Journal of Pure and Applied Mathematics: Advances and Applications
Volume 17, Number 2, 2017, Pages 77-87
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/jpamaa_7100121783

SOLVING THE CONGRUENT NUMBER PROBLEM IS SOLVING THE ELLIPTIC CURVE PROBLEM

EULOGIO GARCIA

Institute Polytechnic of Leon
Leon
Spain
e-mail: eulogiogar3@gmail.com

Abstract

In this paper, we present solution of the congruents numbers problem and it is applied for solved elliptical curve.

1. Introduction

The congruent number problem was proposed by Al-Karaji (953-1029) wondering what numbers $n \in Z$ by subtracting them from a square give another square, i.e., $a^2 - n = b^2$, then $n \in Z$ is congruent. We did not refer to the areas of the triangles. However, we also know that (n) is a number congruent if it is the area of triangle $\frac{b \times a}{2} = n$ and therefore are all the triangles that have by area half of the rectangle (all the triangles rectangles). The best known achievements were in 1982 by Tunell with

2010 Mathematics Subject Classification: 11Mxx.
Keywords and phrases: congruent numbers, equation of Enfer, Tunell theorem, elliptic curve.
Received February 25, 2017; Revised March 25, 2017

his theorem and finally those achieved by (Robert Bradshaw, W. B. Hart, D. Harvey, G. Tornaria and M. Watkins in 2009) with the help of computers. In this work it is verified the mistake that have given by the computers.

2. Main Results

The achievement of my results is a direct consequence of the following equation of Enfer [4]:

$$4 + \sum_{m\geq 2}^{k\to\infty} (2m+1) = a^2. \tag{1}$$

Example. $4 + 5 = 9;\ 9 + 7 = 16;\ 16 + 9 = 25\ldots.$

Theorem 1. All numbers squared are defined by equation $4 + \sum_{n\geq 2}^{k}(2m+1)$.

Proof 1. Subtracting each of the last sums of Equation (1), we have (n) congruent odd.

$$4 + \sum_{m\geq 2}^{k} (2m+1) = b^2,$$

$$4 + \sum_{m\geq 2}^{k} (2m+1) - [2k+1] = (b_n)^2,$$

$$(b_n)^2 = 4 + \sum_{m\geq 2}^{k-1} (2m+1),$$

and so on, we observe that: $\forall(2k+1=n);\ n$ is congruent number.

Proof 2. We take, the last two sums of Equation (1). We subtract between if and we have (n) that is a congruent even.

$$4 + \sum_{m\geq 2}^{k} (2m+1) - [(2k+1) + (2(k-1)) + 1] = c^2 < b^2,$$

$$[2k + 1 + (2(k-1)) + 1] = 4 + \sum_{m\geq 2}^{k-2} (2m+1),$$

again: $\forall[2(k+1) + (2(k-1)) + 1] = n$; (n) is an even congruent.

The method to know the congruent numbers, pairs or odd as quickly and accurately; is with the two expressions of congruent [6], [7] following:

$$\forall[2k + 1 \equiv 5 \bmod 2];$$

$$\forall[4(k+1) \equiv 0 \bmod 2],$$

for: $\forall(k = 2; 3; 4; 5 \ldots)$.

Therefore:

(1) Any odd number with $k > 1$ is a congruent number.

(2) Any even number in the form of $2(2k+1)$ is not congruent; as $4k + 2 \neq 4(k+1)$; let us recall that $\forall 4(k+1) = [2(k+1) + (2(k-1)+1)] = n$; by the Equation (1).

(3) $\exists(2m) = 4(k+1)$, where $(m = n = \text{even})$, congruent number if and only if, is the area of a triangle whose sides are $\forall(a, b, c) \in Z$, i.e., the Pythagoras theorem $a^2 + b^2 = c^2$.

3. Discussion

This section is composed of two parts related to the congruent numbers.

(i) Theorem of Tunell.

(ii) Congruent numbers in the elliptic curves and in the modular forms; Taniyama-Shimura conjecture today called theorem.

Theorem of Tunell. *Given* (n) *a number square free positive integer will be a congruent number if fulfilled the following*:

$$f(n) = (x,\ y,\ z) \in Z^3 \left| x^2 + y^2 + 8z^2 = n, \right.$$

$$g(n) = (x,\ y,\ z) \in Z^3 \left| x^2 + 2y^2 + 8z^2 = n, \right.$$

$$h(n) = (x,\ y,\ z) \in Z^3 \left| x^2 + 2y^2 + 32z^2 = \frac{n}{2}, \right.$$

$$k(n) = (x,\ y,\ z) \in Z^3 \left| x^2 + 4y^2 + 32z^2 = \frac{n}{2}, \right.$$

If $(n = odd)$ *and* (n) *is congruent then* $f(n) = 2g(n)$ *and for* $(n = even)$ *if* (n) *is congruent then* $h(n) = 2k(n)$.

In the previous point (2) it was shown that $\forall(2n)$ with $(n = \text{odd})$ are not congruent and therefore $f(n) \neq 2g(n)$.

For $(n = \text{even})$, $h(n) = 2k(n)$ always that (n) is the area of a rectangle triangle of sides $(a,\ b,\ c) \in Z$ and in turn that $(2n)$ also is congruent (the difference between two squares (point 3).

Therefore

$$h(n) = 4(k + 1) \equiv 0 \bmod 2,$$

$$k(n) = 2(k + 1).$$

With Tunell's theorem few congruent numbers are defined; in relation with that they exist.

(ii) Congruent numbers allow us to know if an existing elliptic curve, (if they have solutions for $(y \in Z)$ and how many).

Let be elliptic curve E_Z.

$$y^2 = x^3 - n^2x. \tag{2}$$

This is the same as: $y^2 = x(x^2 - n^2)$.

By Pythagoras $\forall(x^2 - n^2 = b^2)$ if (x, n, b) are Pythagorean terms; (n) is a congruent number because we know that $\exists(n^2 = n_1)$, where (n_1) is also congruent; example $5^2 = 25 = 2k + 1 \equiv 5 \bmod 2$ and hence the Equation (2) is reduced to the form:

$y^2 = xb^2$, which implies $(x = k^2)$.

$y^2 = (kb)^2$ with $(m, b, y) \in Z$,

example: $(k = 5)$; $(n = 20)$; $(b = 15)$; implies $(y = 75)$

$$75^2 = 25^3 - 20^2 \times 25.$$

Thus the curve exists and is not an elliptic curve modular, it is reducible and violates the law of addition (any sum of two points of a line that cuts to the elliptic curve) gives a third point of the curve of the same group $(P, Q, R) \in Q$, however here we have $P + Q \neq R$ for being $R \in Z$). Therefore this curve can not be parametrized with a modular function. One elliptic curve exist if $(y \in Z)$ and has in its coefficients (a congruent number) and hence will have only one solution for $(y \in Z)$ as a consequence of being (n) the difference between two squares, this makes impossible the existence of another pair of squares along (x).

At this point we shall analyze some of the elliptic curves already demonstrated by Enfer [4]; the reason for its analysis is to see that any curve that exist $(y \in Z)$ has a unique solution for $(y \in Z)$.

We start with the elliptic curve that is the central axis of study of all for the elliptic curves by the Riemann-Roch theorem: The statement is that by means of a series of transformation any elliptical curve arrives at the expression.

$$y^2 = x^3 + bx + c. \tag{3}$$

This is the basis of the article by Richar Taylor et al. [3] to affirm the demonstration of the Taniyama-Shimura conjecture. Unfortunately, the Riemann-Roch theorem cannot be corrected since of being true then there could be no elliptic curve. In this work, we demonstrate the existence of several of them that they have (solution integer), the first Equation (2); the following is the Equation (3) that they step to the form of the following:

$$y^2 = x(x^2 + b) + c,$$

being $(b; c)$ congruent numbers the equation exists; because we known that: $x^2 + b = k^2$ with (b) congruent and therefore $xk^2 = (m_1)^2$ for $\forall(x = (m_2)^2)$.

Leaving the Equation (3) as: $y^2 = ((m_2)^2)(m^2) + c$, where (c = congruent number) $\exists(y \in Z)$. solution: $x = 4$; $b = 9$; $(c = 44)$ and also $(c = 169)$

$$y^2 = 4^3 + 9 \times 4 + 44 = 144 = 12^2,$$

$$y^2 = 4^3 + 9 \times 4 + 69 = 169 = 13^2.$$

There are many elliptical curves of this class with a single solution in each one of them, ((n) is a congruent number, difference between two squares) does not admits others squares.

It is enough that one of the three points above is not fulfilled for the curve to be a modular elliptic curve.

Among the elliptical curves that exist some have their expression of Galois; provided that (x) is a power. Two examples of this are given by Equations (2) and (3), respectively.

$$x^5 + 80x^2 + 1125 = 0, (x = 5); x^5 + 9x + 22 + 72 = 0, (x = 2).$$

Now, we analyze the elliptic curve E_Q of such form that: If $\exists(E_Q) \rightarrow \exists(E_Z)$. For it we have the following:

$$y^2 = \frac{x^3}{j^2} + \frac{n}{mk}x + \frac{n_i}{j^2}.$$

And as first norm of any elliptic curve: the coefficient of the cube will always be the unit, that is to say

$$(j^2 y)^2 = x^3 + nxm + n_i$$

factorizing we have:

$$(jy)^2 = x(x^2 + nm) + n_i.$$

At this point we apply the rules established to that exist $(E_Q) : x = k^2;\ j^2$ and $nm = n'$, where n' = congruent number and in turn (n_i) also is a congruent number, therefore we have $j = 8;\ n = 5;\ x = 4$

$$(8y)^2 = 8^2 + 4nm + n_i.$$

We known that $4nm + n_i = n';$ with $n = 5;\ 4nm = 320$ and $n_i = 192;$ i.e.,

$$(8y)^2 = 8^2 + n',$$

$$y^2 = \frac{8^2 + 512}{64} = 9 = 3^2,$$

solution for the Equation (3) with E_Q is

$$y^2 = \frac{x^3}{j^2} + \frac{n}{mj}x + \frac{n_i}{j^2},$$

$$y^2 = \frac{4^4 + 5 \times 4 \times 16 + 192}{64} = 3^2.$$

Other curve E_Q.

$$y^2 = x^3 - x - c,$$

$$2^2 = \left(\frac{9}{4}\right)^3 - \frac{9}{4} - \frac{329}{64}.$$

Proof 6. The last elliptic curve to be analyzed is: The equation of Frey [5], is relevant for the demonstration of Fermat theorem by Andrw Willes [1]. We will show that the existence of the curve of Frey does not depend on the Fermat theorem (either this true or false), the curve is always modular.

$$y^2 = x^3 + (c^m - b^m)x - (bc)^m.$$

We know that there are Pythagorean terms infinite to apply in the equation and see that the result is: there is no curve for (a = 3, b = 4, and c = 5) and also for $\forall(ka, kb, kc)$; with $k = (1; 2; 3; 4 \ldots \infty)$.

for $m = 2\exists[(c^2 - b^2) = a^2]$.

If we factorize the curve we have:

$$y^2 = x[x^2 + (c^2 - b^2)] - (bc)^2.$$

If we replace $(c^2 - b^2)$ by a^2 we have $y^2 = x[x^2 + a^2] - (bc)^2$; at the same time $x^2 + a^2 = (k_n)^2$ therefore the curve is reduced as

$$y^2 = x(k_n)^2 - (bc)^2.$$

This makes it easy for us to analyze all the Pythagorean terms, we observe that (bc) is an increase on the terms (b), i.e.,: $(kb) = (cb)$ and requires doing the same with (a) therefore, that $(x = c)$; we known that $\forall(x = k^2)$ with which $y^2 = (ka)^2 - (bc)^2$ and also that $(a < b < c)$ and $(c \neq k^2)$ therefore $(ka)^2$ never is a Pythagorean term; does not exist

$(y = Z)$ for any value of (x) and neither it is possible for any other value of (k) is to fulfill $y^2 = (k_n ka)^2 - (k_n bc)^2$. Is always a modular elliptic curve for $(m = 2)$, we will check if it is also for $\forall(m > 2)$.

Let $(m = 2 + m')$ and $(m'$ = even).

$$y^2 = xa^{2+m'} - (bc)^{2+m'}.$$

We have for your analysis the options.

$$(bc)^{2+m'} = (n;\ k^2);\ n = \text{congruent},$$

or

$$(ka)^{2+m'} = (n;\ k^2);\ \text{being } x = k^2.$$

Let's see if $(bc)^{2+m} = (k_n)^2$.

For this we factorize $(bc)^{2+m'} = (bc)^2(bc)^{m'} = (k_n)^2$ for $\forall(m' = 2;\ 4;\ 6\ldots)$; i.e., $\exists(\sqrt{(bc)^{2+m'}} = (k_n))$ is a square, and the same is true for $(ka)^{2+m'}$, this implies that (bc) and (ka) are Pythagorean terms and, as it is already demonstrated, it is not possible to have $(y \in Z)$. Let's see what $(m' = 1;\ 3;\ 5;\ 7\ldots)$.

We have $(bc)^{2+(2m'+1)} = (bc)^{2(m'+1)+1} = (bc)^{2(m'+1)}(bc)$; we know that $\sqrt{(bc)^{2(m'+1)}} = (k_n)$ and therefore we needs that (bc) also be a square, however $\forall(bc) \neq (k_n)^2$; always that $(c \neq b)$ is required by the curve.

In abstract: if Fermat theorem is true for $c^{2+m} - b^{2+m} = a^{2+m}$ the curve would be modular and, if $\exists[c^{2(m'+1)+1} - b^{2(m'+1)+1}] = a^{2(m'+1)+1}$ the curve would also be modular; is verified that the curve of Frey does not exist and therefore is an elliptic modular curve. That is, all semi-stable elliptic curves are elliptic modular curves it is not shown in the Fermat theorem.

4. Conclusion

(1) In the Birch and Swinneron-Dyer conjecture it is demonstrated that because we can know if an elliptic curve exists or not ($y \in Z$ or $y \notin Z$) and if exists then it has only one solution.

(2) It is to solve the congruent numbers problem and with it is verified that with the Tunell theorem not we have all congruent numbers. The question is inverted, at resolve the congruent number problem is verified the existence of elliptic curve.

(3) Goro Shimura asserted that EVERY elliptic curve is an elliptic curve modular; is incorrect, exist elliptic curves and therefore, they are not one elliptic curve modular. All elliptic curve that exist is reduced to the form $[y^2 = (xk)^2 + B]$ and therefore it is not possible they have a function modular $(f(z) + B)$.

Acknowledgements

I thank Enfer Diez for the publication of his article, without it, it would not have been possible to present this demonstration.

References

[1] Andrew Willes, Modular elliptic curves and Fermat lest theorem, Annals of Mathematic 141(3) (1995), 443-551.

[2] Bryan J. Birch and Nelson M. Stephens, The parity of the rank of the mordell-weil group, Topology 5(4) (1966), 295-299.

[3] Christope Breu, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves Q wild 3-adic exercises, J. American Mathematic Society 14 (2001), 843-939.

[4] Enfer Diez, Equation for solve elliptical curve, U. J. Computational Mathematic 1 (2013).

[5] G. Frey, Links between stable elliptic curves and certain diophantine equations, Annales Universitatis Saraviensis: Series Mathematicae 1(1) (1986), 1-40.

[6] Nelson M. Stephens, Congruent properties of congruent number, Bull. London Math. Soc. 7 (1975).

[7] Keqin Fing, Non-congruent, odd graphs and BDS conjecture, Acta Arith. 75(1) (1996).

[8] Keqin Fings and Yan Xue, New series of odd non-congruent numbers, Science in China Series a Mathematics 49(11) (2006).

■