On Congruent Numbers Elliptic Curves

Laurent Djerassem¹, Daniel Tieudjo²

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 for Mathematical 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 \( \mathbb{Q} \) and associated to congruent numbers which are the areas of two congruent right-angled triangles are \( \mathbb{Q} \)-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 congruent number if \( n \) is the area of a right-angled triangle with three rational sides. Jerrod Tunell (in [8]) associated to a congruent number \( n \) an elliptic curve \( E_n \) over the rational field \( \mathbb{Q} \), defined by:

\[
E_n : y^2 = x^3 - n^2x
\]

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 \( n \in \mathbb{Z} \) by subtracting them from a square give another square? i.e., \( a^2 - n = b^2 \), then \( n \) is congruent see [8]. It means that, given a positive integer \( n \), the question is to find a rational square \( a^2 (a \in \mathbb{Q} \setminus \{0\}) \) such that \( a^2 \pm n \) are both rational squares. The triangular version says that, 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 well known that \( n \) is non-congruent if and only if, the rank of the rational points group \( E_n(\mathbb{Q}) \) of Mordell-Weil is zero (see [12]). It is also known that any positive integer \( n \) can be written as \( n = \nu v \), where \( \nu \) has no square factors (\( \nu \) is a 'squarefree integer') and \( v \in \mathbb{Z} \), the set of integers. It is clear that \( n \) is a congruent number if and only if \( v \) is. A well known conjecture made by Alter, Curtz and Kubota in [1] says that: every square free integer \( n \) verifies

\[
n \text{is congruent if } n = 5, 6, 7 \pmod{8}
\]

In 1983 Jerrold Tunnel found an easy formula to test if a number is congruent, see [8]. This formula useth the BSD-conjecture. Consequently, a number \( n \) is congruent if and only if the associated elliptic curve has more than the three obvious solutions \( (0,0), (n,0), (0,-n) \), see [11]. Hence, the following problem arises:

"How can we possibly tell whether or not this cubic equation has lots of solutions or just the three obvious ones?" Bryan Birch and Peter Swinnerton-Dyer found a conjectural answer in the 1960s. Their conjecture, presented at 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 \( f = \sum_{a}a_{q}q^{n} \) and the \( L \)-function associated to the elliptic 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

\[
\frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c} = k \in \mathbb{Q}_+ \setminus \{0\}
\]

i.e. the corresponding right-angled triangles are congruent. Then, for any point \( M_n(X_n,Y_n) \in E_n \) there exists a unique point \( M_n(X'_n,Y'_n) \in E_n \) such that

DOI: 10.9790/5728-1603030105 www.iosrjournals.org
\[ X_n = k^2X_e \quad \text{and} \quad Y_n = k^2Y_e \quad (1.4) \]

We prove the following results.

**Theorem 1.1.** For two congruent numbers \( n \) and \( n' \) associated respectively to the congruent right-angled triangles \( \Delta_n \) and \( \Delta_{n'} \) with the corresponding Pythagorean triples \( (a,b,c) \) and \( (a',b',c') \) such that \( \frac{a'}{a} = \frac{b'}{b} = \frac{c'}{c} = k \in \mathbb{Q} \setminus \{0\} \), the associated respective curves \( E_n \) and \( E_{n'} \) are isomorphic, and the map
\[
\varphi: E_n \to E_{n'} \quad \text{such that} \quad (X_n,Y_n) \mapsto (X_{n'},Y_{n'}) = (k^2X_n,k^2Y_n) \text{ is a } \mathbb{Q}\text{-isomorphism of elliptic curves.}
\]

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

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

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

**Table 1.3:**

<table>
<thead>
<tr>
<th>5</th>
<th>6</th>
<th>7</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>29</th>
<th>30</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>34</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td>41</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>52</td>
<td>53</td>
<td>54</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 classified is conjectured to be congruent by Birch and Swinnerton-Dyer in [2]. The number 897 also is supposed not classified because it does not appear on the table of Alter, Curtz and Kubota, but Girardin made an error by considering 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 on the 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
\[
\Delta(E_{n'}) = d^6 \Delta(E_n) \quad (1.5)
\]

If \( d = k^2 \), then \( E_n \) and \( E_{n'} \) are isomorphic and
\[
\Delta(E_{n'}) = k^{12} \Delta(E_n) \quad (1.6)
\]

**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
\[
N_{E_{n'}} = 2N_{E_n} \quad \text{if} \quad n' = 2n \quad (1.7)
\]
\[
N_{E_{n'}} = 3^2N_{E_n} \quad \text{if} \quad n' = 3n \quad (1.8)
\]

**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 \( n \leq m \). It is well known that the projective space associated to \( E \) denoted \( \mathbb{P}(E) \) is the quotient \( (E \setminus \{0\})/\sim \), where the relation \( \sim \) is defined on \( E \) by:
\[
x, y \in E \setminus \{0\}, x \sim y \text{ if and only if there exists a scalar } \lambda \in K \setminus \{0\} \text{ such that } x = \lambda y.
\]

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

DOI: 10.9790/5728-1603030105 www.iosrjournals.org
**On Congruent Numbers Elliptic Curves**

**Definition and remark 2.1.** An elliptic curve $E$ over the rational field $\mathbb{Q}$ is a projective nonsingular curve defined by the projective closure of the zero locus of an equation of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$  

(2.1)

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. In the others words, $E$ is a set of nonsingular points $P(X : Y : Z) \in P^2(\mathbb{Q})$ such that

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

(2.2)

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

In [15] we know that the set $E(\mathbb{Q})$ 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, $\exists (u, r, s, t) \in K^4$ such that

$$u b_3 = a_3 + ra_1 + 2t$$

$$u^2 b_2 = a_2 - sa_1 + 3r - s^2$$

(2.3)

(ii) Let $E$ and $E'$ be two elliptic curves over the field $\mathbb{Q}$ and defined respectively by the following equations:

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

(2.4)

where $k, k' \in \mathbb{Z}\setminus\{0\}$. Then, these curves are isomorphic over $\mathbb{Q}$.

(iii) Let $E$ be an elliptic curve over a field $K$. Any isomorphism $\phi : E \rightarrow E'$ of elliptic curves over $\mathbb{Q}$ is of the form

$$(x, y) \mapsto (u^2 x + r, u^3 y + u^2 s + t)$$

(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 $\mathbb{Q}$. The group $E(\mathbb{Q})$ of $\mathbb{Q}$-valued points on the elliptic curve $E$ is finitely generated. So,

$$E(\mathbb{Q}) = \mathbb{Z}' \times E(\mathbb{Q})_{\text{tors}}$$

where $E(\mathbb{Q})_{\text{tors}}$ 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 $\mathbb{Q}$.

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

$$L(E_n, s) = \prod_p \left(1 - a_p p^{-s} + p^3 p^{-2s}\right)$$

for all primes dividing 2n, where $a_p = p + 1 - [E_n(F_p)]$ and $E_n(F_p)$ is the curve obtained from $E_n/\mathbb{Q}$ thanks to the map reduction mod $p$, 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 $s = 1$ has 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

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

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

DOI: 10.9790/5728-1603030105  www.iosrjournals.org  3 | Page
The BSD conjecture says that the analytic rank of an elliptic curve is equal to its algebraic rank. We will always specify when talking about analytic rank, whereas if we use the term "rank" alone we refer to the algebraic 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 three arithmetic progressions of squares with common difference $n$: the set $\{a, b, c): a^2 + b^2 = c^2; n = \frac{ab}{2}\}$ and $(r, s, t): s^2 - t^2 = n, t^2 - s^2 = n$ are in one-to-one correspondence defined by:

$$(a, b, c) \mapsto \left( \frac{a-b}{2}, \frac{a+b}{2}, \frac{ab}{2} \right)$$

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:

$$(a, b, c): a^2 + b^2 = c^2; n = \frac{ab}{2} \quad \text{and} \quad E_n = \{x, y): y^2 = x^3 - n^2x, y \neq 0\}.$$ The mutually inverse correspondences between these sets are $(a, b, c) \mapsto \left( \frac{ab}{2}, \frac{ab}{2}, \frac{ab}{2} \right)$ and $(x, y) \mapsto \left( \frac{y^2}{x}, \frac{y^2}{x}, \frac{y^2}{x} \right)$.

**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 $\Delta_n$, $\Delta_{n'}$ respectively and such that $\frac{n'}{a} = \frac{n'}{b} = \frac{n'}{c} = k$. We know by theorem 2.9 that the triple $(a, b, c)$ corresponds to the point $\left( \frac{ab}{2}, \frac{2n^2}{c-a} \right)$ in $E_n$ and the second triple $(a', b', c')$ is associated to the point $\left( \frac{n'c'}{c-a}, \frac{2n^2}{c-a} \right)$. Now even $n' = k^2n$ because there is a k-homothety and the area transformed is multiplied by $k^2$. Plugging $a', b', c'$ by their values in (1.1) 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 by theorem 2.2 that, an isomorphism between two elliptic curves defined over $\mathbb{Q}$ 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 $\mathbb{Q}$ by theorem 2.2(ii), since $Q\left(\sqrt{\frac{n'}{n}}\right) = Q\left(\frac{1}{k}\right) = Q$.

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 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 number $n_i$ for $i = 1, 2, \ldots, m$. For two elliptic curves $E_{n_i}$ and $E_{n_i}$ such that $s < l$, then $n_i = n_i k^{2(j-l)}$. So these curves $E_{n_i}$ and $E_{n_i}$ are isomorphic and all the curves $E_{n_1}, \ldots, E_{n_m}$ form an isomorphism class of elliptic curves because they are all pairwise isomorphic and we have

$$f_k(E_{n_1}) = f_k(E_{n_2}) = \ldots = f_k(E_{n_m}) = f_k \circ \cdots \circ f_k(E_{n_i})$$

for $l \geq 1$, where $f_k$ is defined as follows.
On Congruent Numbers Elliptic Curves

\[ f_k(x, y) = (k^2 x, k^3 y) \quad \text{and} \quad f_k \circ \cdots \circ f_k(x, y) = (k^{2l} x, k^{3l} y) \] for any positive integer \( l \geq 1 \).

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 \( d > 0 \) is an integer. Let \( E_n \) and \( E_{n'} \) be the congruent number curves associated to \( n \) and \( n' \) respectively. We know that every elliptic curve \( E \) defined on the field \( \mathbb{Q} \) has an equation of the form \( y^2 = x^3 + ax + b \). Its discriminant 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 \( \Delta(E_{n'}) = -16(4(-d^2 n^2)^3 + 0) = d^6 \Delta(E_n) \).

2. Now we prove the relation (1.6). Let \( d = k^2 \). Let \( n \) and \( n' \) be two congruent numbers such that \( n' = k^2 n \). 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.

IV. Acknowledgments

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

References