

# Classification of primitive Pythagorean triples

Kuan Peng [titang78@gmail.com](mailto:titang78@gmail.com)

16 September 2025

**Abstract:** In this article we have created the table that classifies all primitive triples, shown some properties of basic triples and discussed about the use of primitive Pythagorean triples in cryptography.

1.	INTRODUCTION.....	1
2.	BASIC PYTHAGOREAN TRIPLES.....	1
3.	LINES OF MULTIPLE TRIPLES.....	2
4.	SPARSE MULTIPLE TRIPLES.....	4
5.	PROPERTIES OF BASIC PYTHAGOREAN TRIPLES.....	6
	a) <i>Primitive Pythagorean triples with equal Z</i> .....	6
	b) <i>Sparse multiple triples and their corresponding primitive triples</i> .....	7
	c) <i>Distribution of sparse multiple triples</i> .....	8
6.	DISCUSSION.....	8
	LETTER TO READERS.....	9
	a) <i>About my research</i> .....	9
	b) <i>About the publication of my papers</i> .....	9

## 1. Introduction

We continue our fascinating study of Pythagorean triples that we have begun in « [Classification of Pythagorean triples](#) and [reflection on Fermat’s last theorem](#)» and «[Parabolic patterns](#) in the [scatter plot of Pythagorean triples](#)». There are two categories of Pythagorean triples: primitive triples and multiple triples. If a triple of integers (X, Y, Z) satisfies  $X^2 + Y^2 = Z^2$ , it is a Pythagorean triple. When we multiply it with an integer k we get (kX, kY, kZ) which is also a Pythagorean triple because :

$$(kX)^2 + (kY)^2 = (kZ)^2 \quad (1)$$

(kX, kY, kZ) is called a multiple Pythagorean triple. If the three components of a Pythagorean triple, X, Y and Z, have no common divisor larger than 1, (X, Y, Z) is called a primitive Pythagorean triple. In « [Classification of Pythagorean triples](#) and [reflection on Fermat’s last theorem](#)» we have classified all Pythagorean triples in a 3D table. The first page of this table is shown in Table 1. All the other pages equal the first page multiplied by an integer k and thus, contain only multiple triples. So, Table 1 has the following property:

*Property 1: Table 1 contains all primitive Pythagorean triples.*

Table 1 contains also multiple triples. So, the triples in Table 1 are called basic Pythagorean triples. In Table 1 the primitive triples are colored in blue and the multiple triples in red. We see that the second and fourth lines are multiple triples, the diagonal also contains only multiple triples. This suggests that we could remove all multiple triples from Table 1 to create a table that contains only primitive triples.

k=1	Z-X = 2			Z-X = 8			Z-X = 18			Z-X = 32			Z-X = 50			...	Z-X = L
Z-Y = 1	3	4	5	5	12	13	7	24	25	9	40	41	11	60	61		
Z-Y = 4	8	6	10	12	16	20	16	30	34	20	48	52	24	70	74		
Z-Y = 9	15	8	17	21	20	29	27	36	45	33	56	65	39	80	89		
Z-Y = 16	24	10	26	32	24	40	40	42	58	48	64	80	56	90	106		
Z-Y = 25	35	12	37	45	28	53	55	48	73	65	72	97	75	100	125		
...																	
Z-Y = K																	

Table 1

## 2. Basic Pythagorean triples

How to find multiple triples? All Pythagorean triples can be generated with two integers a and b as follow:

$$\begin{aligned} X &= a^2 - b^2 \\ Y &= 2ab \\ Z &= a^2 + b^2 \end{aligned} \quad (2)$$

Because X is positive, a must be bigger than b,  $a > b$ . We denote  $a - b$  as j and a equals:

$$a = b+j \quad (3)$$

By introducing equation (3) into (2), X, Y and Z are expressed with b and j:

$$\begin{aligned} X &= (b + j)^2 - b^2 \\ Y &= 2(b + j)b \\ Z &= (b + j)^2 + b^2 \end{aligned} \quad (4)$$

For creating Table 1, we let the parameters b and j equal:

$$b=1, 2, 3\dots, j=1, 2, 3\dots \quad (5)$$

While the value of b and j increase indefinitely all Pythagorean triples of Table 1 will be generated. In Table 1, a column contains triples that have the same value of b, a line contains triples that have the same value of j. So, b is the column index and j the line index.

For identifying multiple triples, we check if a Pythagorean triple verifies the following condition for primitive triple, which is given in the article [Pythagorean triple](#) on Wikipedia:

*By Euclid's formula all primitive Pythagorean triples can be generated from integers m and n with  $m > n > 0$ ,  $m+n$  odd and  $\gcd(m,n)=1$ .*

We reformulate this condition using our convention in which m is replaced by a and n by b:

Condition 1:  $m > n > 0 \Rightarrow a > b > 0$

Condition 2:  $m + n$  odd  $\Rightarrow a + b$  odd

Condition 3:  $\gcd(m, n)=1 \Rightarrow$  **Greatest common divisor of a and b is 1**

### 3. Lines of multiple triples

Let's compute Pythagorean triples with a second formulation :

$$\begin{aligned} X &= cd \\ Y &= \frac{c^2 - d^2}{2} \\ Z &= \frac{c^2 + d^2}{2} \end{aligned} \quad (6)$$

where  $c=a+b$  and  $d=a-b$ .

Y can be expressed as :

$$Y = \frac{(c + d)(c - d)}{2} \quad (7)$$

Because Y is positive, c must be bigger than d,  $c > d$ . Since Y is integer,  $c - d$  must be even. So, we write c as :

$$c = d + 2i \quad (8)$$

where i being integer.

By introducing equation (8) into (6), we express X, Y and Z with d and i:

$$\begin{aligned} X &= (d + 2i)d \\ Y &= \frac{(d + 2i)^2 - d^2}{2} \\ Z &= \frac{(d + 2i)^2 + d^2}{2} \end{aligned} \quad (9)$$

Using equation (9), all Pythagorean triples can be generated with the following values of the parameters d and i:

$$d=1, 2, 3\dots, i=1, 2, 3\dots \quad (10)$$

We have shown in « [Classification of Pythagorean triples](#) and [reflection on Fermat's last theorem](#) » that equation (6) lays Pythagorean triples line by line. So, d is the line index while i is the column index in Table 1, see Table 2 and 3 of this article. How are columns related to lines in Table 1? For answering this question, let's pose:

$$d=b, j=2i \quad (11)$$

By introducing (11) into (4) we get:

$$\begin{aligned}
 X_j &= (b + j)^2 - b^2 \\
 &= (d + 2i)^2 - d^2 \\
 &= 2 \frac{(d + 2i)^2 - d^2}{2} \\
 Y_j &= 2(b + j)b \\
 &= 2(d + 2i)d \\
 &= 2(d + 2i)d \\
 Z_j &= (b + j)^2 + b^2 \\
 &= 2 \frac{(d + 2i)^2 + d^2}{2}
 \end{aligned} \tag{12}$$

By renaming the X, Y and Z in equation (9) as  $X_i$ ,  $Y_i$  and  $Z_i$ , equation (12) gives :

$$\begin{aligned}
 Y_j &= 2X_i \\
 X_j &= 2Y_i \\
 Z_j &= 2Z_i
 \end{aligned} \tag{13}$$

When we keep  $i$  constant with  $d=1,2,3,\dots$ ,  $(X_i, Y_i, Z_i)$  creates the column  $i$  of Table 1. At the same time, because of equation (11),  $(Y_j, X_j, Z_j)$  creates the line  $j = 2i$  of Table 1.

Equation (13) shows that :

$$(Y_j, X_j, Z_j) = 2(X_i, Y_i, Z_i) \tag{14}$$

Then, the line  $2i$  equal two times the column  $i$ .

Equation (14) shows that, the triples of the column  $i$  are  $(X_i, Y_i, Z_i)$ , those of the lines  $j = 2i$  are  $(Y_j, X_j, Z_j)$ . So, the position of X and Y of the lines  $j = 2i$  are reversed with respect to those of the column  $i$ . This is an interesting feature of the table of basic Pythagorean triples. Equation (11) is the cause of the reversal.

For illustrating the reversal of X and Y, the column 1 of Table 1 is transposed into line and shown in Table 2. The line 2 of Table 1 is divided by 2 and shown in Table 3.

C.t1	C.t2	C.t3	C.t4	C.t5										
3	4	5	8	6	10	15	8	17	24	10	26	35	12	37

Table 2

L.t1	L.t2	L.t3	L.t4	L.t5										
4	3	5	6	8	10	8	15	17	10	24	26	12	35	37

Table 3

By comparing Table 2 with Table 3, we notice that the X and Y of the triple L.t1 are reversed with respect to those of the triple C.t1, while both are the same Pythagorean triples. In the same way, the triples L.t2 and C.t2 are the same triples with reversed X and Y. The same thing happens to the triples L.t3 vs C.t3, L.t4 vs C.t4 and L.t5 vs C.t5. These examples show well how the lines with index  $2i$  of Table 1 reverse the order of X and Y with respect to the column  $i$ .

For the sake of simplicity, we have created Table 4 to represent Table 1. Each cell of Table 4 contains only the Z component of a Pythagorean triple to represent this triple. Since Table 4 contains the same Pythagorean triples as Table 1, Table 4 possesses also the *Property 1*. So, Table 4 has the following property:

*Property 2: Table 4 contains all primitive Pythagorean triples.*

We have used the change of variables given in equation (11) to get (14). What if we use the change of variables  $d=b, j=2i-1$  to get odd line index? In this case,  $d=b, j=2i-1$  into equation (4) would give for Z:

$$\begin{aligned}
 Z &= (b + j)^2 + b^2 \\
 &= (d + 2i - 1)^2 + d^2
 \end{aligned} \tag{15}$$

Equation (15) does not correspond the Z in (9). So, this change of variables is invalid.

For illustrating equation (14), in Table 4 we have colored column 1 and line 2 in blue to highlight that line 2 equals two times column 1. In the same way, column 2 and line 4 are colored in red and column 3 and line 6 are colored in green. We see clearly that the colored lines equal two times the corresponding columns. In consequence, all lines with even index contain only multiple triples.

b→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
d↓																				
1	5	13	25	41	61	85	113	145	181	221	265	313	365	421	481	545	613	685	761	841
2	10	20	34	52	74	100	130	164	202	244	290	340	394	452	514	580	650	724	802	884
3	17	29	45	65	89	117	149	185	225	269	317	369	425	485	549	617	689	765	845	929
4	26	40	58	80	106	136	170	208	250	296	346	400	458	520	586	656	730	808	890	976
5	37	53	73	97	125	157	193	233	277	325	377	433	493	557	625	697	773	853	937	1025
6	50	68	90	116	146	180	218	260	306	356	410	468	530	596	666	740	818	900	986	1076
7	65	85	109	137	169	205	245	289	337	389	445	505	569	637	709	785	865	949	1037	1129

Table 4

For constructing the table of primitive Pythagorean triples we remove all the lines with even index from Table 4. The resulting table is Table 5 which contains only the lines whose index equals  $2i-1$ .

b→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
d↓																				
1	5	13	25	41	61	85	113	145	181	221	265	313	365	421	481	545	613	685	761	841
3	17	29	45	65	89	117	149	185	225	269	317	369	425	485	549	617	689	765	845	929
5	37	53	73	97	125	157	193	233	277	325	377	433	493	557	625	697	773	853	937	1025
7	65	85	109	137	169	205	245	289	337	389	445	505	569	637	709	785	865	949	1037	1129
9	101	125	153	185	221	261	305	353	405	461	521	585	653	725	801	881	965	1053	1145	1241
11	145	173	205	241	281	325	373	425	481	541	605	673	745	821	901	985	1073	1165	1261	1361
13	197	229	265	305	349	397	449	505	565	629	697	769	845	925	1009	1097	1189	1285	1385	1489
15	257	293	333	377	425	477	533	593	657	725	797	873	953	1037	1125	1217	1313	1413	1517	1625
17	325	365	409	457	509	565	625	689	757	829	905	985	1069	1157	1249	1345	1445	1549	1657	1769
19	401	445	493	545	601	661	725	793	865	941	1021	1105	1193	1285	1381	1481	1585	1693	1805	1921

Table 5

Let  $(X, Y, Z)$  be a Pythagorean triple. The triple  $(Y, X, Z)$  is the same Pythagorean triple as  $(X, Y, Z)$  except that the order of  $X$  and  $Y$  is reversed. If the triple  $(X, Y, Z)$  exists in Table 5, the reversed triple  $(Y, X, Z)$  does not appear in Table 5 because all Pythagorean triples with reversed  $X$  and  $Y$  are removed with the lines with even index. So, Table 5 has the following property:

*Property 3: If a Pythagorean triple exists in Table 5, it appears only once.*

Let's check if the Pythagorean triples in Table 5 respect the condition for primitive Pythagorean triples. The index of all lines in Table 5 equal  $j = 2i-1$ . From equation (3) we get :

$$a - b = j = 2i - 1 \quad (16)$$

$$a + b = 2b + 2i - 1 \quad (17)$$

So,  $a + b$  is odd for all Pythagorean triples in Table 5 and the condition 2 is respected. Because of equation (3), we have  $a > b > 0$  and the condition 1 is respected in Table 4. Since Table 5 is a subset of Table 4, the Pythagorean triples in Table 5 respect the condition 1 and 2.

#### 4. Sparse multiple triples

Now, let's search for multiple triples remained in Table 5. The values of  $Z$  equal  $(b + j)^2 + b^2$ , see (4). If  $b$  and  $j$  have a common divisor  $h$ , they can be expressed as:

$$b = hb' \text{ and } j = hj' \quad (18)$$

with  $b', j'$  and  $h$  integers.

Then,  $Z$  will be expressed as:

$$Z = h^2((b' + j')^2 + b'^2) \quad (19)$$

Since  $(b' + j')^2 + b'^2$  is the  $Z$  component of a Pythagorean triple, the  $Z$  given by equation (19) is that of a multiple triple. So, when  $b$  and  $j$  have a common divisor, the corresponding triple  $(X, Y, Z)$  is a multiple triple. Such triples are sparsely scattered in Table 5, we call them sparse multiple triples.

For finding sparse multiple triples we compute the greatest common divisor between  $b$  and  $j$  for all cells of Table 5. The resulting greatest common divisors are the number  $h$  in equation (18) and we put them in Table 6. If  $h > 1$  in a cell, the corresponding triple in Table 5 is a multiple triple and we color this cell in red.

b→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
d↓																				
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	3	1	1	3	1	1	3	1	1	3	1	1	3	1	1	3	1	1
5	1	1	1	1	5	1	1	1	1	5	1	1	1	1	5	1	1	1	1	5
7	1	1	1	1	1	1	7	1	1	1	1	1	1	7	1	1	1	1	1	1
9	1	1	3	1	1	3	1	1	9	1	1	3	1	1	3	1	1	9	1	1
11	1	1	1	1	1	1	1	1	1	1	11	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	13	1	1	1	1	1	1	1
15	1	1	3	1	5	3	1	1	3	5	1	3	1	1	15	1	1	3	1	5
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17	1	1	1
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	19	1

Table 6

Can Table 5 contain multiple triples other than sparse multiple triples? According to equation (19), the  $Z$  component of a sparse multiple triple has a divisor that equals the square of an integer. If the divisor of a  $Z$  is not the square of an integer, let it be  $k$ ,  $Z$  will be expressed as :

$$\begin{aligned}
 Z &= k((b' + j')^2 + b'^2) \\
 &= (b'\sqrt{k} + j'\sqrt{k})^2 + (b'\sqrt{k})^2
 \end{aligned}
 \tag{20}$$

Since  $b'\sqrt{k}$  and  $j'\sqrt{k}$  are not integer, they do not correspond to any cell of Table 5. So, Table 5 does not contain such multiple triples. Then, removing all the numbers in red from Table 5 removes all possible multiple triples, which gives Table 7 in which all cells corresponding to former multiple triples are blank. So, Table 7 has the following property:

*Property 4: Table 7 contains only primitive Pythagorean triples.*

b→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
d↓																				
1	5	13	25	41	61	85	113	145	181	221	265	313	365	421	481	545	613	685	761	841
3	17	29		65	89		149	185		269	317		425	485		617	689		845	929
5	37	53	73	97		157	193	233	277		377	433	493	557		697	773	853	937	
7	65	85	109	137	169	205		289	337	389	445	505	569		709	785	865	949	1037	1129
9	101	125		185	221		305	353		461	521		653	725		881	965		1145	1241
11	145	173	205	241	281	325	373	425	481	541		673	745	821	901	985	1073	1165	1261	1361
13	197	229	265	305	349	397	449	505	565	629	697	769		925	1009	1097	1189	1285	1385	1489
15	257	293		377			533	593		797		953	1037		1217	1313		1517		
17	325	365	409	457	509	565	625	689	757	829	905	985	1069	1157	1249	1345		1549	1657	1769
19	401	445	493	545	601	661	725	793	865	941	1021	1105	1193	1285	1381	1481	1585	1693		1921

Table 7

Let's check the Pythagorean triples in Table 7 with the conditions for primitive Pythagorean triples. Because of equation (3),  $a = b+j$  and the greatest common divisor between  $a$  and  $b$  is also  $h$ . As all  $Z$  corresponding to  $h > 1$  are removed, the greatest common divisor between the  $a$  and  $b$  for all the Pythagorean triples in Table 7 equals 1 and the condition 3 is respected. Since Table 7 is a subset of Table 5 which respect the conditions 1 and 2, the Pythagorean triples in Table 7 respect the conditions 1, 2 and 3.

Below, we show the correspondence between the 3 conditions for primitive triple and the 3 operations that create Table 7 :

1. All the Pythagorean triples of Table 4 are generated with  $a > b > 0$ . So, the condition 1 is respected.
2. All the lines with  $a + b$  even are removed from Table 4. So, all the lines in Table 5 have  $a + b$  odd and the condition 2 is respected.
3. All Pythagorean triples that have greatest common divisor of  $a$  and  $b$  bigger than 1 are removed from Table 5 to create Table 7. So, for all the Pythagorean triples in Table 7, the greatest common divisor of  $a$  and  $b$  equal 1 and the condition 3 is respected.

These 3 steps ensure that all Pythagorean triples in Table 7 are primitive. In addition, we get more information from the properties that we have derived above.

1. *Property 2: Table 4 contains all primitive Pythagorean triples.*  
As Table 7 equals Table 4 minus all the multiple triples in the lines with even index and all the sparse multiple triples, Table 7 contains all primitive Pythagorean triples.
2. *Property 3: If a Pythagorean triple exists in Table 5, it appears only once.*  
As Table 7 equals Table 5 minus all the sparse multiple triples, every primitive Pythagorean triple appears once in Table 7.
3. *Property 4: Table 7 contains only primitive Pythagorean triples.*

So, Table 7 contains all primitive Pythagorean triples and only primitive Pythagorean triples. Every primitive Pythagorean triple appears once. Table 7 is well ordered, then primitive Pythagorean triples are well classified in Table 7.

We notice that all numbers in Table 7 are odd, that is, all primitive Pythagorean triples have odd Z. So, the X and Y of primitive Pythagorean triples are one even, one odd.

Figure 1 is the scatter plot of the primitive Pythagorean triples in Table 7. Each black dot represents a primitive Pythagorean triple while the locations corresponding to multiple triples are white. Figure 1 shows that all X are smaller than 1200 and all Y are smaller than 1600, which is consistent with the value of Z contained in the last cell of Table 7, 1921.

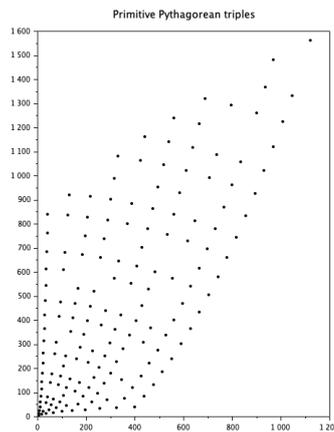


Figure 1

## 5. Properties of basic Pythagorean triples

### a) Primitive Pythagorean triples with equal Z

In Table 7 we see that some numbers are colored in blue and others in magenta. In fact, the blue and magenta numbers are the same numbers. We have classified all the numbers of Table 7 in increasing order and put them in Table 8 where identical numbers are colored in red. We notice that identical numbers appear in couples which means that the maximal number of primitive Pythagorean triples that share the same value of Z is 2.

5	13	17	25	29	37	41	53	61	65	65	73	85	85	89	97	101	109
113	125	137	145	145	149	157	169	173	181	185	185	193	197	205	205	221	221
229	233	241	257	265	265	269	277	281	289	293	305	305	313	317	325	325	337
349	353	365	365	373	377	377	389	397	401	409	421	425	425	433	445	445	449
457	461	481	481	485	493	493	505	505	509	521	533	541	545	545	557	565	565
569	593	601	613	617	625	629	653	661	673	685	689	689	697	697	709	725	725
745	757	761	769	773	785	793	797	821	829	841	845	853	865	865	881	901	905
925	929	937	941	949	953	965	985	985	1009	1021	1037	1037	1069	1073	1097	1105	1129
1145	1157	1165	1189	1193	1217	1241	1249	1261	1285	1285	1313	1345	1361	1381	1385	1481	1489
1517	1549	1585	1657	1693	1769	1921											

Table 8

The point that represents a Pythagorean triple in a (X, Y) coordinates system is at the intersection of two parabolas which are defined in «[Parabolic patterns](#) in the [scatter plot of Pythagorean triples](#)». We call these parabolas Pythagorean parabolas. If two primitive Pythagorean triples share the same value of Z, they sit on the same circle centered at the origin of the coordinates system and the radius of the shared circle equals Z.

Let (X<sub>1</sub>, Y<sub>1</sub>) represent a first primitive Pythagorean triple and (X<sub>2</sub>, Y<sub>2</sub>) a second. If these two triples share the same value Z, the point (X<sub>1</sub>, Y<sub>1</sub>) is at the intersection of three curves, two Pythagorean parabolas and the shared circle. The point (X<sub>2</sub>, Y<sub>2</sub>) is at the intersection of two other Pythagorean parabolas and the same shared circle. Both points have integer coordinates X and Y, the circle has integer radius Z, both (X<sub>1</sub>, Y<sub>1</sub>, Z) and (X<sub>2</sub>, Y<sub>2</sub>, Z) are coprime triples.

In Figure 2 we have plotted all the circles which pass through two different primitive triples, that is, the circles that pass through two black dots.

When multiple triples are included, there are cases where three different Pythagorean triples share the same value of Z with one being multiple triple. It would be interesting to determine whether only 2 primitive Pythagorean triples share a circle is a general property for primitive triples or not. You may find interesting information here: [MULTIPLE PYTHAGOREAN NUMBER TRIPLES](#).

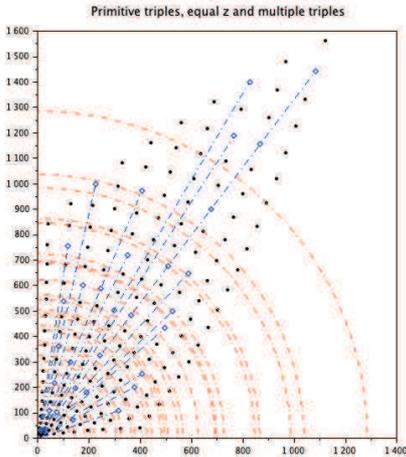


Figure 2

**b) Sparse multiple triples and their corresponding primitive triples**

If we know the multiplier of a multiple triple, we can derive the original primitive triple. Table 5 contains the Z components of Pythagorean triples. A cell of Table 6 contains the greatest common divisor *h* between the column index *b* and the line index *j* of the corresponding cell in Table 5. The square *h*<sup>2</sup> equals the multiplier for the multiple triple in this cell, see equation (19). So, we can derive the original primitive triples of the multiple triple using *h*<sup>2</sup>:

$$\text{Original primitive triple} = \frac{\text{Multiple triple}}{h^2} \quad (21)$$

For example, the cell (*b*=12, *j*=15) in Table 5 contains 873 which is the Z component of a multiple triple. The column and line indexes of this cell are 12 and 15 respectively. The corresponding cell in Table 6 contains 3, which is the number *h*. So, the column and line indexes of the cell that contains the Z of the original primitive triples are *b*=12/3, *j*=15/3 which points to the cell (*b*=4, *j*=5) in Table 5. This cell contains 97 which equals 873/3<sup>2</sup>. This shows that the cells of Table 5 and Table 6 allow to identify the original primitive triples for all sparse multiple triples.

For giving a visual image of the sparse multiple triples, we have plotted in Figure 2 the straight lines that link all sparse multiple triples with their original primitive triples. The diamond markers represent sparse multiple triples and the black dots represent primitive triples.

### c) Distribution of sparse multiple triples

In Table 7 the void cells that represent sparse multiple Pythagorean triples are rather regularly distributed. How are they distributed on large scale? In Figure 3 we have plotted the scatter plot of all the sparse multiple triples for  $b < 200$  and  $j < 400$  in a Cartesian coordinates system where the column indexes  $b$  are on the x axis and the line indexes  $j$  on the y axis. We see that sparse multiple triples are pretty evenly distributed in Figure 3. We see also straight line patterns in this scatter plot.

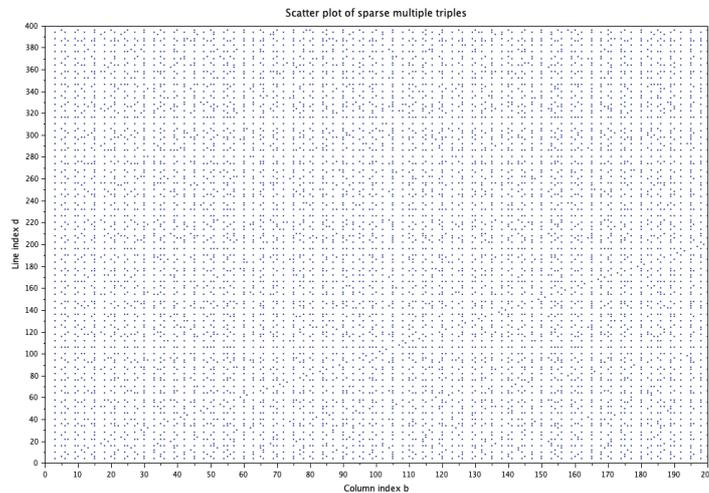


Figure 3

## 6. Discussion

In this article we have created the table that classifies all primitive triples. For doing so, we have started by creating the table that classifies basic Pythagorean triples. Then, we have removed all the lines with even index. From the resulting table we have removed all the sparse multiple triples. The remaining table is a table that classifies all possible primitive triples.

We have discussed three properties of basic Pythagorean triples. For example, two primitive triples can share a same value of  $Z$ . Also, sparse multiple triples are rather evenly distributed on large scale.

Finally, I have pondered about whether we can find a practical use for the classified primitive triple table. One possible use could be in cryptography. We have shown that the  $Z$  component of a primitive triple can be easily generated from two parameters,  $b$  and  $j$ . But we cannot easily work out the original value of  $b$  and  $j$  from a given  $Z$  because we have two unknowns,  $b$  and  $j$ , for only one equation,  $Z = (b + j)^2 + b^2$ . For example, what are the values of  $b$  and  $j$  that generate the primitive Pythagorean triple ( $X=14719726793\dots$ ,  $Y=518663627978\dots$ ,  $Z=518872459612805$ )?

The heart of the RSA cryptosystem is to find two prime integers  $p$  and  $q$  so large that the factoring of the product  $p \cdot q$  is very hard. With large primitive Pythagorean triples, it is also very hard to work out the original  $b$  and  $j$  from a given  $Z$ . So, I think that the three integers  $b$ ,  $j$  and  $Z$  could work at the place of  $p$ ,  $q$  and  $p \cdot q$  for an alternate cryptosystem similar to RSA. In addition, large prime integers are difficult to find while  $b$  and  $j$  can be any integers, which would make the alternate cryptosystem simpler and cheaper than the RSA cryptosystem. The fact that the integers  $X$ ,  $Y$  and  $Z$  are coprime could be useful for cryptography too.

But I am not a cryptographer and cannot evaluate the validity of this idea. Would any cryptographer be interested?