UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLIII
2005

ON A FAMILY OF ELLIPTIC CURVES

by Anna Antoniewicz

Abstract. The main aim of this paper is to put a lower bound on the rank of elliptic curves from the infinite family $C_m:\ y^2 = x^3 - m^2 x + 1,\ m \in \mathbb{Z}_+$. We shall prove that $\operatorname{rank} C_m \geq 2\ for\ m \geq 2$ and that $\operatorname{rank} C_{4k} \geq 3$ for the infinite subfamily $C_{4k},\ k \geq 1$. The idea has been taken from paper [**1**]; in fact we are attempting to solve two problems stated there.

1. Introduction. An **elliptic curve** over the field $\mathbb{Q}$ is a plane curve E defined by the equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$ and the cubic $x^3 + ax + b$ has distinct roots together with the point at infinity denoted $\mathcal{O}$.

A point (x, y) on a curve E is said to be **integer** (resp. **rational**), if both of its coordinates are integer (resp. rational). The set of all rational points of E is denoted by $E(\mathbb{Q})$. We assume the point $\mathcal{O}$ to be integer and rational.

On an elliptic curve E, one can define a law of addition of a curve's points. The definition is very simple and geometrical. In particular, the point at infinity is the neutral element and the opposite of $A = (x, y) \in E(\mathbb{Q})$ is $-A := (x, -y)$. For more details see [**3**].

The set of all points of an elliptic curve E together with this law of addition forms an abelian group, of which $E(\mathbb{Q})$ is a subgroup.

The well-known and absolutely fundamental Mordell Theorem says that the group $E(\mathbb{Q})$ of all rational points of an elliptic curve E is a finitely generated abelian group, which means that

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus \mathit{Tors}E(\mathbb{Q}),$$

where r is a uniquely determined positive integer and $\mathit{Tors}E(\mathbb{Q})$ is the finite abelian group consisting of all elements of finite rank in $E(\mathbb{Q})$.

2000 *Mathematics Subject Classification.* 11G05, 14G05.

Key words and phrases. Rank of an eliptic curve, torsion points, good reduction of an elliptic curve.

Preserving the above notation, we call r the **rank** of an elliptic curve E (denoted *rankE*). The finite subgroup $TorsE(\mathbb{Q})$ is called the **torsion subgroup** of E.

The notion of rank of an elliptic curve has been studied in great detail but its characterisation is in general a really hard task, the main reason being that the rank cannot be computed effectively from the coefficients a, b of the curve equation.

In this note we concentrate on an infinite family of elliptic curves

$$C_m : \ y^2 = x^3 - m^2 x + 1, \qquad m \in \mathbb{Z}_+. \tag{1.1}$$

This equation has a very simple arithmetic interpretation. It can easily be rewritten as

$$(y-1)(y+1) = x(x-m)(x+m),$$

from which we can see that it describes the following problem:
"When the product of two consecutive numbers of the same oddity is equal to the product of three consecutive terms of an arithmetic progression."

Our aim is to show that

$$\begin{aligned} \operatorname{rank} C_m &\geq 2 \quad \text{for} \quad m \geq 2, \\ \operatorname{rank} C_m &\geq 3 \quad \text{for} \quad m \geq 4, \ m \equiv 0 \ (mod\ 4). \end{aligned}$$

2. Preparational theorems. Now we shall focus on some special properties of the curves from the family C_m. The theorems to be proved work as the main tools in our method of bounding the curves' ranks.

First we will show that the torsion subgroup $TorsC_m(\mathbb{Q})$ is trivial for $m \geq 1$, i.e., that any non-trivial element of $C_m(\mathbb{Q})$ is of infinite order in that group.

Next we will describe some useful properties of points lying in $2C_m(\mathbb{Q})$.

The law of addition of a curve's points in the special case of $A = (x, y) \in C_m(\mathbb{Q})$ and $A + A = 2A = (x', y')$ reveals the following formulas for the coordinates of the doubled point:

$$x' = \frac{x^4 + 2m^2x^2 + m^4 - 8x}{4(x^3 - m^2 x + 1)}, \tag{2.1}$$

$$y' = -y - \frac{3x^2 - m^2}{2y}(x' - x). \tag{2.2}$$

The above formulas will be used frequently in the sequel.

2.1. *Triviality of the torsion subgroup.* To prove that the torsion subgroup is trivial, we need to show a few simple properties.

Property 2.1. *For $m \geq 1$, there is no point of order 2 in the group $C_m(\mathbb{Q})$.*

PROOF. Let $A = (x, y) \in C_m(\mathbb{Q})$, $m \geq 1$. Suppose that, on the contrary, $2A = \mathcal{O}$. It means that $A = -A$, or $(x, y) = (x, -y)$, hence $y = 0$, and $x \neq 0$. We then have $x^3 - m^2x + 1 = 0$. Now x has to be an integer. Indeed, putting $x = \frac{u}{v}$, $GCD(u, v) = 1$ and multiplying by v^3 we get $u^3 - m^2uv^2 + v^3 = 0$, hence $v^2 | u^3$, which gives $v^2 = 1$ and $x \in \mathbb{Z}$.
Next we see that

$$x^2 + \frac{1}{x} = \frac{x^3 + 1}{x} = m^2$$

is an integer, so $\frac{1}{x} \in \mathbb{Z}$, which gives $x \in \{-1, 1\}$. From this, $m^2 \in \{0, 2\}$ which is impossible, a contradiction. □

PROPERTY 2.2. *For $m \geq 1$, there is no point of order 3 in the group $C_m(\mathbb{Q})$.*

PROOF. Suppose that, on the contrary, $3A = \mathcal{O}$, or equivalently, $2A = -A$. Putting $A = (x, y)$, $2A = (x', y')$, one can see that in particular $x = x'$. Substituting this equality to formula (2.1), after a short computation one gets

$$(*) \qquad m^4 + 6x^2m^2 - 3x^4 - 12x = 0.$$

As in the previous proof, we substitute $x = \frac{u}{v}$, $GCD(u, v) = 1$ in order to get

$$3u^4 - 6m^2u^2v^2 + 12uv^3 - m^4v^4 = 0,$$

from which $v^2 | 3u^4$, hence $v^2 = 1$ and $x \in \mathbb{Z}$.
The left-hand side of $(*)$ is a square polynomial in the variable m^2. One can compute

$$\Delta = 48x(x^3 + 1) \qquad \text{and} \qquad m^2 = \frac{-6x^2 + \sqrt{\Delta}}{2}.$$

From the second equation there follows that $\Delta = (2m^2 + 6x^2)^2$ is a square of an integer. Hence, $\exists n \in \mathbb{N}$ such that $x(x^3 + 1) = 3n^2$.
First notice that $GCD(x, x^3 + 1) = 1$, so that two cases may occur:

$$\textbf{1.} \begin{cases} x = \alpha^2 \\ x^3 + 1 = 3\beta^2 \end{cases} \qquad \text{or} \qquad \textbf{2.} \begin{cases} x = 3\alpha^2 \\ x^3 + 1 = \beta^2 \end{cases}$$

for some $\alpha, \beta \in \mathbb{N}$. Moreover, since $x^3 + 1 = (x + 1)(x^2 - x + 1)$ and $x^2 - x + 1 = (x + 1)(x - 2) + 3$, there is $GCD(x + 1, x^2 - x + 1) \in \{1, 3\}$.
Let us test these cases.
Ad 1. From the above properties, there are two possible ways of factoring the equation $x^3 + 1 = 3\beta^2$:

$$\textbf{1.}(\boldsymbol{a}) \begin{cases} x = \alpha^2 \\ x + 1 = \gamma^2 \\ x^2 - x + 1 = 3\delta^2 \end{cases} \qquad \text{or} \qquad \textbf{1.}(\boldsymbol{b}) \begin{cases} x = \alpha^2 \\ x + 1 = 3\gamma^2 \\ x^2 - x + 1 = \delta^2 \end{cases}$$

for some $\alpha, \gamma, \delta \in \mathbb{N}$.

In case **1.(*a*)**, there is $\gamma^2 - \alpha^2 = x + 1 - x = 1$, so $\gamma = 1$ and $\alpha = 0$, hence $x = 0$, a contradiction.
In case **1.(*b*)**, there is $\delta^2 = x^2 - x + 1 = \alpha^4 - \alpha^2 + 1$, so for $\alpha \geq 2$ there is

$$\alpha^4 - 2\alpha^2 + 1 < \delta^2 < \alpha^4$$

or equivalently $\alpha^2 - 1 < \delta < \alpha^2$, which is impossible.
The remaining $\alpha \in \{0, 1\}$ implies $x \in \{0, 1\}$, a contradiction.
Ad 2. Similarly, factoring the equation $x^3 + 1 = \beta^2$, we get

$$\textbf{2.(}\boldsymbol{a}\textbf{)} \begin{cases} x = 3\alpha^2 \\ x + 1 = \gamma^2 \\ x^2 - x + 1 = \delta^2 \end{cases} \quad \text{or} \quad \textbf{2.(}\boldsymbol{b}\textbf{)} \begin{cases} x = 3\alpha^2 \\ x + 1 = 3\gamma^2 \\ x^2 - x + 1 = 3\delta^2 \end{cases}$$

In case **2.(*a*)**, there is $\delta^2 = x^2 - x + 1 = 9\alpha^4 - 3\alpha^2 + 1$. If $\alpha \geq 1$, then

$$(3\alpha^2)^2 > 9\alpha^4 - 3\alpha^2 + 1 > (3\alpha^2 - 1)^2,$$

or equivalently $3\alpha^2 > \delta > 3\alpha^2 - 1$, which is impossible. The remaining $\alpha = 0$ implies $x = 0$ and from $(*)$, $m = 0$.
In case **2.(*b*)**, there is $3\gamma^2 - 3\alpha^2 = x + 1 - x = 1$, a contradiction.
So the only solution is $x = m = 0$, which completes the proof. □

The last tool we need is the Nagell–Lutz theorem. For a prime p and $a, b \in \mathbb{Z}$, we may regard the elliptic curve $E\colon\ y^2 = x^3 + ax + b$ as a curve over the field $\mathbb{F}_p$ of p elements, with $a, b, x, y \in \mathbb{F}_p$. It is an elliptic curve over $\mathbb{F}_p$ iff the discriminant $\Delta(E) = -16(4a^3 + 27b^2)$ is prime to p (then it is non-zero in $\mathbb{F}_p$ so the curve is nonsingular); we then say that E has **good reduction** at p. By $E(\mathbb{F}_p)$ we denote the group of $\mathbb{F}_p$-points of E. The theorem says that if E has good reduction at a prime p, then $TorsE(\mathbb{Q})$ can be embedded into the group $E(\mathbb{F}_p)$ ([**3**], 5.5, Theorem 5.1).

Theorem 2.3.

$$TorsC_m(\mathbb{Q}) = \{\mathcal{O}\} \quad \textit{for} \quad m \geq 1.$$

Proof. Compute the discriminant for a curve C_m:

$$\Delta(C_m) = 16(4m^6 - 27).$$

Notice that $p = 5$ is prime to $\Delta(C_m)$, so we may consider the curve reduced modulo 5. To this end, we test cases, depending on the remainder of m modulo 5.
1. Case $m \equiv 0$ $(mod\ 5)$. The reduced curve is of the form

$$C_m^5 :\ y^2 = x^3 + 1.$$

One can easily compute that $C_m^5(\mathbb{F}_5) = \{\mathcal{O}, (4, 0), \pm(0, 1), \pm(2, 2)\}$, so $|C_m^5(\mathbb{F}_5)| = 6$. From the Nagell–Lutz Theorem and the Lagrange Theorem,

$TorsC_m(\mathbb{Q})$ may in this case consist of elements of order $1, 2, 3, 6$ only. Due to Properties 2.1, 2.2, there is $TorsC_m(\mathbb{Q}) = \{\mathcal{O}\}$ for $m \equiv 0$ $(mod\ 5)$.
The other cases: $m \equiv \pm 1$ $(mod\ 5)$ and $m \equiv \pm 2$ $(mod\ 5)$ can be analysed in the same way. □

REMARK 2.4. The above theorem is not true for $m = 0$. In that case, we get the curve $C_0 :\ y^2 = x^3 + 1$, which is well known and characterised; in particular, $C_0(\mathbb{Q}) = TorsC_0(\mathbb{Q}) \cong \mathbb{Z}_6$ ([**3**], 1.3, Theorem 3.3).

2.2. *Doubling a point on a curve.* We shall now describe a few properties of doubling an element of the group $C_m(\mathbb{Q})$.

PROPERTY 2.5. *Let* $A = (x', y')$ *and* $B = (x, y)$ *be points in* $C_m(\mathbb{Q})$, $m \geq 1$, *such that* $A = 2B$ *and* $x' \in \mathbb{Z}$. *Then:*
(*i*) $x \in \mathbb{Z}$,
(*ii*) $x \equiv m$ $(mod\ 2)$.

PROOF. Ad (*i*). Substituting $x = \frac{u}{s}$, $GCD(u, s) = 1$ to (2.1), after a short computation we get

$$u^4 - 4x'u^3s + 2m^2u^2s^2 + (4x'm^2 - 8)us^3 + (m^4 - 4x')s^4 = 0,$$

from which $s \mid u^4$, so $s \in \{-1, 1\}$ and $x \in \mathbb{Z}$.
Ad (*ii*). Observe that (2.1) can be rewritten as

$$(x^2 + m^2)^2 = 4\big(x'(x^3 - m^2x + 1) + 2x\big),$$

which gives $2 \mid (x^2 + m^2)$ and finally $x \equiv m$ $(mod\ 2)$.

□

PROPERTY 2.6. *Let* $A \in 2C_m(\mathbb{Q})$, $m \geq 1$, $A = (\frac{a}{b}, y)$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $GCD(a, b) = 1$. *Then:*
(*i*) *If* $m \equiv 0$ $(mod\ 2)$ *and* $b \equiv 1$ $(mod\ 2)$ *then* $a \equiv 0$ $(mod\ 4)$ *and* $\frac{a}{4} \equiv \frac{m^4}{16}$ $(mod\ 2)$.
(*ii*) *If* $m \equiv 1$ $(mod\ 2)$ *and* $b \equiv 1$ $(mod\ 2)$ *then* $a + b \equiv 0$ $(mod\ 4)$.

PROOF. Take formula (2.1) and substitute $x' = \frac{a}{b}$, $x = \frac{u}{s}$, $GCD(u, s) = 1$. After a computation we get

$$4as(u^3 - m^2us^2 + s^3) - b(u^4 + 2m^2u^2s^2 + m^4s^4 - 8us^3) = 0.$$

In the proof we will work on this equation.
Ad (*i*). Let $m \equiv 0$ $(mod\ 2)$. Clearly, u is even and s is odd, so we can substitute $m = 2k$, $b = 2c + 1$, $u = 2v$. After dividing the equation by 4 and reducing, we get $as^4 \equiv 0$ $(mod\ 4)$ and, since s is odd, $a \equiv 0$ $(mod\ 4)$.
For the other equivalence, substitute $a = 4e$ and divide the equation by 16. After the reduction we get

$$s^4(e + k^4) + v(v^3 + s^3) \equiv 0\ (mod\ 2).$$

The second component is always even, s is odd, so $e \equiv k^4 \ (mod\ 2)$, as desired.

Ad (*ii*). Let $m \equiv 1 \ (mod\ 2)$. Reducing the equation, we get $b(s^4 + u^4) \equiv 0 \ (mod\ 2)$. So in our case, since $GCD(u, s) = 1$, both u and s are odd. After substitutions $m = 2k + 1$, $s = 2t + 1$, $u = 2v + 1$ we divide the equation by 4 and, upon reducing, we get $a + b \equiv 0 \ (mod\ 4)$. □

3. Lower bound of the C_m curves' rank. The principal aim of this paper is to show, using methods as simple as possible, that

$$\operatorname{rank} C_m \geq 2 \qquad \text{for} \quad m \geq 2.$$

To this end, it is sufficient to find at least two independent points, say P_m and Q_m, in each curve. To check their independence we must show that none of P_m, Q_m and $P_m + Q_m$ is an element of $2C_m(\mathbb{Q})$.

Moreover, we will prove that $\operatorname{rank} C_m \geq 3$ for $m \geq 4$, $m \equiv 0 \ (mod\ 4)$. In this purpose we shall find the third point, independent of P_m and Q_m for such m.

The proof consists of two main steps. First we show that the chosen third point is in $2C_m(\mathbb{Q})$ iff $m \in \{3, 7, 24\}$ for $m \geq 1$. This is not an easy task; in fact, it has been stated in [**1**] as a separate problem. Some calculations needed to be done by a computer. After this we shall prove the independence of three points for $m \equiv 0 \ (mod\ 4)$. The proof goes analogically as the one for two points. It is important to notice that without the trivial torsion subgroup of C_m (Theorem 2.3) it would not be possible to show the independence of points with these methods, because the image of torsion subgroup in $C_m(\mathbb{Q})/2C_m(\mathbb{Q})$, not necessarily trivial, could affect the proof of Theorem 3.4.

3.1. *The general boundary:* $\operatorname{rank} C_m \geq 2$ *for* $m \geq 2$. In each curve C_m one can find the obvious points

$$P_m = P = (0, 1), \quad Q_m = (-1, m).$$

In order to bound the rank of C_m, we shall prove their independence.

Lemma 3.1. *The point* $P = (0, 1)$ *is an element of* $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ *for* $m \geq 1$.

Proof. Suppose that $P = 2B$ for some $m \in \mathbb{N}$ and $B \in C_m(\mathbb{Q})$. Letting $B = (x, y)$, from (2.1) we derive:

$$\frac{x^4 + 2m^2x^2 + m^4 - 8x}{4(x^3 - m^2x + 1)} = 0,$$

from which $(x^2 + m^2)^2 = 8x$. Using Property 2.5 (*i*) we see that $\exists k \in \mathbb{N} : x = 2k^2$. Solving the previous equation in m^2, we get $m^2 = -x^2 + 2\sqrt{2x}$, which, together with the above, gives $m^2 = -4k(k^3 - 1)$. Since $m^2 \geq 0$, we get $k = 0, 1$, for which $m = 0$. There are no solutions for $m \geq 1$. □

Lemma 3.2. *The point $Q_m = (-1, m)$ is an element of $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ for $m \geq 2$.*

Proof. Proceeding as in the previous proof, from (2.1) one gets

$$\frac{x^4 + 2m^2x^2 + m^4 - 8x}{4(x^3 - m^2x + 1)} = -1,$$

which gives

$$8x = 4(x^3 - m^2x + 1) + (x^2 + m^2)^2 = 4y^2 + (x^2 + m^2)^2 \geq 0,$$

so that $x \geq 0$.
The above formula can be transformed into a quadratic equation in m^2:

$$m^4 + m^2(2x^2 - 4x) + (x^4 + 4x^3 - 8x + 4) = 0,$$

which has real solutions iff $\Delta = -32(x-1)(x+1)(x-\frac{1}{2}) \geq 0$, from which $x \in (-\infty, -1] \cup [\frac{1}{2}, 1]$. By Property 2.5 (i) and the condition $x \geq 0$, only $x = 1$ remains. Hence, $y^2 = 2 - m^2$, a contradiction for $m \geq 2$. □

Lemma 3.3. *The point $P + Q_m = (m^2 - 2m + 2, m^3 - 3m^2 + 4m - 3)$ is an element of $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ for $m \geq 1$.*

Proof. Take $m \geq 1$ and put $P + Q_m =: (x', y')$. Letting $m = 2n$ for even m, one gets $x' = 4n^2 - 4n + 2 \equiv 2\ (mod\ 4)$. For odd m, let $m = 2n + 1$. Then $x' = 4n^2 + 1 \equiv 1\ (mod\ 4)$. Now apply Property 2.6. □

We are now in a position to prove that rank $C_m \geq 2$.

Theorem 3.4. *The points $P = (0, 1)$ and $Q_m = (-1, m)$ are $\mathbb{Z}$-independent in $C_m(\mathbb{Q})$ for $m \geq 2$, i.e., $\forall n, k \in \mathbb{Z}: (nP + kQ_m = \mathcal{O} \Rightarrow k = n = 0)$.*

Proof. Fix an arbitrary $m \geq 2$ and put $Q_m =: Q$. Let $nP + kQ = \mathcal{O}$ for some $k, n \in \mathbb{Z}$ with minimal positive n. If k is even and n is odd then in the group $C_m(\mathbb{Q})/2C_m(\mathbb{Q})$ there is $[\mathcal{O}] = [nP + kQ] = [P]$, which contradicts 3.1. Similarly, for n even and k odd, one gets $[Q] = [\mathcal{O}]$, which contradicts 3.2, and for both odd there is $[P + Q] = [\mathcal{O}]$ which contradicts 3.3. For both k and n even there is $2(n'P + k'Q) = \mathcal{O}$, which means that $n'P + k'Q$ is a 2-order torsion point. Due to Th. 2.3, there is $n'P + k'Q = \mathcal{O}$, which contradicts the minimality of n. □

Remark 3.5. For $m = 1$ the point $Q = (-1, 1)$ is the double of the point $R := (1, 1)$ and is not independent of P. Indeed, one can easily compute that $P + R = -Q$. Multiplying by 2 and substuting $Q = 2R$ one gets $2P + 3Q = \mathcal{O}$.

The attempts to find another point independent of P have failed. Computer calculations (using MWrank by J. E. Cremona) revealed that rank $C_1 = 1$.

Thus we have proved that rank $C_m(\mathbb{Q}) \geq 2$ for $m \geq 2$.

3.2. *The third point problem.* In order to lift up the lower bound of our curves' rank, we need to find a third point, $\mathbb{Z}$-independent of P and Q_m. This will require much more computation and more theorems to be applied.

Note that on each curve C_m there is a third obvious point,

$$R_m := (m, 1).$$

THEOREM 3.6. *For $m \geq 1$, the point $R_m = (m,1)$ is an element of $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ iff $m \notin \{3,7,24\}$.*

PROOF. Suppose that $R_m = 2B$ for some $m \geq 1$ and $B = (x,y) \in C_m(\mathbb{Q})$. From formula (2.1) there follows

$$x^4 - 4mx^3 + 2m^2x^2 + (4m^3 - 8)x + m^4 - 4m = 0.$$

We shall find all the values of m for which any integral solutions in x exist. From Property 2.5 (i) we know that there can be no other rational solutions. The above formula can be easily put into the form

$$(x-m)^4 - 4(x-m)^2m^2 - 8(x-m) - 12m + 4m^4 = 0.$$

Due to Property 2.5 (ii), we can substitute $x - m =: 2s$, which puts our equation in the form $(2s^2 - m^2)^2 = 4s + 3m$. Next, substituting $n := 2s^2 - m^2$, we obtain $n^2 = 4s + 3m$, from which

$$(*) \qquad m = \frac{n^2 - 4s}{3}.$$

Now substituting $(*)$ to the definition of n, one gets

$$\binom{*}{*} \qquad 2(s + 2n^2)^2 - 9n^4 - 9n = 0.$$

From this we can see that $n^4 + n$ is of the form $2k^2$ for some $k \in \mathbb{Z}$. There is the decomposition $n^4 + n = n(n+1)(n^2 - n + 1)$, where the last factor is odd; moreover, $GCD(n+1, n^2 - n + 1) \in \{1,3\}$. By this, there are the two possibilities:

$$\textbf{1.} \begin{cases} n^2 - n + 1 = u^2 \\ n(n+1) = 2v^2 \end{cases} \qquad \text{or} \qquad \textbf{2.} \begin{cases} n^2 - n + 1 = 3u^2 \\ n(n+1) = 6v^2 \end{cases}$$

for some $u, v \in \mathbb{N}$.

Ad 1. Compute the discriminant $\Delta = 4u^2 - 3$ of the quadratic equation $n^2 - n + (1 - u^2) = 0$ in the variable n. The solution is $n = \frac{1 \pm \sqrt{\Delta}}{2}$, so $\Delta = (2n-1)^2$, the square of a positive integer t. Hence, there is $4u^2 - 3 = t^2$, thus $(2u - t)(2u + t) = 3$. The factors of the above product can only take values in the set $\{1, -1, 3, -3\}$, all of which give $u^2 = 1$. Our equation gets the form $n^2 - n = 0$, from which $n \in \{0, 1\}$.
For $n = 0$, from $\binom{*}{*}$ and $(*)$, we get $s = m = 0$.

For $n = 1$, in the same way as above, we get $(s, m) = (1, -1)$ and $(s, m) = (-5, 7)$.
To sum up, the case **(1.)** gives rise to the solutions $m \in \{-1, 0, 7\}$.

Ad 2. Due to n and $n+1$ being relatively prime, the equation $n(n+1) = 6v^2$ allows four possible decompositions, namely

$$2.(a) \begin{cases} n^2 - n + 1 = 3u^2 \\ n = \pm 2w^2 \\ n + 1 = \pm 3z^2 \end{cases} \quad \text{or} \quad 2.(b) \begin{cases} n^2 - n + 1 = 3u^2 \\ n = \pm w^2 \\ n + 1 = \pm 6z^2 \end{cases}$$

Transforming the first of the above equations one gets

$$n(n + 1) - 2n + 1 = 3u^2.$$

Since $n(n+1) = 6v^2$, there is $-2n+1 \equiv 0 (mod\ 3)$, so $n \equiv 2(mod\ 3)$. Thus, we need to consider two cases only:

$$\textbf{2.}(\boldsymbol{a'}) \begin{cases} n^2 - n + 1 = 3u^2 \\ n = 2w^2 \\ n + 1 = 3z^2 \end{cases} \quad \text{and} \quad \textbf{2.}(\boldsymbol{b'}) \begin{cases} n^2 - n + 1 = 3u^2 \\ n = -w^2 \\ n + 1 = -6z^2 \end{cases}$$

In case **(2.*a'*)** there is

$$u^2 = 3z^4 - 3z^2 + 1$$

which is the equation of a quartic with a rational point $(z, u) = (0, 1)$, hence it can be birationally transformed into an elliptic curve ([**2**]) by the following substitution:

$$z = \frac{2X - 4}{Y}, \quad u = \frac{X^3 - 6X^2 + 15X - 14}{Y^2}$$

with the inverse given by

$$X = \frac{2u + 2 - z^2}{z^2}, \quad Y = \frac{4u + 4 - 6z^2}{z^3}.$$

We get the elliptic curve

$$E_1 : Y^2 = X^3 - 15X + 22 = (X - 2)(X^2 + 2X - 11)$$

birational to our quartic. For the elliptic curves of this form, it is easy to compute $\operatorname{rank} E_1 = 0$ and $TorsE_1(\mathbb{Q}) \cong \mathbb{Z}_6$. The whole calculation connected with this kind of transformations has been done by computer using Apecs (Maple V, I. Connell).

The following table lists the points $(X, Y) \in TorsE_1(\mathbb{Q})$ (since $\operatorname{rank} E_1 = 0$, these are all of the rational points of E_1) and their corresponding rational solutions (z, u).

(X, Y)	(z, u)
$(-1, 6)$	$(-1, -1)$
$(-1, -6)$	$(1, -1)$
$(3, 2)$	$(1, 1)$
$(3, -2)$	$(-1, 1)$
$(2, 0)$	$(0, -1), (0, 1)$ – singularity of the parametrization

For the points (z, u) with $z = 0$, we get $n + 1 = 0$ and $2w^2 = -1$, a contradiction. The points with $z^2 = 1$ give the solution $n = 2$, from which $w^2 = 1$, $u^2 = 1$. As in the previous case, we compute $(s, m) = (1, 0)$ and $(s, m) = (-17, 24)$.

In case **(2.*b*')** there is

$$u^2 = \frac{1}{3}w^4 + \frac{1}{3}w^2 + \frac{1}{3}.$$

It is, similarly, a quartic with a rational point $(z, u) = (1, 1)$. Applying the birational substitution:

$$w = \frac{Y + 3X + 15}{Y - 3X - 15}, \quad u = \frac{X^3 + 15X^2 + 39X - 55}{(Y - 3X - 15)^2},$$

with the inverse given by

$$X = \frac{18u + 4w + 7w^2 + 7}{(w-1)^2}, \quad Y = \frac{54u + 36 + 18w + 18w^2 + 54uw + 36w^3}{(w-1)^3}$$

we get the following elliptic curve

$$E_2: \ Y^2 = X^3 - 39X - 70 = (X + 2)(X + 5)(X - 7).$$

As above, we compute $\operatorname{rank} E_2 = 0$ and $TorsE_2(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
The following table contains the points $(X, Y) \in TorsE_2(\mathbb{Q})$ which are all the rational points of E_2 (since $\operatorname{rank} E_2 = 0$) and their corresponding rational solutions (w, u).

(X, Y)	(w, u)
$(-2, 0)$	$(-1, -1)$
$(7, 0)$	$(-1, 1)$
$(-5, 0)$	$(1, -1), (1, 1)$ – singularity of the parametrisation

From this, $n = -1$ and we get $(s, m) = (-1, 3)$. Together with the above, case (**2.**) gives solutions $m \in \{0, 3, 24\}$.

To sum up, cases (**1.**) and (**2.**) supply the solutions $m \in \{-1, 0, 3, 7, 24\}$, which completes the proof. □

A natural question arises of what happens for $R_m \in 2C_m(\mathbb{Q})$, or equally for $m \in \{3, 7, 24\}$.
For $m = 3$ we shall not find the third point. In this case $R = 2Q$, so these three points are not independent. Indeed, computer calculations revealed that $\operatorname{rank} C_3 = 2$.
The cases $m = 7$ and $m = 24$ are considered below.

Fact 3.7. *Let $m = 7$. Then:*

1. *The point $R = (7, 1)$ is the double of the point $R' := (-3, 11)$.*
2. *The points R', $P + R' = (\frac{127}{9}, \frac{1243}{27})$, $Q + R' = (8, 11)$, $P + Q + R' = (-\frac{103}{16}, \frac{451}{64})$ are the elements of $C_7(\mathbb{Q}) \setminus 2C_7(\mathbb{Q})$.*

Proof. For the points R' and $Q + R'$, apply Property 2.6 (ii). For $P+R'$ and $P+Q+R'$, do computations using (2.1); the appearing polynomials have no rational zeros. □

Fact 3.8. *Let $m = 24$. Then:*

1. *The point $R = (24, 1)$ is the double of the point $R'' := (-10, 69)$.*
2. *The points R'', $P+R'' = (\frac{1406}{25}, \frac{47679}{125})$, $Q+R'' = (36, 161)$, $P+Q+R'' = (-\frac{1316}{81}, \frac{51911}{729})$ are the elements of $C_{24}(\mathbb{Q}) \setminus 2C_{24}(\mathbb{Q})$.*

Proof. Apply Property 2.6 (i). □

Thus we have proved that $\operatorname{rank} C_7 \geq 3$ and $\operatorname{rank} C_{24} \geq 3$.

3.3. *The subfamily of higher rank.* We are now left to consider the general case of $m \geq 4$, $m \neq 7, 24$. We choose

$$S_m := -(P + R_m) = (-m, 1)$$

as the third independent point.

The choice of S_m was designed to minimalize the complexity of required computation, such complexity depending on the coordinates of points involved in the computation.

To simplify the notation we shall omit the indices when denoting P_m, Q_m, R_m and S_m.

We are now in a position to prove that the points P, Q and S are independent for $m \equiv 0\ (mod\ 4)$. This will provide

$$\operatorname{rank} C_m \geq 3 \quad \text{for} \quad m \geq 4,\ m \equiv 0\ (mod\ 4).$$

Lemma 3.9. *Let $m \geq 4$ and $m \neq 7, 24$. The points S and $S + P$ are the elements of $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$.*

Proof. Notice that the coordinates of points S and R differ only by the sign at m, so there is

$$\{m :\ S \in 2C_m(\mathbb{Q})\} = \{-m :\ R \in 2C_m(\mathbb{Q})\} = \{1, 0, -3, -7, -24\},$$

hence $S \notin 2C_m(\mathbb{Q})$. Next, there is $P + S = P - (P + R) = -R$, so $P + S \notin 2C_m(\mathbb{Q})$, because $R \notin 2C_m(\mathbb{Q})$. □

The combinations of the point S with points Q, $P + Q$ are considered in the following lemma, which is a direct consequence of Property 2.5.

LEMMA 3.10. *Under the above assumptions, there is*

1. $Q + S = (m + 2, -2m - 3)$ *is an element of* $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ *for* $m \equiv 0\ (mod\ 4)$, $m \equiv -1\ (mod\ 4)$.
2. $P + Q + S = (2 - m, -2m + 3)$ *is an element of* $C_m(\mathbb{Q}) \setminus 2C_m(\mathbb{Q})$ *for* $m \equiv 0\ (mod\ 4)$, $m \equiv 1\ (mod\ 4)$. □

So we managed to bound the rank of elliptic curves from the family C_m applying elementary methods. The obtained results are summarised in the following theorem.

THEOREM 3.11.

1. *For* $m \geq 2$, *there is* $\operatorname{rank} C_m \geq 2$.
2. *For* $m \geq 4$, $m \equiv 0(mod\ 4)$ *and for* $m = 7$, *there is* $\operatorname{rank} C_m \geq 3$.

For the further research, it seems possible to prove that the ranks of all curves C_m are at least equal to 3; also, one may look for a subfamily of rank at least equal to 4.

References

1. Brown E., Myers B.T., *Elliptic Curves from Mordell to Diophantus and Back*, Amer. Math. Monthly, **109**, Aug-Sept 2002, 639–648.
2. Cremona J.E., *Rational Points on Curves, Lecture Notes*, `http://www.maths.nottingham.ac.uk/personal/jec/courses/G1CRPC`
3. Husemöller D., *Elliptic Curves*, Springer-Verlag, New York, 1987.
4. Lang S., *Algebra*, Graduate Texts in Mathematics, Vol. **211**, Springer-Verlag, 2002.
5. Silverman J.H., *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

Received October 12, 2005

Jagiellonian University
Institute of Mathematics
ul. Reymonta 4
30-059 Kraków
Poland
e-mail: anna_antoniewicz@yahoo.com