Universal Journal of Computational Mathematics 1(1): 1-4, 2013
DOI: 10.13189/ujcmj.2013.010101 http://www.hrpub.org

Equation to Solve the Elliptical Curves

Enfer Diez
Department of Mathematics, Institute Polytechnic, G Riol (Lyon France)
*Corresponding Author: en.fer@hotmail.es

Abstract this aim of this article is simply to present the process to define the equation that allows to know if a elliptical curve has solution and which is. $y^2 = x^3 + ax^2 + bx + c$

Keywords proposition; (1.1) ; (1.2) ; elliptical curve exist (E) beloge (Q)

1 Introduction

As the itle indicates, the relevancy of the article is in solving one of the big mathematical problems; to know if an elliptical curve exist (Diophantine equation). We all in major or minor measure know the diverses areas (modulars functions) that have been applied to this problem and nevertheless, is the Arithmetic the that contributes to the solution.

2 Methodology

I initiate problem in the year 1995 when the teacher Andrew Wiles affirm in his article [6] the demonstration of the T. Fermat. In this moment I have checked that elliptical curve Gherar Frey [1] analyzed for K. Ribet [5] not exist for (n = 2). Therefore asumi that the connection of the elliptical curve with Fermat's theorem is a mistake. Continue analyzing values for (n ¿ 2) with the modular functions [5], [6],[7].[8], [10] and observe that not have a method that apply of general form in the elliptical curves; I decides to come back to the origin arithmetic and it gave result.

3 Results

We know the difficulty that has the elliptical curves to be solve in his terms of reference (is a impossibility till now).

$$\forall[a; b; c; (y > o)] \in Z$$

There equation of origin has his expression in the form of: $y^2 = x^3 + ax^2 + bx + c$ therefore if we have the factorized.

$$x(x^2 + ax + b) + c = x^3 + ax^2 + bx + c \qquad (1)$$

Since $(y \in Z)$ and $\forall Z = (2c; 2c+1)$; we take the expression $(2c + 1)$ and we the indicate her in the form.

$$2(c + 1) + 1 \qquad (2)$$

Now we raise this equation to the square.

$$[2(c + 1) + 1]^2 = 4(x^2 + 2x + 1^2) + 4x + 4 + 1^2 \qquad (3)$$

If, we observe the equation (1) and the equation (3) we see that they have certain similarity. Therefore we will do that.

$$x(x^2 + ax + bx) = 4(x^2 + 2x + 1)$$

and

$$c = 4x + 4 + 1$$

It is to say that for $(x = 4)$ we have the equation (3) in the form of.

$$x^3 + 2x^2 + 5x + 5$$

$$x^3 + 2x^2 + 5x + 5 = y^2$$

If $(a = 2; b = 5; c = 5)$ **we have come to an elliptical curve with the particularity of being** $(b = c)$. It is obvious that replacing in the (2) the number two with any other integer major number, we will have an infinity of elliptical curve of the same particularity $(b = c)$.

Come to this point will say, that the same that we deduce elliptical curve; we will determine the equation to solve them. [1]; [3], [9] For it I take again the (3) and indicate her of widespread form, $(m > 2)$ and $(n_1 > 1)$ that is to say.

$$[m(x-n)+n_1]^2 = m^2(x-2xn+n^2)+2m.n_1x-2m.n_1+(n_1)^2$$

$$[m(x + n) + n_1]^2 = ...$$

$$[m(x - n) - n_1]^2 = ...$$

$$[m(x + n) - n_1]^2 = ...$$

Proposition, now we give to the coefficients (a,b,c) of the elliptical curves the following:

$$a = \pm 2n; b = n^2 \pm 2m.n_1; c = (b - n^2)n + (n_1)^2$$

I will explain the because the values of (b) and (c);to (b) it corresponds to him.

$$b = n^2 \pm 2m.n_1.x;$$

we know for the beginning (3) that $(m^2 = x)$ and therefore we have that.

$$b = (mn)^2+2m.n_1.m^2 = m^2(n^2+2m.n_1) = x(n^2+2m.n_1)$$

$b = x(n^2 + 2m.n_1)$; implies that it is the value of (bx). Therefore

$$b = n^2 \pm 2m.n_1 \tag{4}$$

In turn to (c) the corresponds the value $c = 2m.n_1 + (n_1)^2$. If we clear in the (4) the value of $(2m.n_1)$ and we replace it in the previous equality (c); it is to say.

$$b - n^2 = 2m.n_1$$

with which.

$$c = (b - n^2)n + (n_1)^2 \tag{5}$$

Done the explanations of the values that take $(a; b; c)$ in the elliptical curves. Following thing be to define the general equation for it,we replace in the (4) the value of (m) and in the (5) the value of (n_1).

$$m = \frac{b - n^2}{2n_1}$$

$$(n_1)^2 = c - n(b - n^2)$$

$$n_1 = \sqrt{c - n(b - n^2)}$$

Now we replace the value of (n_1) **in the equality of (m) and we have that:**

$$m = \frac{b - n^2}{2\sqrt{c - n(b - n^2)}}$$

Later we replace in this equation the value of (n) we know that $(a = 2n)$ and therefore $(n = \frac{a}{2})$ then.

$$m = \frac{b - (\frac{a}{2})^2}{2\sqrt{c - [b - (\frac{a}{2})^2](\frac{a}{2})}}$$

we know for the (3) that $(m^2 = x)$ **therefore the GENERAL EQUATION stays in the form of.**

for $\forall(x > 1)$

$$x = \frac{[b - (\frac{a}{2})^2]^2}{4[c - [b - (\frac{a}{2})^2](\pm\frac{a}{2})]]}$$

(1.1)

$$x = \frac{[(\frac{a}{2})^2 - b]^2}{4[c - [(\frac{a}{2})^2 - b](\pm\frac{a}{2})]]}$$

(2.2)

This general equation applies to itself in any elliptical curve with the **exception of those that do not take as minimum two of the coefficients of origin of values bigger than the unit.**

Summarizing: elliptical curves exist with $(a; b; c; x) \in Z$**,and also elliptical curves exist (E) belongs Q** [7].[8]

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

Before going on to the examples I indicate the equation by any square.

$$4 + \sum_{n\geq 2}(2n + 1) = A^2, (1.3)$$

4 Discussion

It is evident with examples that I mention later; since I analyze all the possible forms of elliptical curves. Checking is so much for those exist as the that not exist.

EXAMPLE 1

$$y^2 = x^3 + bx + c$$

$$x = \frac{[b - (\frac{0}{2})^2]^2}{4[c - [b - (\frac{0}{2})^2](\frac{0}{2})]} = \frac{b^2}{4c}$$

It is to say: $\forall(b^2 = 4c.x)$.We have $(c = 2^{k'}; b^2 = 4c)$ always $(x = c)$.

Therefore $b = 2^k$ **and** $c = 2^{k'}$**; example** $k = 3$**;** $k' = 2$

$$x = \frac{(2^3)^2}{4 \cdot 2^2} = 4$$

$$x = \frac{(2^4)^2}{4 \cdot 2^3} = 8$$

$$10^2 = 4^3 + 8 \cdot 4 + 4$$

Summarizing by the general equation is deduced that the elliptical curve in the form,$y^2 = x^3 + bx + c$ **do not exist if** $x \neq c$**.** If $(c = 0)$ then we have.

$y^2 = x^3 + xb$ **; they exist with** $(b = x)$

Is to say: $y^2 = x^2(x + 1); 3^2(3 + 1) = 6^2$

Other values exist for $(x > 3)$ **by the (1.3) of the cuadrado** , for $\forall[x = 3 + \sum(2n + 1)]$

EXAMPLE 2

$$y^2 = x^3 - ax^2 + bx$$

In this equation we have that (a) takes a negative value (-a) and therefore: $y^2 = x^3 + (-a)x^2 + bx$

$$x = \frac{[b - (\frac{a}{2})^2]^2}{4[0 - [b - (\frac{a}{2})^2](\frac{a}{2})]] = \frac{4b - a^2}{8(-a)}$$

With which: $8x(-a) = 4b - a^2$; in order that (x) is positive ($a^2 > b$) is to say.

$$a = b; a = 4b; a = 4b + b'$$

; with which.

$$x = \frac{4b - (4b)^2}{8(-a)} = \frac{b(1-4b)}{2(-a)} \Rightarrow \frac{b}{2(-a)} = Z$$

And as: $a = (b; 4b; 4b+b')$, **if we replace these values in** $\frac{b}{2(-a)}$**we have that.**

$$\frac{b}{2(-a)} \neq Z$$

Therefore the elliptical curves do not exist in the form $y^2 = x^3 - ax^2 + bx$**.**

EXAMPLE 3

If we admit as value (-x) in the elliptical curve of origin it takes following form.

$y^2 = (-x)^3 + (-a)x^2 - bx + c$; we know for the general equations that this is a consequence of being always (a) negative and in turn ($a > b$) for the (1.1); or well (a) negative in turn ($a < b$) in (2.2).

$$y^2 = (-x)^3 - ax^2 - bx + c \Rightarrow c > [(-x)^3 - ax^2 - bx]$$

Therefore with the (1.1) and (1.2) we observe that in order that (x) should be a negative value (-x); the value of $[b - ([\frac{a}{2})^2]^2$ it have that be a negative number; and is not possible. Therefore would have to be negative the value of $4[c - [b - (\frac{a}{2})^2](\frac{a}{2})]$. This is not also possible because $c > [(-x)^3 - ax^2 - bx]$; with which this elliptical curve $y^2 = (-x)^3 - ax^2 - bx + c$ **; do not exist.**

EXAMPLE 4

$$y^2 = x^3 + 4x^2 + 34x + 85$$

$$x = \frac{[34 - (\frac{4}{2})^2]^2}{4[85 - [34 - (\frac{4}{2})^2(\frac{4}{2}]]} = 9$$

$$38^2 = 9^3 + 4 \cdot 9^2 + 34 \cdot 9 + 85$$

EXAMPLE 5

$$y^2 = x^3 + ax^2 + c$$

$$x = \frac{[0 - (\frac{a}{2})^2]^2}{4[c - [0 - (\frac{a}{2})^2]\frac{a}{2}]} = \frac{a^4}{8[8c - a^3]}$$

therefore: $8x[8c - a^3] = a^4$; is to say that.

$$\sqrt{8[8c - a^3]} = a^2 \Rightarrow 8c \geq a^3$$

For

$$c = 8$$

we have $8^2 - 4^3 = 0$ with wich $a^2 = 0$

if ($8c > a^3$) them always $\sqrt{(8c - a^3)} = 8$ therefore $(8c - 8^2) = a^3$ implies that $8(c - 8) = a^3$, with which $(c - 8 = 8^2)$, it is to say that c = 72

We take again the value of $x = \frac{a^4}{8[8c - a^3]}$ and we replace the value of ($c = 72$).

$$x = \frac{8^4}{8[8 \cdot 72 - 8^3]} = 8$$

consequently the elliptical curve : $y^2 = x^3 + ax^2 + c$ **does not exist for being (x = a = 8) and (c = 72).**

EXAMPLE 6

Elliptical curves in the form: $(Y^2 = X^3 - X + C)$ and $(Y^2 = X^3 - X - C)$. they are elliptical curves that do not take as minimum, two of the coefficients of the equation of origin of bigger values than the unit. Therefore is not applicable the **(1.1)**. The solution of these elliptical curves is trivial, because it implies $(x^3 > y^2)$ therefore the solution is obtained choosing a number to the equare that precedes the value $(x^3 - x)$.

$$5^2 = 3^3 - 3 + 1$$

$$11^2 = 5^3 - 5 + 1$$

$$12^2 = 6^3 - 6 - 56$$

$$13^2 = 8^3 - 8 - 335$$

$$14^2 = 7^3 - 7 - 140$$

$$14^2 = 6^3 - 6 - 14; \rightarrow (y^2 + y = x^3 - x)$$

$$17^2 = 11^3 - 11 - 1031$$

.....

The only difficulty is in the alliptical curve with ($c = 1$); demonstration that already there did the teacher Taylor [8] as elliptical modular curves. Nevertheless this type of elliptical curves are demonstrated they same, because: $(y^2 - 1 \neq y^2 + 1)$.

EXAMPLE 7

We verify **elliptical curve Gerhara Frey's** [1], [6] with the (1.1).

$$y^2 = x^3 + x^2(C^n - B^n) - (BC)^2$$

For it we have: $a = C^n - B^n$; $b = 0$; $c = (BC)^2$,therefore.

$$x = \frac{[0 - (\frac{C^n - B^n}{2})^2]^2}{4[(BC)^2 - [0 - (\frac{C^n - B^n}{2})^2]\frac{C^n - B^n}{2}]}$$

$$x = \frac{(\frac{C^n - B^n}{2})^4}{4[(BC)^2 - (\frac{C^n - B^n}{2})^3]}$$

$$x = \frac{(C^n - B^n)^4}{8^2[(BC)^2 - (\frac{C^n - B^n}{2})^3]}$$

If we admit that it exist $C^n - B^n = m^n$ then:

$$x = \frac{(m^n)^4}{8^2[(BC)^2 - (\frac{m^n}{2})^3]}$$

It implies that: $m = (8; 8A)$ with which.

$$x = \frac{(8^n)^3(8^{n-2})}{(BC)^2 - (\frac{m^n}{2})^3}$$

Always: $[(BC)^2 - (\frac{m^n}{2})^3 = 8^m]$

$$(BC)^2 - 8^m = \frac{(m^n)^3}{8}$$

$$8[(BC)^2 - 8^{m-1}] = (m^n)^3$$

It is to say that: $(BC)^2 - 8^{m-1} = 8^2$ therefore $(BC)^2 = 8^2 + 8^{m-1}$ **this is not possible.**

Therefore not exist values of $(x = Z)$ for $(n \geq 2)$. **Gerhara Frey's curve does not exist** for any of the values of (n).

5 Conclusions

The article gives solution to the elliptical curves and refutes the following.
The conjecture Taniyama-Shimura affirms in his terms that. all elliptical curve is an elliptical modular curve

Falsely, [8] **because if an elliptical curve exist it does not have symmetrical projection and therefore, it cannot be an elliptical modular curve.** Andrew Wiles's work [6] does not demonstrate Fermats's theorem because equation G. Frey's does not exist for value $(n \geq 2)$. To see example (6).

References

[1] G. Frey . links between stable elliptic curve and certain diophante equation, *Annales Universitati Saraniensis 1* (1986) 1-40

[2] Silverman J.H, the Arithmetic of elliptic curves, *Springer, New York* 1986

[3] M. Flach, a finitiness theorem for the symmetic square of an elliptic curve, *Invent. Math.* 109 (1992), 563-594

[4] Silverman J.H, advanced topics in the Arithmetic of elliptic curve, *Springer,New York* 1994

[5] K.A.Ribet, on modular representations of arising from modular forms, *Invet. Math,100, 431-476*, 1990

[6] K.A. Ribet. report on mod l representations of Gal(Q/Q), *Proc. of Symp.in Pure Math* 55, 639-676, 1994

[7] Andrew Wiles, modular elliptic curves and Fermat's lest theorem, *Annals of Mathematic 141 (3) 443-551* 1995

[8] Darmon .H , Wiles' theorem and the arithmetic of elliptic curves, in modular forms and Fermat's last theorem549-569, *Springer* 1997

[9] Breuil. C, B. Diamond, F. Taylor, on the modularity of elliptic cueves over Q: wild 3-adic exercises, *J. Amer. Math. Soc 14, 843-939* 2001

[10] Silverman Joseph H. arithmetic of elliptical curves; *graduate texts in Mathematics 106* ; New York, Springer 2009