# A GENERALIZATION OF A FIXED POINT THEOREM FOR CM ELLIPTIC CURVES

Bogdan Cânepă[1], Radu Gaba[2]

*This paper deals with the classification of the complex elliptic curves $E$ for which there exist subgroups (not necessarily cyclic) $C \leq (E,+)$ of order $n$ such that the elliptic curves $E/C$ and $E$ are isomorphic, extending in this way the results of [1]. We implement in Magma the algorithms developed for this classification and provide several examples.*

**Keywords:** elliptic curve, algorithm, non-cyclic subgroup

**MSC2010:** 11G 07, 11G 15, 11Y 16, 68W 01.

## 1. Introduction

Let us denote by $\mathcal{H}$ the upper half plane, $\mathcal{H} := \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$. Let $E$ be a complex elliptic curve and $C$ a subgroup (not necessarily cyclic) of order $n < \infty$ of $(E,+)$. This means that $C$ is a subgroup of order $n$ of the $n$-torsion subgroup of $E$, $E[n] := \{P \in E : [n]P = O\}$. It is known that since $C$ acts effectively and properly discontinuous on $E$, the group $E/C$ has a structure of Riemann variety, compatible with the natural projection $\pi : E \to E/C$ and that the isogeny $\pi$ is unramified of degree $n$: $\deg\pi = |\pi^{-1}(O)| = |C| = n$ (see [5], Theorem 3.4). It is also known that $E/C$ is a complex elliptic curve. Moreover, if $C$ is cyclic, one has $E[n]/C \cong \mathbb{Z}/n\mathbb{Z}$ (see [7], Proposition 5.4, Chapter VI or [2], Theorem 4.16).

In this work we study the complex elliptic curves $E$ for which there exist subgroups (not necessarily cyclic) $C \leq (E,+)$ of order $n$ such that the elliptic curves $E$ and $E/C$ are isomorphic, where $n$ is a positive integer. We extend in this way the results of [1] where the classification was made for the case $C$ cyclic. More explicitly, the authors proved in [1] the following:

**Theorem 1.1.** *i) $\exists C \leq (E,+)$ finite cyclic subgroup such that $\frac{E}{C} \simeq E \Leftrightarrow \exists u, v \in \mathbb{Q}$ such that $\tau^2 = u\tau + v$ with $\Delta = u^2 + 4v < 0$ (i.e. $E$ admits complex multiplication);*

*ii) If $\tau$ satisfies the conditions of i) and $u = \frac{u_1}{u_2}, v = \frac{v_1}{v_2}, u_2 \neq 0, v_2 \neq 0, u_1, u_2, v_1, v_2 \in \mathbb{Z}, \mathrm{Gcd}(u_1, u_2) = \mathrm{Gcd}(v_1, v_2) = 1, d_2 = \mathrm{Gcd}(u_2, v_2)$, then:*

*$\exists C \leq (E,+)$ cyclic subgroup of order $n$ which satisfies $\frac{E}{C} \simeq E \Longleftrightarrow \exists (a, b') \in \mathbb{Z}^2$ with $\mathrm{Gcd}(a, b') = 1$ such that $n = \det M$, where $M$ is the matrix*

$$M = \begin{pmatrix} a & A \\ b & B \end{pmatrix}$$

*and $(a, A, b, B) = \left(a, \frac{u_2 v_1}{d_2} b', \frac{u_2 v_2}{d_2} b', a + \frac{u_1 v_2}{d_2} b'\right)$;*

"UAIC" University of Iasi, 11 Carol 1 Blvd., 700506 Iasi Romania e-mail: bogdan_canepa@yahoo.com
Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P.O. BOX 1-764 RO-014700 Bucharest e-mail: radu.gaba@imar.ro

*iii) The subgroup $C$ from ii) is $C=\langle\frac{u_{11}+u_{21}\tau}{n}\rangle$, where $u_{11}, u_{21}$ are obtained in the following way: since* $\det M = n$ *and* $\mathrm{Gcd}(a, A, b, B) = 1$ *(one deduces easily this), the matrix $M$ is arithmetically equivalent with the matrix:*

$$M \sim \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix},$$

*hence*

$$\exists U, V \in GL_2(\mathbb{Z}) \quad \textit{such that} \quad M = U \cdot \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \cdot V.$$

*The elements $u_{11}, u_{21}$ are the first column of the matrix*

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}.$$

We point out that in [1], after characterizing the above mentioned class of Heegner points via Theorem 1.1, upon imposing certain conditions (see Theorem 2.3 of [1]), we further answered the following question: "given a complex elliptic curve when can one find a cyclic subgroup of order $n$ of E such that $(E, C) \simeq (E/C, E[n]/C)$ and classified in this manner the fixed points of the action of the Fricke involution

$$w_n := \begin{pmatrix} 0 & -1 \\ n & 0 \end{pmatrix} \in GL_2(\mathbb{Q}^+)$$

on the open modular curves $Y_0(n)$. We recall that one defines $Y_0(n)$ as the quotient space $\Gamma_0(n)/\mathcal{H}$ where $\mathcal{H}$ is the upper half plane i.e. $\{z \in \mathbb{C} |\ \mathrm{Im}(z) > 0\}$, in other words $Y_0(n)$ is the set of orbits $\{\Gamma_0(n)\tau : \tau \in \mathcal{H}\}$, where $\Gamma_0(n)$ is the "Nebentypus" congruence subgroup of level $n$ of $SL_2(\mathbb{Z})$, acting on $\mathcal{H}$ from the left:

$$\Gamma_0(n) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Z}) |\ c \equiv 0(\mathrm{mod} n)\}.$$

Moreover, slightly modified versions of the algorithms developed in this paper, also implemented by ourselves, work correctly in establishing the fixed points of the action of the Fricke involution on the open modular curves $Y_0(n)$, points which are known but weren't studied in the above specified manner. This number of fixed points was computed by Ogg (see [6], Proposition 3) and Kenku (see [4], Theorem 2) and, for $n > 3$, it is $\nu(n) = h(-n) + h(-4n)$ if $n \equiv 3(\mathrm{mod} 4)$ and $\nu(n) = h(-4n)$ otherwise, where $h(-n)$ is the class number of primitive quadratic forms of discriminant $-n$ and $\nu(2) = \nu(3) = 2$.

## 2. **Main Result**

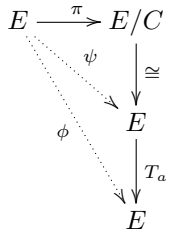
In Theorem 1.1 of [1] we only studied the cyclic subgroups $C \leq (E, +)$ of order $n$ satisfying $E \simeq \frac{E}{C}$. It is natural to study this problem in general and answer the question of for which complex elliptic curves $E$ and for which subgroups $C \leq (E, +)$ of order $n$ the elliptic curves $E$ and $E/C$ are isomorphic. We observe that if $C$ is a subgroup of order $n$ of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ then $C$ is of the form $\mathbb{Z}/D_1\mathbb{Z} \times \mathbb{Z}/D_2\mathbb{Z}$ with $D_1, D_2$ positive integers such that $D_1 \cdot D_2 = n$ and $D_1 | D_2$. Moreover, we are not interested in the case $D_1 = D_2 := D$ as $C$ would be a torsion subgroup, in which case $E/E[D] \cong E$. We prove now the following:

**Theorem 2.1.** *Let $E$ be a complex elliptic curve:*
*Then there exists a finite subgroup $C$ of $(E, +)$ such that $C \cong \mathbb{Z}/D_1\mathbb{Z} \times \mathbb{Z}/D_2\mathbb{Z}$, $D_1 | D_2$, $D_1 \neq D_2$ and with the property that $\frac{E}{C} \simeq E$, if and only if $\tau$ satisfies the equation $\tau^2 = u\tau + v, u, v \in \mathbb{Q}, \Delta = u^2 + 4v < 0$ and there exist $(a, b') \in \mathbb{Z}^2$ with $\mathrm{Gcd}(a, b') = D_1$ such that, if we denote by $a, A, b, B$ the numbers $(a, A, b, B) = \left(a, \frac{u_2 v_1}{d_2} b', \frac{u_2 v_2}{d_2} b', a + \frac{u_1 v_2}{d_2} b'\right)$ and by $M$ the matrix*

$$M = \begin{pmatrix} a & A \\ b & B \end{pmatrix}$$

*we have the relation* $\det(M) = D_1 \cdot D_2$. *We denoted by* $u = \frac{u_1}{u_2}, v = \frac{v_1}{v_2}$, $u_2 \neq 0, v_2 \neq 0, u_1, u_2, v_1, v_2 \in \mathbb{Z}$, $\mathrm{Gcd}(u_1, u_2) = \mathrm{Gcd}(v_1, v_2) = 1, d_2 = \mathrm{Gcd}(u_2, v_2)$. *Moreover, the isomorphism* $\frac{E}{C} \simeq E$ *comes from a morphism of varieties:* $\phi_{a,b'} : E \longrightarrow E$ *which has the following properties:* $\deg(\phi_{a,b'}) = D_1 \cdot D_2$, *it is a group homomorphism,* $\mathrm{Ker}(\phi) = C$ *and* $\phi(z) = \lambda z$, *where* $\lambda = a + b\tau$.

*Proof.* By composing the isomorphism $\frac{E}{C} \simeq E$ with the natural projection $E \to E/C$ one obtains a morphism $\psi : E \to \frac{E}{C} \simeq E$. By further composing a translation $T_a : E \longrightarrow E$ with it, we obtain a morphism $\phi : E \longrightarrow E, \phi(z) = \lambda \cdot z$ with $\mathrm{Ker}(\phi) = C$ (the reason for doing this is that a morphism of complex elliptic curves is the composition of a translation with an homothety). More explicitly, we have the following commutative diagram:




In fact, there exists a one-to-one correspondence between the set of isomorphisms $\{\frac{E}{C} \simeq E\}$ and the set of morphisms $\{\phi : E \longrightarrow E : \phi$ is morphism of complex varieties and of groups, $\mathrm{Ker}(\phi) = C\}$. Therefore it is enough to study the kernel of $\phi : E \longrightarrow E$, $\phi(z) = \lambda \cdot z$. We have that $\mathrm{Ker}(\phi) = \{\hat{z} \in E/\lambda z \in L\} = \{\hat{z} \in E/z \in \frac{1}{\lambda}L\} = \frac{\frac{1}{\lambda}L}{L} \leq \frac{\mathbb{C}}{L} = E$. Consequently $\mathrm{Ker}(\phi) = \frac{\frac{1}{\lambda}L}{L} \simeq \frac{L}{\lambda L}$, where $\lambda L \subseteq L$.
We would like to find the group with which $\frac{L}{\lambda L}$ is isomorphic. A $\mathbb{Z}$ - basis for $\lambda L$ is $\{\lambda, \lambda \cdot \tau\}$. The inclusion $\lambda L \subseteq L$ is equivalent to the existence of the numbers $a, A, b, B \in \mathbb{Z}$ such that

$$\begin{pmatrix} \lambda \\ \lambda\tau \end{pmatrix} = \begin{pmatrix} a & b \\ A & B \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}$$

As in Theorem 1.1, $a, A, b, B$ have certain properties. From the above matrix equality we have that $(a + b\tau)\tau = A + B\tau \iff b\tau^2 = (B - a)\tau + A$, i.e. $\tau$ is algebraic over $\mathbb{Q}$ provided $b \neq 0$. If $b = 0$ then one would obtain $D_1 = D_2 = a$. If $b \neq 0$, let $\mu_\tau = X^2 - uX - v \in \mathbb{Q}[X]$ be the minimal polynomial of $\tau$, $u = \frac{u_1}{u_2} \in \mathbb{Q}, v = \frac{v_1}{v_2} \in \mathbb{Q}, u_1, u_2, v_1, v_2 \in \mathbb{Z}, \mathrm{Gcd}(u_1, u_2) = \mathrm{Gcd}(v_1, v_2) = 1, d_2 = \mathrm{Gcd}(u_2, v_2)$. Upon identifying the coefficients of $\mu_\tau$ and $b\tau^2 = (B - a)\tau + A$, we obtain:

$$\begin{cases} \frac{A}{b} = v = \frac{v_1}{v_2} \\ \frac{B-a}{b} = u = \frac{u_1}{u_2} \end{cases} \quad \text{hence} \begin{cases} v_2 A = v_1 b \\ u_2(B - a) = u_1 b. \end{cases}$$

Since $v_2 A = v_1 b$ and $\mathrm{Gcd}(v_1, v_2) = 1$ it follows that $v_2 | b$ and $v_1 | A$. Since $u_2(B - a) = u_1 b$ and $\mathrm{Gcd}(u_1, u_2) = 1$ it follows that $\mathrm{Lcm}[u_2, v_2] | b$. Consequently there exists $b' \in \mathbb{Z}$ such that $b = \mathrm{Lcm}[u_2, v_2]b' = \frac{u_2 v_2}{d_2} b'$, $v_2 A = v_1 b$ and $u_2(B - a) = u_1 b$ where $d_2 = \mathrm{Gcd}(u_2, v_2)$ and $\tau^2 = u\tau + v$. We've obtained that $(a, A, b, B) = \left(a, \frac{u_2 v_1}{d_2} b', \frac{u_2 v_2}{d_2} b', a + \frac{u_1 v_2}{d_2} b'\right)$.

On the other hand, $M$ is arithmetically equivalent with:

$$M = \begin{pmatrix} a & A \\ b & B \end{pmatrix} \sim \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix}, D_1 | D_2 \quad \text{i.e. there exist } U, V \in SL_2(\mathbb{Z}) \text{ with}$$

$$\begin{pmatrix} a & A \\ b & B \end{pmatrix} = U \cdot \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \cdot V.$$

We show now that $D_1 = \mathrm{Gcd}(a, b')$.
Indeed, $D_1 = \mathrm{Gcd}(a, A, b, B) = \mathrm{Gcd}\Big(a, \frac{u_2v_1}{d_2}b', \frac{u_2v_2}{d_2}b', a + \frac{u_1v_2}{d_2}b'\Big)$. Since $\mathrm{Gcd}(v_1, v_2) = 1$ it follows that $\mathrm{Gcd}(A, b) = \mathrm{Gcd}(\frac{u_2v_1}{d_2}b', \frac{u_2v_2}{d_2}b') = b'\frac{u_2}{d_2}$. Consequently $D_1|b'\frac{u_2}{d_2}$. Since $D_1|a$ and $D_1|B = a + \frac{u_1v_2}{d_2}b'$, we obtain that $D_1|b'u_1\frac{v_2}{d_2}$. From:

$$\begin{cases} D_1|b'\frac{u_2}{d_2} \\ D_1|b'u_1\frac{v_2}{d_2} \\ \mathrm{Gcd}\Big(\frac{u_2}{d_2}, \frac{v_2}{d_2}\Big) = 1 \end{cases} \tag{1}$$

it follows that $D_1|b'u_1$. Similarly, we have that

$$\begin{cases} D_1|b'u_1 \\ D_1|b'\frac{u_2}{d_2} \\ \mathrm{Gcd}(u_1, u_2) = 1 \end{cases} \quad \text{hence } D_1|b'. \tag{2}$$

We've obtained that $D_1 = \mathrm{Gcd}(a, b')$.
Finally, it is easy to see that $\mathrm{Ker}(\phi) \simeq \mathbb{Z}/D_1\mathbb{Z} \times \mathbb{Z}/D_2\mathbb{Z}$. Indeed, from

$$\begin{pmatrix} a & A \\ b & B \end{pmatrix} = U \cdot \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \cdot V, \text{ we get } \begin{pmatrix} a & b \\ A & B \end{pmatrix} = V^t \cdot \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \cdot U^t.$$

By denoting

$$\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = U^t \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}, \text{we obtain } \begin{pmatrix} \lambda \\ \lambda\tau \end{pmatrix} = V^t \cdot \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}.$$

On the other hand $L = \mathbb{Z}\langle f_1, f_2\rangle$, and consequently $\lambda L = \mathbb{Z}\langle D_1f_1, D_2f_2\rangle$. It follows that $\ker(\phi) = \frac{L}{\lambda L} \simeq \frac{\mathbb{Z}f_1 \oplus \mathbb{Z}f_2}{\mathbb{Z}D_1f_1 \oplus \mathbb{Z}D_2f_2} \simeq \mathbb{Z}/D_1\mathbb{Z} \times \mathbb{Z}/D_2\mathbb{Z}$, q.e.d. □

## 3. **Examples.**

In this section we classify (up to an isomorphism) the elliptic curves $E$ which admit a subgroup $C \leq (E, +)$ of order 12, $C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ such that $\frac{E}{C} \simeq E$. Recall first that complex elliptic curves are of the form $\frac{\mathbb{C}}{L}$ for some $L = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ where $\tau \in G = \Big\{z = x + iy \in \mathbb{C} : -\frac{1}{2} \leq x < \frac{1}{2} \text{ and either } |z| \geq 1 \text{ if } x \leq 0 \text{ or } |z| > 1 \text{ if } x > 0\Big\}$ (see [2], Theorem 4.15B). Let $E$ be an elliptic curve satisfying the condition i) of Theorem 1.1. $E$ is isomorphic to an elliptic curve $E' = \frac{\mathbb{C}}{L}$, where $L = \mathbb{Z} + \mathbb{Z}\tau$ and $\tau \in G$. Since an isomorphism $u : E \longrightarrow E'$ is of the type $u(z) = \sigma \cdot z, \sigma \in SL_2(\mathbb{Z})$ (see [3], Theorem 1.4, Chapter 11) one easily obtains that $E'$ satisfies the condition i) of Theorem 1.1. Hence we can assume (up to an isomorphism) that $E$ is of the form $\frac{\mathbb{C}}{L}$ with $L = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ and $\tau \in G$. Moreover, we observe that if $\tau = x + iy \in G$, $|x| \leq \frac{1}{2}$ and $|z| = x^2 + y^2 \geq 1$ lead to $y^2 \geq \frac{3}{4}$.

Let $\tau^2 - u\tau - v = 0, u, v \in \mathbb{Q}, \Delta = u^2 + 4v < 0$ and $\tau \in G$. Then $\tau = \frac{u \pm i\sqrt{|\Delta|}}{2}$ and, since $\tau \in G$, we obtain that $-1 \leq u < 1$ and $|\Delta| \geq 3$. Since $\Delta = u^2 + 4v < 0$ we have that $v < 0$. Without loss of generality, we can assume that $v_2 > 0, v_1 < 0$ and $u_2 > 0$. By using Theorem 2.1 and these restrictions imposed to $\tau$ we obtain the following results:

**Proposition 3.1.** *There are precisely* 4 *elliptic curves $E$ (up to an isomorphism) which admit at least one subgroup $C \leq (E, +)$ of order* 12, *$C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ such that $\frac{E}{C} \simeq E$. If we put $L = \mathbb{Z} + \mathbb{Z}\tau$, they are:*
*a) $E = \frac{\mathbb{C}}{L}, \tau^2 = -2$;*
*b) $E = \frac{\mathbb{C}}{L}, \tau^2 = -3$;*

*c)* $E = \frac{\mathbb{C}}{L}, \tau^2 = -\tau - 1$;
*d)* $E = \frac{\mathbb{C}}{L}, \tau^2 = -\tau - 3$.

**Remark 3.1.** *For* $n = 12$, $(D_1, D_2) \in \{(1, 12), (2, 6)\}$ *and we analyze the case* $C$ *non-cyclic i.e.* $(D_1, D_2) = (2, 6)$.

*Proof.* By using Theorem 2.1 we have that:

$$12 = aB - bA = \left(a + \frac{u_1 v_2}{2d} b'\right)^2 - \frac{u_2^2 v_2^2 \Delta}{4d^2} b'^2 \tag{3}$$

where from now on $d := d_2 = \mathrm{Gcd}(u_2, v_2)$ in order to simplify the notations. Since $|\Delta| \geq 3$ we obtain that $12 \geq \frac{3u_2^2 v_2^2}{4d^2} b'^2 \geq \frac{3}{4} b'^2$. Consequently $b'^2 \leq 16$ so $b'^2 \in \{0, 1, 4, 16\}$.

The cases $b'^2 = 0$ and $b'^2 = 1$ are easily eliminated: $b'^2 = 0$ leads to $12 = a^2$ which has no integer solutions and $b'^2 = 1$ is not possible since $\mathrm{Gcd}(a, b') = 2$. Consequently, there are 2 cases left:

I) If $b'^2 = 16$, both sides of the previous inequality are equal since $12 = \frac{3}{4} b'^2$, hence $\Delta = -3$ and $\frac{u_2 v_2}{d} = 1$. Since $u_2 > 0$ and $v_2 > 0$ we get that $u_2 = v_2 = d = 1$. Consequently $\tau$ satisfies the equation $\tau^2 - u_1 \tau - v_1 = 0, u_1, v_1 \in \mathbb{Z}, \Delta = u_1^2 + 4v_1 < 0$. From $\tau \in G$ and $\tau = \frac{u_1 \pm i\sqrt{|\Delta|}}{2}$ we obtain that $-1 \leq u_1 < 1$. Since $u_1 \in \mathbb{Z}$ we get that $u_1 \in \{-1, 0\}$. By using the equation $\Delta = -3$ we obtain that $u_1^2 + 4v_1 = -3$, consequently $u_1$ is odd. It follows that $u_1 = -1$ and $v_1 = -1$, consequently $\tau$ satisfies $\tau^2 + \tau + 1 = 0$. Moreover, $(a, b') \in \{(2, 4), (-2, -4)\}$.

II) If $b'^2 = 4$, by using the equation (3) we get that $12 \geq \frac{3}{4} \cdot \left(\frac{u_2 v_2}{d}\right)^2 \cdot 4$. We denote by $\frac{u_2 v_2}{d} = \xi \in \mathbb{Z}$. Since $u_2 > 0$ and $v_2 > 0$ we have that $\xi > 0$. From the above inequality we obtain that $\xi \in \{1, 2\}$.

a) If $\xi = 1$ we have that $u_2 = v_2 = d = 1$. Consequently $\tau$ satisfies the equation $\tau^2 - u_1 \tau - v_1 = 0, u_1, v_1 \in \mathbb{Z}, \Delta = u_1^2 + 4v_1 < 0$. Since $\tau \in G$ and $\tau = \frac{u_1 \pm i\sqrt{|\Delta|}}{2}$ we get that $-1 \leq u_1 < 1$. Since $u_1 \in \mathbb{Z}$ it follows that $u_1 \in \{-1, 0\}$. We distinguish two cases:

a1) If $u_1 = 0$ the equation (3) becomes $12 = a^2 - \Delta = a^2 - 4v_1$. On the other hand $v_1 < 0$ and $v_1 \in \mathbb{Z}$, consequently either $a^2 = 0, v_1 = -3$ or $a^2 = 4, v_1 = -2$. If $a^2 = 0, v_1 = -3$ we have that $u_1 = 0$ and $v_1 = -3$. It follows that $\tau$ satisfies the equation $\tau^2 = -3$; in this case $(a, b') \in \{(0, \pm 2)\}$.
If $a^2 = 4, v_1 = -2$ we have that $u_1 = 0$ and $v_1 = -2$. It follows that $\tau$ satisfies the equation $\tau^2 = -2$; in this case $(a, b') \in \{(\pm 2, 2)\}$.

a2) If $u_1 = -1$ the equation (3) becomes $12 = \left(a - \frac{b'}{2}\right)^2 - \frac{1}{4}\Delta = \left(a - \frac{b'}{2}\right)^2 - \frac{1}{4} \cdot (1 + 4v_1)$ and, since $b' = \pm 2$ we get $13 = (a \pm 1)^2 - 4 \cdot v_1$. Since $v_1 \leq -1$ and $v_1 \in \mathbb{Z}$ the last equality leads to $((a \pm 1)^2, v_1) \in \{(1, -3), (9, -1)\}$. If $((a \pm 1)^2, v_1) = (1, -3)$ then $\tau$ satisfies the equation $\tau^2 + \tau + 3 = 0$ and $(a, b') \in \{(0, \pm 2), (\pm 2, \pm 2)\}$. If $((a \pm 1)^2, v_1) = (9, -1)$ then $\tau$ satisfies the equation $\tau^2 + \tau + 1 = 0$ and $(a, b') \in \{(-2, 2), (2, -2), (\pm 4, \pm 2)\}$.

b) If $\xi = 2$ we have that $\frac{u_2 v_2}{d} = 2$ hence $u_2 \cdot \frac{v_2}{d} = v_2 \cdot \frac{u_2}{d} = 2$. Since $u_2 > 0$ and $v_2 > 0$ we get that $(u_2, v_2) \in \{(2, 1), (1, 2), (2, 2)\}$. We distinguish 3 cases:

b1) If $(u_2, v_2) = (2, 1)$ the equation (3) becomes $12 = \left(a + \frac{u_1 b'}{2}\right)^2 - 4\Delta$. Since $\Delta \leq -3$ we get that $a + \frac{u_1 b'}{2} = 0$ and $\Delta = -3$. We have that $\tau^2 - \frac{u_1}{2}\tau - v_1 = 0$, $\tau \in G$ and $-1 \leq \frac{u_1}{2} < 1$. Consequently $-2 \leq u_1 < 2$ hence $u_1 \in \{-2, -1, 0\}$.

If $u_1 = -2$, since $u_2 = 2$ we get $\mathrm{Gcd}(u_1, u_2) = 2 \neq 1$ and consequently this case is not possible.

If $u_1 = -1$, from $\Delta = -3$ we get that $\frac{u_1^2}{4} + 4v_1 = -3$ i.e. $\frac{1}{4} + 4v_1 = -3$, contradiction with $v_1 \in \mathbb{Z}$.

If $u_1 = 0$, from $\Delta = -3$ we get that $\frac{u_1^2}{4} + 4v_1 = -3$ hence $v_1 = -\frac{3}{4}$, contradiction.

b2) If $(u_2, v_2) = (1, 2)$ the equation (3) becomes $12 = (a + u_1 b')^2 - 4\Delta$.
We have that $\tau^2 - u_1\tau - \frac{v_1}{2} = 0$, $\tau \in G$ and $-1 \leq u_1 < 1$ hence $u_1 \in \{-1, 0\}$.

If $u_1 = -1$, (3) leads to $16 = (a-b')^2 - 8v_1$ and since $v_1 \leq -1$ we get that $(a-b')^2 \leq 8$. Since $v_1 \in \mathbb{Z}$ one obtains $(a - b', v_1) = (0, -2)$. Consequently $\tau$ satisfies the equation $\tau^2 + \tau + 1 = 0$ and $(a, b') \in \{(\pm 2, \pm 2)\}$.

If $u_1 = 0$ we get that $\Delta = 2v_1$ and (3) becomes $12 = a^2 - 4\Delta$. Since $\Delta \leq -3$ one obtains $a = 0$ and $\Delta = -3$ the later being equivalent to $2v_1 = -3$ which is impossible in $\mathbb{Z}$.

b3) If $(u_2, v_2) = (2, 2)$ the equation (3) becomes $12 = \left(a + \frac{u_1 b'}{2}\right)^2 - 4\Delta$. Since $\Delta \leq -3$ we obtain $a + \frac{u_1 b'}{2} = 0$ and $\Delta = -3$. From $\tau \in G$ and $\tau^2 - \frac{u_1}{2}\tau - \frac{v_1}{2} = 0$ we obtain that $-2 \leq u_1 < 2$ hence $u_1 \in \{-2, -1, 0\}$.

If $u_1 = -2$, from $\Delta = -3$ it follows that $\frac{u_1^2}{4} + 2v_1 = -3$ hence $v_1 = -2$. In conclusion, $\tau$ satisfies the equation $\tau^2 + \tau + 1 = 0$; in this case $(a, b') \in \{(\pm 2, \pm 2)\}$.

If $u_1 = -1$, from $\Delta = -3$ we obtain that $\frac{u_1^2}{4} + 2v_1 = -3$ hence $v_1 = -\frac{13}{8}$, contradiction with $v_1 \in \mathbb{Z}$.

If $u_1 = 0$, since $u_2 = 2$ we get that $\mathrm{Gcd}(u_1, u_2) = 2 \neq 1$ hence this case is not possible. □

**Remark 3.2.** *In order to include the cyclic case ($D_1 = 1, D_2 = 12$) and get the list of classes of elliptic curves $E$ which admit subgroups $C \leq (E, +)$ of order 12 such that the elliptic curves $E$ and $E/C$ are isomorphic, the reader may set the condition* $\mathrm{Gcd}(a, b') = 1$ *and proceed as in Proposition 3.1 or use the Algorithm 2 provided in the next section. The complete list of the above mentioned classes of CM elliptic curves for $n = 12$ is summarized in Table 2.*

## 4. The Algorithms

In this section, in a similar manner to the one used by us in [1], we implement in Magma the algorithm developed for the classification of the complex elliptic curves $E$ which admit non-cyclic subgroups $C \leq (E, +)$ of order $n$ such $E$ and $E/C$ are isomorphic. We mainly follow our Algorithm 1 of [1] by setting up the conditions $D_1 := \mathrm{Gcd(a, b')} > 1$, $\mathrm{Gcd}(a, b')|n$, $\mathrm{Gcd}(a, b') < n/\mathrm{Gcd}(a, b') =: D_2$ and $D_1|D_2$. Afterwards we modify the code by including the cyclic case. Finally, by mean of these codes, some interesting examples including the one analyzed in Proposition 3.1 are provided.
Recall first that complex elliptic curves are of the form $\frac{\mathbb{C}}{L}$ for some $L = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ where $\tau \in G = \left\{z = x + iy \in \mathbb{C} : -\frac{1}{2} \leq x < \frac{1}{2} \text{ and either } |z| \geq 1 \text{ if } x \leq 0 \text{ or } |z| > 1 \text{ if } x > 0\right\}$.
Let $E$ be an elliptic curve satisfying the condition i) of Theorem 1.1. Recall that we can assume (up to an isomorphism) that $E$ is of the form $\frac{\mathbb{C}}{L}$ with $L = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ and $\tau \in G$ (see the beginning of the previous section for details). Recall also that if $\tau^2 - u\tau - v = 0, u, v \in \mathbb{Q}, \Delta = u^2 + 4v < 0$ and $\tau \in G$, then one obtains $\tau = \frac{u \pm i\sqrt{|\Delta|}}{2}$, $-1 \leq u < 1$ and $|\Delta| \geq 3$. Furthermore, since $\Delta = u^2 + 4v < 0$ we have that $v < 0$. We can assume that $u_2 > 0$ and $v_2 > 0, v_1 < 0$.

Let us describe now the main algorithm: by using Theorem 1.1, ii), we have that:

$$n = aB - bA = \left(a + \frac{u_1 v_2}{2d} b'\right)^2 - \frac{u_2^2 v_2^2 \Delta}{4d^2} b'^2 \tag{4}$$

Recall that $d = \mathrm{Gcd}(u_2, v_2)$, $\Delta = \frac{u_1^2}{u_2^2} + 4\frac{v_1}{v_2}$ and let $u_2' := u_2/d$ and $v_2' := v_2/d$. Let also $v_1 := -v_1$ and note that $u_2, v_2, v_1 > 0$ and that $\Delta \leq -3$. We multiply (4) by 4 and obtain:

$$4n = (2a + u_1 v_2' b')^2 + v_2' b'^2 (4v_1 d u_2'^2 - v_2' u_1^2) \tag{5}$$

| $n$ | corresponding classes of CM elliptic curves: the non-cyclic case |
|---|---|
| 12 | [-1,-3],[-1,-1],[0,-3],[0,-2] |
| 16 | [ -1, -4 ], [ -1/2, -1 ], [ -1, -2 ], [ 0, -4 ], [ 0, -3 ] |
| 24 | [ 0, -3/2 ], [ -1/2, -1 ], [ 0, -5 ], [ -1, -4 ], [ -1/2, -3/2 ], [ -1, -6 ], [ 1/2, -3/2 ], [ 0, -2 ], [ 0, -6 ], [ -1, -3/2 ] |
| 245 | [-1,-3],[0,-5],[-1,-3/2],[0,-4],[0,-1],[-1,-5] |

TABLE 1. classes of CM elliptic curves for various $n$

| $n$ | corresponding classes of CM elliptic curves: the general case |
|---|---|
| 12 | [ -1, -3 ], [ -1, -4/3 ], [ -2/3, -4/3 ], [ 1/2, -3/2 ], [ -1, -1 ], [ 1/2, -3 ], [ -1/2, -5/2 ], [ -2/3, -1 ], [ 2/3, -4/3 ], [ -1/2, -3 ], [ -1/2, -3/2 ], [ 0, -12 ], [ 0, -11 ], [ -1, -12 ], [ 0, -8 ], [ -1/3, -4/3 ], [ -1, -10 ], [ 1/3, -4/3 ], [ 0, -4/3 ], [ -1, -6 ], [ 0, -3 ], [ 0, -2 ], [ 1/2, -5/2 ] |
| 16 | [ -1/2, -5/2 ], [ -1/2, -7/2 ], [ 0, -4/3 ], [ 0, -3 ], [ 0, -5/3 ], [ 0, -4 ], [ -1/4, -1 ], [ -1, -10 ], [ 0, -7 ], [ -3/4, -1 ], [ -1, -14 ], [ -1, -16 ], [ 1/2, -4 ], [ 1/2, -5/2 ], [ -1, -2 ], [ 1/2, -7/2 ], [ -1, -4 ], [ -1, -4/3 ], [ -1/2, -1 ], [ 0, -12 ], [ -1, -5/4 ], [ 0, -15 ], [ -1/2, -4 ], [ 0, -16 ] |

TABLE 2. classes of CM elliptic curves for various $n$

Consequently, we get $4n \geq v_2'b'^2 \cdot 4v_1du_2'^2$ hence $n \geq v_2'b'^2 \cdot v_1du_2'^2$. As in [1], denote now by $\xi := 4v_1du_2'^2 - v_2'u_1^2$ and remark that $\Delta \leq -3$ is equivalent to $\frac{u_1^2}{d^2u_2'^2} - 4\frac{v_1}{dv_2'} \leq -3$ and furthermore to $-\xi \leq -3d^2u_2'^2v_2'$, i.e. $\xi \geq 3d^2u_2'^2v_2'$. Using (5) we obtain that $4n \geq v_2'b'^2 \cdot 3d^2u_2'^2v_2'$ hence $4n/3 \geq v_2'^2b'^2 \cdot d^2u_2'^2$. Put $k := \sqrt{4n/3}$. We obtain that $u_2'$ runs from 1 to the integer part of $k$, $[k]$, $v_2'$ from 1 to $[k/u_2']$, $b'$ from 1 to $[k/u_2'/v_2']$ and $d$ from 1 to $[k/u_2'/v_2'/b']$. Moreover, $-1/2 \leq \mathrm{Re}(\tau) < 1/2$ is equivalent to $-1/2 \leq u_1/(2u_2) < 1/2$ that is $-u_2 \leq u_1 < u_2$. Consequently $u_1$ runs from $-du_2'$ to $du_2' - 1$.

Denote by $m := (2a+u_1v_2'b')^2$. From (5) we get that $4n+v_2'^2b'^2u_1^2 = m+4v_2'b'^2v_1du_2'^2 \geq 4v_2'b'^2v_1du_2'^2$ hence $v_1 \leq \frac{4n+v_2'^2b'^2u_1^2}{4v_2'b'^2du_2'^2}$. Consequently, $v_1$ will run from 1 to $[\frac{4n+v_2'^2b'^2u_1^2}{4v_2'b'^2du_2'^2}]$.

Recall that $D_1 = \mathrm{Gcd}(a, b')$ and $D_2 = n/\mathrm{Gcd}(a, b')$. We set the conditions Gcd(a, b′) > 1, $\mathrm{Gcd}(a, b')|n$, $\mathrm{Gcd}(a, b') < n/\mathrm{Gcd}(a, b')$ and $\mathrm{Gcd}(a, b')$ divides $n/\mathrm{Gcd}(a, b')$. Moreover, $\mathrm{Gcd}(u_1, u_2) = 1$ and $\mathrm{Gcd}(v_1, v_2) = 1$.

Finally, condition $\tau \in G$ is entirely fulfilled by setting: ($u_1 > 0$ or $v_1 \geq v_2$) and ($u_1 \leq 0$ or $v_1 > v_2$).

In our codes, we made the substitutions $b := b'$, $u_2 := u_2/d$ and $v_2 := v_2/d$, where $d = \mathrm{Gcd}(\mathrm{u}_2, \mathrm{v}_2)$ and $b', u_2, v_2$ are defined in Theorem 2.1.

**Remark 4.1.** *We further modify the first code by including the cyclic case. In other words, by using the notations of Theorem 2.1 we allow the case $D_1 = 1$ where $D_1 = \mathrm{Gcd}(a, b')$, (see Algorithm 2, line 16).*

The corresponding results for the same cases analyzed in Table 1 are summarized in Table 2. We point out that for the cases $n = 24$ and $n = 245$ the number of classes are 51 and 328 respectively and due to their size, they are not included in Table 2. The reader may run the Algorithm 2 in order to see the detailed list.

Finally, for large $n$, several examples of the numbers of classes of CM elliptic curves $E$ which admit subgroups $C$ of order $n$ such that $E \cong E/C$ are provided in Table 3. The computations were done using Magma 2.19-9 on a Lenovo i30-3110M laptop at 2.40 GHz

**Algorithm 4.1** Input: any random integer; Output: $u_1/u_2, v_1/v_2$.

```
noncyclic := function(n);
E:={}; k:=Sqrt(4*n/3);
for u2:=1 to Floor(k) do
  for v2:=1 to Floor(k/u2) do
    if Gcd(u2,v2) eq 1 then
      for b:=1 to Floor(k/u2/v2) do
        for d:=1 to Floor(k/u2/v2/b) do
          for u1:=-d*u2 to d*u2-1 do
            for v1:=1 to Floor((4*n+v2^ 2*u1^ 2*b^ 2)/(4*v2*b^ 2*d*u2^ 2)) do
              if u1^ 2/d^ 2/u2^ 2-4*v1/d/v2 le -3 then
                m:=4*n-v2*b^ 2*(4*v1*d*u2^ 2-v2*u1^ 2);
                x,y:=IsSquare(m);
                if x then
                  if IsEven(y-u1*v2*b) then
                    a:=Floor((y-u1*v2*b)/2);
                    if (n mod Gcd(a,b) eq 0) and ( Gcd(a,b) ne 1) and ( Gcd(a,b) lt
                    Floor(n/Gcd(a,b))) and (Gcd(u1,d*u2) eq 1) and (Gcd (v1,d*v2)
                    eq 1) then
                      if (Floor(n/Gcd(a,b)) mod Gcd(a,b) eq 0) then
                        if (u1 gt 0 or v1 ge d*v2) and (u1 le 0 or v1 gt d*v2) then
                          E join:=[u1/d/u2,-v1/d/v2];
                        end if;
                      end if;
                    end if;
                  end if;
                end if;
              end for;
            end for;
          end for;
        end for;
      end if;
    end for;
end for;
return E;
end function;
```

| $n$ | the non-cyclic case | CPU time | the general case | CPU time |
|---|---|---|---|---|
| 297 | 43 | 0.156s | 440 | 0.172s |
| 2012 | 524 | 3.104s | 3563 | 3.323s |
| 2017 | 0 | 2.948s | 2023 | 3.276s |
| 4536 | 3733 | 10.982s | 13585 | 11.840s |
| 12825 | 2884 | 54.382s | 23581 | 58.734s |

TABLE 3. number of classes of CM elliptic curves for various $n$

and 4 GB RAM. For each $n$ we have also recorded the CPU time it took to complete these calculations.

**Algorithm 4.2** Input: any random integer; Output: $u_1/u_2, v_1/v_2$.

```
generaliz := function(n);
E:={}; k:=Sqrt(4*n/3);
for u2:=1 to Floor(k) do
  for v2:=1 to Floor(k/u2) do
    if Gcd(u2,v2) eq 1 then
      for b:=1 to Floor(k/u2/v2) do
        for d:=1 to Floor(k/u2/v2/b) do
          for u1:=-d*u2 to d*u2-1 do
            for v1:=1 to Floor((4*n+v2^ 2*u1^ 2*b^ 2)/(4*v2*b^ 2*d*u2^ 2)) do
              if u1^ 2/d^ 2/u2^ 2-4*v1/d/v2 le -3 then
                m:=4*n-v2*b^ 2*(4*v1*d*u2^ 2-v2*u1^ 2);
                x,y:=IsSquare(m);
                if x then
                  if IsEven(y-u1*v2*b) then
                    a:=Floor((y-u1*v2*b)/2);
                    if (n mod Gcd(a,b) eq 0) and ( Gcd(a,b) lt Floor(n/Gcd(a,b)))
                    and (Gcd(u1,d*u2) eq 1) and (Gcd (v1,d*v2) eq 1) then
                      if (Floor(n/Gcd(a,b)) mod Gcd(a,b) eq 0) then
                        if (u1 gt 0 or v1 ge d*v2) and (u1 le 0 or v1 gt d*v2) then
                          E join:=[u1/d/u2,-v1/d/v2];
                        end if;
                      end if;
                    end if;
                  end if;
                end if;
              end if;
            end for;
          end for;
        end for;
      end for;
    end if;
  end for;
end for;
return E;
end function;
```

## REFERENCES


[1] *B. Canepa and R. Gaba*, On some special classes of complex elliptic curves and related algorithms, Mathematical Reports, VOL.16(66), No.4(2014), 477-502, available online at URL: http://imar.ro/journals/Mathematical_Reports/Pdfs/2014/4/2.pdf

[2] *R. Hartshorne*, Algebraic Geometry, Graduate Texts in Mathematics, volume 52, Springer, New-York, 1977.

[3] *D. Husemoeller*, Elliptic curves, Graduate Texts in Mathematics, volume 111, Springer, New-York, 2004.

[4] *M. A. Kenku*, Atkin-Lehner involutions and class number residuality, Acta Arithmetica, 23 (1977), 1-9.

[5] *R. Miranda*, Algebraic curves and Riemann surfaces, Graduate Studies in Mathematics, volume 5, AMS.

[6] *A. P. Ogg*, Hyperelliptic modular curves, Bulletin de la S.M.F., tome 102 (1974), 449-462.

[7] *J. Silverman*, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, volume 106, Springer, New-York, 1986.