 \mid d \vee 2 \mid e \vee 2 \mid f$.
- II) $(pj)^p + (eh)^p = (fi)^p \Leftrightarrow a = 0 \pmod{p}$, with p, e, f, j, h, i pairwise coprime, $j > 1$; besides $y = e^p$, $z = f^p$ with $2 \mid j \vee 2 \mid e \vee 2 \mid f$.
- III) $(dg)^p + (pl)^p = (fi)^p \Leftrightarrow b = 0 \pmod{p}$, with d, p, f, g, l, i pairwise coprime, $l > 1$, $d \geq 1$; besides $x = d^p$, $z = f^p$ with $2 \mid d \vee 2 \mid l \vee 2 \mid f$.
- IV) $(dg)^p + (eh)^p = (pm)^p \Leftrightarrow c = 0 \pmod{p}$, with d, e, f, g, p, m pairwise coprime, $d \geq 1$; besides $x = d^p$, $y = e^p$ with $2 \mid d \vee 2 \mid e \vee 2 \mid m$.

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 $\neg \exists a, b, c, x, y, z \in \mathbb{N}$: $z - c = a - x = b - y$, 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 $a = 22038731 = 11 \cdot 13 \cdot 229 \cdot 673$; $b = 19945108 = 47 \cdot 2^2 \cdot 277 \cdot 383$; $c = 22869315 = 3^2 \cdot 5 \cdot 79 \cdot 7 \cdot 919$; $x = 2924207 = 11^3 \cdot 13^3$; $y = 830584 = 47^3 \cdot 2^3$; $z = 41983839 = 79 \cdot 3^{12}$.

The restriction $z - c = a - x = b - y$ becomes impossibility only when combined with the conditions $x \mid a^n$, $x \mid b^n$, $z \mid c^n$. 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 $z \neq 0 \pmod{p}$) or φ_z/p (if $z = 0 \pmod{p}$) 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 $y \neq 0 \pmod{p}$) or φ_y/p (if $y = 0 \pmod{p}$) 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 $x \neq 0 \pmod{p}$) or φ_x/p (if $x = 0 \pmod{p}$) are larger 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 $k \in \mathbb{Z}^+$ 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:

$$\text{IV) } s_1 = (r-q)/ku;$$

$$\text{V) } s_2 = t-kqu;$$

$$\text{VI) } s_3 = (u-v)/kq;$$

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

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

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

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

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

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

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

$$\varphi(k) = k^3u^2 - k(1+qut) + rq = 0.$$

$$\varphi(k) = k^3z - k(1+qut) + a = 0.$$

According to the *Rational Root Theorem*, the eventually integer solutions of the polynomial $\varphi(k)$ 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 $\varphi(k)=0$ admits exclusively fractional roots $k \notin \mathbb{N}$, in contradiction with the hypothesis $k \in \mathbb{Z}^+$.

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:

$$\varphi(k)=0 \Leftrightarrow k \notin \mathbb{N}, \text{ in contradiction with } k \in \mathbb{Z}^+.$$

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

$$\varphi(k) = a_n k^n + a_{n-1} k^{n-1} + \dots + a_2 k^2 + a_1 k + a_0 = 0;$$

the eventual roots $k \in \mathbb{N}$ 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 $\neg \exists a, b, c \in \mathbb{N}: c^p = a^p + b^p$, 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 $\neg \exists n \in \mathbb{N}, n > 2: c^n = a^n + b^n$, 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 $c^{7p} = a^{7p} + b^{7p}$ can be easily transformed into triples with prime p exponent $(c^7)^p = (a^7)^p + (b^7)^p$.

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

2.5.8 $\neg \exists n, A, B, C \in \mathbb{N}, n > 2: C^n = A^n + B^n$, 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 $m = \text{GCF}(A, B, C)$: $a = A/m$, $b = B/m$ and $c = C/m$.

2.5.9 $\exists A, B, C \in \mathbb{N}: C^2 = A^2 + B^2$, 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 $z-c=a-x=b-y$.

MULTIDIMENSIONAL EXTENSION OF THE COSINE LAW ON SYNCLASTIC SURFACES

3.1 Algebraic extension of the Cosine Law to superior powers.

Denote a, b, c the three sides of a flat triangle, being $a, b, c > 2$ unity of measure.

By triangular properties, we have $\forall n, k \in \mathbb{N}, 0 < k < 2n$:

$$\begin{aligned} & c-b < a < b+c \\ & (c-b)^{2n} < a^{2n} < (b+c)^{2n} \\ & c^{2n} + b^{2n} - \sum_k (-1)^k * C_{2n,k} * b^{2n-k} * c^k < a^{2n} < c^{2n} + b^{2n} - \sum_k C_{2n,k} * b^{2n-k} * c^k \end{aligned}$$

According to the binomial Properties 1.4.1 and 1.4.2:

$$3.1.1 \quad \forall n, k \in \mathbb{N}, 0 < k < 2n: 0 < \sum_k C_{2n,k} / (2n * 2^{2n-2}) < 1;$$

$$3.1.2 \quad \forall n, k \in \mathbb{N}, 0 < k < 2n: -1 < \sum_k (-1)^k * C_{2n,k} / (2n * 2^{2n-2}) < 0;$$

we have that in the above binomial expansion:

$$3.1.3 \quad 0 < \sum_k C_{2n,k} * b^{2n-k} * c^k / [2n * (bc)^{2n-1}] < \sum_k C_{2n,k} / (2n * 2^{2n-2}) < 1;$$

$$3.1.4 \quad -1 < \sum_k (-1)^k * C_{2n,k} / [2n * (2^{2n-2})] < \sum_k (-1)^k * C_{2n,k} * b^{2n-k} * c^k / [2n * (bc)^{2n-1}] < 0;$$

hence there exist two values, whose moduli are inferior to the unity, interpretable as cosines of two angles $\alpha_1 \in (0; \pi/2)$ and $\alpha_0 \in (\pi/2; \pi)$:

$$3.1.5 \quad \cos \alpha_1 = \sum_k C_{2n,k} * b^{2n-k} * c^k / [2n * (bc)^{2n-1}];$$

$$3.1.6 \quad \cos \alpha_0 = \sum_k (-1)^k * C_{2n,k} * b^{2n-k} * c^k / [2n * (bc)^{2n-1}];$$

therefore:

$$b^{2n} + c^{2n} - 2n * (bc)^{2n-1} * \cos \alpha_0 < a^{2n} < b^{2n} + c^{2n} - 2n * (bc)^{2n-1} * \cos \alpha_1$$

By comparing, there is an angle $\alpha_{2n} \in (\alpha_0, \alpha_1)$ such that: $a^{2n} = b^{2n} + c^{2n} - 2n * (bc)^{2n-1} * \cos \alpha_{2n}$.

Since a is any side, the Cosine Law is extendable to any $2n$ indexes:

$$\begin{aligned} 3.1.7 \quad \forall a, b, c, n \in \mathbb{N}, a, b, c > 2, \exists \alpha_{2n}, \beta_{2n}, \gamma_{2n} \in [0; \pi]: & a^{2n} = b^{2n} + c^{2n} - 2n * (bc)^{2n-1} * \cos \alpha_{2n}; \\ & b^{2n} = a^{2n} + c^{2n} - 2n * (ca)^{2n-1} * \cos \beta_{2n}; \\ & c^{2n} = a^{2n} + b^{2n} - 2n * (ab)^{2n-1} * \cos \gamma_{2n}. \end{aligned}$$

3.2 Geometrical extension of the Cosine Law on synclastic surfaces.

The triple of angles deriving from the $2n$ -dimensional extension of the Cosine Law:

$$3.2.1 \quad \alpha_{2n} = \arccos\{(b^{2n} + c^{2n} - a^{2n}) / [2n * (cb)^{2n-1}]\};$$

$$3.2.2 \quad \beta_{2n} = \arccos\{(a^{2n} + c^{2n} - b^{2n}) / [2n * (ca)^{2n-1}]\};$$

$$3.2.3 \quad \gamma_{2n} = \arccos\{(a^{2n} + b^{2n} - c^{2n}) / [2n * (ab)^{2n-1}]\};$$

belongs to triangles Δ_{2n} with same sides $a, b, c > 2$ but variable curvatures $K(\Delta_{2n}) \geq 0$.

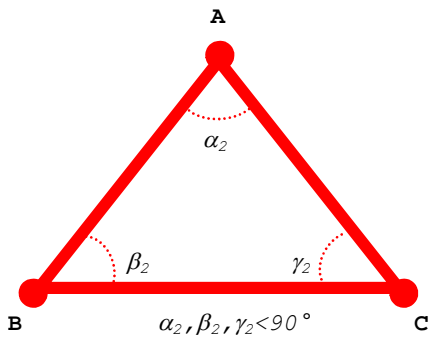
3.2.4 If $n=1$ the triangle Δ_2 is flat, i.e., at null curvature $K(\Delta_2) = 0$.

3.2.5 If $n > 1$ the triangle Δ_{2n} is geodetic, i.e., at positive curvature $K(\Delta_{2n}) > 0$.

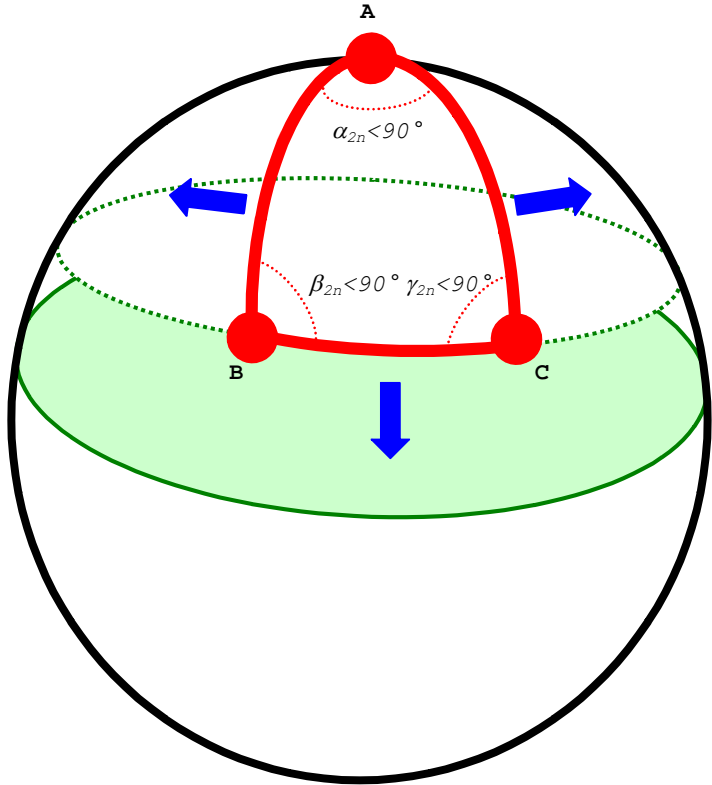
3.2.6 If $n \rightarrow \infty$ the triangle Δ_∞ is degenerate, i.e., at curvature $K(\Delta_\infty) = \pi/2$, with $\alpha_\infty = \beta_\infty = \gamma_\infty = 90^\circ$.

Therefore, while n grows from 1 to ∞ there is the passage from a flat surface, i.e., in a null curvature space $K(\Delta_2) = 0$, to a synclastic surface, i.e., in a positive curvature space $K(\Delta_{2n}) > 0$.

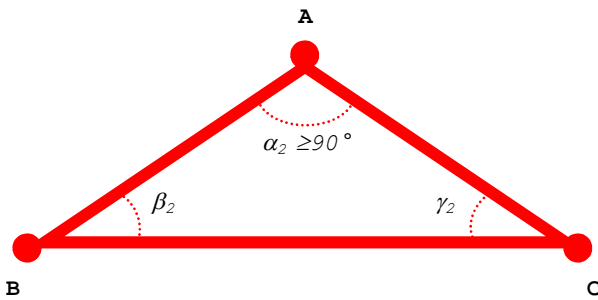
3.3 Multidimensional increase from: $\alpha_2, \beta_2, \gamma_2 < 90^\circ$.



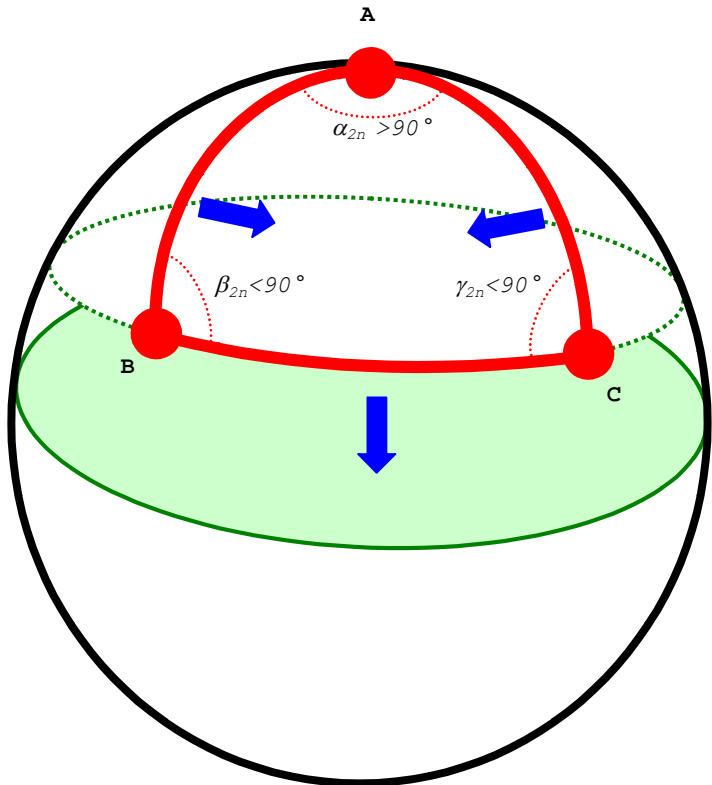
$$\forall n \in \mathbb{N}, n > 1: \begin{aligned} \alpha_2 &< \alpha_{2n-1} < \alpha_{2n} < 90^\circ \\ \beta_2 &< \beta_{2n-1} < \beta_{2n} < 90^\circ \\ \gamma_2 &< \gamma_{2n-1} < \gamma_{2n} < 90^\circ \end{aligned}$$



3.4 Multidimensional increase from: $\alpha_2 \geq 90^\circ$.

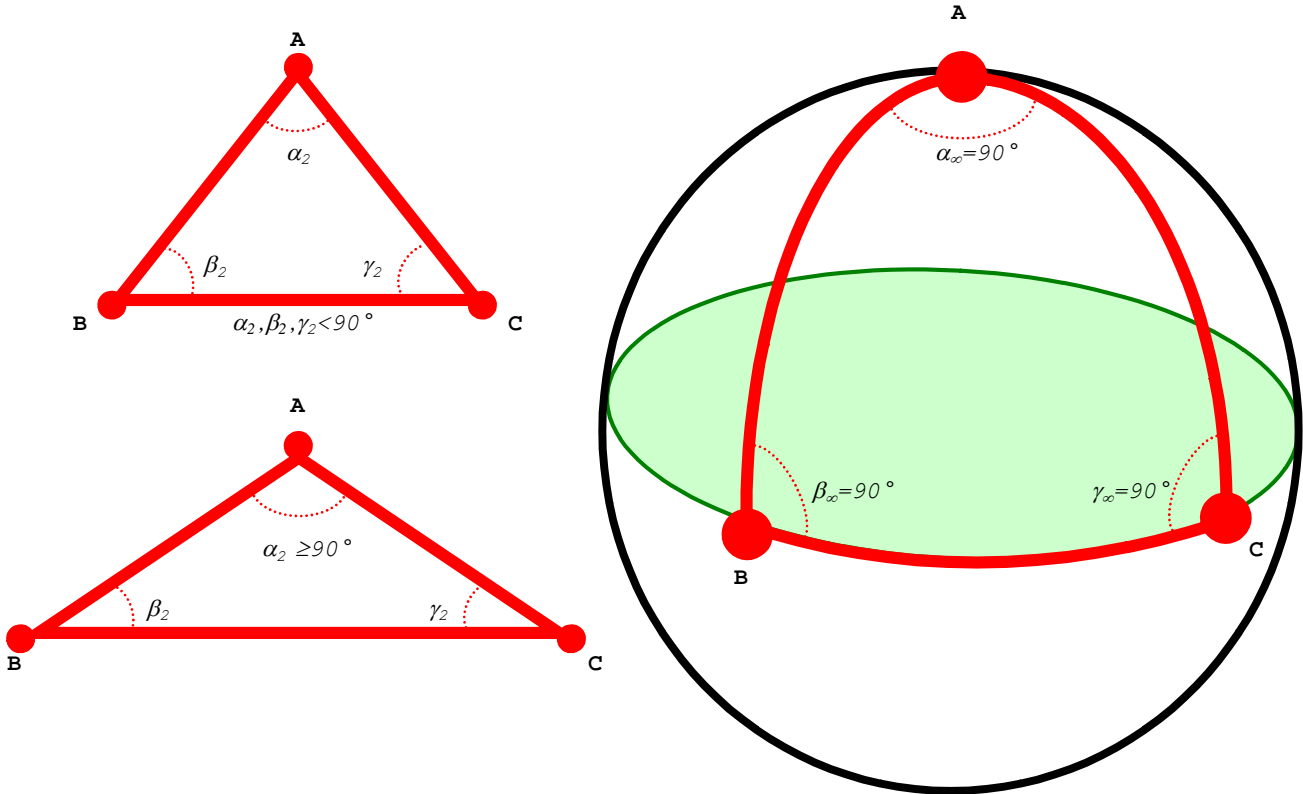


$$\forall n \in \mathbb{N}, n > 1: \begin{aligned} 90^\circ &\leq \alpha_{2n} < \alpha_{2n-1} < \alpha_2 \\ \beta_2 &< \beta_{2n-1} < \beta_{2n} < 90^\circ \\ \gamma_2 &< \gamma_{2n-1} < \gamma_{2n} < 90^\circ \end{aligned}$$



3.5 **Degenerate triangle Δ_∞ .**

Any flat triangle Δ_2 degenerates in a triangle Δ_∞ whose inner angles are $\alpha_\infty=\beta_\infty=\gamma_\infty=90^\circ$ and whose curvature is $K(\Delta_\infty)=\alpha+\beta+\gamma-\pi=\pi/2$.



3.6 **Conclusions.**

2-dimensional triangle:	2n-dimensional triangle:	∞ -dimensional triangle:
Bidimensional curvature: $K(\Delta_2)=\alpha+\beta+\gamma-\pi=0$ (flat surface)	2n-dimensionale curvature: $K(\Delta_2)=\alpha+\beta+\gamma-\pi>0$ (synclastic surface)	∞ -dimensional curvature: $K(\Delta_\infty)=\alpha+\beta+\gamma-\pi=\pi/2$ (synclastic surface)
Bidimensional Cosine Law: $a^2=b^2+c^2-2cb*\cos\alpha_2$ $b^2=a^2+c^2-2ca*\cos\beta_2$ $c^2=a^2+b^2-2ab*\cos\gamma_2$	2n-dimensional Cosine Law: $a^{2n}=b^{2n}+c^{2n}-2n[(cb)^{2n-1}]*\cos\alpha_{2n}$ $b^{2n}=a^{2n}+c^{2n}-2n[(ca)^{2n-1}]*\cos\beta_{2n}$ $c^{2n}=a^{2n}+b^{2n}-2n[(ab)^{2n-1}]*\cos\gamma_{2n}$	∞ -dimensional Cosine Law: $a^\infty=b^\infty+c^\infty$ $b^\infty=a^\infty+c^\infty$ $c^\infty=a^\infty+b^\infty$

AN OLD ELEMENTARY ATTEMPT AT PROVING FERMAT'S LAST THEOREM*

1 INTRODUCTION

MSC2000: 11D41.

Keywords: Fermat, elementary, reductio ad absurdum, coprime, binomial expansion.

Abstract: Elementary *reductio ad absurdum* of FLT based upon some coprimes' properties and on the following binomial expansion:

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

$$\text{With } n_k = [1 + (-1)^{k+2} C_{p-1, k+1}] / p + (-1)^{k+1} C_{p-3, k} + (-1)^k n_1 C_{p-5, k-1} + (-1)^{k-1} n_2 C_{p-7, k-2} + \dots + n_{k-1} C_{k+1, 1}.$$

The negation of Fermat triples derives from the impossibility of corresponding primitive triples.

2 DEFINITIONS

2.1 Let $c^p = a^p + b^p$ be a Fermat's primitive equation with $a, b, c \in \mathbb{N}$ pairwise coprime and $p > 2$ prime.

2.2 Let $x = c - b$, by construction x, b, c are pairwise coprime and $0 < x < a$; denote $d = x^{1/p}$.

2.3 Let $y = c - a$, by construction y, a, c are pairwise coprime and $0 < y < b$; denote $e = y^{1/p}$.

2.4 Let $z = a + b$, by construction z, a, b are pairwise coprime and $b < c < z$; denote $f = z^{1/p}$.

2.5 Let $\varphi_x = a^p / x$; denote $g = \varphi_x^{1/p}$.

2.6 Let $\varphi_y = b^p / y$; denote $h = \varphi_y^{1/p}$.

2.7 Let $\varphi_z = c^p / z$; denote $i = \varphi_z^{1/p}$.

2.8 $k \in [1, (p-5)/2] \subset \mathbb{Z}$: $n_k = [1 + (-1)^{k+2} C_{p-1, k+1}] / p + (-1)^{k+1} C_{p-3, k} + (-1)^k n_1 C_{p-5, k-1} + (-1)^{k-1} n_2 C_{p-7, k-2} + \dots + n_{k-1} C_{k+1, 1}$.
Examples. Let us expand the above iterative formula in detail, as follows:

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

$$n_2 = (1 + C_{p-1, 3}) / p - C_{p-3, 2} + n_1 C_{p-5, 1}$$

$$n_3 = (1 - C_{p-1, 4}) / p + C_{p-3, 3} - n_1 C_{p-5, 2} + n_2 C_{p-7, 1}$$

...

$$j \in [3, (p-5)/2] \subset \mathbb{Z}: n_j = [1 + (-1)^{j+2} C_{p-1, j+1}] / p + (-1)^{j+1} C_{p-3, j} + (-1)^j n_1 C_{p-5, j-1} + (-1)^{j-1} n_2 C_{p-7, j-2} + \dots + n_{j-1} C_{j+1, 1}$$

...

$$n_{(p-5)/2} = [1 + (-1)^{(p-1)/2} C_{p-1, (p-3)/2}] / p + (-1)^{(p-3)/2} C_{p-3, (p-5)/2} + (-1)^{(p-5)/2} n_1 C_{p-5, (p-7)/2} + (-1)^{(p-7)/2} n_2 C_{p-7, (p-9)/2} + \dots + n_{(p-7)/2} C_{(p-3)/2, 1}.$$

3 PROPOSITIONS

3.1 $\varphi_x, \varphi_y, \varphi_z \in \mathbb{N}$.

Proof. According to Definitions 2.5, 2.6, 2.7 and since $a^p, b^p, c^p \in \mathbb{N}$, it suffices that x is factor of a^p , y of b^p and z of c^p . By the binomial coefficients' property $C_{p, 1} = p$:

$$\varphi^{p-1}(b) = c^p - c^p = (b+x)^p - (b^p + a^p) = pxb^{p-1} + \dots + x^p - a^p = 0;$$

therefore $(a^p - x^p) / px \in \mathbb{Z}$, i.e., $x | (a^p - x^p)$; hence $x | a^p$.

Analogously we find $y | b^p$ and $z | c^p$.

3.2 $a^p - c^p - b^p = x \{ x^{p-1} + pbc [x^{p-3} + bc [n_1 x^{p-5} + bc [n_2 x^{p-7} + \dots + bc (n_{(p-5)/2} x^2 + bc) \dots]] \}$.

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

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

$$+ pcb (c-b)^{p-2} +$$

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

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

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

+ ... +

(*) From an algebraic research presented in *New Ideas on Number Theory* (Carta e Penna, Turin, 2006) by Mr. Enzo Bonacci (Ph.D. Honoris Causa in Theoretical Physics by Cosmopolitan University).

$$\begin{aligned}
& + (cb)^{(p-3)/2} (c-b)^3 \{ 1 + (-1)^{(p-1)/2} C_{p-1, (p-3)/2} + \\
& \quad + (-1)^{(p-3)/2} p C_{p-3, (p-5)/2} + \\
& \quad + (-1)^{(p-5)/2} (1 - C_{p-1, 2} + p C_{p-3, 1}) C_{p-5, (p-7)/2} + \\
& \quad + (-1)^{(p-7)/2} [1 + C_{p-1, 3} - p C_{p-3, 2} + (1 - C_{p-1, 2} + p C_{p-3, 1}) C_{p-5, 1}] C_{p-7, (p-9)/2} + \\
& \quad + \dots + \\
& \quad + [1 + (-1)^{(p-3)/2} C_{p-1, (p-5)/2} + p (-1)^{(p-5)/2} C_{p-3, (p-7)/2} + p (-1)^{(p-7)/2} n_1 C_{p-5, (p-9)/2} + \\
& \quad + \dots + p n_{(p-9)/2} C_{(p-5)/2, 1}] C_{(p-3)/2, 1} \} + \\
& + (cb)^{(p-1)/2} (c-b) p.
\end{aligned}$$

According to Definitions 2.2 and 2.8,

$$\begin{aligned}
c^p - b^p &= x^p + \\
& + bcx^{p-2} p + \\
& + (bc)^2 x^{p-4} p n_1 + \\
& + (bc)^3 x^{p-6} (1 + C_{p-1, 3} - p C_{p-3, 2} + p n_1 C_{p-5, 1}) + \\
& + (bc)^4 x^{p-8} (1 - C_{p-1, 4} + p C_{p-3, 3} - p n_1 C_{p-5, 2} + p n_2 C_{p-7, 1}) + \\
& + \dots + \\
& + (bc)^{(p-3)/2} x^3 [1 + (-1)^{(p-1)/2} C_{p-1, (p-3)/2} + (-1)^{(p-3)/2} p C_{p-3, (p-5)/2} + (-1)^{(p-5)/2} p n_1 C_{p-5, (p-7)/2} + (-1)^{(p-7)/2} p n_2 C_{p-7, (p-9)/2} + \\
& \quad + \dots + p n_{(p-7)/2} C_{(p-3)/2, 1}] + \\
& + (bc)^{(p-1)/2} x p.
\end{aligned}$$

Further,

$$\begin{aligned}
c^p - b^p &= x^p + \\
& + pbcx^{p-2} + \\
& + p n_1 (bc)^2 x^{p-4} + \\
& + p n_2 (bc)^3 x^{p-6} + \\
& + p n_3 (bc)^4 x^{p-8} + \\
& + \dots + \\
& + p n_{(p-5)/2} (bc)^{(p-3)/2} x^3 + \\
& + p (bc)^{(p-1)/2} x.
\end{aligned}$$

Therefore,

$$\begin{aligned}
c^p - b^p &= x^p + pbcx^{p-2} + p n_1 (bc)^2 x^{p-4} + p n_2 (bc)^3 x^{p-6} + \dots + p n_{(p-5)/2} (bc)^{(p-3)/2} x^3 + p (bc)^{(p-1)/2} x = \\
& = x [x^{p-1} + pbcx^{p-3} + p n_1 (bc)^2 x^{p-5} + p n_2 (bc)^3 x^{p-7} + \dots + p n_{(p-5)/2} (bc)^{(p-5)/2} x^2 + p (bc)^{(p-3)/2}] = \\
& = x \{ x^{p-1} + pbc [x^{p-3} + n_1 bcx^{p-5} + n_2 (bc)^2 x^{p-7} + \dots + n_{(p-5)/2} (bc)^{(p-7)/2} x^2 + (bc)^{(p-5)/2}] \} = \\
& = x \{ x^{p-1} + pbc [x^{p-3} + bc [n_1 x^{p-5} + n_2 bcx^{p-7} + \dots + n_{(p-5)/2} (bc)^{(p-9)/2} x^2 + (bc)^{(p-7)/2}]] \} = \\
& = x \{ x^{p-1} + pbc [x^{p-3} + bc [n_1 x^{p-5} + bc [n_2 x^{p-7} + \dots + n_{(p-5)/2} (bc)^{(p-11)/2} x^2 + (bc)^{(p-9)/2}]]] \} = \\
& = \dots = \\
& = x \{ x^{p-1} + pbc [x^{p-3} + bc [n_1 x^{p-5} + bc [n_2 x^{p-7} + \dots + bc (n_{(p-5)/2} x^2 + bc) \dots]]] \}.
\end{aligned}$$

3.3 $\varphi_x = a^p/x = x^{p-1} + pbc[x^{p-3} + bc[n_1 x^{p-5} + bc[n_2 x^{p-7} + \dots + bc(n_{(p-5)/2} x^2 + bc) \dots]]]$.

Proof. By Definitions 2.2 and 2.5 and according to Proposition 3.2.

3.4 **x and φ_x are not coprime if and only if $p = \text{GCF}(x, \varphi_x)$; then $\varphi_x \neq 0 \pmod{p^2}$.**

Proof. By Definitions 2.2 and 2.5 and according to Proposition 3.3.

3.5 **If x and φ_x are coprime, then $d, g \in \mathbb{N}$: d and g are relatively prime factors of a .**

Proof. According to Definition 2.5: $a^p = x \varphi_x$. Since each prime factor of a^p must be at least "p-indexed", there exist $k \in \mathbb{N}$ primes $p_1, p_2, p_3, \dots, p_{k-1}, p_k$ and relative indexes $n_1, n_2, n_3, \dots, n_{k-1}, n_k$, such that: $a^p = (p_1^{n_1})^p \cdot (p_2^{n_2})^p \cdot (p_3^{n_3})^p \cdot \dots \cdot (p_{k-1}^{n_{k-1}})^p \cdot (p_k^{n_k})^p$.

By hypothesis, x and φ_x can not share any factor, so some primes divide only x , for example: p_1, p_2, p_3, \dots , while all the others divide only φ_x , for the same example: $\dots p_{k-1}, p_k$. Therefore $x = (p_1^{n_1})^p \cdot (p_2^{n_2})^p \cdot (p_3^{n_3})^p \cdot \dots$ while $\varphi_x = \dots (p_{k-1}^{n_{k-1}})^p \cdot (p_k^{n_k})^p$.

Hence $x = (p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \dots)^p = d^p$, i.e., $d = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \dots \in \mathbb{N}$;

and $\varphi_x = (\dots p_{k-1}^{n_{k-1}} \cdot p_k^{n_k})^p = g^p$, i.e., $g = \dots p_{k-1}^{n_{k-1}} \cdot p_k^{n_k} \in \mathbb{N}$.

According to Definitions 2.2 and 2.5: $d^p | a$ and $g^p | a$, i.e., $d | a$ and $g | a$.

Since $x = d^p$ and $\varphi_x = g^p$ are coprime by hypothesis, then d and g are relatively prime as well.

3.6 $b^p = c^p - a^p = y \{ y^{p-1} + pac[y^{p-3} + ac[n_1 y^{p-5} + ac[n_2 y^{p-7} + \dots + ac(n_{(p-5)/2} y^2 + ac) \dots]]] \}$.

Proof. Analogously to Prop. 3.2, after substituting x by y and b by a .

3.7 $\varphi_y = b^p/y = y^{p-1} + pac[y^{p-3} + ac[n_1 y^{p-5} + ac[n_2 y^{p-7} + \dots + ac(n_{(p-5)/2} y^2 + ac) \dots]]]$.

Proof. By Defs. 2.3, 2.6 and according to Prop. 3.6.

3.8 **y and φ_y are not coprime if and only if $p = \text{GCF}(y, \varphi_y)$; then $\varphi_y \neq 0 \pmod{p^2}$.**

Proof. By Defs. 2.3, 2.6 and according to Prop. 3.7.

- 3.9** *If y and φ_y are coprime, then $e, h \in \mathbb{N}$: h and e are relatively prime factors of b .*
Proof. Analogously to Prop. 3.5, after substituting x by y , b by a , Def. 2.2 by 2.3 and 2.5 by 2.6.
- 3.10** $c^p = a^p + b^p = z \{ z^{p-1} - pab [z^{p-3} - ab [n_1 z^{p-5} - ab [n_2 z^{p-7} + \dots - ab [n_{(p-5)/2} z^2 - ab] \dots]]] \}$.
Proof. Analogously to Prop. 3.2, after substituting x by z , a by c , "+" by "-" and vice versa.
- 3.11** $\varphi_z = c^p / z = z^{p-1} - pab [z^{p-3} - ab [n_1 z^{p-5} - ab [n_2 z^{p-7} + \dots - ab [n_{(p-5)/2} z^2 - ab] \dots]]]$.
Proof. By Defs. 2.4, 2.7 and according to Prop. 3.10.
- 3.12** z and φ_z are not coprime if and only if $p = \text{GCF}(z, \varphi_z)$; then $\varphi_z \neq 0 \pmod{p^2}$.
Proof. By Defs. 2.4, 2.7 and according to Prop. 3.11.
- 3.13** *If z and φ_z are coprime, then $f, i \in \mathbb{N}$: f and i are relatively prime factors of c .*
Proof. Analogously to Prop. 3.5, after substituting x by z , a by c , Def. 2.2 by 2.4 and 2.5 by 2.7.

4 THEOREMS

- 4.1** φ_x, φ_y and φ_z are pairwise relatively prime.
Proof. According to Def. 2.1: a, b and c are pairwise coprime, then a^p, b^p and c^p are pairwise coprime. By Defs. 2.5, 2.6 and 2.7: $\varphi_x | a^p, \varphi_y | b^p$ and $\varphi_z | c^p$, then φ_x, φ_y and φ_z are pairwise coprime.
- 4.2** $\varphi_x > a^{p-1}$ and $\varphi_y > b^{p-1}$.
Proof. According to Def. 2.2: $a > x$, then $\varphi_x = a^p / x > a^p / a = a^{p-1}$.
 According to Def. 2.3: $b > y$, then $\varphi_y = b^p / y > b^p / b = b^{p-1}$.
- 4.3** *There are at least two pairs of coprimes out of the following three:*
 $(x, \varphi_x), (y, \varphi_y), (z, \varphi_z)$.
Proof. According to Props. 3.4, 3.8 and 3.12 if a pair doesn't consist of coprimes then p divides it.
 By Theorem 4.1, if $p | \varphi_x$ then $\varphi_y \neq 0 \pmod{p}$ and $\varphi_z \neq 0 \pmod{p}$; therefore by Prop. 3.8 (y, φ_y) is a pair of coprimes, by Prop. 3.12 (z, φ_z) is a pair of coprimes.
 By Theorem 4.1, if $p | \varphi_y$ then $\varphi_x \neq 0 \pmod{p}$ and $\varphi_z \neq 0 \pmod{p}$; therefore by Prop. 3.4 (x, φ_x) is a pair of coprimes, by Prop. 3.12 (z, φ_z) is a pair of coprimes.
 By Theorem 4.1, if $p | \varphi_z$ then $\varphi_x \neq 0 \pmod{p}$ and $\varphi_y \neq 0 \pmod{p}$; therefore by Prop. 3.4 (x, φ_x) is a pair of coprimes, by Prop. 3.8 (y, φ_y) is a pair of coprimes.
- 4.4** $2a - x = z - y, 2b - y = z - x, 2c - z = x + y$.
Proof. By Definitions 2.5, 2.6, 2.7:
 $2a = (c - b) - (c - a) + (a + b)$, i.e., $2a - x = z - y$.
 $2b = (c - a) - (c - b) + (a + b)$, i.e., $2b - y = z - x$.
 $2c = (c - b) + (c - a) + (a + b)$, i.e., $2c - z = x + y$.
- 4.5** *If $c \neq 0 \pmod{p}$ then $c | z$; if $a \neq 0 \pmod{p}$ then $a | x$; if $b \neq 0 \pmod{p}$ then $b | y$.*
Proof. By Prop. 3.2, $a^p = x^p + xpbc [x^{p-3} + bc [n_1 x^{p-5} + bc [n_2 x^{p-7} + \dots + bc [n_{(p-5)/2} x^2 + bc] \dots]]]$; hence:
4.5.1 $(a^p - x^p) = 0 \pmod{b} \wedge (a^p - x^p) = 0 \pmod{c}$.
 By Prop. 3.6, $b^p = y^p + ypac [y^{p-3} + ac [n_1 y^{p-5} + ac [n_2 y^{p-7} + \dots + ac [n_{(p-5)/2} y^2 + ac] \dots]]]$; hence:
4.5.2 $(b^p - y^p) = 0 \pmod{a} \wedge (b^p - y^p) = 0 \pmod{c}$.
 By Prop. 3.10, $c^p = z^p - zpab [z^{p-3} - ab [n_1 z^{p-5} - ab [n_2 z^{p-7} + \dots - ab [n_{(p-5)/2} z^2 - ab] \dots]]]$; hence:
4.5.3 $(z^p - c^p) = 0 \pmod{a} \wedge (z^p - c^p) = 0 \pmod{b}$.
 By 4.5.1+4.5.2:
4.5.4 $(a^p + b^p) - (x^p + y^p) = 0 \pmod{c}$.
 By 4.5.3-4.5.2:
4.5.5 $(z^p - y^p) - (c^p - b^p) = 0 \pmod{a}$.
 By 4.5.3-4.5.1:
4.5.6 $(z^p - x^p) - (c^p - a^p) = 0 \pmod{b}$.
 Since $a^p + b^p = 0 \pmod{c}$, by 4.5.4:
4.5.7 $x^p + y^p = 0 \pmod{c}$.
 Since $c^p - b^p = 0 \pmod{a}$, by 4.5.5:
4.5.8 $z^p - y^p = 0 \pmod{a}$.

Since $c^p - a^p = 0 \pmod{b}$, by 4.5.6:

4.5.9 $z^p - x^p = 0 \pmod{b}$.

By Props. 3.11 and 3.13 and by Theorem 4.4: if $c \neq 0 \pmod{p}$ then $(x+y) \neq 0 \pmod{p}$; hence:

4.5.10 If $c \neq 0 \pmod{p}$, then $(x+y)$ is coprime to:

$$\{(x+y)^{p-1} - pxy[(x+y)^{p-3} - xy[n_1(x+y)^{p-5} + \dots - xy[n_{(p-5)/2}(x+y)^2 - xy] \dots]]\}.$$

By Props. 3.3 and 3.5 and by Theorem 4.4: if $a \neq 0 \pmod{p}$ then $(z-y) \neq 0 \pmod{p}$; hence:

4.5.11 If $a \neq 0 \pmod{p}$, then $(z-y)$ is coprime to:

$$\{(z-y)^{p-1} + pzy[(z-y)^{p-3} + zy[n_1(z-y)^{p-5} + \dots + zy[n_{(p-5)/2}(z-y)^2 + zy] \dots]]\}.$$

By Props. 3.7 and 3.9 and by Theorem 4.4: if $b \neq 0 \pmod{p}$ then $(z-x) \neq 0 \pmod{p}$; hence:

4.5.12 If $b \neq 0 \pmod{p}$, then $(z-x)$ is coprime to:

$$\{(z-x)^{p-1} + pzx[(z-x)^{p-3} + zx[n_1(z-x)^{p-5} + \dots + zx[n_{(p-5)/2}(z-x)^2 + zx] \dots]]\}.$$

By Theorem 4.4: $2c - z = x + y$ and since $z = f^p$ and $c = fi$, being $GCF(f, i) = 1$, according to Props. 3.12 e 3.13, then: $(x+y) = f(2i - f^{p-1}) = fr$.

By $2i - f^{p-1} = r$:

4.5.A If i is even then r is odd without any factor greater than one in common with both f and i . In fact, if $r, f = 0 \pmod{q}$, being $q > 2$, then $2i = r + f^{p-1} = 0 \pmod{q}$, i.e., $i = 0 \pmod{q}$ inconsistent with i and f coprime. If $r, i = 0 \pmod{q}$, $q > 2$, then $2i - r = f^{p-1} = 0 \pmod{q}$, i.e., f is not coprime to q then to i , inconsistent with Prop. 3.13.

Analogously to 4.5.A:

4.5.B If f is even then r is even without any odd factor greater than one in common with both f and i .

As a *reductio ad absurdum* let us assume:

$(x+y)^{p-1} - pxy[(x+y)^{p-3} - xy[n_1(x+y)^{p-5} + \dots - xy[n_{(p-5)/2}(x+y)^2 - xy] \dots]]$ not to be coprime to c .

According to 4.5.7, by substituting $(x+y) = fr$:

$x^p + y^p = (fr) \{(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots]\} = 0 \pmod{c}$, since $c = fi$:

$(fr) \{(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots]\} = 0 \pmod{fi}$.

If i is even then r is coprime to f and i , according to 4.5.A:

$(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots] = 0 \pmod{fi}$, hence:

$(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots] = is$, being s, r and p pairwise coprime; therefore:

$f^{p-1} r^{p-1} - is = 0 \pmod{p}$, i.e., $\exists u \in \mathbb{N}$:

4.5.C $f^{p-1} r^{p-1} - is = 0 \pmod{p^u}$.

By Prop. 4.10: $c^p = a^p + b^p = f^p \{(f^p)^{p-1} - pab[(f^p)^{p-3} + \dots - ab[n_{(p-5)/2}(f^p)^2 - ab] \dots]\} = f^p i^p$,

i.e., $(f^p)^{p-1} - pab[(f^p)^{p-3} + \dots - ab[n_{(p-5)/2}(f^p)^2 - ab] \dots] = i^p$, then:

$(f^{p-1})^p - i^p = 0 \pmod{p}$, therefore:

$(f^{p-1})^p - i^p = (f^{p-1} - i) \{(f^{p-1} - i)^{p-1} + p f^{p-1} i [(f^{p-1} - i)^{p-3} + \dots + f^{p-1} i [n_{(p-5)/2} (f^{p-1} - i)^2 + f^{p-1} i] \dots]\} = 0 \pmod{p}$, hence:

$f^{p-1} - i = 0 \pmod{p}$, i.e., $\exists z \in \mathbb{N}$:

4.5.D $f^{p-1} - i = 0 \pmod{p^z}$.

By 4.5.D and since $f^{p-1} = 2i - r$:

4.5.E $i - r = 0 \pmod{p^z}$.

According to 4.5.E, by squaring:

4.5.F $(i-r)^2 = 0 \pmod{p^{2z}}$.

According to 4.5.E, by multiplying for r^{p-2} coprime to p :

4.5.G $r^{p-2} (i-r) = 0 \pmod{p^z}$.

By 4.5.C e 4.5.D: $r^{p-1} - s = 0 \pmod{p}$, i.e., $\exists v = \text{MIN}(z, u)$:

4.5.H $r^{p-1} - s = 0 \pmod{p^v}$.

By 4.5.G. e 4.5.H: $r^{p-2} i - s = 0 \pmod{p}$, i.e., $\exists w = \text{MIN}(v, z)$:

4.5.I $r^{p-2} i - s = 0 \pmod{p^w}$.

According to 4.5.I, by multiplying for i , coprime to p as factor of c :

4.5.J $i^2 r^{p-2} - is = 0 \pmod{p^w}$.

By 4.5.C e 4.5.J: $r^{p-2} (i^2 - f^{p-1} r) = 0 \pmod{p}$, i.e., since r and p are coprime $\exists t = \text{MIN}(u, w)$:

4.5.K $i^2 - f^{p-1} r = 0 \pmod{p^t}$.

By 4.5.K, since $f^{p-1} = 2i - r$:

4.5.L $(i-r)^2 = 0 \pmod{p^t}$.

4.5.L is inconsistent with 4.5.F requiring an index $t = 2z$ while $t = \text{MIN}(u, \text{MIN}(\text{MIN}(z, u), z)) \leq z$. Vice versa, if f is even then r is still coprime to i but shares only the factor "2" with f , by 4.5.B, let us assume that:

$\{(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots]\}$ is not coprime to (fr) only by factor 2.

If f is even then c is even as well, therefore a and b are odd (a, b, c is a primitive triple pairwise coprime by hypothesis).

Therefore $x = c - b$ and $y = c - a$ are both odd, hence:

$\{(fr)^{p-1} - pxy[(fr)^{p-3} + \dots - xy[n_{(p-5)/2}(fr)^2 - xy] \dots]\}$.

Consequently $\{(fr)^{p-1}-pxy[(fr)^{p-3}+ \dots -xy[n_{(p-5)/2}(fr)^2-xy] \dots]\}$ is anyway coprime to (fr) , which means:

4.5.13 $\{(x+y)^{p-1}-pxy[(x+y)^{p-3}-xy[n_1(x+y)^{p-5}+ \dots -xy[n_{(p-5)/2}(x+y)^2-xy] \dots]]\}$ is coprime to c .

By 4.5.7, 4.5.10 and 4.5.13:

4.5.14 If $c \neq 0 \pmod{p}$ then $x+y=0 \pmod{c}$.

Analogously to 4.5.13:

4.5.15 $\{(z-y)^{p-1}+pzy[(z-y)^{p-3}+zy[n_1(z-y)^{p-5}+ \dots +zy[n_{(p-5)/2}(z-y)^2+zy] \dots]]\}$ is coprime to a .

By 4.5.8, 4.5.11 and 4.5.15:

4.5.16 If $a \neq 0 \pmod{p}$ then $z-y=0 \pmod{a}$.

Analogously to 4.5.13:

4.5.17 $\{(z-x)^{p-1}+pzx[(z-x)^{p-3}+zx[n_1(z-x)^{p-5}+ \dots +zx[n_{(p-5)/2}(z-x)^2+zx] \dots]]\}$ is coprime to b .

By 4.5.9, 4.5.12 and 4.5.17:

4.5.18 If $b \neq 0 \pmod{p}$ then $z-x=0 \pmod{b}$.

By Theorem 4.4: $2c-z=x+y$ and by 4.5.14:

4.5.19 If $c \neq 0 \pmod{p}$ then $z=0 \pmod{c}$.

By Theorem 4.4: $2a-x=z-y$ and by 4.5.16:

4.5.20 If $a \neq 0 \pmod{p}$ then $x=0 \pmod{a}$.

By Theorem 4.4: $2b-y=z-x$ and by 4.5.18:

4.5.21 If $b \neq 0 \pmod{p}$ then $y=0 \pmod{b}$.

4.6 **Theorem 4.5 is inconsistent with Theorem 4.2.**

Proof. By Theorem 4.3 there are at least two pairs of coprimes out of the following three: (x, φ_x) , (y, φ_y) , (z, φ_z) ; by Props. 3.4, 3.5, 3.8, 3.9, 3.12 and 3.13 it means that there is at least a pair of numbers not divisible by p out of: a, b, c .

Necessarily: $a \neq 0 \pmod{p} \vee b \neq 0 \pmod{p}$.

According to Theorem 4.5: if $a \neq 0 \pmod{p}$, then $x=0 \pmod{a}$.

Since φ_x is coprime to x and a is a factor of x then φ_x is coprime to a .

By Prop. 3.3: $a^p=0 \pmod{\varphi_x}$, but φ_x is coprime to a^p , then $\varphi_x=1$, inconsistent with Theorem 4.2. Analogously if $b \neq 0 \pmod{p}$ then $\varphi_y=1$, inconsistent with Theorem 4.2.

5 COROLLARIES

5.1 $\neg \exists a, b, c \in \mathbb{N}: c^p = a^p + b^p$,

i.e., no Fermat primitive triple with any prime index $p > 2$.

Proof. By Theorem 4.6, the hypothesis of a valid triple $c^p = a^p + b^p$ generates an inconsistency.

5.2 $\neg \exists n \in \mathbb{N}, n > 2: c^n = a^n + b^n$,

i.e., no Fermat primitive triple with any natural index $n > 2$.

Proof. If $p|n$, then it's an obvious consequence of Corollary 5.1.

Else $4|n$, case excluded by a known Fermat's proof.

5.3 $\neg \exists n, A, B, C \in \mathbb{N}, n > 2: C^n = A^n + B^n$, *i.e., FLT.*

Proof. By Corollary 5.2, because any natural triple A, B, C is reducible to its primitive a, b, c , dividing it by its greatest common factor $m = \text{GCF}(A, B, C)$: $a = A/m$, $b = B/m$ e $c = C/m$.

SIMPLIFICATION OF GOLDBACH'S CONJECTURE AND ITS NEGATIVE TWIN*

1 INTRODUCTION

MSC2000: 11A41.

Keywords: conjecture, Goldbach.

Abstract: This is an elementary *reductio ad absurdum* of Goldbach's conjecture and its negative twin, which requires the introduction of two new conjectures about primes.

2 DEFINITIONS

2.1 Let $n \in \mathbb{N}$ and denote F the set of all its prime factors $f: f \in F \Leftrightarrow f|n$.

2.2 Let P be the set of all primes $p \in P: 2 < p < n$.

3 PROPOSITIONS

3.1 **If p and n are coprime, then $(2n-p)$, $(n-p)$ and $(n+p)$ are each relatively prime to p and n .**
Proof. If $\exists q \in P: n, (2n-p) = 0 \pmod{q}$, then $p = 2n - (2n-p) = 0 \pmod{q}$, inconsistent with the hypothesis " p and n coprime".

If $\exists q \in P: n, (n-p) = 0 \pmod{q}$, then $p = n - (n-p) = 0 \pmod{q}$, inconsistent with hypothesis.

If $\exists q \in P: n, (2n+p) = 0 \pmod{q}$, then $p = (2n+p) - 2n = 0 \pmod{q}$, inconsistent with hypothesis.

Since p is prime, then the hypothesis that p is coprime to n is equivalent to $n \neq 0 \pmod{p}$.

If $2n-p = 0 \pmod{p}$, then $2n = 2n-p+p = 0 \pmod{p}$, inconsistent with $n \neq 0 \pmod{p}$.

If $n-p = 0 \pmod{p}$, then $n = n-p+p = 0 \pmod{p}$, inconsistent with $n \neq 0 \pmod{p}$.

If $n+p = 0 \pmod{p}$, then $n = n+p-p = 0 \pmod{p}$, inconsistent with $n \neq 0 \pmod{p}$.

3.2 **If p and n are coprime, then $(2n-p)$ and $(n-p)$ are relatively prime as well.**

Proof. If $\exists q \in P: (2n-p), (n-p) = 0 \pmod{q}$, then $n = (2n-p) - (n-p) = 0 \pmod{q}$, inconsistent with Prop. 3.1.

3.3 **If p and n are coprime and n is even, then $(n-p)$ and $(n+p)$ are relatively prime as well.**

Proof. If $\exists q \in P: (2n-p), (2n+p) = 0 \pmod{q}$, then $4n = (2n-p) + (2n+p) = 0 \pmod{q}$, inconsistent with Prop. 3.1.

3.4 **$(2n-1)$, $(n-1)$ and $(n+1)$ are each coprime to n .**

Proof. If $\exists q \in P: n, (2n-1) = 0 \pmod{q}$, then $1 = 2n - (2n-1) = 0 \pmod{q}$, therefore $q=1$.

If $\exists q \in P: n, (n-1) = 0 \pmod{q}$, then $1 = n - (n-1) = 0 \pmod{q}$, therefore $q=1$.

If $\exists q \in P: n, (n+1) = 0 \pmod{q}$, then $1 = (n+1) - n = 0 \pmod{q}$, therefore $q=1$.

3.5 **$(2n-1)$ and $(n-1)$ are relatively prime.**

Proof. If $\exists q \in P: (2n-1), (n-1) = 0 \pmod{q}$, then $n = (2n-1) - (n-1) = 0 \pmod{q}$, inconsistent with Prop. 3.4.

3.6 **If n is even, then $(n+1)$ and $(n-1)$ are relatively prime.**

Proof. If $\exists q \in P: (n+1), (n-1) = 0 \pmod{q}$, then $2n = (n-1) + (n+1) = 0 \pmod{q}$, inconsistent with Prop. 3.4.

3.7 **If $\exists p, q, r \in P, p < q: (2n-p) \wedge (2n-q) = 0 \pmod{r}$,
 then $\exists s \in P, s \neq r: (2n-p) \vee (2n-q) = 0 \pmod{s}$.**

Proof. If $\exists! r \in P: (2n-p), (2n-q) = 0 \pmod{r}$ then there exist $\alpha, \beta \in \mathbb{N}, \alpha < \beta: 2n-p = r^\alpha$ and $2n-q = r^\beta$. Since $r^\alpha > n$ and $r^{\beta-\alpha} > 2$, we have: $r^\beta > 2n$, inconsistent with $2n-p = r^\alpha < 2n$.

3.8 **If $2|n$ and $\exists p, q, r \in P, p \neq q: (n+p) \wedge (n+q) = 0 \pmod{r}$,
 then $\exists s \in P, s \neq r: (n+p) \vee (n+q) = 0 \pmod{s}$.**

Proof. If $\exists! r \in P: (n+p), (n+q) = 0 \pmod{r}$, then there exist $\alpha, \beta \in \mathbb{N}, \alpha < \beta: n+p = r^\alpha$ e $n+q = r^\beta$. Since $r^\alpha > n$ and $r^{\beta-\alpha} > 2$, we have: $r^\beta > 2n$, inconsistent with $n+q = r^\beta < 2n$.

(*) From an algebraic research presented in *New Ideas on Number Theory* (Carta e Penna, Turin, 2006) by Mr. Enzo Bonacci (Ph.D. Honoris Causa in Theoretical Physics by Cosmopolitan University).

4 CONJECTURES

4.1 Let $p, q \in (P-F) \cup \{1\}$ and $r, s \in P \cup \{2\}$.

If $(n-p)$ and $(n-q)$ have identical prime factors, i.e., $r | (n-p) \Leftrightarrow r | (n-q)$, then $\exists s \neq r: (2n-p) \vee (2n-q) = 0 \pmod{s} \wedge (2n-p) \vee (2n-q) \neq 0 \pmod{s}$, i.e., $(2n-p)$ e $(2n-q)$ differ for at least a prime factor $s > 1$. Vice versa if $r | (2n-p) \Leftrightarrow r | (2n-q)$, then $\exists s \neq r: (n-p) \vee (n-q) = 0 \pmod{s} \wedge (n-p) \vee (n-q) \neq 0 \pmod{s}$.

4.2 Let $p, q \in (P-F) \cup \{1\}$ and $r, s \in P$ and $2 | n$.

If $(n-p)$ and $(n-q)$ have identical prime factors, i.e., $r | (n-p) \Leftrightarrow r | (n-q)$, then $\exists s \neq r: (n+p) \vee (n+q) = 0 \pmod{s} \wedge (n+p) \vee (n+q) \neq 0 \pmod{s}$, i.e., $(n+p)$ e $(n+q)$ differ for at least a prime factor $s > 1$. Vice versa if $r | (n+p) \Leftrightarrow r | (n+q)$, then $\exists s \neq r: (n-p) \vee (n-q) = 0 \pmod{s} \wedge (n-p) \vee (n-q) \neq 0 \pmod{s}$.

5 THEOREMS

5.1 If $P=F$, then $(2n-1)$ is prime.

Proof. If $\forall p \in P: p | n$, then $\forall p \in P: (2n-1) \neq 0 \pmod{p}$, according to Prop. 3.4.

5.2 If $2 | n$ and $P=F$, then $(n+1)$ is prime.

Proof. If $\forall p \in P: p | n$, then $\forall p \in P: (n+1) \neq 0 \pmod{p}$, according to Prop. 3.4.

5.3 If $P-F=\{p\}$, then $(2n-p)$ is prime.

Proof. If $\forall q \in P-\{p\}: q | n$, then $\forall q \in P-\{p\}: (2n-p) \neq 0 \pmod{q}$, according to Prop. 3.1. If $(2n-p)$ is not prime, then $(2n-p) = 0 \pmod{p}$, inconsistent with Prop. 3.1.

5.4 If $2 | n$ and $P-F=\{p\}$, then $(n+p)$ is prime.

Proof. If $\forall q \in P-\{p\}: q | n$ then $\forall q \in P-\{p\}: (n+p) \neq 0 \pmod{q}$ according to Prop. 3.1. If $(n+p)$ is not prime, then $(n+p) = 0 \pmod{p}$ inconsistent with Prop. 3.1.

5.5 If $P-F=\{p_1; p_2; \dots; p_k\}$, then there is at least a prime out of: $2n-1, 2n-p_1, 2n-p_2, \dots, 2n-p_k$.

Proof. Let us consider the following sets, each consisting of $k+1$ elements:

I) $n-1, n-p_1, n-p_2, \dots, n-p_k$;

II) $2n-1, 2n-p_1, 2n-p_2, \dots, 2n-p_k$.

By Props 3.1 and 3.4 each element of set I must be divided by 2 or by primes: p_1, p_2, \dots, p_k . The different prime factors available for set I are $k+1$ considering also the number 2.

The possible "unique factor" for all the elements of set I is only the prime "2".

Therefore the minimum number of factors for set I is 1, when it is just number "2".

By Props 3.1 and 3.4, each element of set II can be divided only by odd primes out of: p_1, p_2, \dots, p_k . The different prime factors available for set II are k , because it consists of odds only. It is impossible an odd "unique factor" for all the elements of set II.

In fact if, for example, it is p_k then we have: $2n-p_k = 0 \pmod{p_k}$, inconsistent with Prop. 4.1. Therefore the minimum number of factors for set II is 3, according to Prop. 3.7.

The available different factors are $k+1$ (k odd primes for both sets, number 2 only for set I). By definition, each element of set I is divided by at least a prime factor out of: 2, p_1, p_2, \dots, p_k . Hence the available k odd prime factors are not enough to divide all the elements of set II. In fact in the most unfavourable case, if all the $k+1$ elements of set I have altogether $k+1$ different factors, then set II consists of only prime elements according to Props. 3.2 and 3.5. In the most favourable case, if there are k repetitions of the same prime factor 2 for set I, i.e., no odd factor for set I, then for set II there are k different factors by Conjecture 4.1, plus another one required by Prop. 3.7. So the necessary factors for set II are $k+1$, one more than possible p_1, p_2, \dots, p_k . Due to the lack of factors, there is at least one prime number in set II.

5.6 If $2 | n$ and $P-F=\{p_1; p_2; \dots; p_k\}$ then there is at least a prime out of: $n+1, n+p_1, n+p_2, \dots, n+p_k$.

Proof. Analogously to Theorem 5.5, after substituting set II by the following:

II) $n+1, n+p_1, n+p_2, \dots, n+p_k$;

and after substituting Propositions 3.2, 3.5 and 3.7 respectively by 3.3, 3.6 and 3.8 and Conjecture 4.1 by 4.2.

6 COROLLARIES

- 6.1 $\forall n \in \mathbb{N}: \exists p \in \mathcal{P} \cup \{1\}$ such that $2n-p$ is prime,
i.e., Goldbach's conjecture is valid.
Proof. According to Theorems 5.1, 5.3 and 5.5.
- 6.2 $\forall n \in \mathbb{N}, 2|n: \exists p \in \mathcal{P} \cup \{1\}$ such that $n+p$ is prime,
i.e., its twin conjecture is valid.
Proof. According to Theorems 5.2, 5.4 and 5.6.

REFERENCES

- [1] Bonacci, E., *New Ideas on Number Theory*, Carta e Penna, Turin, 2006
- [2] Bonacci, E., *Six moves to checkmate Fermat?*, Carta e Penna, Turin, 2007
- [3] Bonacci, E., *Multidimensional extension of the Cosine Law*, «Periodico di Matematiche», N°1, Mathesis, 2008
- [4] Bonacci, E., De Paz, M., “Consequences of binomial expansion’s unexplored properties on Fermat’s triples and Cosine Law,” Amsterdam, *5ecm-Programme and Abstracts* (2008), p. 85
- [5] Bonacci, E., De Paz, M., *Consequences of binomial expansion’s unexplored properties on Fermat’s triples and Cosine Law at the 5ecm in Amsterdam*, Rome, Aracne Sec. A1 n. 121, 2008
- [6] Bonacci, E., “Multidimensional Extension of the Cosine Law,” USA, *Cosmopolitan University Archives* (2008)
- [7] Bonacci, E., “Consequences of binomial expansion’s unexplored properties on Fermat’s Triples,” USA, *Cosmopolitan University Archives* (2008)