

# Pythagorean Triples, Goldbach's Conjecture and De Fermat's Last Theorem

Updated 2025-11-25: §§2,3 and 4 edited.

[Dr.I.noordzij@leennoordzij.nl](mailto:Dr.I.noordzij@leennoordzij.nl)  
[www.leennoordzij.me](http://www.leennoordzij.me)

## Content

§0 Prologue, The Babylonians .....	2
§1 Introduction.....	2
§1.1 Notation.....	2
§1.2 The Proof .....	3
§1.3 Factorise $a$ or $a^2$ ?.....	4
§1.4 Euclid's Formula for Pythagorean Triples.....	6
§2 Pythagorean Triples.....	6
§3 A Roadmap for Triples .....	9
§4 Examples of Triples.....	10
§5 Triples, Coprime and Goldbach's Conjecture Proved? .....	11
5.1 Triples .....	11
5.2 Coprime .....	11
5.3 Goldbach's Conjecture .....	12
5.4 Another Roadmap and an algorithm to obtain Pythagorean triples.....	13
§6 Another Representation, Number of Triples for a given $a$ . ....	15
§7 From Pythagoras to De Fermat's Last Theorem .....	17
§8 Literature .....	18

Tags: Culture, De Fermat's Last Theorem, Euclid, Goldbach, History, Mathematics, Prime Numbers, Proof by Contradiction, Pythagorean Triples.

## §0 Prologue, The Babylonians

The Babylonians used Pythagorean ideas long before Pythagoras (The Economist, August 7<sup>th</sup>, 2021). An intriguing statement. In their section on *Science and Technology*, The Economist reports research by Mansfield about the subject matter.

I cite here The Economist: *“Dr Mansfield’s answer is surveying, for this was a period when agriculture was developing, and with it the idea of landownership. One way to measure the size of a field is to divide it into rectangles and right-angled triangles, both have easily calculated areas. Knowing Pythagorean triples makes drawing the right angles needed to construct these figures easier, and so is useful information. QED.”*

## §1 Introduction.

To find the solutions of

$$a^2 + b^2 = c^2. \quad (1.1)$$

$a, b$  en  $c$  are positive integer numbers,  $\{a, b, c \in \mathbb{N} | a, b, c > 0\}$ , is a standard procedure.

Instructive reading on Pythagorean Triples can be found, e.g., in [www.en.wikipedia.org](http://www.en.wikipedia.org).

$a, b$  en  $c$  constitute a so-called Pythagorean Triple. In general,  $a$  is even,  $b$  and  $c$  are odd.

(1.1):

$$c = a \sqrt{1 + \frac{b^2}{a^2}}. \quad (1.1a)$$

### §1.1 Notation

*The Fundamental Theorem*: any integer greater than 1 is either a prime number, or can be written as a unique product of prime numbers

We write  $a$  and  $b$  as a product of prime numbers,

$$a = 2^l 3^{n_1} 5^{n_2} 7^{n_3} \dots p_s^{n_i} \dots,^1 \quad (1.2)$$

with  $n_1, n_2, \dots, n_k, \dots, \geq 0$ .

So  $a = 2^l \prod_{k=1}^t p_k^{n_k}$ .

With  $\{n_k \in \mathbb{N} \cup 0\}, \{t \in \mathbb{N}\}$  and  $\{l \in \mathbb{N} | l \geq 2\}$ .

$l \geq 2$  is explained in §3, where we choose  $a$  to be even.

$p_k$  belongs to the subset of odd prime numbers  $\mathbb{P}$ :  $\{p_k \in \mathbb{P} | p_k \text{ odd}\}$  and  $\mathbb{P} \subset \mathbb{N}$ .

Note: in the literature  $\mathbb{P}$  is also used to denote  $\mathbb{N} > 0$ .

A concise notation

$$a = 2^l \prod_{k=1}^t p_k^{n_k} = 2^l P_t.$$

$P_k$  is a product of powers of prime numbers

---

<sup>1</sup> In the following paragraphs I will sometimes choose  $a$  to be an odd or an even integer.

Furthermore:  $p_{k+1} > p_k$ .

Note:  $\prod_{k=1}^t p_k^{n_k}$ , can be equal 1, then  $a = 2^l$ .

$$b = 3^{m_1} 5^{m_2} 7^{m_3} \dots p_s^{m_s} = \prod_{s=1}^v p_s^{m_s}; \quad (1.3)$$

$\{m_s \in \mathbb{N} \cup \emptyset\}, \{v \in \mathbb{N}\}$  and  $\{p_s \in \mathbb{P}\}$ ,

and  $k \neq s$ .

A concise notation :

$$b = P_s,$$

$P_s$  is another product of powers of prime numbers.

## §1.2 The Proof

I assume the existence of a solution of (1.1) denominated a “Pythagorean Triple”:  $[a, b, c]$ ,  $\{b \in \mathbb{N} | b > 0 \text{ and even}\}$  and  $\{a, c \in \mathbb{N} | a, c > 0 \text{ and odd}\}$ .

Remark: I could have chosen  $b$  to be odd and  $a$  and  $c$  to be even and odd, respectively.  $c$  is always an odd number (see § 5).

Does this lead(proof) to the contradiction for  $c$  not being a positive integer?  $a$  and  $b$  are relative or co-prime, i.e, no common factors.

In this proof I start with values for  $a$  and  $b$  chosen independently.

With (1.2) and (1.3), (1.1a) can be written as

$$c = (2^{2l} P_k^2 + P_s^2)^{1/2}. \quad (1.4)$$

In order to find out whether or not  $c$  can be an integer I rewrite (1.4)

$$c = P_k 2^l \left(1 + \left(\frac{P_s}{P_k 2^l}\right)^2\right)^{1/2}. \quad (1.5)$$

$c$  is an integer when the expression

$\left(1 + \left(\frac{P_s}{P_k 2^l}\right)^2\right)^{1/2}$  in (1.5) is an integer number  $P$ :

$$\left(1 + \left(\frac{P_s}{P_k 2^l}\right)^2\right)^{1/2} = P. \quad (1.6)$$

$P_k 2^l$  is an integer and  $\left(1 + \left(\frac{P_s}{P_k 2^l}\right)^2\right)^{1/2}$ , is Algebraic irrational  $\rightarrow c$  is Algebraic irrational.

This is to be expected. Since there are no triples for randomly chosen integers  $a$  and  $b$ .

As I will demonstrate in the following Proof,  $b$  and  $c$  need to be expressed in factors of  $a$ .

### **Proof**

Next, with  $a = a_1 a_2$ , where  $a_1, a_2$  are products of powers of prime numbers and no common factors. Here, I assume  $a$  to be odd as mentioned above. Obviously, with  $a = a_1, a_2 = 1$ . Furthermore,  $a_1 > a_2$ .

With (1.1):

$$c = \sqrt{(a_1 a_2)^2 + b^2}. \quad (1.7)$$

If I can compose an expression for  $b^2$  of which  $(a_1 a_2)^2$  in (1.7) is part of a cross product of  $b^2$ , then an integer  $c$  can be obtained.

The composition

$$b^2 = \frac{1}{4}(a_1^4 - 2(a_1 a_2)^2 + a_2^4) \rightarrow b = \frac{1}{2}(a_1^2 - a_2^2) = \frac{1}{2}(a_1 - a_2)(a_1 + a_2),$$

will do the job.

Substitute  $b^2 = \frac{1}{4}[a_1^4 - 2(a_1 a_2)^2 + a_2^4]$  into  $\sqrt{(a_1 a_2)^2 + b^2}$ , (1.7):

$$(a_1 a_2)^2 + \frac{1}{4}[a_1^4 - 2(a_1 a_2)^2 + a_2^4] = \frac{1}{4}[a_1^4 + 2(a_1 a_2)^2 + a_2^4].$$

Hence,  $c$  in (1.7) :

$$c = \sqrt{(a_1 a_2)^2 + b^2} = \sqrt{\frac{1}{4}(a_1^4 + 2(a_1 a_2)^2 + a_2^4)} = \frac{1}{2}(a_1^2 + a_2^2). \quad (1.8)$$

So,

$$\text{with } a = a_1 a_2 \quad (1.9)$$

$$b = \frac{1}{2}(a_1^2 - a_2^2), \quad (1.10)$$

$$c = \frac{1}{2}(a_1^2 + a_2^2), \quad (1.11)$$

are both integers.

In addition,  $b$  is even and  $c$  is odd.

**End of Proof.**

An example  $a = 15$ :

-  $a_1 = 15$ , and  $a_2 = 1$ .

Then, with (1.10) and (1.11)

$b = 112$ , and  $c = 113$ .

-  $a_1 = 5$ , and  $a_2 = 3$ .

Then, with (1.10) and (1.11)

$b = 8$ , and  $c = 17$ .

So, choose  $a = 15$  and you will find two sets of triples:  $[15, 112, 113]$  and  $[15, 8, 17]$ .

Remark:

Look at (1.9)-(1.11):

These expressions look familiar  $\Rightarrow$  similar to Euclid's formula to obtain Pythagorean triples.

Instead of  $a$  to be odd we could have chosen  $a$  to be even. We can use the formulas (1.10) and (1.11). However, with the condition for the lowest possible value of  $a_2$  to be 2 to obtain natural numbers for  $b$  and  $c$ . In §2 this assumption is proved.

### §1.3 Factorise $a$ or $a^2$ ?

We use the notation presented in §1.2

First we consider  $a$  to be even. We factorise  $a$ .

$$a = 2^l P_i P_j,$$

or

$$a^2 = 2^{2l} P_i^2 P_j^2.$$

Factorise  $a$ :

$$a = 2^{l-k} P_i 2^k P_j.$$

Then

$$b = \frac{1}{2}(2^{2l-2k} P_i^2 - 2^{2k} P_j^2) = 2^{2l-2k-1} P_i^2 - 2^{2k-1} P_j^2,$$

$$c = 2^{2l-2k-1} P_i^2 + 2^{2k-1} P_j^2.$$

For a triple to be primitive,

$$2k - 1 = 0 \rightarrow k = \frac{1}{2}, \text{ this contradicts } k \text{ to be a natural number,}$$

or

$$2l - 2k - 1 = 0 \rightarrow k = l - \frac{1}{2}, \text{ this contradicts } k \text{ to be a natural number.}$$

Hence, factorization of  $a = 2^l P_i P_j$ , creates a non-primitive triple:

$$[2^l P_i P_j, 2^{2l-2k-1} P_i^2 - 2^{2k-1} P_j^2, 2^{2l-2k-1} P_i^2 + 2^{2k-1} P_j^2].$$

Divide each element of this triple by 2:

$$[2^{l-1} P_i P_j, 2^{2l-2k-2} P_i^2 - 2^{2k-2} P_j^2, 2^{2l-2k-2} P_i^2 + 2^{2k-2} P_j^2].$$

With  $k = 1$ , this triple reads

$$[2^{l-1} P_i P_j, 2^{2l-4} P_i^2 - P_j^2, 2^{2l-4} P_i^2 + P_j^2].$$

For  $l = 2$ , this triple can again be divided by 2 →

$$[P_i P_j, \frac{1}{2}(P_i^2 - P_j^2), \frac{1}{2}(P_i^2 + P_j^2)].$$

Next, factorise  $a^2 = 2^{2l} P_i^2 P_j^2 \rightarrow a^2 = 2^{2l-k} P_i^2 2^k P_j^2$ .

Note:  $a_1 = 2^{2l-k} P_i^2$ , and  $a_2 = 2^k P_j^2$ .

Then

$$b = 2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2,$$

$$c = 2^{2l-k-1} P_i^2 + 2^{k-1} P_j^2.$$

Now a primitive triple is found for

$$k - 1 = 0 \rightarrow k = 1,$$

or

$$2l - k - 1 = 0 \rightarrow k = 2l - 1.$$

Note:  $k$  is odd.

For  $k = 1$ ,  $2l - k - 1 \geq 1 \rightarrow l \geq 2$ .

Now we will analyse  $a$  to be odd.

$a = P_i P_j$ , this represents the factorisation

or

$$a^2 = P_m P_n,$$

where  $P_m$  and  $P_n$  are products of powers of prime numbers with no common factors.

Factorise  $a = P_i P_j = P_i \cdot P_j \rightarrow a^2 = P_i^2 \cdot P_j^2$ .

The lowest possible value of  $P_j$  is 1.

$$b = \frac{1}{2}(P_i^2 - P_j^2) = \frac{1}{2}(P_i - P_j)(P_i + P_j) \rightarrow b \text{ is even,}$$

$$c = \frac{1}{2}(P_i^2 + P_j^2) = \frac{1}{2}(P_i + P_j)^2 - P_i P_j \rightarrow c \text{ is odd.}$$

With factorising  $a$  primitive triples are produced.

Factorise  $a^2 \rightarrow a^2 = P_m \cdot P_n = P_i^2 \cdot P_j^2$

$$b = \frac{1}{2}(P_m - P_n) = \frac{1}{2}(P_i^2 - P_j^2) \rightarrow b \text{ is even,} \quad (1.12)$$

$$c = \frac{1}{2}(P_m + P_n) = \frac{1}{2}(P_i^2 + P_j^2) \rightarrow c \text{ is odd.} \quad (1.13)$$

Hence, choosing

$$a^2 = P_i^2 P_j^2,$$

or

$$a = P_i P_j$$

primitive triples are obtained.

Conclusion:

To find triples with  $a$  is even, we factorise  $a^2$ .

To find triples with  $a$  is odd, we factorise  $a$  or  $a^2$ .

An example of the factorisation of  $a = P_i P_j : a = 105 = 3 \cdot 5 \cdot 7$ .

$P_i$	$P_j$
$3 \cdot 5 \cdot 7$	1
$3 \cdot 5$	7
$7 \cdot 3$	5
$5 \cdot 7$	3

Four primitive triples are obtained.

### §1.4 Euclid's Formula for Pythagorean Triples

See: *Formulas for generating Pythagorean Triples*, ( [www.en.wikipedia.org](http://www.en.wikipedia.org) )

For  $\{m, n \in \mathbb{N}\}$ :

$$- a = m^2 - n^2,$$

$$- b = 2mn,$$

$$- c = m^2 + n^2.$$

Then,

$$a^2 + b^2 = c^2.$$

Caveat: not all triples found in this way are primitive.

Set  $m, n$  to be odd  $\Rightarrow a^2 + b^2 = c^2$ , can be, at least, divided by 2.

To obtain primitive triples:

set  $m$  to be odd and  $n$  to be even, or the other way around  $\Rightarrow a$  is odd and  $c$  is odd, resulting into primitive triples.

Note: when we had chosen in the preceding paragraph,  $a = 4a_1 a_2$ , Euclid's result is obtained.

In addition we answer the following question: can another sequence like 3,4 and 5 be found? Let us look into it:

With

$$a^2 + (a+1)^2 = (a+2)^2 \rightarrow (a-3)(a+1) = 0 \rightarrow a = 3.$$

Consequently there is just one sequence:

$$a = 3, b = 4, \text{ and } c = 5.$$

## §2 Pythagorean Triples

First, I want to deal with the question: can  $c$ , **(1.1)**, be even (see also §5)?

**Proof** (Giorello, ea.):

Set  $a$  and  $b$  both to be odd

$$a = 2k + 1, \{k \in \mathbb{N}\}, \text{ and}$$

$b = 2m + 1, \{m \in \mathbb{N}\}.$   
 The sum of the squares of  $a$  and  $b$ :  
 $4k^2 + 4k + 1 + 4m^2 + 4m + 1 = 4(k^2 + m^2) + 4(k + m) + 2.$   
 So a quadruple plus 2 is obtained.  
 $c$  is even,  
 $c = 2r, \{r \in \mathbb{N}\}.$   
 Then,  
 $4(k^2 + m^2) + 4(k + m) + 2 = 4r^2 \rightarrow 2(k^2 + m^2) + 2(k + m) + 1 \neq 2r^2$   
 Hence, a contradiction:  
 $c$  cannot be even. See also § 5.1.  
 Consequently,  $a$  or  $b$  is even.  
**End of Proof.**

$b$  en  $c$  can be expressed in  $a$ , with **(1.1)**, and  $a$  is now chosen to be even:

$$(c + b)(c - b) = a^2. \quad (2.1)$$

$c + b$  and  $c - b, \{c \pm b \in \mathbb{N} | c \pm b > 0 \text{ and even}\}.$

For a triple to exist,  $c + b$  and  $c - b$  are integer factors of  $a^2$ ; *the fundamental theorem of arithmetic*.

For example: with  $a = 4, c + b = 8$  and  $c - b = 2 \rightarrow c = 5, b = 3.$

With Eq. **(2.1)** we have  $c + b < a^2$ , since  $c - b > 1$ .

Also  $c - b < a^2$ , since  $c + b > 1$ .

With  $c + b$  and  $c - b$  to be even and positive,  $c + b$  and  $c - b$  are integer factors of  $a^2$  indeed. So,  $c + b = \frac{a^2}{c-b}$ , and  $c - b = \frac{a^2}{c+b}$ .

For convenience I write

$$a = 2^l \prod_{k=1}^{\infty} p_k^{n_k} = 2^l P_i P_j, \quad (2.2)$$

where  $P_i$  and  $P_j$  are products of powers of odd prime numbers.  $P_i$  and  $P_j$  being co-prime:

$$P_i \cap P_j = \emptyset \text{ and } \{P_i, P_j \subseteq \prod_{k=1}^t p_k^{n_k}\}.$$

For  $n_k = 0 : P_i = 1$  and  $P_j = 1$ .

For  $n_k \neq 0$  : a possible combination of  $\{P_i, P_j\}$  is:

$$P_i = \prod_{k=1}^t p_k^{n_k} \text{ and } P_j = 1,$$

and

$$P_j = \prod_{s=1}^t p_s^{n_s} \text{ and } P_i = 1.$$

Furthermore:  $P_i < P_j$  or  $P_j < P_i$ .

The lowest possible triple is obtained for  $P_i, P_j = 1$  and  $l = 2 : [4, 3, 5]$ .

For any combination of  $b$  and  $c$ ,  $P_i$  en  $P_j$  can be found from different combinations of products of powers of prime numbers given in Eq. **(1.2)**.

In general, with **(2.1)** and **(2.2)** :

$$(c + b)(c - b) = a^2 = 2^{2l} P_i^2 P_j^2. \quad (2.3)$$

Since  $b$  and  $c$  are co-prime, the above representation of  $a$  in **(2.2)** is not just for convenience.

With **(2.3)**,  $c + b$  and  $c - b$ , both even, are represented respectively:

$$c + b = 2^{2l-k} P_i^2, \quad (2.4)$$

$$c - b = 2^k P_j^2. \quad (2.5)$$

For  $c$  and  $b$  we have:

$$c = 2^{2l-k-1} P_i^2 + 2^{k-1} P_j^2, \quad (2.6)$$

$$b = |2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2|. \quad (2.7)$$

$$\{k \in \mathbb{N} | 0 < k < 2l\}.$$

With the expressions in (2.6) and (2.7), I can analyse (1.1a) again:

$$c = (a^2 + b^2)^{1/2},$$

similar to (1.8) and (1.9).

Plug (2.2) and (2.7) into  $c = (a^2 + b^2)^{1/2}$ :

$$\begin{aligned} c(2^{2l} P_i^2 P_j^2 + 2^{4l-2k-2} P_i^4 - 2^{2l-1} P_i^2 P_j^2 + 2^{2k-2} P_j^4)^{1/2} = \\ = (2^{4l-2k-2} P_i^4 + 2^{2l-1} P_i^2 P_j^2 + 2^{2k-2} P_j^4)^{1/2} = 2^{2l-k-1} P_i^2 + 2^{k-1} P_j^2, \text{ equal to } c \text{ derived in} \\ (2.6). \text{ See proof in §1.2.} \end{aligned}$$

**Caveat:** expression (2.7)  $\rightarrow b = |2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2|$ , as follows from the proof in §1.2

Keep in mind:  $c > b$  and  $c, b$  odd. Consequently,  $c - b > 1$  and  $(c + b) < 2^{2l} P_i^2 P_j^2$ .

To make  $c$  and  $b$  co-prime indeed, we found in §1.3:

$$k - 1 = 0 \text{ or } 2l - k - 1 = 0, \quad (2.8)$$

and with (2.6) and (2.7) a primitive triple is obtained.

$l \geq 2$ ?

Since for  $l = 1$ , the right-hand sides of Eqs. (2.6) and (2.7) represent the sum of two odd integers and become consequently even. This is wrong:  $b$  and  $c$  must be odd in order Eqs. (2.6) and (2.7) to represent primitive triples.

So, we found something interesting for  $a$  is even  **$a$ , in the Triples, is at least an integer that can be divided by four.**

Now, let us analyse  $b = |2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2|$  with  $k - 1 = 0$  to obtain a primitive triple:

$$b = |2^{2l-2} P_i^2 - P_j^2|. \quad (2.9)$$

The question to be answered is: does  $2l - k - 1 = 0$ , (2.8), added information?

So,  $2l - k - 1 = 0 \rightarrow k = 2l - 1$ . Plug this result into

$$b = |2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2| \rightarrow b = |P_i^2 - 2^{2l-2} P_j^2|.$$

Hence,  $2l - k - 1 = 0$  does not create no new information  $\rightarrow$  no additional primitive triples.

When we start with  $a$  a natural number and odd, do we find  $b$  to contain the factor making  $b$  an even natural number is:  $2^l$ , with  $l \geq 2$ ?

To analyse this we will use (1.10)

$$b = \frac{1}{2}(a_1^2 - a_2^2).$$

$$a_1 \text{ is odd and } a_1 = 2n + 1, \quad a_1 \geq 5,$$

$$a_2 \text{ is odd and } a_2 = 2m + 1, \quad a_2 \geq 3.$$

Then

$$b = 2(n - m)(n + m + 1).$$

We have



$n - m$  is even  $\rightarrow n + m + 1$  is odd ,

$n - m$  is odd  $\rightarrow n + m + 1$  even

and

$n > m$ .

$n - m$  is even  $\rightarrow 2^p, \{p \in \mathbb{N} | p \geq 1\}$ ,

$n + m + 1$  even  $\rightarrow 2^q, \{q \in \mathbb{N} | q \geq 1\}$ .

$\therefore$

$$b = 2^{p+1}(n + m + 1),$$

or

$$b = 2^{q+1}(n - m).$$

With  $a$  a natural number and odd, we find  $b$  to contain the factor making  $b$  an even natural number to be  $2^l$ , with  $l \geq 2$ .

### §3 A Roadmap for Triples

Summary:

$a$  even

$a = 2^l P_i P_j$ , **(2.2)**, factorize  $a^2 = 2^{2l} P_i^2 P_j^2$

$|2^{2l-2} P_i^2 \pm P_j^2| : \pm \rightarrow +c$  and  $- \rightarrow b$

**Table Roadmap:**

$ 2^{2l-2} P_i^2 P_j^2 \pm 1 $
$ 2^{2l-2} P_i^2 \pm P_j^2 $
$ 2^{2l-2} P_j^2 \pm P_i^2 $
$ 2^{2l-2} \pm P_i^2 P_j^2 $

Note: the minimum value of  $l = 2$ .

$a$  odd

$a = P_i P_j$ , factorize  $a$  or  $a^2$

$\frac{1}{2} |P_i^2 \pm P_j^2| : \pm \rightarrow +c$  and  $- \rightarrow b$

**Table Roadmap**

$ P_i^2 P_j^2 \pm 1 $
$ P_i^2 \pm P_j^2 $

## §4 Examples of Triples

An example summarized in the Table below:

$a = 60 (= 2^2 \cdot 3 \cdot 5)$  produces four Pythagorean Triples:  
[60,11,61], [60,91,109], [60,221,229] and [60,899,901].

As promised in §§1.2 and 1.3 the following assumption will be tested:  
factorise  $a$  or  $a^2$

$$a = 2^l P_i P_j, \text{ or } a^2 = 2^{2l} P_i^2 P_j^2 \text{ with } a = 12 = 2^2 \cdot 3.$$

We use Eqs. (1.10) and (1.11).

Factorise  $a = (2 \cdot 3) \cdot 2$

$$b = \frac{1}{2}(4 \cdot 9 - 4) = 16,$$

$$c = \frac{1}{2}(4 \cdot 9 + 4) = 20.$$

We obtain one non-primitive triple  $[12,16,20] \rightarrow [3,4,5]$ .

Next, factorise  $a^2 = 2^4 \cdot 3^2 \rightarrow 72 \cdot 2$ , and  $18 \cdot 8$

$$72 \cdot 2$$

$$b = \frac{1}{2}(72 - 2) = 35,$$

$$c = \frac{1}{2}(72 + 2) = 37.$$

$$18 \cdot 8$$

$$b = \frac{1}{2}(18 - 8) = 5,$$

$$c = \frac{1}{2}(18 + 8) = 13.$$

We obtain two primitive triples:  $[12,35,37]$ , and  $[12,5,13]$ .

We summarize the set of equations for the elements of the triples and constraints to prevent non-primitive triples: with  $a^2 = 2^{2l} P_i^2 P_j^2$

$b = 2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2$
$c = 2^{2l-k-1} P_i^2 + 2^{k-1} P_j^2$
$k - 1 = 0, \text{ or } 2l - k - 1 = 0$

Note:

- given  $a = 180 (= 2^2 \cdot 3^2 \cdot 5)$ , again four triples are found.
- given  $a = 2^2 \cdot 3 \cdot 5 \cdot 7$ , you will find eight triples.
- given  $a = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ , you will find sixteen triples.

A question to be answered is: do we find all the triples with  $a$  is odd and starting with  $a = 3$ ? Well, the answer to this question is yes, we do find all the triples since the Pythagorean equation is symmetric with respect to  $a$  and  $b$ :  $[a, b, c] \equiv [b, a, c]$ .

## §5 Triples, Coprime and Goldbach's Conjecture Proved?

### 5.1 Triples

In the analysis above, I choose  $a$  to be even. Let's set  $a$  to be odd, see §1.2,

$a = P_i P_j$  ; *the fundamental theorem of arithmetic.*

$P_i$  and  $P_j$  are products of powers of odd prime numbers and relative prime. See §2, Eq.(2.2).

Similar to the analysis in §1.2,

$$c = \frac{P_i^2 + P_j^2}{2}, \quad (5.1)$$

and

$$b = \frac{P_i^2 - P_j^2}{2}. \quad (5.2)$$

The question is:  $c$  odd or  $b$  odd? From the above expressions the conclusion could be:

$b$  is "more even"<sup>2</sup> than  $c$  , since

$$b = \frac{(P_i + P_j)(P_i - P_j)}{2}. \quad (5.3)$$

With

$$P_i^2 = 2b + P_j^2$$

we have

$$c = b + P_j^2.$$

Since  $b$  is even,  $c$  is odd. Suppose  $c$  to be even, consequently  $b$  must be odd. That

contradicts  $b = \frac{(P_i + P_j)(P_i - P_j)}{2}$ .

Hence, I conclude  $c$  can never be even. In addition,  $c$  is the largest number in a triple. In a trivial triple,  $b = 0$  , we have  $c = a$ .

So, for a non-trivial triple the largest number is never even.

By choosing  $a$  to be odd the algorithm to find the triple becomes simpler. The only constraint to be taken care off is:

$$\frac{P_i^2}{P_j^2} > 1, \quad (5.4)$$

or with (2.1):

$$c = \frac{P_i^2 + P_j^2}{2} > P_i P_j (= a).$$

Consequently:

$$P_i^2 - 2P_i P_j + P_j^2 > 0 \rightarrow P_i - P_j > 0.$$

Start with the lowest possible value of  $a = P_i P_j = 3^1 5^0$  .

So  $P_i = 3$  and  $P_j = 1$ ,

and we have the triple (3,4,5) .

### 5.2 Coprime

To obtain triples,  $a, b, c$  are considered to be coprime.

Now I assume

---

<sup>2</sup> An Orwellian mathematical expression, sort of.

$b$  and  $c$  to have a common integer factor  $p$ .

Then

$$c = pc_1,$$

and

$$b = pb_1,$$

where  $\{c_1, b_1 \in \mathbb{N} \mid > 0\}$ .

Plug this into

$$a^2 = c^2 - b^2 \rightarrow a^2 = p^2(c_1^2 - b_1^2).$$

Since  $\{a \in \mathbb{N} \mid > 0\}$  and *the fundamental theorem of arithmetic*,  $a$  can be factorized.

Consequently,  $p$  is a factor of  $a$  and the Pythagorean equation can be divided by  $p$ .

### 5.3 Goldbach's Conjecture

There is more.

Let us look at **(5.3)**. Rearranging:

$$\frac{2b}{(P_i - P_j)} = (P_i + P_j). \quad (5.5)$$

**(5.5)** in words: an even number,  $\frac{2b}{(P_i - P_j)}$ , equals the sum of two primes,  $(P_i + P_j)$ .

Note: to find the triples,  $P_i$  and  $P_j$  are defined to be products of powers of primes. Still  $P_i$  and  $P_j$  can also represent single primes:  $\{P_i, P_j \in \mathbb{P}\}$ .

Caveat:  $(P_i - P_j) > 0$ . When  $b = 0$  then  $(P_i - P_j) = 0$ .

Goldbach's Conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states: Every even integer greater than 2 can be expressed as the sum of two primes ([www.en.m.wikipedia.org](http://www.en.m.wikipedia.org)).

After inspection of **(5.5)** it appears this expression cannot be used for 4 and 6. It can be demonstrated for  $\frac{2b}{(P_i - P_j)} > 6$ , **(5.5)** can do the job. This equivalent to:

$$P_i \geq 5 \text{ and } P_j \geq 3.$$

This is not a proof? To prove **(5.5)** do we need a general expression for deriving primes? This expression is still not there.

However, what we learn from **(5.5)** is: an even number can be expressed as the sum of two primes. In general:

$$2(n + 1) = (P_i + P_j), \quad (5.6)$$

where

$$\{n \in \mathbb{N} \mid n > 0\}.$$

Goldbach's Conjecture solved?

Well, with an infinite number of primes we find an infinite number of even integers. Do we have all of them? That is the question.

**Remark:** Every even integer greater than 2 can be expressed as the difference of two primes.

An example:

$$4 = 2 + 2,$$

and

$$4 = 7 - 3 = 11 - 7 = 17 - 13 = 21 - 17 = 23 - 19 = 41 - 37 = \dots$$

#### 5.4 Another Roadmap and an algorithm to obtain Pythagorean triples.

We have

$$a^2 + b^2 = c^2, (1.1).$$

I start with

$$c^2 = (c-1)^2 + (c-2)^2 \rightarrow (c-1)(c-5) = 0 \rightarrow c = 5, b = 4 \text{ and } a = 3.$$

$$c^2 = (c-1)^2 + (c-4)^2 \rightarrow \text{no solutions.}$$

$$c^2 = (c-1)^2 + (c-6)^2 \rightarrow \text{no solutions.}$$

$$c^2 = (c-1)^2 + (c-8)^2 \rightarrow (c-5)(c-13) = 0 \rightarrow c = 13, b = 12 \text{ and } a = 5.$$

$$c^2 = (c-1)^2 + (c-10)^2 \rightarrow \text{no solutions.}$$

$$c^2 = (c-1)^2 + (c-12)^2 \rightarrow \text{no solutions.}$$

Etc.

Then,

$$c^2 = (c-3)^2 + (c-2)^2 \rightarrow \text{no solutions.}$$

$$c^2 = (c-3)^2 + (c-4)^2 \rightarrow \text{no solutions.}$$

$$c^2 = (c-3)^2 + (c-6)^2 \rightarrow (c-3)(c-15) = 0 \rightarrow c = 15, b = 12 \text{ and } a = 9.$$

Etc.

Then,

$$c^2 = (c-5)^2 + (c-2)^2 \rightarrow \text{no solutions.}$$

Etc.

In general:

$$c^2 = (c-l)^2 + (c-m)^2, \text{ with } \{l \in \mathbb{N}|\text{odd}\} \text{ and } \{m \in \mathbb{N}|\text{even}\}.$$
<sup>3</sup>

This results into an expression for  $c$ :

$$c = (l+m) \pm \sqrt{2lm}. \tag{5.7}$$

With this expression and  $l = 1, m = 2 \rightarrow c = 3 \pm 2$ ,

and  $l = 1, m = 8 \rightarrow c = 9 \pm 4$ .

The latter result demonstrates: a new  $c = 13$  and the former  $c = 5$ .

Next:

$$l = 1, m = 18 \rightarrow c = 19 \pm 6.$$

Again, a new  $c = 25$  and the former  $c = 13$ .

This is what should be found. Since, (5.7) results from a quadratic equation  $\rightarrow$  two roots, integers, are found: a new value for  $c$  and consequently the preceding one of the Pythagorean triple.

To demonstrate this by applying (5.7) to  $c = 25$ , as the preceding value of the Pythagorean triple, and  $l = 1$ ,

$$c = (l+m) \pm \sqrt{2lm} \rightarrow (1+m) - \sqrt{2m} = 25 \rightarrow (m-18)(m-32) = 0.$$

The new  $m = 32$  and the former ( $m = 18$ ) are obtained. The new value, with  $l = 1$ , for

---

<sup>3</sup> Here we used  $l$  as a general integer not being the power of 2.

$$c = (l + m) \pm \sqrt{2lm} \rightarrow 33 \pm 8 \rightarrow 41,$$

and the preceding value of  $c = 25$ .

Note: in the former procedure, I kept  $l = 1$ .

To find another set of Pythagorean triples, I keep  $m = 2$  and look for the lowest possible value of  $l$ .

As an educated guess, I start with the preceding value of  $c = 5$ , and use the procedure developed above.

So,

$$c = (l + 2) - \sqrt{4l} = 5 \rightarrow (l - 9)(l - 1) = 0 \rightarrow l = 9.$$

With this value for  $l$ ,  $m = 2$  and **(5.7)**:

$$c = (l + m) \pm \sqrt{2lm} \rightarrow 11 \pm 6 \rightarrow 17 \text{ giving } [8, 15, 17].$$

Again, with the developed procedure:

$$c = (l + 2) - \sqrt{4l} = 17 \rightarrow (l - 25)(l - 9) = 0 \rightarrow l = 25, \text{ where I did use } l = 9.$$

With  $l = 25$ ,  $m = 2$  and **(5.7)**:

$$c = (l + m) \pm \sqrt{2lm} \rightarrow 27 \pm 10 \rightarrow 37 \text{ giving } [12, 35, 37].$$

In this way an efficient algorithm is obtained to find Pythagorean triples in a systematic way:

- alternating keep  $l$  and  $m$  fixated,
- start with  $c = 5$  and  $c = (l + m) - \sqrt{2lm}$ , to find the next value of  $m$  or  $l$ ,
- calculate the new value of  $c = (l + m) + \sqrt{2lm}$ ,
- plug this new value of  $c$  into  $c = (l + m) - \sqrt{2lm}$ , to find the next value of  $m$  or  $l$ ,
- etc.

Now, I set  $l = 3$  and start with  $m = 2$ .

$$\text{First, inspect } c = (l + m) \pm \sqrt{2lm} \rightarrow (3 + m) \pm \sqrt{6m}.$$

To obtain an integer value for  $c \rightarrow m = 2^k 3^r$ ,

where  $\{k \in \mathbb{N} | k \text{ odd}\}$  and  $\{r \in \mathbb{N} | r \text{ odd}\}$ .

Then,

$c = (3 + m) \pm \sqrt{6m} = (3 + 2^k 3^r) \pm 2^{(k+1)/2} 3^{(r+1)/2}$ . This illustrates the Pythagorean triple to be non-primitive or, I denoted such a Pythagorean Triple, to be trivial.

Since,

$$c = (3 + m) \pm \sqrt{6m} = 3[(1 + 2^k 3^{r-1}) \pm 2^{\frac{k+1}{2}} 3^{\frac{r-1}{2}}],$$

for  $r \geq 3$ .

Conclusion: no Pythagorean Triple for  $m = 2$ . For  $m = 6(k = 1, r = 1)$ , a non-primitive triple is found:

$$[9, 12, 15] \rightarrow [3, 4, 5].$$

So, to complete the algorithm a test has to be passed.

To summarize:

- $a^2 + b^2 = c^2$
- $c^2 = (c - l)^2 + (c - m)^2$ , with  $\{l \in \mathbb{N} | \text{odd}\}$  and  $\{m \in \mathbb{N} | \text{even}\}$ ,
- $a = c - l$ , and  $b = c - m$ ,
- $c = (l + m) \pm \sqrt{2lm}$ ,

- $2lm$  a quadratic integer,
- $l$  and  $m$  coprime to prevent non-primitive triples,
- $m = 2^k P_m$  and  $l = P_l$ ;  $\{k \in \mathbb{N} \mid k \neq 0 \text{ and odd}\}$ ,  $P_m$  and  $P_l$  coprime and shorthand for products of even powers of prime numbers.

Example:

$l = 3$  and  $m = 2$  are not possible  $\rightarrow l$ , should have been for example  $3^2$ . As shown above,  $3^0$  is correct.

## §6 Another Representation, Number of Triples for a given $a$ .

In §2:

$$c + b = 2^{2l-k} P_i^2, \quad (2.4).$$

$$c - b = 2^k P_j^2, \quad (2.5).$$

$$c = 2^{2l-k-1} P_i^2 + 2^{k-1} P_j^2, \quad (2.6).$$

$$b = 2^{2l-k-1} P_i^2 - 2^{k-1} P_j^2, \quad (2.7).$$

Or more concise:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2^{2l-k-1} P_i^2 \\ 2^{k-1} P_j^2 \end{pmatrix} = \begin{pmatrix} c \\ b \end{pmatrix}.$$

On the other hand we could have chosen:

$$c + b = 2^r P_i^2, \text{ and} \quad (6.1)$$

$$c - b = 2^{2l-r} P_j^2. \quad (6.2)$$

Giving:

$$c = 2^{r-1} P_i^2 + 2^{2l-r-1} P_j^2, \quad (6.3)$$

$$b = 2^{r-1} P_i^2 - 2^{2l-r-1} P_j^2, \quad (6.4)$$

and

$$\{r \in \mathbb{N} \mid 0 < r < 2l\}.$$

Or more concise:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2^{r-1} P_i^2 \\ 2^{2l-r-1} P_j^2 \end{pmatrix} = \begin{pmatrix} c \\ b \end{pmatrix}.$$

In order to find triples we have the condition:

$$r - 1 = 0 \text{ or } 2l - r - 1 = 0. \quad (6.5)$$

In addition the following constraint applies:

$b > 0$ . With (6.4) we obtain:

$$2^{r-1} P_i^2 > 2^{2l-r-1} P_j^2 \rightarrow \frac{P_i}{P_j} > \frac{2^l}{2^r}. \quad (6.6)$$

I expect the distribution of the prime numbers given in (6.1) and (6.2) to produce the same results for the Triples.

Well, comparing the conditions (6.5) with Eqs. (2.6) and (2.7) :

$(r - 1)$  to be equivalent with  $(2l - k - 1)$ ,

and

$(2l - r - 1)$  to be equivalent with  $(k - 1)$ .

Plug  $r - 1 = 0$  into (6.6) we find

$$\frac{P_i}{P_j} > \frac{2^l}{2} (= 2^{(l-1)}). \quad (6.7)$$

Now, plug  $(2l - k - 1) = 0$  into

$$2^{2l-k-1}P_i^2 > 2^{k-1}P_j^2 \rightarrow \frac{P_i}{P_j} > \frac{2^k}{2^l}, \quad (1.11),$$

then,

$$\frac{P_i}{P_j} > \frac{2^{2l-1}}{2^l} (= 2^{l-1}),$$

equivalent to (6.7) .

Plug  $2l - r - 1 = 0$  into (6.6) we find

$$\frac{P_i}{P_j} > \frac{2^l}{2^{2l-1}} (= 1/2^{(l-1)}). \quad (6.8)$$

Now, plug  $(k - 1 = 0)$  into

$$2^{2l-k-1}P_i^2 > 2^{k-1}P_j^2 \rightarrow \frac{P_i}{P_j} > \frac{2^k}{2^l}, \quad (1.11),$$

$$\text{then } \frac{P_i}{P_j} > \frac{1}{2^{l-1}}$$

equivalent to (6.8).

Hence, we find with the distribution of the prime numbers given in (6.1) and (6.2) the same Triples indeed.

For creating the Pythagorean Triples you need an efficient algorithm for producing the prime numbers: *Generating Primes* , [www.en.m.wikipedia.org](http://www.en.m.wikipedia.org) .

However, in general we can formulate a Prime Number Theorem:

Any odd number  $k = 2n - 1, \{n \in \mathbb{N}, n > 0\}$  is a prime number unless  $k$  can be divided by a prime number  $P_j < k$  , *the Fundamental Theorem of Arithmetic*.

The hard work begins with finding an efficient algorithm for producing the prime numbers.

But that is not the point. It is about the formulation of the Theorem on Prime Numbers.

Question: how many triples can we obtain for a given value of  $a$  ? Choose  $a$  to be even.

Well, for  $a = 2^l$  and  $\prod_s p_s^{n_s} = 1$  , and for a particular value of  $l \geq 2$  one triple is found. This is equivalent to the statement: for  $n_s = 0$  , one triple is obtained.

Now we choose  $a = 2^l p_t^{n_t}$  , i.e.,  $p_t$  one odd prime number and  $n_t \geq 1$ . We find at least one triple. Since for  $P_i = p_t^{n_t}$  and  $P_j = 1$  :  $\frac{P_i}{P_j} > \frac{1}{2^{l-1}}$  .

Is there another triple? We have two possibilities:

$$k = 1, \text{ then } P_i = 1 \text{ and } P_j = p_t^{n_t},$$

and

$$k = 2l - 1, \text{ then } P_i = p_t^{n_t} \text{ and } P_j = 1.$$

We analyse  $k = 1$  :

Plug into  $\frac{P_i}{P_j} > \frac{1}{2^{l-1}}$  the values for  $P_i$  and  $P_j$ :

$$l > 1 + \frac{n_t \ln(p_t)}{\ln 2} .$$



Next  $k = 2l - 1$  :

$$l < 1 + \frac{n_t \ln(p_t)}{\ln 2}.$$

We conclude to find another triple for  $l > 1 + \frac{n_t \ln(p_t)}{\ln 2}$  or  $l < 1 + \frac{n_t \ln(p_t)}{\ln 2}$ .

Hence: for  $a = 2^l p_t^{n_t}$ , i.e. one odd prime number and  $n_t \geq 1$ , we obtain two Pythagorean triples.

**Conjecture:** for a given  $a$  the number of triples equals  $2^s$ ,

where  $s$  is the number of odd-coprime-triples of which  $a$  is composed.

Note: I use the wording “coprime”, since for example  $5^2$  is a separate number in the triple of odd prime number series.

You will notice not to find, e.g., a combination such as: [9,12,15]. This is a non-primitive triple. Well, set  $l = 2$ ,  $P_i = P_j$ , and  $a = 12$  you will find this non-primitive solution. In this case by  $P_i = P_j (\neq 1)$  a non-primitive solution is obtained. A simpler approach is by multiplying the primitive Triple [3,4,5] by any positive integer you like. The Triple [4,3,5] is found with  $n_s = 0$  in (2.2) giving  $P_i$  and  $P_j$  equal 1 in (2.6) and (2.7) .

In §5.3 as a spin-off of Pythagorean Triples, sort of, a solution for Goldbach’s Conjecture is found?

De Fermat’s last theorem leads to the conclusion no Pythagorean triples to be found constituted of powers of integers.

An example is sufficient.

Assume the triple to be  $(a^2, b^2, c^2)$ .

Then the Pythagorean equation and De Fermat’s last theorem gives:

$$(a^2)^2 + (b^2)^2 = (c^2)^2 \rightarrow a^4 + b^4 \neq c^4,$$

QED.

I appreciate the comment by Steve Hurley,

<https://explainscience.org/2019/09/01/the-goldbach-conjecture/>

## §7 From Pythagoras to De Fermat’s Last Theorem

In §6 we used the result of De Fermat’s Last Theorem to show the Pythagorean triple not to be composed of equal powers of integers.

See also Noordzij(1), *De Fermat’s Last Theorem, Pythagorean Triples and The Descente Infinie revisited*, [www.leennoordzij.me](http://www.leennoordzij.me) .

Andrew Wiles did prove De Fermat’s Last Theorem.

De Fermat’s theorem in a nutshell

$$a^n + b^n \neq c^n,$$

with

$$\{a, b, c \in \mathbb{N} \mid \text{and } > 0\} \text{ and } \{n \in \mathbb{N} \mid n > 2\}.$$

Let us look once more into De Fermat’s equation.

$$a^n + b^n = c^n \rightarrow (a^{n/2})^2 + (b^{n/2})^2 = (c^{n/2})^2.$$

$$(a^{n/2})^2 + (b^{n/2})^2 = (c^{n/2})^2,$$

represents the Pythagorean equation where  $[a^{\frac{n}{2}}, b^{\frac{n}{2}}, c^{\frac{n}{2}}]$  constitutes a Pythagorean triple for any integer  $n \geq 3$ . "Any integer  $n$ " the key to De Fermat's Last Theorem.

$$\left[ a^{\frac{n}{2}}, b^{\frac{n}{2}}, c^{\frac{n}{2}} \right] \rightarrow$$

[3,4,5], [5,12,13], [7,24,25], [9,40,41]<sup>4</sup>, [11,60,61], [13,84,85], [15,112,113], [15,8,17], ... .. for  $\{n \in \mathbb{N} > 0\}$ .

Now we have the integers

$$A = a^{n/2}, B = b^{n/2}, \text{ and } C = c^{n/2}.$$

Then

$$a = A^{2/n}, b = B^{2/n}, \text{ and } c = C^{2/n}.$$

The question to be answered: can  $a, b$  and  $c$  be integers for  $n > 2$ ?

An example:

we choose  $A = 3$ .

This leads to the Pythagorean triple [3,4,5]  $\rightarrow$

$$\rightarrow a = 3^{2/n}, b = 4^{2/n}, \text{ and } c = 5^{2/n}.$$

The conclusion is

$a$  is not an integer, and  $c$  is not an integer.

Hence, for this example De Fermat's theorem is correct.

The above example [3,4,5] indicates the route to be followed.<sup>5</sup>

Is there a possibility to find a Pythagorean triple  $[A, B, C]$  resulting into  $a, b, c$  being integers?

**Proof:**

Well, choose  $A = x^s, B = y^s$ , and  $C = z^s$ , with  $\{x, y, z \text{ and } s \in \mathbb{N} \text{ and } > 0\}$ .

We use the results from the proof of the existence of Pythagorean triples §1.2

Then

$$- z^s - y^s = 1,$$

and

$$- z^s + y^s = A^2.$$

$z^s - y^s = 1$ , cannot be true and the assumption Pythagorean triple  $[A, B, C]$  to exist is contradicted.

Consequently, a Pythagorean triple  $[x^s, y^s, z^s]$  cannot be found and  $a, b, c$  do not represent a set of integers.

Conclusion: De Fermat's Theorem is correct.

**End of Proof.**

Finally, we conclude De Fermat's Theorem to be correct using the above approach via the route of Pythagorean triples. Is this sufficient? The subject matter is paid attention to in Noordzij (2).

## §8 Literature

Giorello, G. and C. Sinigaglia, *Fermat- I sogni di un magistrato all'origine della matematica moderna*, 2001, Le Science, Milano.

<sup>4</sup> Nine can be factorized:  $3 \cdot 3$ . However, this leads to a trivial Pythagorean triple  $[9,0,9] \rightarrow [1,0,1]$

<sup>5</sup> Note: We conclude for all values of  $A$  to be prime De Fermat's theorem is correct.

Noordzij, L.(1), *De Fermat's Last Theorem, Pythagorean Triples and The Descente Infinie revisited*, [www.leennoordzij.me](http://www.leennoordzij.me) .

Noordzij, L.(2), *De Fermat's Last Theorem and the margin of De Fermat's Diophantus*, [www.leennoordzij.me](http://www.leennoordzij.me) .

The Economist, *Ancient Geometry, No need for a protractor*, Section Science and Technology, August 7<sup>th</sup> 2021.