SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Pythagorean triples and congruent numbers

av

Vinicius Rocha

2018 - No K21

Pythagorean triples and congruent numbers

Vinicius Rocha

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torbjörn Tambour

2018

Pythagorean triples and congruent numbers

Vinicius Rocha

June 6, 2018

Acknowledgement

I offer my sincerest gratitude to my supervisor Torbjörn Tambour who throughout this study was always attentive, helpful and very patient. I also would like to thank him for all the work-hours from his busy schedule he gave up in order to monitor the work presented here.

Yours sincerely

Vinicius Rocha

Abstract

One of the most known and important geometric proposition within mathematics is the one called Pythagoras theorem, Throughout the years it has been the theme of study among prominent mathematicians. This paper will focus on explaining methods that can be used to generate non-proportional triples that satisfy the Pythagoras equation $a^2 + b^2 = c^2$, where a, b, and c are integers. Furthermore, we will extend our study by branching into the the concept called congruent numbers, which is the study of the area of a right-angled triangle.

Keywords: Primitive, co-prime, triples, congruent, parity

Contents

1 Pythagorean theorem

1.1 Introduction

The impact that the Pythagoras theorem has had within mathematics cannot be overstated. Some people would say that the Pythagoras theorem is one of geometry's most influential proposition[1] . This theorem has found its way into various fields of science and calculations and it is also known by different names such as Euclid I 47 because it is included in the Book I of Euclid's Elements, proposition 47. Although the name is giving credit to the Greek philosopher, and Mathematician Pythagoras as the one who discovered it, it has been proven that this geometrical relation was known even to the Babylonians thousands of years before Pythagoras. The tablet below is called Plimpton 322, it is a list of Pythagorean triples believed to be dated about 1800 BC. The tablet of four columns and fifteen rows shows triples that satisfies the Pythagorean equation $a^2 + b^2 = c^2$.

Plimption 322

In this paper we will focus our attention on the study of the so-called Primitive triples. The primitive set (a, b, c) is the same as Pythagoras triples (a, b, c) satisfying the equation $a^2 + b^2 = c^2$, but have no common factor among them. A triple with a common factor d is simply a scalar multiple of

[1]Maor (2007)

another triple, it means that to find all Pythagorean triples is equivalent to find all solutions with no common divisor.

1.2 The Theorem

The Pythagorean theorem asserts that in a right triangle the length of side c in Figure 1, squared, is equal to the sum of the squares of a and b. The opposite leg c is known as hypotenuse while the other two legs as catheter. Algebraically we say

$$a^2 + b^2 = c^2 \tag{1-1}$$

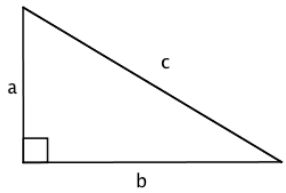


Figure 1: Right Triangle

Definition 1.1. *Any set of three positive integers that satisfies (1-1) is called a Pythagorean triple.*

Example 1.1. $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$ are Pythagorean triples since

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2$$

$$7^2 + 24^2 = 49 + 576 = 625 = 25^2$$

Take notice that if (a, b, c) is a Pythagorean triple, then so is (ta, tb, tc) where t is any positive integer, however (ta, tb, tc) forms a triangle that is similar to (a, b, c), hence a triple with a common divisor t is simply proportional to the triple without it.

Triples that satisfy (1-1) that are not three integers cannot be a Pythagorean triple. For instance, if $a = 1$ and $b = 1$, then $c = \sqrt{2}$, but since $c \notin Z$, then (a, b, c) is not a Pythagorean triple

1.2.1 Integer formula

In one of Proclus comments on the book Euclid's Element he tells us that Pythagoras and Platon knew varieties of triples yielded by the form[2]

$$a = 2n + 1, b = 2n^2 + 2n, c = 2n^2 + 2n + 1 \quad \text{where } n \,\epsilon\, N. \tag{1-2}$$

We do not know, however, exactly how these triples were found. It says, of unknown sources, that the equation was interpreted as $c^2 - b^2 = a^2$, the subtraction of a small square from a bigger square must result in a square. The bigger square c^2 having the side lengths say $n + 1$, and $a = n$; implies that b must be squared.

In Table 1 by letting n go from 1 to 5, we see that (1-2) yields triples.

n	2n+1	$2n^2 + 2n$	$2n^2 + 2n + 1$
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61

Table 1 : Pythagorean triples

Theorem 1.1. *The numbers* $a = 2n + 1, b = 2n^2 + 2n, c = 2n^2 + 2n + 1$ *satisfies (1-1)*

Proof. We substitute a and b according to (1-1) to see the left side it is equal to right side c according to (1-1)

$$(2n + 1)^2 + (2n^2 + 2n)^2 =$$

$$(4n^2 + 2n + 2n + 1) + (4n^4 + 4n^3 + 4n^3 + 4n^2) =$$

$$4n^4 + 8n^3 + 8n^2 + 4n + 1$$

the right side of the equation is:

$$(2n^2 + 2n + 1)^2 = 4n^4 + 4n^3 + 2n^2 + 4n^3 + 4n^2 + 2n + 2n^2 + 2n + 1) =$$

[2]Lundström (2008, p.112)

$$= 4n^4 + 8n^3 + 8n^2 + 4n + 1$$

□

When observing (1-2) it is possible to notice a few things. Two legs of which one is the hypotenuse have to be odd numbers while the remaining leg is even. Another thing is the fact that the hypotenuse extends the larger leg by one. Therefore the formula does not find all valid Pythagoras triples since there are triples such as (8,15,17) where the hypotenuse extends the larger leg by two.

2 Primitive triples

2.1 What is a primitive triple?

Earlier we said that if (a, b, c) satisfies (1-1) then (ta, tb, tc) also does (where $t \epsilon N$). Therefore, it is sufficient for us to analyze triples where the greatest common divisor is 1; otherwise we could simply cancel the equation by the common divisor t^2. The study of triples a, b and c that are co-prime leads us to the concept called *Primitive Triples*. Let us define and look at some characteristics of a co-prime set (a, b, c)

Definition 2.1. *Any set of three positive integers co-prime, i.e GCD(a,b,c)=1, integers that satisfies (1-1) is called primitive Pythagorean triple.*

The definition of a primitive triples opens the way for us to make a few observations on certain attributes of a, b and c.

Lemma 2.1. *For a primitive solution any pair of the numbers a, b and c must be relatively prime. If (a, b, c) are primitive triple then $GCD(a, b) = GCD(a, c) = GCD(b, c) = 1$.*

Proof. Suppose that (a, b, c) are co-prime and that $GCD(a, b) > 1$. Let p be a prime number that divides $GCD(a, b)$. We consequently have that $p|a$ and $p|b$ and considering (1-1) it follows that $p|c^2$. We then know that $p|c$ which means that $p|GCD(a, b, c)$; this contradicts itself since (a, b, c) are co-prime. □

Lemma 2.2. *The square of an odd number is congruent to 1 mod 4. If the number squared is even, then it is congruent to 0 mod 4.*

Proof. **even integer:** $a = 2k \Rightarrow a^2 = 4k^2 \equiv 0 \bmod 4 \qquad k \epsilon N$
odd integer: $a = 2k + 1 \Rightarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \bmod 4 \qquad k \epsilon N$ □

Lemma 2.3. *In a primitive solution a, b and c the numbers a and b cannot both be odd. Furthermore, c must be odd.*

Proof. If a and b are both even numbers then the $GCD(a, b) \neq 1$ thus it is not a primitive solution according to Lemma 2.1. If a and b are both odd numbers then $a^2 \equiv 1 \bmod 4$, and $b^2 \equiv 1 \bmod 4$. According to what we've established above, any integer squared either leaves remainder 0 or 1 when divided by 4. Thus, $c^2 = a^2 + b^2 \equiv 2 \bmod 4$ is an impossibility. □

Having established the above attributes we determined that in a primitive solution (a, b, c) only a or b can be odd and c must be odd. We will now look at the full theorem for primitive triples and later analyze two methods that prove the theorem to be true.

Theorem 2.1. *Let (a, b, c) be a primitive triple, then a or b is odd, and the other is even. Taking b as odd, there exists two co-prime integers u and v, where $u > v$, $SGD(u, v) = 1$, and either u or v is odd and the other is even such that:*

$$a = 2uv, \qquad b = u^2 - v^2, \qquad c = u^2 + v^2$$

2.2 First Proof

Proof. In the tenth book of Euclid's elements is found the oldest known method to prove that Theorem 2.1 generates all Pythagorean triplets. Consider the equation (1-1) and suppose that a is even, consequently b and c are odd according to Lemma 2.3. The equation (1-1) can be rewritten

$$a^2 = c^2 - b^2 = (c + b) \cdot (c - b)$$

We said that b and c are both odd numbers, then $c+b$, and $c-b$ are positive even integers. Hence, according to Lemma 2.2. both sides are divisible by 4, which gives us:

$$\frac{a^2}{4} = \frac{(c + b) \cdot (c - b)}{4} \Leftrightarrow \left(\frac{a}{2}\right)^2 = \frac{c + b}{2} \cdot \frac{c - b}{2} \tag{2-1}$$

Let us notice that the two factors $(c + b)/2$ and $(c - b)/2$ are relatively prime. Suppose that they are not. Then, there is a common divisor $d > 1$ that divides the sum and the difference of them.

$$\frac{c + b}{2} + \frac{c - b}{2} = c \qquad \frac{c + b}{2} - \frac{c - b}{2} = b$$

However, $SGD(b, c) = 1$.Therefore d has to be equal to 1 contrary to the assumption above.

Lemma 2.4. *If the square of an integer k is the product of two numbers a and b, and there are no common factors between these, the a and b are also perfect squares.*

Proof. Let us first notice that in the prime factorization of a square number, each factor appears an even number of times, i.e $(k_1^{q_1}k_2^{q_2}...k_l^{q_l})^2 = k_1^{2q_1}k_2^{2q_2}...k_l^{2q_l}$. Suppose that $GCD(a,b) = 1$, and that $a \cdot b = k^2$. Let us also suppose that a is not square, then one of the factors $a = a_1^{p_1}a_2^{p_2}...a_n^{p_n}$ appears a odd numbers of times, say a_1. However, all the prime factors in $ab = k^2$ must appear a even amount of times, this means that a_1 must be a factor in b as well, which is a contradiction since $GCD(a,b) = 1$

□

Therefore we can call the factors on the right side of (2-1) for

$$\frac{c+b}{2} = u^2 \qquad \frac{c-b}{2} = v^2$$

$$\left(\frac{a}{2}\right)^2 = u^2 \cdot v^2 \Rightarrow a = 2uv, \qquad b = u^2 - v^2, \qquad c = u^2 + v^2 \qquad (2\text{-}2)$$

Let us ensure that the triple $(a,b,c) = (2uv, u^2 - v^2, u^2 + v^2)$ yields only primitive solution. We notice that there are certain restrictions on u and v. Firstly, u and v and co-prime, here is why: Let d be a integer that divides both u and v. Then we know that $d|u^2$ and $d|v^2$. The number d will also divide the sum and the difference of u^2 and v^2 so $d|u^2+v^2$ and $d|u^2-v^2$. But, $u^2+v^2 = c$ and $u^2-v^2 = b$ and $GCD(b,c) = 1$, therefore d must be 1, hence $GCD(u,v) = 1$. Another restrictions on u and v is that $u^2 - v^2$ and $u^2 + v^2$ are odd numbers, it means that u and v cannot be both even, otherwise b and c would not be co-prime. For the same reason u and v cannot both be odd; the sum of two odd numbers is even. Therefore the numbers u and v, one must be odd and the other even. □

Table 2 below shows some primitive triples. We let u be $2 \leq u \leq 5$ and the triples will look like as the following

		a	b	c
u=2,	v=1	4	3	5
u=3,	v=2	12	5	13
u=4,	v=1	8	15	17
u=4,	v=3	24	7	25
u=5,	v=2	21	20	29

Table 2 : Primitive triples

2.3 Second Proof

The second method is very different from the first one. Here we will go beyond integer solutions and study triples that satisfies $a^2 + b^2 = c^2$ where $a, b, c \epsilon Q$. In order to do that we study the connections between Pythagorean triples and the unit circle. Surprisingly enough, there is a connection between the two, which has been studied since ancient Greece by Pythagoras, Euclid, Diophantus and others. Consider the following:

Let us work with the equation (1-1) by dividing both sides by c^2

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = \frac{c^2}{c^2}$$

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

We see that (a/c) and (b/c) are rational numbers, say x and y, thus the the equation above gives the rational points on the unit circle $x^2+y^2 = 1$. Let C be the set of rational points on the unit circle with positive coordinates, in other words, the rational points found in the first quadrant. Thus C is defined as

$$C = \{(x, y) \epsilon Q^2; x > 0, y > 0, x^2 + y^2 = 1\}$$

Lemma 2.5. *There is a bijection relation $\psi : (a, b, c) \to (a/c, b/c)$ between the primitive Pythagorean triples and the set of rational points on first quadrant of the unit circle C (rs-axles not included) .*

Proof. Let us first begin with studying the relation between the slope k and the points (x, y) According to figure 2, we draw a line between $(-1, 0)$ and (x, y) with slope k.

Let us calculate what the slope k is.

$$k = \frac{\Delta y}{\Delta x} = \frac{b/c - 0}{a/c - (-1)} = \frac{b/c}{a/c + c/c} = \frac{b/c}{(a + c)/c} = \frac{b}{a + c} = \frac{y}{x + 1}$$

The equation of the line enables us to calculate the coordinates of $P(x(k), y(k))$ by solving the system of equation

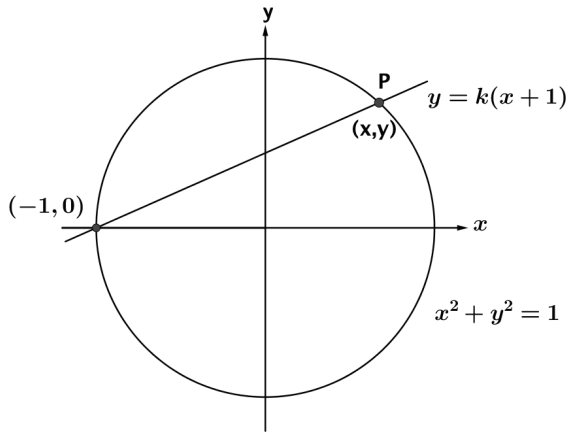


Figure 2: Unit circle

$$\begin{cases} y = k(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

By substituting y from the first equation onto the second we get

$$x^2 + (k(x+1))^2 = 1 \Leftrightarrow$$
$$\Leftrightarrow x^2 + k^2(x+1)^2 = 1 \Leftrightarrow$$
$$\Leftrightarrow x^2 - 1 + k^2(x+1)^2 = 0 \Leftrightarrow$$
$$\Leftrightarrow (x-1)(x+1) + k^2(x+1)^2 = 0 \Leftrightarrow$$

Let us divide both sides of the equation by $(x+1)$

$$(x-1) + k^2(x+1) = 0 \Leftrightarrow$$
$$\Leftrightarrow x - 1 + k^2x + k^2 = 0 \Leftrightarrow$$
$$\Leftrightarrow x(1+k^2) + k^2 - 1 = 0 \Leftrightarrow$$
$$\Leftrightarrow x = \frac{1-k^2}{1+k^2}$$

Let us now solve y

$$y = k\left(\frac{1-k^2}{1+k^2}+1\right) =$$
$$= k\left(\frac{1-k^2}{1+k^2}+\frac{1+k^2}{1+k^2}\right) = \frac{2k}{1+k^2}$$

The coordinates for our point $P(x(k), y(k)$ is thus

$$P(x(k), y(k)) = \left(\frac{1-k^2}{1+k^2}, \frac{2k}{1+k^2}\right)$$

Let us observe that k is $0 < k < 1$ if and only if $(x(k), y(k)) \; \epsilon \; C$, and $(x, y) \; \epsilon \; Q^2$ if and only if $k \; \epsilon \; Q$ Therefore we can say $k = q/p$ where $p > q > 0$ and $GCD(p, q) = 1$, thus the coordinates of P can be written as

$$P(x(k), y(k)) = \left(\frac{1-q^2/p^2}{1+q^2/p^2}, \frac{2q/p}{1+q^2/p^2}\right)$$
$$P(x(k), y(k)) = \left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$$

Let $t = GCD(p^2 - q^2, p^2 + q^2)$. Then we know that t divides both their the sum and difference, $2p^2$ and $2q^2$. But p and q are co-prime hence $t|2$ which means that $t = 1$ or $t = 2$.
If $t = 1$ then there is no common factor between the numerator and the denominator , and since $a/c = (p^2 - q^2)/(p^2 + q^2)$, it follows therefore that $a = p^2 - q^2$ and $c = p^2 + q^2$, and consequently $b = 2pq$. Notice that one of p or q is even and the other is odd, otherwise $t \geq 2$.
If $t = 2$, then $GCD((p^2 - q^2)/2, (p^2 + q^2)/2) = 1$, which means that $a = (p^2 - q^2)/2, c = (p^2 + q^2)/2$, and consequently $b = pq$. But in this case both p and q must be odd, both can not be even because $GCD(p, q) = 1$; neither one odd and the other even, otherwise would both $p^2 \pm q^2$ be odd, contradicting the supposition. In this case we write $p = 2n + 1, q = 2m + 1$, which gives us

$$a = \frac{((2n+1)^2 - (2m+1)^2)}{2} = 2(n + m + 1)(n - m)$$
$$b = (2n + 1)(2m + 1) = (n + m + 1)^2 - (n - m)^2$$
$$c = \frac{((2n+1)^2 + (2m+1)^2)}{2} = (n + m + 1)^2 + (n - m)^2$$

Let $p_1 = n + m + 1$ and $q_1 = n - m$. Notice that $n > m$ because $p > q$ and therefore $p_1 > q_1 > 0$. Moreover we have that $p_1 + q_1 = 2n + 1$ is odd, which means that p_1 or q_1 must be odd the other even; and to conclude.

if $t = 1$ the

$$a = p^2 - q^2, \quad b = 2pq, \quad c = p^2 + q^2$$

if $t = 2$

$$a = 2p_1q_1, \quad b = p_1^2 - q_1^2, \quad c = p_1^2 + q_1^2$$

□

Table 3 shows primitive triples that Corresponds to rational points on the unit circle $x^2 + y^2 = 1$.

k	a	b	
1/2	3/5	4/5	
1/3	4/5	3/5	
2/5	21/29	20/29	
7/9	16/65	63/65	

Table 3 : Triples as rational points on $x^2 + y^2 = 1$

3 Congruent numbers

3.1 Introduction

The study of primitive triples where the values of a, b, c are taken from slopes on a unit circle brought us from integer to rational solutions to $a^2 + b^2 = c^2$, leaving us with a so called *rational triangle*. If the sides and hypotenuse of a right angled triangle are rational numbers, then the triangle is called rational. This section will focus on studying the *area* of such a triangle, which leads us to the concept called congruent numbers

Definition 3.1. *A positive integer n is called congruent number if there exists a right-angled rational triangle whose sides* $(a, b, c) \epsilon Q^+$ *such that* $\frac{ab}{2} = n$

Table 4 and Figure 3 give examples of congruent numbers.

n	a	b	c
5	3/2	20/3	41/6
6	3	4	5
7	24/5	35/12	337/60

Table 4 : Congruent numbers

We see that the use of the word congruent is different from what is otherwise known as modular arithmetic. And just as with primitive triples, the congruent numbers raise different questions such as [3]

- the existence of a method that generate congruent numbers
- given an integer n, is there a method to know that n is congruent?

3.2 Classifying congruent numbers

When working with Pythagorean triples we said that it suffices to study primitive solutions since all other triples are just proportional to the primitive solutions. The same principle can be applied to begin our study on congruent numbers. When we say congruent numbers, by definition, it includes right-angled triangles with integer sides, and triangles with rational sides. Let

[3] Chandrasekar, (1998)

us suppose that (a, b, c) are the sides of a rational triangle whose area is the congruent number n. By multiplying all three sides with s, the smallest common multiple between the denominator of a and b, the congruent number n becomes s^2n. Thus, we go from a rational triangle to a proportional triangle with integer sides, and the congruent number n is divisible by the square number s^2. The opposite also works, if the area of a triangle with integer sides is s^2n, then we can divide all sides by s and get a proportional triangle with rational sides. Therefore it suffices to study triangles where n is square free. Before proceeding to theorem 3.1 let us look at two lemma that will help us to understand theorem 3.1

Lemma 3.1. *If x is a rational number so that x^2 is an integer, then x itself must be an integer.*

Proof. Let $x = a/b$, where a and b are integers and relatively prime. Let $c = x^2$. It follows that $c = a^2/b^2$ and $a^2 = cb^2$. If $b > 1$, there exists a prime number p such that $p|b$. Since $p|cb^2$, then p also divides a^2 and a. However, in that case, a and b are not co-prime, which is contradiction. Therefore $b = 1$ and $x = a$ □

Lemma 3.2. *Let a and b be two integers where a is a square and b is square free. Let d be an integer whose square divides a^2b, then $d^2|a^2$ and $d|a$*

Proof. The integer b, being square free, can be factorized as a product where the factors $p_1 \cdot p_2 \cdot ...p_m$ are different from each other. Whereas d^2, being a square, can be written as $q_1^{2k_1} \cdot q_2^{2k_2} \cdot ...q_l^{2k_l}$ where each factor is different but appears an even number of times. Thus we have.

$$\frac{a^2b}{d^2} = \frac{a^2 \cdot p_1 \cdot p_2 \cdot ...p_m}{q_1^{2k_1} \cdot q_2^{2k_2} \cdot ...q_l^{2k_l}}$$

If p_i is different from q_j, then we can conclude that $d^2|a^2$ and our point is proven. However, we have to consider that a factor from q_j can be equal to a factor from p_i. Without any loss of generality, let's say that $p_1 = q_1$ and divide them out. We are left with

$$\frac{a^2 \cdot p_2 \cdot ...p_m}{q_1^{2k_1-1} \cdot q_2^{2k_2} \cdot ...q_l^{2k_l}}$$

We said that the factors in b are all different, meaning that no other number in $p_2, ..., p_m$ is equal to q_1; this implies that $q_1^{2k_1-1}|a^2$, which in turn also implies that $q_1|a$, because $q_1|q_1^{2k_1-1} \Rightarrow q_1|a^2 \Rightarrow q_1|a$.

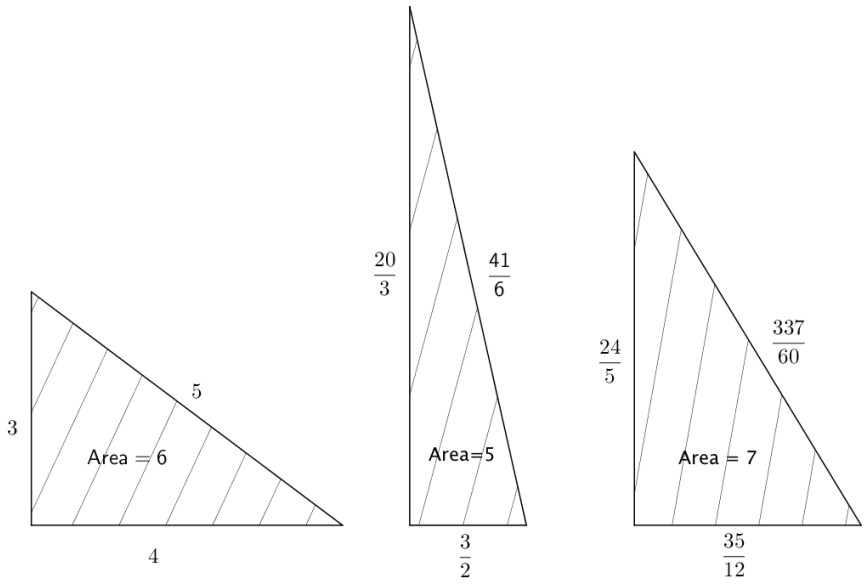


Figure 3: Rational triangles with area 5,6,7

We know that q_1 can only divide a if $\exists m \, \epsilon \, Z$, such that $a = q_1^{l_1} \cdot m$, $q_1 \nmid m$

$$a = q_1^{l_1} \cdot m \Rightarrow$$

$$\Rightarrow a^2 = q_1^{2l_1} \cdot m^2$$

$$q_1^{2k_1-1} | a^2 = q_1^{2l_1} \cdot m^2$$

From here we can observe that $q_1^{2k_1-1} | q_1^{2l_1} \cdot m^2$ which implies that

$$2k_1 - 1 \leq 2l_1$$

However, $2k_1 - 1$ is odd, and $2l_1$ is even, it implies that

$$2k_1 - 1 < 2l_1 \Rightarrow$$

$$\Rightarrow 2k_1 \leq 2l_1 \Rightarrow q_1^{2k_1} | a^2$$

□

Theorem 3.1. *Let n be a square-free congruent number to the rational triangle with sides (a, b, c). If s is the smallest common multiple of the denominators of a, b and c then, the triangle with sides (sa, sb, sc) is a primitive triangle with the area $s^2 n$*

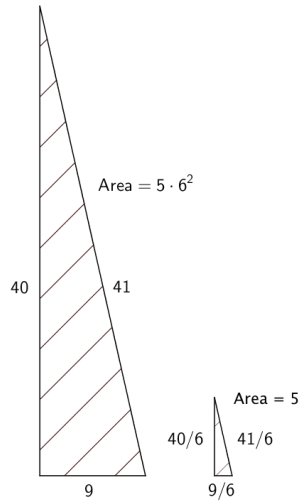


Figure 4: Proportionality of square vs square free congruent numbers

Proof. It is self evident that (sa, sb, sc) is a Pythagoras triple if $(a, b, c,)$ is a triple as well. It is also evident that if the area of $(a, b, c) = n$, then the area of $(sa, sb, sc) = s^2n$. Let us see if (sa, sb, sc) is a primitive triangle.
Firstly, we can see that if d divides sa and sb, consequently, according to Lemma 3.1, it also divides sc. Hence $(sa/d, sb/d, sc/d)$ is a Pythagoras triples.
The area of the triangle is then s^2n/d^2, meaning that $d^2|s^2n$. But n is a squarefree number, and according to Lemma 3.2, $d^2|s^2$, hence $d|s$. It means that $s = ds'$, and as a consequence $s'a, s'b, s'c \, \epsilon \, N$. Notice that s' is a common multiple among the denominators of a, b, c. However, we said that s is the smallest common multiple, which means that $s = s'$, therefore d must be 1. □

Example 3.1. Let the primitive triple (sa, sb, sc) be equal to $(9, 40, 41)$ Then $n = \dfrac{9 \cdot 40}{2} = 180 = 5 \cdot 6^2$, where $n = 5$, and $s = 6$ Thus, the rational triple $(a, b, c) = (9/6, 40/6, 41/6) = (3/2, 20/3, 41/6)$ must be a proportional triangle to (a, b, c) and $n = \frac{(3/2)(20/3)}{2} = \frac{10}{2} = 5$. Notice table 5.

(a,b,c)	s^2n	Squarefree part
(3,4,5)	6	6
(15,8,17)	60	15
(5,12,13)	30	30
(35,12,37)	210	210
(21,20,29)	210	210
(7,24,25)	84	21
(63,16,65)	504	126

Table 5 : Congruent numbers

Another way to generate congruent numbers is by rewriting the equation $a^2 + b^2 = c^2$ by using the same proposition for primitive triples. [4]

$$(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2$$

Each number corresponds to the sides of a right triangle, the hypotenuse being $(p^2 + q^2)$. We can obtain congruent numbers by substituting p and q at our choice, and the equation will be $n = pq(p^2 - q^2)$.

		(pq)	$(p^2 - q^2)$	n
p=2,	q=1	2	3	6
p=3,	q=2	6	5	30
p=4,	q=1	4	15	60
p=4,	q=3	12	7	84
p=5,	q=2	10	21	210

Table 6 : Congruent Numbers

Theorem 3.2. *Let p,q be co-prime $p > q$, and positive integers of opposite parity (one is odd and the other is even). When three of the numbers $p, q, p+q, p-q$ are squares, then the fourth number is s^2n where n is a congruent number, and s an integer.*

Proof. Let us check when p,q,$p + q$ are square. Considering the premises established above, we have triangle T whose sides are the primitive triple $(p^2 - q^2, 2pq, p^2 + q^2)$ and whose area is $2pq(p^2 - q^2)/2 = pq(p^2 - q^2) = pq(p + q)(p - q)$. If $p, q, p + q$ are square numbers, by implication, it follows

[4]Chandrasekar, (1998)

that $pq(p+q)$ also is a square, hence $r^2 = pq(p+q)$. By substituting r^2 we can see that the area of the triangle T is now

$$r^2(p-q).$$

It means that $p-q$ is the area of a rational triangle with sides $\frac{p^2-q^2}{r}, \frac{pq}{r}$ since

$$\frac{p^2-q^2}{r} \cdot \frac{2pq}{r} \cdot \frac{1}{2} = \frac{r^2(p-q)}{r^2} = p-q.$$

Let us reduce both fractions $p^2 - q^2/r, 2pq/r$ such that there remains no common factor between the numerator and denominator. We write

$$\frac{p^2-q^2}{r} = \frac{p'}{q'} \quad , \quad \frac{2pq}{r} = \frac{p''}{q''}$$

$$\Rightarrow p-q = \frac{p'}{q'} \cdot \frac{p''}{q''} \cdot \frac{1}{2}$$

Let $s = GCD(p', p'')$, thus $p' = p'_1 \cdot s$ and $p'' = p''_1 \cdot s$. It follows that

$$p-q = \frac{p'_1 \cdot s}{q'} \cdot \frac{p''_1 \cdot s}{q''}$$

since $p-q \, \epsilon \, N$, it implies and $q'q''$ divides $p'_1 p''_1$. However, the $GCD(p'_1, q') = GCD(p''_1, q'') = 1$, hence $q'|p''_1$, and $q''|p'_1$. And therefore $p - q = s^2 n$, where n is a congruent number. □

Taking the same steps above, we will obtain the same results, that any of the numbers p,q,$p+q$,$p-q$ is equal to $s^2 n$ as long as the other three are square.

Example 3.2. Let us take some Pythagorean triples and use the method above to find congruent numbers. For instance, $(a, b, c) = (3, 4, 5)$, $a^2 = 9$, $b^2 = 16$, $c^2 = 25$. We have that $b^2 - a^2 = 7$, so 7 is a congruent number. If $a > b$ then $n = a^2 - b^2$, if $b > a$, then $n = b^2 - a^2$.

(a,b,c)	$a^2 - b^2$ or $b^2 - a^2$
(3,4,5)	7
(15,8,17)	161
(5,12,13)	119
(35,12,37)	1081
(21,20,29)	41
(7,24,25)	527

Table 7 : Congruent numbers

Example 3.3. Let us also see how theorem 3.2 works using the steps throughout the proof to find the congruent number 7. We have $p = 4$, $q = 3$, $p+q = 5$ and $r = pq(p + q) = 3 \cdot 4 \cdot 5$

$$\frac{p^2 - q^2}{r} = \frac{16^2 - 9^2}{3 \cdot 4 \cdot 5} = \frac{(16 + 9)(16 - 9)}{3 \cdot 4 \cdot 5} = \frac{5 \cdot 7}{3 \cdot 4}$$

$$\frac{2pq}{r} = \frac{2 \cdot 16 \cdot 9}{3 \cdot 4 \cdot 5} = \frac{24}{5}$$

$$\frac{1}{2} \cdot \frac{p^2 - q^2}{r} \cdot \frac{2pq}{r} = \frac{1}{2} \cdot \frac{5 \cdot 7}{3 \cdot 4} \cdot \frac{24}{5} = 7$$

Theorem 3.3. *A number n is congruent if and only if there exists a rational number d such that $d^2 + n$ and $d^2 - n$ are both squares of rational numbers.*

Proof. Let n be a congruent number and let a,b,c be rational numbers such that

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = n \Leftrightarrow 2ab = 4n$$

$$a^2 + b^2 \pm 2ab = c^2 \pm 4n \Leftrightarrow$$

$$\Leftrightarrow \left(\frac{a \pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n$$

By taking $d = c/2$ we have that d is rational and that $d^2 + n$ and $d^2 - n$ are squares of $(a \pm b/2)^2$.

Now, given that $d^2 \pm n$ are square of rational numbers. We can write $\sqrt{d^2 \pm n}$, and say that $a = \sqrt{d^2 + n} + \sqrt{d^2 - n}$; and $b = \sqrt{d^2 + n} - \sqrt{d^2 - n}$ By substituting these values in $a^2 + b^2 = c^2$ we obtain the following

$$a^2+b^2 = (d^2+n+2\sqrt{d^2+n}\cdot\sqrt{d^2-n}+d^2-n)+(d^2+n-2\sqrt{d^2+n}\sqrt{d^2-n}+d^2-n) =$$

$$= 4d^2 = c^2$$

$$c = \sqrt{a^2 + b^2} = 2d$$

Now we know the sides of the rational triangles (a, b, c) whose area is

$$\frac{a \cdot b}{2} = \frac{(\sqrt{d^2 + n} + \sqrt{d^2 - n})(\sqrt{d^2 + n} - \sqrt{d^2 - n})}{2} =$$

$$= \frac{(\sqrt{d^2+n})^2 - (\sqrt{d^2-n})^2}{2} =$$
$$= \frac{(d^2+n) - (d^2-n)}{2} = \frac{2n}{2} = n$$

□

3.3 Non-congruent numbers

The discussion concerning whether or not a certain integer is congruent brings us back all the way to the 10th century. There exists Arab manuscripts approximately 1000 years old that lists tabulations of congruent numbers[5]. Around 300 years later, in the 13th century, Fibonacci discovered that 7 is a congruent number, furthermore, he claimed that 1 is not a congruent number. However, the first accepted proof came hundreds of years later in the 17th century due to Fermat's contribution, which were useful to even show that 2 and 3 are not congruent.

In order to prove that 1 is not a congruent number, we will use the method discovered by Fermat, namely the method of infinite descent [6]. But before looking at the theorem and its proof we can observe that if 1 is a congruent number, then there exists a rational triangle whose sides are $a/d, b/d, c/d$ (a,b,c,d ϵ N) such that

$$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2, \quad \text{and} \quad \frac{a/d \cdot b/d}{2} = n = 1 \tag{3-1}$$

And therefore

$$a^2 + b^2 = c^2, \quad \text{and} \quad \frac{ab}{2} = d^2 n = d^2 \cdot 1 = d^2 \tag{3-2}$$

The above identities tells us that a right angled triangle with rational sides has a area equal to 1 *if and only if* there exists a right angled triangle with integral sides whose area is a perfect square. Hence, to show that 1 is not a congruent number, we simply need to show that the area of a integer right-angled triangle can not be a perfect square. Before we look at the theorem, let us quickly establish a lemma that will serve us when studying the fact that 1 is not a congruent number.

[5]Conrad, (2008)
[6]Chandrasekar. (1998)

Lemma 3.3. *Let p and q be relatively prime of different parity, and $p > q > 0$. Then, the $GCD(p, p \pm q) = GCD(q, p \pm q) = GCD(p + q, p - q) = 1$*

Proof. Let $GCD(p, p + q) = d$. Then $d|p$, and $d|p + q$. It implies that $d|(p + q) - p = q$. So if $d|p, q \Rightarrow d = 1$.

Let $GCD(q, p+q) = d$. Then $d|q$, and $d|p+q$. It implies that $d|(p+q)-q = p$. So if $d|q, p \Rightarrow d = 1$.

Let $GCD(p - q, p + q) = d$. Then $d|2p$, and $d|2q$. But p, q are coprime, hence $d|2$. However, $p + q, p - q$ are odd, hence $d = 1$

□

Theorem 3.4. *1 is not a congruent number.*

Proof. Let us suppose that 1 is a congruent number, that is to say, according to (3-2), there exists a right angled triangle T with integral sides whose area is a perfect square, and whose sides, according to theorem 2.1, are

$$a = 2pq, \qquad b = p^2 - q^2, \qquad c = p^2 + q^2$$

where $p > q > 0$, $GCD(p, q) = 1$, and either p or q is odd and the other is even. The area A of triangle T must therefore be

$$A = \frac{2pq(p^2 - q^2)}{2} = pq(p - q)(p + q)$$

The product of $pq, p+q, p-q$ is the area of T. Moreover, given the fact that $GCD(p, q) = 1$, according to lemma 3.3; $GCD(p, p \pm q) = GCD(p+q, p-q) = 1$. So we can write

$$p = x^2, \quad q = y^2, \quad p + q = u^2, \quad p - q = v^2 \tag{3-3}$$

With the identities in (3-3), we make a few useful observations.

1. The length of the hypotenuse is $p^2 + q^2 = (x^2)^2 + (y^2)^2 = x^4 + y^4$
2. Since $GCD(p + q, p - q) = 1$, it follows that u^2, v^2 are also co-prime, hence u, v are co-prime as well
3. $GCD(u + v, u - v) = GCD(2u, 2v) = 2$, because according to the 2nd observation u and v are co-prime.
4. $p = x^2 = \dfrac{u^2 + v^2}{2}$

5. $2y^2 = 2q = u^2 - v^2 = (u+v)(u-v)$

The above list tells us that u, v are co-prime, and that $u+v$,$u-v$ are even numbers. This means that the number 2 divides one of the numbers $u+v, u-v$ only one time, suppose it is $u+v$, we can thus write

$$2y^2 = (u+v)(u-v) \Leftrightarrow y^2 = \frac{u+v}{2} \cdot (u-v)$$

Let $r = \frac{(u+v)}{2}$ and $s = u-v$; the numbers r, s are co-prime, it follows that, according to lemma 2.3, r, s must be square; hence $2r^2 = u+v$, and $s^2 = u-v$. Furthermore, since $(u+v)+(u-v) = 2u = 2r^2 + s^2$, and $2u$ is a even number, we can conclude that s^2 must be even as well, so there exists an integer t, such that $s = 2t \Rightarrow s^2 = 4t^2$. So, $u = r^2 + 2t^2$

Similar results will we obtain by instead subtracting $(u-v)$ from $(u+v)$, we get $2v = 2r^2 - s^2$, which must be a even number, therefore there exists a integer t such that $s = 2t$, so $v = r^2 - 2t^2$.

The fourth item on the list above tells us that

$$p = x^2 = \frac{u^2 + v^2}{2}$$

Let's substitute u with $r^2 + 2t^2$, and v with $r^2 - 2t^2$. Thus we acquire

$$p = x^2 = \frac{u^2 + v^2}{2} = r^4 + 4t^4$$
$$r^4 + 4t^4 = x^2$$

The triple $(r^2, 2t^2, x)$ constitute the sides of triangle T' with area $(rt)^2$. The sides of T' are shorter than the sides of triangle T. For instance, the hypotenuse of T is $p^2 + q^2$, whereas of T' is x; but we know that $x = \sqrt{p} < p^2 + q^2$.

The value we now have for x is less than the length of the hypotenuse we had in the beginning $p^2 + q^2$. The same is true for the sides of the triangle. Hence, starting from a right angled triangle we generated a proportional triangle whose sides are shorter. Nothing stops us from generating yet another triangle doing the same thing, consequently, we can infinitely continue descending the value of the triangle T. As a result, we are brought to a contradiction and therefore conclude that 1 is not a congruent number $\square$

.

The proof above leads us to a rather uncommon way to prove that $\sqrt{2}$ is irrational[7]. Let us say that $\sqrt{2}$ is a rational number, we could have a triangle with sides $(\sqrt{2}, \sqrt{2}, 2)$, this triangle's area would thus be, $\frac{\sqrt{2} \cdot \sqrt{2}}{2} = 1$, but one is not a congruent number, leading us to a contradiction.

3.4 The infinite descent method

When proving that 1 is not a congruent number, we showed that starting, let us say, from the smallest possible triangle with integral sides, we were able to produce another triangle that was smaller to the first, we compared their hypotenuse to draw such a conclusion. Certainly the process can be repeated, and this continuous decrease is what is called "the infinite descent method" devised by Fermat. The way in which Fermat's proves the method of infinite descent is by showing that the Diophantine equation $x^4 + y^2 = z^2$ has no solution in nonzero integers x,y, and z. Fermat showed that for every solution there is a "smaller" solution, contradicting the well-ordering property [8].

3.5 The problem with congruent numbers

All throughout this section on congruent numbers, we have been focusing on ways to generate such numbers by developing different forms and establishing theorems, answering our first question in the beginning of the section, namely, if there was a way to generate congruent numbers. Nevertheless, we also asked ourselves if given an integer n, is there a method to know that n is congruent? This is exactly the problem with congruent numbers, that is, to decide whether or not a given number n is congruent. In order for us to have a better understanding of how problematic it can be, consider the right angled triangle below. In 1914, L.Bastien proved that its area corresponds to the congruent number 101 [9]. These are the sides of the triangle.

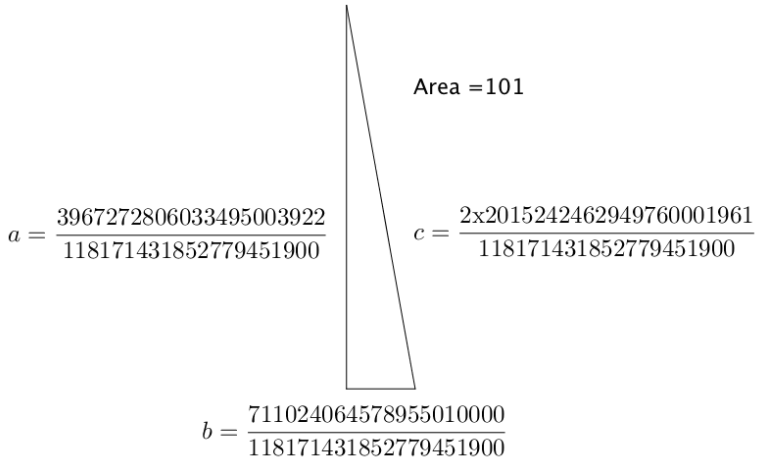
$$b = \frac{3967272806033495003922}{118171431852779451900}$$

[7]Conrad, (2008)
[8]Rosen, (1993)
[9]Chandrasekar, (1998)

$$a = \frac{711024064578955010000}{118171431852779451900}$$

$$c = \frac{2 \times 2015242462949760001961}{118171431852779451900}$$

So, it is not an exaggeration to say that to find out whether or not an integer n is congruent is nothing less than an exhaustive work.



Right angled triangle with area 101

3.6 History behind congruent numbers

Early in this paper we mentioned that there exists an Arab manuscripts dated from the 10th century asserting that congruent numbers were already known to local mathematicians[10]. It is said that there is no evidence that the Arabs knew Diophantus prior to the translation of his work at 998 A.D. However, the Arabs found out that $5, 6, 14, 15, 21, 30, 34, 65, 70, 110, 154, 190$ and more, are congruent numbers. In their list, one can even find numbers greater than 100, like 10374 [11].

[10]Conrad, (2008)
[11]Chandrasekar, (1998)

From the 10th century until the 13th century, there is not much said or heard concerning congruent numbers, until a man called Leonardo Pisano, also known as, Fibonnacci, considered to be the most talented Western mathematician of the Middle Ages, was challenged by the king's scholars. The challenge was not asking Fibonacci to solve a congruent number problem, but its solution was the same as proving that 5 is a congruent number. Fibbonnacci recorded this work in the so called Liber Quadratorum (1225), which became known to the public hundred of years later after been found by Prince Boncompaign. In this work, Fibonnacci also proved that 7 is a congruent number, moreover, he asserted, without any proof, that 1 is not congruent. As shown above the proof came many years later when Fermat discovered the infinite descent method.

4 Conclusion

We have now presented a study on the properties of a right-angled triangle. By defining the relation of its sides we were able to establish different theorems that led us to a formula that generates primitive triples to Pythagoras triangle. We saw that it was possible to understand the theorem for primitive triples by examining the points on a unit circle, how the points on the first quadrant of the unit circle can yield triples that satisfy the equation $a^2 + b^2 = c^2$.

Lastly, we went from studying the sides of a right-angles triangle, to study the area of such a triangle. We were thus led to the concept called congruent numbers. We saw that there are many different methods one can use in order to find a congruent number. Furthermore, we were able to present one method that shows that 1 is not congruent, the same method is used to show that 2 and 3 are not either. Despite the fact that there are many numbers we know are not congruent, it still does not exist a certain method one can use to tell whether or not a given integer is congruent. We conclude this study hoping that it will inspire readers to continue develop the solution.

References

[1] Chandrasekar, V. (1998). The congruent number problem. Resonance, 3(8), 33-45.

[2] Maor, E. (2007). "The Pythagorean Theorem, a 4,000-year history, Princeton Science Library."

[3] Ore, Oystein. (1948). Number theory and its history. Courier Corporation.

[4] Conrad, Keith. 2008. The Congruent Number Problem. The Harvard Collage Mathematics Review. Available: http://www.math.rug.nl/~top/congnumber.pdf

[5] Conrad, Kieth. (2008). Pythagorean Triplets. University of Connecticut. Available: http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pythagtriple.pdf

[6] Koblitz, Neal. (1993). Introduction to Elliptic Curves and Modular Forms. Vol 2. New York: Springer-Verlag.

[7] Lundström, Partrik. (2008). Pythagoreiska tripplar på sex olika sätt. Available: http://https://ncm.gu.se/pdf/normat/111119_lundstrom.pdf

[8] Otthén, H. (2016). Rätvinkliga rationella trianglar och kongruenta tal.

[9] Rosen, K. H. (1993). Elementary number theory and its applications. Addison-Wesley.

[10] Wikipedia. 2018. Pythagorean triple. https://en.wikipedia.org/wiki/Pythagorean_triple (Taken 2018-03-24)