European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 8, 2020

TWO EXCEPTIONAL PYTHAGOREAN TRIANGLES: A KEY FOR ENCRYPTION

Mita Darbari
Department of Mathematics, St. Aloysius College (Autonomous), Jabalpur, Madhya Pradesh, India

Prashans Darbari and Sarvadev Kumar
Department of Mathematics, X Semester BS-MS Programme, Indian Institute of Science Education & Research, Mohali, Punjab, India

Arpita Sen , Megha Tamrakar and Vibha Sahu
Department of Mathematics, M.Sc. III Semester, St. Aloysius College (Autonomous), Jabalpur, Madhya Pradesh, India

Abstract - ***Two remarkably special Pythagorean Triangles are found with their perimeter as eleventh power. These are exceptional in the sense that with the given constraint that their perimeter should be of the eleventh power, do not comply with Euclidean formula of obtaining primitive Pythagorean Triangles. Interesting properties of these Pythagorean Triangles are observed. An application of their use in cryptography is also proposed.***

Keywords- Euclidean formula, Mathematica, Opposite Parity, Primitive Pythagorean Triangle, Undecic.

1.INTRODUCTION

The search for special Pythagorean Triangles has held in fascination those who love numbers. Darbari and Darbari (2019) have found out special Pythagorean Triangles with their sum of two legs as undecic and their application, while Darbari et al. (2019) and Darbari et al. (2020) have suggested alternative methods to apply these.

In this paper, exploring the problem further, an attempt has been made to find Pythagorean Triangles with their perimeter as eleventh power of a positive integer. These exceptional triangles are also applied in cryptography in a unique way.

2. DEFINITIONS

2.1 Pythagorean Equation: A quadratic equation

$$X^2 + Y^2 = Z^2$$

is called Pythagorean equation (Robbins, 2006) after the famous mathematician and philosopher Pythagoras. It is one of the most important equations of the world in all times.

2.2 Pythagorean Triangle (Niven et al., 2018)**:** A right angled triangle with sides X, Y and Z is called Pythagorean Triangle if X, Y and Z are positive integers. X and Y are called its legs and Z is called its hypotenuse. Pythagorean triangles satisfy Pythagorean equation $X^2 + Y^2 = Z^2$.

If X, Y and Z satisfy Pythagorean equation, then aX, aY and aZ also satisfy it, where a is positive integer. Therefore, one Pythagorean Triangle can generate infinite Pythagorean triangles.

2.3 Primitive Pythagorean Triangle: A Pythagorean Triangle is said to be primitive if X, Y and Z are co-primes, i.e., their greatest common divisor is one. Or, we can say, GCD (X, Y, Z) = 1.

2.4 Opposite Parity: Two natural numbers m and n are called of opposite parity if one of them is even and other is odd, i.e., $m \not\equiv n \ (mod 2)$.

2.5 Euclidean Formula (Posamentier, 2010)**:** The positive primitive solutions of Pythagorean Equation with Y even are

$$X = m^2 - n^2, \qquad Y = 2mn, \qquad Z = m^2 + n^2,$$

where m and n are arbitrary integers of opposite parity with $m > n > 0$ and $(m, n) = 1$.

2.6 Undecic: Of the eleventh degree.

3 METHOD OF ANALYSIS

Let a Pythagorean Equation be given by

$$X^2 + Y^2 = Z^2 \tag{1}$$

We seek to find its solution with the constraint that its perimeter should be a positive integer which is eleventh power of some natural number, i.e.,

$$X + Y + Z = \alpha^{11},\ \alpha \in N \tag{2}$$

The Primitive solutions of (1) is given by Euclidean formula (2)

$$X = m^2 - n^2,\ Y = 2mn,\ Z = m^2 + n^2, \tag{3}$$

where m and n are arbitrary integers of opposite parity with $m > n > 0$ and $(m, n) = 1$.

Substituting the values of X, Y and Z given by equation (3) in equation (2), we get the following undecic equation

$$m^2 + 2mn = \alpha^{11} \tag{4}$$

Solving equation (4) by software *Mathematica*, using the following command

$$Reduce[m^2 + 2mn - \alpha^{11} == 0, \{m, n, \alpha\}]$$

We get eleven solutions as follows:

$$\alpha = (m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = -(-1)^{\frac{1}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = (-1)^{\frac{2}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = -(-1)^{\frac{3}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = (-1)^{\frac{4}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = -(-1)^{\frac{5}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = (-1)^{\frac{6}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = -(-1)^{\frac{7}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = (-1)^{\frac{8}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = -(-1)^{\frac{9}{11}}(m^2 + 2mn)^{\frac{1}{11}},$$

$$\alpha = (-1)^{\frac{10}{11}}(m^2 + 2mn)^{\frac{1}{11}}.$$

Seeking the integral solutions of equation (4), using FindInstance command of *Mathematica*, we get only two solutions for α as given by Table 1, when $m < 10^{21}\ and\ n < 10^{21}$!

Table 1: Values of *m, n* and *α*.

M	***n***	***α***
31381059609	18618940391	90
285311670611	86192514733	132

It is obvious from Table 1 that both the values of *m* and *n* are odd. Therefore, they cannot be of opposite parity. Although m and n are relatively prime, the values of *X*, *Y* and *Z* obtained from them are not co-primes as their GCD is two. The two Pythagorean Triangles are presented in Table 2. Verification of $X^2 + Y^2 = Z^2$ is shown by Table 3 and Table 4 and $X + Y + Z = \alpha^{11}$ is verified in Table 5.

Table 2: Values of X, Y and Z

$X = m^2 - n^2$	$Y = 2mn$	$Z = m^2 + n^2$
638105960900000000000	1168564156532777534238	1331435843467222465762
7397359979084133905203 2	4918346074527092122372 6	8883189898283818317461 0

Table 3: Values of X^2 and Y^2

X^2	Y^2
407179217336112328810000000000000000000 0	136554218793316179554903104724472326224 06 44
547209346601556180074613415994703410440 33 29024	241901281088160564176930356558120519334 53 23076

Table 4: Verification of $X^2 + Y^2 = Z^2$

$X^2 + Y^2$	Z^2
177272140526927412435903104724472326224 06 44	177272140526927412435903104724472326224 06 44
789110627689716744251543772552823929774 86 52100	789110627689716744251543772552823929774 86 52100

Table 5: Verification of $X + Y = \alpha^{11}$

$X + Y + Z$	α^{11}
3138105960900000000000	3138105960900000000000
21198895951895044345036 8	21198895951895044345036 8

4 RESULTS AND OBSERVATIONS

1. *m* and *n* are both odd which is an exception to Euclidean Formula.

2. (*X*, *Y*, *Z*) = 2 which is again an exception to Euclidean formula. The question is, whether {*X*, *Y*, *Z*} is primitive? Yes, they are, as they satisfy $X + Y + Z = \alpha^{11}$,

Although (*X/2*, *Y/2*, *Z/2*) satisfies equation (1) while no α ∈ N satisfy $\{X + Y + Z\}/2 = \alpha^{11}$. Therefore, (*X/2*, *Y/2*, *Z/2*) cannot be a primitive solution of given problem.

3. $X + Y + Z = 0[\text{mod}20]$

4. $4X + Y + 4Z = 0[\text{mod}6]$

5. $X + Y + Z = 0[\text{mod}2^{10}\alpha]$

5 APPLICATION IN CRYPTOGRAPHY

Number theory plays an important role in cryptography. Now-a-days most of the work is done online. Security online is a major concern for all of us. Darbari and others [1][2][3] have given novel methods for encrypting the messages. We propose yet another method for encrypting and decrypting of messages using these exceptional Pythagorean triangles. These messages can be deciphered only when one has a knowledge of these exceptional Pythagorean triangles.

6. ALGORITHM

We take the first triple (X, Y, Z) to code numerals, special characters and gap between the two words. The second triple (X, Y, Z) is used to code alphabets. We code numerals from Y, special characters from Z and gap between the two words from X.

6.1 Construction Of Codes For Gap Between The Words

We take three sets of three digits from left to right of X of first Pythagorean triangle to obtain three codes for gaps between the words. It is done as follows:

X = 638105960900000000000, Code 638 105 960 900000000000

From left to right I II III

Table 6: Codes for gap between the words

S.N.	X	Code 1	Code 2	Code 3	Code for
1	638105960900000000000	638	105	960	Gap

For the first gap, we take code 1, for the second gap, take code two and for the third gap, take code 3. If there are more gaps in the message, then these gaps can be repeated in the same order.

6.2 Construction Of Codes For Numerals

To obtain the codes for 1, 2, 3, 4, 5, 6, 7, 8, 9 and 0, we take Y, 2Y, 3Y, 4Y, 5Y, 6Y, 7Y, 8Y, 9Y, 11Y respectively. We again take three sets of three digits from left to right of multiple of Y to get three codes for each number from 0 to 9. If any three digits number is repeated, we leave that number and take the next set. Repeated numbers are shown in bold. These codes are presented in Table 7.

Table 7: Codes for Numbers 0-9

S.N.	Multiple of Y	Code 1	Code 2	Code 3	Number
1.	Y = 1168564156532777534238	116	856	415	1
2.	2Y = 2337128313065555068476	233	712	831	2
3.	3Y = 3505692469598332602714	350	569	246	3
4.	4Y = 4674256626131110136952	467	425	662	4
5.	5Y = 5842820782663887671190	584	282	078	5
6.	6Y = 7011384939196665205428	701	138	493	6
7.	7Y = 8179949095729442739666	817	994	909	7
8.	8Y = 9348513252262220273904	934	851	325	8
9.	9Y = **105**17077408794997808142	170	774	087	9
10.	11Y = 12854205721860552876618	128	542	057	0

6.3 Construction For The Codes Of Special Characters

For coding predecided special characters, multiple of Z of first exceptional Pythagorean triangle is chosen, as we have done in for coding numbers 0-9 in Table 7. Repeated numbers are shown in red in bold. We take the next set of numbers for repeated code. It is done as follows:

Table 8: Codes for Special Characters

S.N.	Multiples of Z	Code 1	Code 2	Code 3	Character
1.	Z = 133143**584**3467222465762	133	143	346	.
2.	2Z = 2662871686934444931524	266	287	168	,
3.	3Z = 3994307530401667397286	399	430	753	:
4.	4Z = 5325743373868889863048	532	574	337	;
5.	5Z = 6657179217336112328810	665	717	921	“
6.	6Z = 7988615060803334794572	798	861	506	‘

7.	7Z = 9320050904270557260334	932	005	090	?
8.	8Z = 10651486747737779726096	106	514	867	-
9.	9Z = 11982922591205002191858	119	829	225	!
10.	11Z = 14645794278139447123382	146	457	942	(
11.	12Z = 15977230121606669589144	159	772	301	)
12.	13Z = 17308665965073892054906	173	086	659	/
13.	14Z = 18640101808541114520668	186	401	018	=

6.4 Construction For The Codes Of Alphabets

To obtain the codes for alphabets a-z, we use multiples of X, Y, Z from second Pythagorean triangle. For a, b and c, we take X, Y and Z respectively. For d, e and f, we take 2X, 2Y and 2Z in that order. Similarly, for next set of alphabets, we take 3X, 3Y and 3Z. Continuing this way, we obtain the codes of all the alphabets a to z. As before, repeated three digits numbers are left and the next three digits number is taken.

These codes are shown in Table 9.

Table 9: Codes for Alphabets

S.N.	Multiples of X, Y, Z	Code 1	Code 2	Code 3	Alphabet
1.	X = 73973599790841339052032	739	735	997	A
2.	Y = 49183460745270921223726	491	834	607	B
3.	Z = 88831898982838183174610	888	318	989	C
4.	2X = 147947199581682678104064	147	947	199	D
5.	2Y = 98366921490541842447452	983	669	214	E
6.	2Z = 17766379656766366349220	177	663	797	F
7.	3X = 221920799372524017156096	221	920	799	G
8.	3Y = **147**550382235812763671178	550	382	235	H
9.	3Z = **266**495696948514549523830	495	696	948	I
10.	4X = 295894**399**163365356208128	295	894	163	J
11.	4Y = 196733842981083684894904	196	733	842	K
12.	4Z = 355327595931352732698440	355	327	595	L
13.	5X = 369**867**998954206695260160	369	998	954	M
14.	5Y = 245917303726354606118630	245	917	303	N
15.	5Z = 444**159**494914190915873050	444	494	914	O
16.	6X = 443841598745048034312192	443	841	598	P
17.	6Y = **295**100764471625527342356	100	764	471	Q
18.	6Z = **532**991393897029099047660	991	393	897	R
19.	7X = 517815198535889373364224	517	815	198	S
20.	7Y = 344284**225**216896448566082	344	284	216	T
21.	7Z = 621823292879867282222270	621	823	292	U
22.	8X = 591788**798**326730712416256	591	788	326	V
23.	8Y = **393467**685962167369789808	685	962	167	W
24.	8Z = 710655191862705465396880	710	655	191	X
25.	9X = **665**762398117572051468288	762	398	117	Y
26.	9Y = 442651**146**707438291013534	442	651	707	Z

6.5 Method For Encryption

To encrypt a message, we follow the following procedure:

1. There are three codes for each alphabet. First code is used for a letter which occurs for the first time. If it occurs for the second time, second code is used and if it occurs for the third time, third code is used.

If the letter occurs for the fourth time, then again first code is used. That is, after three codes are exhausted, these codes are taken again in the same order.

2. For each special character again three codes are given. As in the case of alphabets, first code is taken for first occurrence of special character, second code is taken for second occurrence for the same special character and the third code is used if the same special character occurs for the third time. These codes are repeated in the same order if there are more than three occurrences.
3. To encrypt numbers, we follow the same steps as we do for alphabets and special characters.
4. To differentiate between two words, a blank space is given and its codes are given as gaps. After encryption of first word, we give first code of gap, after second word, second code of gap and after third word, third code of gap is given. If there are more words, then these codes for gaps are repeated in same order.
5. In the end of each sentence, we put code for full stop. Since there are only three codes for full stop, these codes are repeated in the same order if there are more than three sentences.

7 EXAMPLE FOR ENCRYPTION

Let us encrypt the following message:

Hardy came in a taxicab with number 1729, and saying that it seemed to him a rather dull number—to which Ramanujan replied: “No, it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways”.

Writing the codes from Table 6, 7, 8 and 9, we get following table:

Table 10: Codes for Message

1. Hardy came in a

Item	H	a	r	d	y	Gap	c	a	m	e	Gap	i	n	Gap	a	Gap
Code No.	1	1	1	1	1	1	1	2	1	1	2	1	1	3	3	1
Code	550	739	991	147	762	638	888	735	369	983	105	495	245	960	997	638

2. taxicab with

Item	t	a	x	i	c	a	b	Gap	w	i	t	h	Gap
Code No.	1	1	1	2	2	2	1	2	1	3	2	2	3
Code	344	739	710	696	318	735	491	105	685	948	284	382	960

3. number 1729,

Item	n	u	m	b	e	r	Gap	1	7	2	9	,	Gap
Code No.	2	1	2	2	2	2	1	1	1	1	1	1	2
Code	917	621	998	834	669	393	638	116	817	233	170	266	105

4. and saying that

Item	a	n	d	Gap	s	a	y	i	n	g	Gap	t	h	a	t	Gap
Code No.	3	3	2	3	1	1	2	1	1	1	1	3	3	2	1	2
Code	997	303	947	960	517	739	398	495	245	221	638	216	235	735	344	105

5. it seemed to him

Item	I	t	Gap	s	e	e	m	e	d	Gap	t	o	Gap	h	i	m
Code No.	2	2	3	2	3	1	3	2	3	1	3	1	2	1	3	1
Code	696	284	960	815	214	983	954	669	199	638	216	444	105	550	948	369

6. a rather dull

Item	Gap	a	Gap	r	a	t	h	e	r	Gap	d	u	l	l	Gap

Code No.	3	3	1	3	1	1	2	3	1	2	1	2	1	2	3
Code	960	997	638	897	739	344	382	214	991	105	147	823	355	327	960

7. number-to which

Item	n	u	m	b	e	r	—	t	o	Gap	w	h	i	c	h	Gap
Code No.	2	3	2	3	1	2	1	2	2	1	2	3	1	3	1	2
Code	917	292	998	607	983	393	106	284	494	638	962	235	495	989	550	105

8. Ramanujan replied

Item	R	a	m	a	n	u	j	a	n	Gap	r	e	p	l	i	e	d
Co.No.	3	2	3	3	3	1	1	1	1	3	1	2	1	3	2	3	2
Code	897	735	954	997	303	621	295	739	245	960	991	669	443	595	696	214	947

9. : “No, it is a

Item	:	Gap	“	N	o	,	Gap	i	t	Gap	i	s	Gap	a	Gap
Code No.	1	1	1	2	3	2	2	3	3	3	1	3	1	2	2
Code	399	638	665	917	914	287	105	948	216	960	495	198	638	735	105

10. very interesting

Item	v	e	r	y	Gap	i	n	t	e	r	e	s	t	i	n	g
Code No.	1	1	2	3	3	2	3	1	2	3	3	1	2	3	1	2
Code	591	983	393	117	960	696	303	344	669	897	214	517	284	948	245	920

11. number; it

Item	Gap	n	u	m	b	e	r	;	Gap	i	t	Gap
Code No.	1	2	2	1	1	1	1	1	2	1	3	3
Code	638	917	823	369	491	983	991	532	105	495	216	960

12. is the smallest

Item	i	s	Gap	t	h	e	Gap	s	m	a	l	l	e	s	t	Gap
Code No.	2	2	1	1	2	2	2	3	2	3	1	2	3	1	2	3
Code	696	815	638	344	382	669	105	198	998	997	355	327	214	517	284	960

13. number

Item	n	u	m	b	e	r	Gap
Code No.	3	3	3	2	1	2	1
Code	303	292	954	834	983	393	638

14. expressible

Item	e	x	p	r	e	s	s	i	b	l	e
Code No.	2	2	2	3	3	2	3	3	3	3	1
Code	669	655	841	897	214	815	198	948	607	595	983

15. as the sum of

Item	Gap	a	s	Gap	t	h	e	Gap	s	u	m	Gap	o	f	Gap
Code No.	2	1	1	3	3	3	2	1	2	1	1	2	1	1	3
Code	105	739	517	960	216	235	669	638	815	621	369	105	444	177	960

16. two cubes in two

Item	t	w	o	Gap	c	u	b	e	s	Gap	i	n	Gap	t	w	o	Gap

Code No.	1	3	2	1	1	2	1	3	3	2	1	1	3	2	1	3	1
Code	344	167	494	638	888	823	491	214	198	105	495	245	960	284	962	914	638

17. different ways".

Item	d	i	f	f	e	r	e	n	t	Gap	w	a	y	s	"	.
Code No.	3	2	2	3	1	1	2	2	3	2	2	2	1	1	2	1
Code	199	696	663	797	983	991	669	917	216	105	962	735	762	517	717	133

The receiver gets the converted message in the number codes as
5507399911477626388887353699831054952459609976383447397106963187354911056859482843829
6091762199883466939363811681723317026610599730394796051773939849524522163821623573534
4105696284960815214983954669199638216444105550948369960997638897739344382214991105147
8233553279609172929986079833931062844946389622354959895501058977359549973036212957392
4596099166944359569621494739963866591791428710594821696049519863873510559198339311796
0696303344669897214517284948245920638917823369491983991532105495216960696815638344382
6691051989989973553272145172849603032929548349833936386696558418972148151989486075959
8310573951796021623566963881562136910544417796034416749463888882349121419810549524596
028496291463819969666379798399166991721610596273576251771713

9. CONCLUSION

The existence of these exceptional Pythagorean Triangles shows that Euclidean formula for obtaining primitive Pythagorean Triangles is valid only for the Pythagorean Equation $X^2 + Y^2 = Z^2$. But, if any constraint is added, like in this case, $X + Y + Z = \alpha^{11}$, we may obtain primitive Pythagorean Triangles which do not comply with Euclidean formula. These triangles can be used in another way to encrypt the messages so that no code is repeated and our message become totally secure.

10. FUTURE SCOPE

The existence of many more such exceptional Pythagorean Triangles may be explored and their applications can be sought for.

11. CONFLICT OF INTEREST: NA

REFERENCES

- Darbari, M. & Darbari, P. (2019). Special pythagorean with sum of their two legs as undecic. International Journal of Innovative Technology and Exploring Engineering, 8(11), 2019-2023.
- Darbari, M., Darbari, P., Nema, S., Sahu, M. & Soni, R. (2019). Fortifying the messages. International Journal of Scientific Technology and Research, 8(12), 544–552.
- Darbari, M., Darbari, P., Singh, A., Uikey, J. & Irshad, M. (2020). Special pythagorean triangles and cryptography. International Journal of Scientific Technology and Research, 9(3), 1966-1968.
- Niven, I., Zuckerman, H.S. & Montgomery, H.L. (2018). An Introduction to the Theory of Numbers. Wiley India, New Delhi, p. 231.
- Posamentier, A.S. (2010). The Pythagorean Theorem: The Story of its Power and Beauty. Prometheus Books, New York, pp. 127-128.
- Robbins, N. (2006). Beginning Number Theory. Jones and Bartlett, Sudbury, p. 2.