IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 16, Issue 3 Ser. III (May – June 2020), PP 01-05
www.iosrjournals.org

On Congruent Numbers Elliptic Curves

Laurent Djerassem[1], Daniel Tieudjo[2]
[1](*Département de Mathématiques, Faculté des Sciences, Université de N'djamena Tchad)*
[2](*Department of Mathematics and Computer Science, University of Ngaoundere and African Institute forMathematical Sciences (AIMS) Cameroon)*

Abstract:*We present here a result on congruent numbers elliptic curves. We construct an isomorphism class of elliptic curves associated to congruent numbers. We show that, two elliptic curves defined over*Q *and associated to congruent numbers which are the areas of two congruent right-angled triangles are* Q*-isomorphic. We prove a relation on the discriminants of congruent numbers elliptic curves, and we pose a conjecture on the conductors of congruent numbers elliptic curves.*

Key Word*:Congruent number, congruent elliptic curves, isomorphism, rank of an elliptic curve, BSD-conjecture.*

Date of Submission: 13-05-2020 Date of Acceptance: 25-05-2020

I. Introduction

The congruent numbers problem has been the concern of many mathematicians over the years. The term"Congruent Number" (CN) comes from Fibonacci, who, in his work Liber Quadratorum (Book of Squares),defined a congruum to be an integer *n* such that $x^2 \pm n$ is a square. A positive integer *n* is called a congruentnumber if *n* is the area of a right-angled triangle with three rational sides. Jerrold Tunell (in [8]) associated to a congruent number *n* an elliptic curve E_n over the rational field Q, defied by:

$$E_n : y^2 = x^3 - n^2 x \tag{1.1}$$

where $y \neq 0$. An anonymous manuscript [6], written before 972 showed that this problem was proposed by Al-Karaji (953–1029) wondering what integers $n \in \mathrm{Z}$ by subtracting them from a square give anothersquare? i.e., $a^2 - n = b^2$, then *n* is congruent see [8]. It means that, given a positive integer *n*, the question isto find a rational square a^2 $(a \in \mathrm{Q} \setminus \{0\})$ such that $a^2 \pm n$ are both rational squares. The triangular version saysthat, given a positive integer *n*, find a right-angled triangle such that its sides are rational and its area equals*n*. These two versions are equivalent by [6]. Else *n* is called a non-congruent number (non-CN). It is wellknown that *n* is non-congruent if and only if, the rank of the rational points group E_n(Q) ofMordell-Weil iszero (see [12]). It is also known that any positive integer *n* can be written as $n = u^2 v$, where *v* has no squarefactors (*v* is a 'squarefree integer') and $u \in \mathrm{Z}$, the set of integers. It is clear that *n* is a congruent number if and only if *v* is. Awell-known conjecture made by Alter, Curtz and Kubota in [1] says that: every square free integer *n* verifies

$$n \text{ is congruent if } n \equiv 5, 6, 7 \pmod 8 \tag{1.2}$$

In 1983 Jerrold Tunnel found an easy formula to test if a number is congruent, see [8]. This formula usesthe BSD-conjecture. Consequently, a number *n* is congruent if and only if the associated elliptic curve hasmore than the three obvious solutions $(0,0)$, $(n,0)$ $(-n,0)$, see [11].Hence, the following problem arises: "How can we possibly tell whether or not this cubic equation has lotsof solutions or just the three obvious ones?"Bryan Birch and Peter Swinnerton-Dyer found a conjectural answer in the 1960s. Their conjecture, presentedat the Clay Math Institute, is already solved by Mohamed Sghiar in [14]. In [5, 7], it is known that for a congruent number *n*, the newform $f = \sum_{l \in \mathrm{Z}} a_l q^l$ and the *L*-function associated to theelliptic curve $E_n$have the same coefficients.

Let *n* and *n′* be two congruent numbers associated respectively to the Pythagorean triples (a,b,c) and (a',b',c') such that

$$\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c} = k \in \mathrm{Q}_+ \setminus \{0\} \tag{1.3}$$

i.e. the corresponding right-angled triangles are congruent. Then, for any point $M_{n'}(X_{n'}, Y_{n'}) \in E_{n'}$ thereexists a unique point $M_n(X_n, Y_n) \in E_n$ such that

$$X_{n'} = k^2 X_n \quad \text{and} \quad Y_{n'} = k^3 Y_n \tag{1.4}$$

We prove the following results.

Theorem 1.1. For two congruent numbers n and n' associated respectively to the congruent right-angledtriangles Δ_n and $\Delta_{n'}$ with the corresponding Pythagorean triples (a,b,c) and (a',b',c') such that $\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c} = k \in \mathrm{Q}_+ \setminus \{0\}$, the associated respectivecurves E_n and $E_{n'}$ are isomorphic, and the map $\varphi : E_n \to E_{n'}$ such that $(X_n, Y_n) \mapsto (X_{n'}, Y_{n'}) = (k^2 X_n, k^3 Y_n)$ is a Q-isomorphism of elliptic curves.

This theorem can be generalized for $n_1, \dots, n_m$ congruent numbers associated to congruentright-angled triangles $\Delta_{n_1}, \dots, \Delta_{n_m}$, where$m$ is a non-zero natural number $(m \in \mathrm{N} \setminus \{0\})$.Let $(a_i, b_i, c_i)_{1 \le i \le m}$ be the corresponding pythagorean triples such that $\frac{a_{i+1}}{a_i} = \frac{b_{i+1}}{b_i} = \frac{c_{i+1}}{c_i} = k \in \mathrm{Q}_+ \setminus \{0\},\ 1 \le i \le m-1$. We have the following corollary.

Corollary 1.2. Let $n_1, \dots n_m$ $(m \in \mathrm{N} \setminus \{0\})$ be congruent numbers associated to congruent right-angled triangles $\Delta_{n_1}, \dots, \Delta_{n_m}$ with corresponding pythagorean triples $(a_i, b_i, c_i)_{1 \le i \le m}$ such that $\frac{a_{i+1}}{a_i} = \frac{b_{i+1}}{b_i} = \frac{c_{i+1}}{c_i} = k \in Q_+ \setminus \{0\}$ for $1 \le i \le m-1$. Then for $i = 1, \dots, m$ there exists a sequence of points $(X_i, Y_i) \in E_{n_i}$ such that $(X_{i+1}, Y_{i+1}) = (k^2 X_i, k^3 Y_i)$ $1 \le i \le m-1$.The curves $E_{n_1}, \dots, E_{n_m}$ associated to congruent numbers $n_1, \dots n_m$ are isomorphic over Q.

Consider the following table of congruent numbers, obtained by conjectural relation (1.2) above. This is the table ofAlter, Curtz and Kubota (see [1]).

Table 1.3.

Table 1.3: Some congruent numbers

5	6	7	13	14	15	20	21	22	23	24	28	29	30	31
34	37	38	39	41	45	46	47	52	53	54	55	56	…	…
…														

Remark 1.4. There is also a table of non-congruent numbers and a table of unclassified numbers, see[13].There is no information on the so-called unclassified numbers. For example, the number 113 not classifiedis conjectured non-congruent by Birch and Swinnerton-Dyer in [2]. The number 897 also is supposed notclassified because it does not appear on the table of Alter, Curtz and Kubota, but Girardin made an error byconsidering it as congruent on his table,see [9]. We prove the following theorem and, based on SAGE software, we state the below conjecture.

Theorem 1.5. Let n and n' be two congruent numbers chosen arbitrarily onthe table 1.3 such that $n' = dn, n' > n$ where d is a positive integer. Let $\Delta(E_n)$ and $\Delta(E_{n'})$ be the discriminants of the congruent curves E_n and$E_{n'}$ respectively. Then

$$\Delta(E_{n'}) = d^6 \Delta(E_n) \tag{1.5}$$

If $d = k^2$, then E_n and $E_{n'}$ are isomorphic and

$$\Delta(E_{n'}) = k^{12} \Delta(E_n) \tag{1.6}$$

Conjecture 1.6. Let n and n' be two congruent numbers chosen arbitrarily on the table 1.3 such that $n' = dn$, $n' > n$ where d is a positive integer. Let N_{E_n} and $N_{E_{n'}}$ be the conductors of E_n and $E_{n'}$ respectively.Then

$$N_{E_{n'}} = 2 N_{E_n} \quad \text{if} \quad n' = 2n \tag{1.7}$$

$$N_{E_{n'}} = 3^2 N_{E_n} \quad \text{if} \quad n' = 3n \tag{1.8}$$

II. Preliminaries

Let K be a commutative field. The set K^{n+1} can be considered as a K-vector space of dimension $n+1$ .Let $E = K^{n+1}$, $F = K^{m+1}$ be two K-vector spaces of dimension $n+1$ and $m+1$ respectively, where $n \le m$. It is well known that the projective space associated to Edenoted $\mathbf{P}(E)$ is the quotient $(E \setminus \{0\})/\sim$,where the relation $\sim$ is defined on E by:

$x, y \in E \setminus \{0\}$, $x \sim y$ if and only if there exists a scalar $\lambda \in K \setminus \{0\}$ such that $x = \lambda y$.

The map $\pi_E : E \setminus \{0\} \to \mathbf{P}(E)$ is the canonical surjection and $[x]$ represents the class of x.

Definition and remark 2.1. An elliptic curve *E* over the rational field Q is a projective nonsingular curve definedby the projective closure of the zero locus of an equation of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathrm{Q}$. In the others words, *E* is a set of nonsingular points $P[X:Y:Z] \in \mathbf{P}^2(Q)$ suchthat

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.2}$$

This last equation is obtained by changing of variables $x = \dfrac{X}{Z},\ \ y = \dfrac{Y}{Z}$.

In [15] we know that the set *E*(Q) of rational points on *E* is equipped with an abelian group structure.

Theorem 2.2. See [10] and [19] theorem 15, c) page 13.

(i) Let E_a and E_b be two elliptic curves defined over a field *K* by:

$$E_a : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E_b : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

Then E_a and E_b are isomorphic, if and only if, $\exists(u,r,s,t) \in K^* \times K^3$ such that

$$\begin{cases} ub_1 &= & a_1 + 2s \\ u^2b_2 &= & a_2 - sa_1 + 3r - s^2 \\ u^3b_3 &= & a_3 + ra_1 + 2t \\ u^4b_4 &= & a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st \\ u^6b_6 &= & a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \end{cases} \tag{2.3}$$

(ii) Let *E* and *E*′ be two elliptic curves over the field Q and defined respectively by the following equations:

$$y^2 = x^3 + kx \quad \text{and} \quad y^2 = x^3 + k'x \tag{2.4}$$

where $k, k' \in Z \setminus \{0\}$. Then, these curves are isomorphic over $Q\left(\sqrt[4]{\dfrac{k}{k'}}\right)$.

(iii) Let *E* be an elliptic curve over a field *K*. Any isomorphism $\varphi : E \to E'$ of elliptic curves over Qis of the form

$$(x,y) \mapsto (u^2x + r, u^3y + u^2sy + t) \tag{2.5}$$

for some $u, r, s, t \in K, u \neq 0$.

Theorem 2.3. (Mordell-Weil) Let *E* be an elliptic curve over Q. The group *E*(Q) of Q-valued points onthe elliptic curve *E* is finitely generated. So,

$$E(\mathrm{Q}) = Z^r \times E(\mathrm{Q})_{tors}$$

where $E(\mathrm{Q})_{tors}$ is the finite torsion group.

Proof 2.4. See [17].

Definition 2.5. The number *r* in the above theorem is called the algebraic rank of the curve *E* over Q.

Definition 2.6. See [20]. Assume*n* is a square-free integer. Let E_n/Q be the congruentelliptic curve defined over Q associated to *n*. Then the *L*-series of E_n/Q for $\Re e(s) > \frac{3}{2}$ is defined by

$$L(E_n, s) = \prod_p \left(1 - a_p p^{-s} + p^{-2s}\right)^{-1} \text{ for all } p \text{not dividing } 2n,\ \Re e(s) \text{ is the real part of } s$$

where $a_p = p + 1 - \left|\overline{E}_n(F_p)\right|$ and $\overline{E}_n(F_p)$ is the curve obtained from E_n/Q thanks to the map reduction modulo*p*, i.e. the curve defined over the finite field F_p of *p* elements, for primes *p*.

Conjecture 2.1. (BSD conjecture (weak form)). If *r* is the algebraic rank of an elliptic curve E_n, then $L(E_n,1)$ has a zero of order *r*. Equivalently, the Taylor expansion of $L(E_n, s)$ at a neighborhood of *s* = 1has the form:

$$c_0(s-1)^r + c_1(s-1)^{r+1} + c_2(s-1)^{r+2} + \cdots$$

where all c_i are complex numbers and $c_0 \neq 0$.

Definition 2.7. If $L(E_n, s)$ has the following Taylor expansion

$$L(E_n, s) = c_0(s-1)^\rho + c_1(s-1)^{\rho+1} + c_2(s-1)^{\rho+2} + \cdots$$

at 1with $c_0 \neq 0$, then we call $\rho$the analytic rank of E_n.

The BSD conjecture says that the analytic rank of an elliptic curve is equal to its algebraic rank. We willalways specify when talking about analytic rank, whereas if we use the term "rank" alone we refer to thealgebraic rank.

Theorem 2.8. 1. If BSD holds, then $L(E_n,1)=0$ if and only if *n* is a congruent number.

2. Let *n* be a squarefree positive integer. Then *n* is a congruent number if and only if the rank of E_n is positive.

Proof 2.9. See [18] Theorem 4.8, p. 14 and theorem 5.11, p. 17.

Theorem 2.10. 1. Let $n>0$. There is a one-to-one correspondence between right triangles with area *n*and 3-terms arithmetic progressions of squares with common difference *n*: the sets $\left\{(a,b,c): a^2+b^2=c^2; n=\frac{ab}{2}\right\}$ and $\left\{(r,s,t): s^2-r^2=n, t^2-s^2=n\right\}$are in one-to-one correspondence defined by:

$(a,b,c)\mapsto\left(\frac{b-a}{2},\frac{c}{2},\frac{b+a}{2}\right)$ and conversely $(r,s,t)\mapsto(t-r,t+r,2s)$.

2. For $n>0$, there is a one-to-one correspondence between the following two sets: $\left\{(a,b,c): a^2+b^2=c^2; n=\frac{ab}{2}\right\}$ and $E_n=\left\{(x,y): y^2=x^3-n^2x, y\neq 0\right\}$. The mutually inverse correspondences between these sets are $(a,b,c)\mapsto\left(\frac{nb}{c-a},\frac{2n^2}{c-a}\right)$ and $(x,y)\mapsto\left(\frac{x^2-n^2}{y},\frac{2nx}{y},\frac{x^2+n^2}{y}\right)$.

Proof 2.11. See [18], proposition 2.3, page 6.

III. Proofs of theorems

We prove Theorem 1.1 first. Corollary 1.2 is proved by induction. We then prove Theorem 1.5.

3.1 Proof of Theorem 1.1

Proof 3.1. Let *n*, *n′* be congruent numbers associated to right angled triangles Δ_n, $\Delta_{n'}$ respectively andsuch that $\frac{a'}{a}=\frac{b'}{b}=\frac{c'}{c}=k$. We know by theorem 2.9 that the triple (a,b,c) corresponds to the point $\left(\frac{nb}{c-a},\frac{2n^2}{c-a}\right)$of E_n and the second triple $(a',b',c')$is associated to the point $\left(\frac{n'b'}{c'-a'},\frac{2n'^2}{c'-a'}\right)$. Now ever $n'=k^2n$ becausethere is a *k*-homothety and the area transformed is multiplied by k^2. Plugging a',b',c' by their values in(1.3) we have the coordinates $(X_{n'},Y_{n'})$ on the curve $E_{n'}$ given by $X_{n'}=k^2X_n$ and $Y_{n'}=k^3Y_n$, where (X_n,Y_n) are the coordinates of an arbitrary point on E_n. It is clear bytheorem 2.2 that, an isomorphism between two elliptic curves defined over Q is of the form:

$$f_k: E\to E'$$
$$(X,Y)\mapsto(k^2X+r, k^3Y+sk^2Y+t)$$

Therefore, the curves E_n and $E_{n'}$ are clearly isomorphic over Q by theorem 2.2.(ii), since $\mathbb{Q}\left(\sqrt[4]{\frac{n^2}{n'^2}}\right)=\mathbb{Q}\left(\frac{1}{k}\right)=\mathbb{Q}$.

Note that the inverse application of such f_k, noted g_k is defined by

$$g_k: E_{n'}\to E_n$$
$$(X_{n'},Y_{n'})\mapsto(k^{-2}X_{n'},k^{-3}Y_{n'}).$$ □

Example 3.2. Let us consider the three following congruent numbers n_1 = 6, n_2 = 24 and n_3 = 96 with the triples $(4,3,6)$, $(8,6,10)$ and $(16,12,20)$.We see here that k = 2, $P_1=(18,72)$, $P_2=(72,576)=f_2(P_1)$ and $P_3=(288,4608)=f_2^2(P_1)$.

3.2 Proof of Corollary 1.2

This corollary is a generalization of the theorem 1.1.

Proof 3.3. Let us note (a_i,b_i,c_i) the pythagorean triple associated to each congruent numbern_i, for i = 1, 2, …, *m*. Fortwo elliptic curves E_{n_s} and E_{n_l} such that $s<l$, then $n_l=n_sk^{2(l-s)}$. So these curves E_{n_s} and E_{n_l} areisomorphic and all the curves $E_{n_1},\ldots,E_{n_m}$ form an isomorphism class of elliptic curves because theyare all pairwise isomorphic and we have

$$f_k(E_{n_1})=E_{n_2},\ldots,f_k^l(E_{n_1})=\underbrace{f_k\circ\cdots\circ f_k}_{l\text{ times}}(E_{n_1})$$

for $l\geq 1$, where f_k is defined as follows

$$f_k(x,y)=(k^2x,k^3y) \quad \text{and} \quad \underbrace{f_k\circ\cdots\circ f_k}_{l \text{ times}}(x,y)=(k^{2l}x,k^{3l}y) \text{ for any positive integer } l\geq 1. \qquad \square$$

3.3 Proof of Theorem 1.5

1. We prove relation (1.5). Let n and n' be two congruent numbers such that $n'=dn$, where $d>0$ isan integer. Let E_n and $E_{n'}$ be the congruent number curves associated to n and n' respectively. Weknow that every elliptic curve Edefined on the field Q has equation of the form $y^2=x^3+ax+b$. Itsdiscriminant is given by

$$\Delta(E)=-16(4a^3+27b^2)$$

So, the discriminant of the curve E_n is

$$\Delta(E_n)=64n^2$$

Hence, since $n'=dn$, we have $\Delta(E_{n'})=-16(4(-d^2n^2)^3+0)=d^6\Delta(E_n)$.

2. Now we prove the relation (1.6). Let $d=k^2$. Let n and n' be two congruent numbers such that $n'=k^2n$ .Since E_n and $E_{n'}$ are isomorphic by theorem 1.1, then $\Delta(E_n)$ and $\Delta(E_{n'})$ are linked by the relation(1.6). So the relation (1.7) is verified. $\square$

IV. Acknowledgments

L. Djerassem acknowledges the support of the African Institute for Mathematics Sciences (AIMS-Cameroon) during his research visit in Cameroon.

References

[1]. R. Alter, T. B. Curtz and K. K. Kubota. Remarks and results on congruent numbers. In Proc. 3rd South Eastern Conf. Combin., Graph theory and Comput., (1972), p. 27-35.

[2]. B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves II, J. reineangew. Math., 218,(1965), p. 79-108.

[3]. P. Colmez, Le problème des nombres congruents. Séminaire des élèves de l'Ecole Polytechnique, (2005), available at https://webusers.imj-prg.fr/~pierre.colmez/congruents.pdf.

[4]. W. A. Coppel, Number theory: An introduction to Mathematics. Part B, Springer-Verlag, New York,(2006).

[5]. G. Cornnel, J. Silverman and G. Stevens, Modular forms and Fermat's last theorem, Springer, (1997).

[6]. L. E. Dickson, History of Theory of Number, Vol. 2 (1920), p. 462.

[7]. H. Darmon, F. Diamond, R. Taylor, Fermat's Last Theorem, Current Developments in Mathematics,International Press, (1995),p. 1-157.

[8]. E. Garcia, Solving the congruent numbers problem is solving the elliptic curve problem, Journal of Pureand Applied Mathematics: Advances and Applications, Volume 17, Number 2, (2017), p. 77-87.

[9]. A. Girardin. Nombres congruents, Intermediaire des Math., vol. 22, 1915, p. 52-53.

[10]. M. Hedabou, Amélioration et sécurisation des calculs arithmétiques pour la cryptographie basée sur lescourbes elliptiques, LESIA (Laboratoire d'Etudes des Systèmes Informatiques et Automatiques);thèse de doctorat, Numéro d'ordre 844, soutenue le 20 octobre 2006, (2006).

[11]. N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer,(1984).

[12]. N. Koblitz, Introduction to Elliptic Curves and Modulars Forms. Graduate Texts in Mathematics, Volume 97, Springer,(1993).

[13]. J. Lagrange, Construction d'une table de nombres congruents, Mémoires de la S.M.F., Tome 49-50 (1977), p. 125-130, available at www.numdam.org/

[14]. M. Sghiar, La preuve de la conjecture de Birch et Swinnerton-Dyer, IOSR journal of Mathematics(IOSR-JM) 14 (3)(2018), p. 50-59, available at www.iorsjournals.org.

[15]. J. H. Silverman. The arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Volume 106, Springer-Verlag, New York, (1986).

[16]. J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math., Volume151, Springer-Verlag, Berlin and New York, (1994).

[17]. J. H. Silverman and J. Tate, Rational points on Elliptic Curves, Springer-Verlag, New York (1992).

[18]. J. Star, Elliptic Curves and the Congruent Number Problem, CMC Senior Theses, Paper 1120, (2015).

[19]. S. Thiboutot, Courbes elliptiques, représentations galoisiennes de l'équation $x^2+y^3=z^5$, Mémoirede Master ès Sciences, Faculté des Etudes Supérieures de l'Université McGill, (1996).

[20]. J. Top and N. Yui, Congruent number problems and their variants, Algorithmic Number Theory MSRIPublications, Volume 44,(2008).

Laurent Djerassem, et. al. "On Congruent Numbers Elliptic Curves." *IOSR Journal of Mathematics (IOSR-JM)*, 16(3), (2020): pp. 01-05.