ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 45, Number 5, 2015

# ON THE MORDELL-WEIL GROUP OF ELLIPTIC CURVES INDUCED BY FAMILIES OF DIOPHANTINE TRIPLES

MILJEN MIKIĆ

ABSTRACT. The problem of the extendibility of Diophantine triples is closely connected with the Mordell-Weil group of the associated elliptic curve. In this paper, we examine Diophantine triples $\{k-1, k+1, c_l(k)\}$ and prove that the torsion group of the associated curves is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $l = 3, 4$ and $l \equiv 1$ or $2 \pmod 4$. Additionally, we prove that the rank is greater than or equal to 2 for all $l \geq 2$. This represents an improvement of previous results by Dujella, Pethő and Najman, where cases $k = 2$ and $l \leq 3$ were considered.

**1. Introduction.** A set of $m$ positive integers $\{a_1, a_2, \ldots, a_m\}$ is called a *Diophantine $m$-tuple* if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. One of the most interesting questions about Diophantine $m$-tuples is how large these sets can be, or, in other words, what is the upper bound for $m$. The first Diophantine quadruple, $\{1, 3, 8, 120\}$ was found by Fermat (see **[2]**). Dujella **[3]** proved that there does not exist a Diophantine sextuple and that there are only finitely many Diophantine quintuples.

Let $\{a, b, c\}$ be a Diophantine triple, i.e.,

$$ab + 1 = r^2, \qquad ac + 1 = s^2, \qquad bc + 1 = t^2, \quad r, s, t \in \mathbb{N}.$$

In order to extend a Diophantine triple $\{a, b, c\}$ to a quadruple, one has to solve the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{1.1}$$

It is natural to assign to the system (1.1) the elliptic curve

$$E : y^2 = (ax + 1)(bx + 1)(cx + 1)$$

2010 AMS *Mathematics subject classification.* Primary 11G05.

*Keywords and phrases.* Diophantine triples, elliptic curves, Mordell-Weil group.

Received by the editors on October 14, 2013, and in revised form on November 15, 2013.

DOI:10.1216/RMJ-2015-45-5-1565

(we say that $E$ is induced by the system (1.1)). $E$ has three obvious rational points of order 2:

$$A = \left(-\frac{1}{a}, 0\right), \qquad B = \left(-\frac{1}{b}, 0\right), \qquad C = \left(-\frac{1}{c}, 0\right),$$

and two additional rational points:

$$P = (0,1), \qquad R = \left(\frac{1}{abc}, \frac{rst}{abc}\right).$$

$P$ and $R$ are in many cases independent and of infinite order, which immediately gives rank $E(\mathbb{Q}) \geq 2$ in such cases.

It is clear that every solution of the system (1.1) induces an integer point on the elliptic curve $E$. The converse of this statement depends on the Mordell-Weil group of $E$. By the Mordell-Weil theorem, the group $E(\mathbb{Q})$ of rational points on every elliptic curve $E$ is a finitely generated abelian group. Hence, it is the product of the torsion group and $r$ ($r \geq 0$) copies of the infinite cyclic group:

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

Therefore, to find the conditions for extending Diophantine triples to quadruples, in this paper, we are going to examine the rank and the torsion group of $E$ induced by certain families of Diophantine triples. By Mazur's theorem [**12**], we know that $E(\mathbb{Q})_{\mathrm{tors}}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$, with $1 \leq n \leq 10$, or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with $1 \leq m \leq 4$. However, in our joint paper with Dujella ([**6,** Corollary 4]) we proved that there are no rational points of order 4 on any elliptic curve induced by a Diophantine triple. In other words, the only possible torsion groups of $E(\mathbb{Q})$ are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Now, when we determine how elliptic curves can be used to resolve the problem of extending Diophantine triples to quadruples (and this is also the case with extending quadruples to quintuples, see [**5**]), let us mention that there is also an important connection between elliptic curves and Diophantine $m$-tuples, but in the opposite direction. Namely, Diophantine triples have been a useful tool for constructing families of elliptic curves with high rank. An elliptic curve over the field of rational functions with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank equal to 4, and an elliptic curve over $\mathbb{Q}$ with the same torsion group and rank 9, both induced by rational Diophantine triples, have been constructed by

Dujella and Peral [**7**], and these are the current rank records for this torsion group.

Let us define, for $k \geq 2$ and $l \in \mathbb{N}$, a sequence $\{c_l(k)\}$ as:

$$c_l(k) = \frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1} - 2k}{2(k^2-1)}. \tag{1.2}$$

Then $(k-1)c_l(k)+1$ and $(k+1)c_l(k)+1$ are perfect squares, i.e., $\{k-1, k+1, c_l(k)\}$ is a Diophantine triple. To prove that, let us define for $k \geq 2$ and $l \in \mathbb{N}$ the sequences $\{s_l(k)\}$ and $\{t_l(k)\}$ as:

$$s_l(k)^2 = (k-1)c_l(k)+1, \tag{1.3}$$

$$t_l(k)^2 = (k+1)c_l(k)+1. \tag{1.4}$$

We will show that $s_l(k)$ and $t_l(k)$ are given by the following explicit formulas:

$$\begin{aligned} s_l(k) = {} & \frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k+1}} \\ & + \frac{(k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k+1}}, \end{aligned} \tag{1.5}$$

$$\begin{aligned} t_l(k) = {} & \frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k-1}} \\ & - \frac{(k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k-1}}. \end{aligned} \tag{1.6}$$

Namely, from (1.2) and (1.3), it follows that

$$\begin{aligned} s_l(k)^2 &= \frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1} + 2}{2(k+1)} \\ &= \Bigg(\frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k+1}} \\ &\quad + \frac{(k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k+1}}\Bigg)^2. \end{aligned}$$

The formula (1.6) is analogously proved. With the explicit formulas provided, one can easily verify that these sequences satisfy the following recurrence relations:

$$s_l(k) = 2ks_{l-1}(k) - s_{l-2}(k), \tag{1.7}$$

$$t_l(k) = 2kt_{l-1}(k) - t_{l-2}(k). \tag{1.8}$$

Thus, $s_l(k)$ and $t_l(k)$ are positive integers for all $k \geq 2$ and $l \in \mathbb{N}$, which, together with (1.3) and (1.4), implies that $\{k-1, k+1, c_l(k)\}$ is a Diophantine triple.

Dujella [**4**] was the first who examined a parametric family of elliptic curves induced by Diophantine triples $\{k-1, k+1, c_1(k)\}$. All integer points on the elliptic curves associated with these triples have been found for the curves with rank 1 and for certain subfamilies of the curves with ranks 2 and 3. Dujella and Pethő [**8**] considered a special case $k = 2$, i.e., triples $\{1, 3, c_l(2)\}$, and found all integer points when the rank of the associated curve is 2, or $l \leq 40$. Najman [**14**] continued studying the families of the curves induced by $\{k-1, k+1, c_l(k)\}$ and successfully found all integer points on the families induced by triples $\{k-1, k+1, c_2(k)\}$ and $\{k-1, k+1, c_3(k)\}$ under the assumption that the rank of the associated curve is 2, or $2 \leq k \leq 10000$. There are also results about the extendibility of Diophantine triples $\{k-1, k+1, c_l(k)\}$; in [**1, 9**] it was proved that, if $\{k-1, k+1, c_l(k), d\}$ is a Diophantine quadruple, $d$ has to be either $c_{l-1}(k)$ or $c_{l+1}(k)$.

This paper further extends findings about the families of curves induced by triples $\{k-1, k+1, c_l(k)\}$, with the focus on their torsion group and rank. The latter is particularly interesting because it has been conjectured (see [**16**]) that the number of integer points on an elliptic curve $E$ in Weierstrass form grows exponentially with the rank of $E(\mathbb{Q})$. In [**14,** Lemma 7], it was proved that the torsion group of the curves induced by $\{k-1, k+1, c_3(k)\}$ has to be isomorphic to the one of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. However, there remained an open question whether the latter can occur, and our Theorem 2.1 eliminates that case. As the next logical step, Theorem 2.2 establishes the same result for the family induced by Diophantine triples $\{k-1, k+1, c_4(k)\}$. Finally, Theorem 2.3 expands that result on the one half of all families of curves induced by triples $\{k-1, k+1, c_l(k)\}$, namely, those with $l \equiv 1$ or $2 \pmod 4$. The question of the rank is covered by Theorem 3.11. It was previously proved that the rank of the associated elliptic curve is greater than or equal to 2 in the cases $l = 2, 3$ [**14,** Proposition 5 and 11] and $k = 2$ [**8,** Proposition 2]. We extended this statement to all elliptic curves induced by $\{k-1, k+1, c_l(k)\}$ with $l \geq 2$.

In order to extend a Diophantine triple $\{k-1, k+1, c_l(k)\}$ to a quadruple, we have to solve the system

$$(1.9) \quad (k-1)x+1=\square, \qquad (k+1)x+1=\square, \qquad c_l(k)x+1=\square.$$

We assign to the system (1.9) the elliptic curve

$$E_l(k): y^2 = ((k-1)x+1)((k+1)x+1)(c_l(k)x+1).$$

**2. Torsion group of $E_l(k)$.** The coordinate transformation

$$x \longmapsto \frac{x}{(k-1)(k+1)c_l(k)}, \qquad y \longmapsto \frac{y}{(k-1)(k+1)c_l(k)}$$

applied on the curve $E_l(k)$ leads to the elliptic curve

$$(2.1) \quad E_l(k)': y^2 = (x+(k-1)(k+1))(x+(k-1)c_l(k))(x+(k+1)c_l(k)).$$

There are three rational points on $E_l(k)'$ of order two:

$$A' = (1-k^2,\ 0), \qquad B' = ((1-k)c_l(k),\ 0), \qquad C' = (-(k+1)c_l(k),\ 0).$$

We will prove these are the only rational points of finite order for $l=3$, $l=4$, and for all $l$ of the form $l=4m-2$ and $l=4m-3$ where $m \in \mathbb{N}$.

At the beginning, let us list the first few members of $\{c_l(k)\}$:

$$\begin{aligned} c_1(k) &= 4k, \\ c_2(k) &= 16k^3 - 4k, \\ c_3(k) &= 64k^5 - 48k^3 + 8k, \\ c_4(k) &= 256k^7 - 320k^5 + 112k^3 - 8k. \end{aligned}$$

One can easily verify by the induction on $l$ that the members of $\{c_l(k)\}$ satisfy the following recurrence relation:

$$(2.2) \qquad c_{l+2}(k) = (4k^2-2)c_{l+1}(k) - c_l(k) + 4k.$$

**Theorem 2.1.** *$E_3(k)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*Proof.* Putting $l=3$ in (2.1) gives the elliptic curve:

$$\begin{aligned} E_3(k)': y^2 = (x+(k-1)(k+1)) &\left(x+(k-1)(64k^5-48k^3+8k)\right) \\ &\times \left(x+(k+1)(64k^5-48k^3+8k)\right). \end{aligned}$$

With a simple transformation $x \mapsto x-(k-1)(k+1)$ we get a curve in the form $y^2=x(x+M)(x+N)$:

$$\begin{aligned} E_3(k)'' : y^2 = x(x+(k-1)&(64k^5-48k^3+7k-1)) \\ &\times (x+(k+1)(64k^5-48k^3+7k+1)). \end{aligned}$$

Since $\{k-1, k+1, 64k^5-48k^3+8k\}$ is a Diophantine triple, it follows from [**6,** Corollary 4] that the only possible torsion groups of $E_3(k)''$ are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. We will prove that the latter case is impossible. Let us suppose the contrary, that the torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. By [**15,** Main Theorem 1] (more precisely stated in [**11,** Proposition 2]) there exist coprime integers $a$, $b$ and a positive integer $d$ such that:

$$\begin{aligned} M &= d^2(a^4+2a^3b), \\ N &= d^2(b^4+2ab^3) \end{aligned}$$

and $a/b \notin \{-2,-1,-1/2,0,1\}$. Therefore, we have:

$$M=(k-1)(64k^5-48k^3+7k-1)=d^2(a^4+2a^3b), \tag{2.3}$$

$$N=(k+1)(64k^5-48k^3+7k+1)=d^2(b^4+2ab^3). \tag{2.4}$$

Notice that

$$N+M=128k^6-96k^4+14k^2+2, \tag{2.5}$$

$$N-M=128k^5-96k^3+16k. \tag{2.6}$$

Let us define $m=\gcd(M,N)$. We will prove that $m=2^a3^b$, where $a \le 4, b \le 1$ which will imply that $d^2 \in \{1,4,16\}$.

Obviously, $m \mid N-M$, which is equivalent to $m \mid 16k(8k^4-6k^2+1)$, and that gives

$$m \mid 16k(4k^2-1)(2k^2-1). \tag{2.7}$$

Let $p$ be any prime divisor of $m$. From (2.7), we have several possibilities:

(i) $p \mid k$. Because of (2.4), we have:

$$N=64k^6+64k^5-48k^4-48k^3+7k^2+8k+1 \equiv 1 \pmod{p},$$

which contradicts $N \equiv 0 \pmod{p}$.

(ii) $p \mid 2k^2-1$. We have:

$$14k^2 \equiv 7 \pmod p,\ 96k^4 \equiv 24 \pmod p,\ 128k^6 \equiv 16 \pmod p.$$

Therefore, from (2.5):

$$N+M \equiv 16-24+7+2 \equiv 1 \pmod p,$$

which contradicts $N+M \equiv 0 \pmod p$.

(iii) $p \mid 16$. In this case it is obvious that $p=2$.

(iv) $p \mid 4k^2-1$. We will only consider the case $p \mid 2k-1$ (case $p \mid 2k+1$ is analogous). We have:

$$8k \equiv 4 \pmod p, \qquad 8k^2 \equiv 2 \pmod p, \qquad 48k^3 \equiv 6 \pmod p,$$
$$48k^4 \equiv 3 \pmod p, \qquad 64k^5 \equiv 2 \pmod p, \qquad 64k^6 \equiv 1 \pmod p.$$

Therefore, again from (2.4):

$$N \equiv 1+2-3-6+(2-k^2)+4+1 \equiv 1-k^2 \pmod p,$$

and we know that $N \equiv 0 \pmod p$, which implies $1-k^2 \equiv 0 \pmod p$, and this is equivalent to

$$4k^2 \equiv 4 \pmod p. \tag{2.8}$$

Combining (2.8) with $4k^2 \equiv 1 \pmod p$ gives $p=3$. Notice that 1 is the highest power of 3 contained in $m$ because $3^n$ with $n \geq 2$ cannot divide both $4k^2-1$ and $4k^2-4$. Additionally, $p=3$ cannot divide $2k-1$ and $2k+1$ at the same time, and it does not divide other factors of (2.7), as well.

It is thus clear that $m=2^a3^b$, where $a \leq 4, b \leq 1$ so $d^2$ can be one of $\{1,4,16\}$. Firstly, we will show that the case $d^2=4$ cannot appear. Namely, in that case, the system (2.3) and (2.4) becomes

$$64k^6-64k^5-48k^4+48k^3+7k^2-8k+1 = 4(a^4+2a^3b),$$
$$64k^6+64k^5-48k^4-48k^3+7k^2+8k+1 = 4(b^4+2ab^3),$$

so the left hand sides must be divisible by 4, and that is possible only if $7k^2+1 \equiv 0 \pmod 4$, which implies $7k^2+1 \equiv 0 \pmod 8$. Hence, the left hand sides are divisible by 8, so the right hand sides must be divisible by 8 as well, which is only possible for even $a$ and $b$. However, $a$ and $b$ are coprime, and therefore the case $d^2=4$ is impossible. In the two remaining cases note that $d^2 \equiv 1 \pmod 5$. Hence, our system implies:

$$\begin{aligned} M &= (k-1)(64k^5 - 48k^3 + 7k - 1) \equiv a^4 + 2a^3b \pmod 5, \\ N &= (k+1)(64k^5 - 48k^3 + 7k + 1) \equiv b^4 + 2ab^3 \pmod 5. \end{aligned}$$

We shall now observe congruences modulo 5 and consequently conclude that this system does not have a solution in integers. When $k \equiv 0$ or 2 or 3 (mod 5) the left hand sides of this system are either both congruent to 1 or 2 modulo 5. In cases $k \equiv 1$ or $4 \pmod 5$, one of them is congruent to 0, and the other to 3 modulo 5. However, by listing all possible remainders modulo 5 for $a$ and $b$, we easily verify that none of these combinations can appear on the right hand sides of this system. Hence, there is no solution in integers. A contradiction. □

Next, we will prove the same result for the family $\{k-1, k+1, c_4(k)\}$.

**Theorem 2.2.** *$E_4(k)(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*Proof.* Like in the previous proof, let us assume that the torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. With similar reasoning, we get:

$$\begin{aligned} E_4(k)'' : y^2 = x\, &\big(x + (k-1)(256k^7 - 320k^5 + 112k^3 - 9k - 1)\big) \\ &\times \big(x + (k+1)(256k^7 - 320k^5 + 112k^3 - 9k + 1)\big) \end{aligned}$$

and

$$M = (k-1)(256k^7 - 320k^5 + 112k^3 - 9k - 1) = d^2(a^4 + 2a^3b), \tag{2.9}$$

$$N = (k+1)(256k^7 - 320k^5 + 112k^3 - 9k + 1) = d^2(b^4 + 2ab^3). \tag{2.10}$$

Here, we will observe congruences modulo 3. Naturally, there are three possibilities:

(i) $k \equiv 2 \pmod 3$. The left hand side of (2.9) is congruent to 2 modulo 3, and the left hand side of (2.10) is congruent to 0 modulo 3. Thus, the right hand side of (2.10) must also be divisible by 3. This implies one of the following:
   (a) $d \equiv 0 \pmod 3$. The right hand side of (2.9) is divisible by 3, a contradiction.

(b) $b \equiv 0 \pmod 3$. The right hand side of (2.9) is congruent to $d^2a^3(a+2b)$ modulo 3, which further gives $d^2a^3(a+2b) \equiv d^2a^4 \equiv (da^2)^2 \pmod 3$. This is impossible since the right hand side of (2.9) is congruent to 2 modulo 3, and 2 is not quadratic residue modulo 3.

(c) $a \equiv b \pmod 3$. The right hand side of (2.9) is divisible by 3, a contradiction.

(ii) $k \equiv 1 \pmod 3$. The left hand side of (2.10) is congruent to 2 modulo 3 and the left hand side of (2.9) is congruent to 0 modulo 3. Thus, the right hand side of (2.9) must also be divisible by 3. This case is hence analogous to the previous one, a contradiction.

(iii) $k \equiv 0 \pmod 3$. The left hand sides of both (2.9) and (2.10) are congruent to 1 modulo 3. This implies $d^2 \equiv 1 \pmod 3$ and $a^3(a+2b) \equiv b^3(b+2a) \equiv 1 \pmod 3$, which is impossible. Namely, if either $a$ or $b$ is divisible by 3, then at least one of the previous expression will be divisible by 3. If $a$ and $b$ are congruent modulo 3, then the factors $(a+2b)$ and $(b+2a)$ will be divisible by 3. Therefore, the only possible combination is that one of them is congruent 1 modulo 3, and the other is congruent 2 modulo 3. But, that does not satisfy the requirement $a^3(a+2b) \equiv b^3(b+2a) \equiv 1 \pmod 3$. □

The following result is substantially wider since it covers all elliptic curves induced by the triples $\{k-1, k+1, c_l(k)\}$, where $l \equiv 1$ or $2 \pmod 4$.

**Theorem 2.3.** *$E_l(k)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for all $l = 4m-2$ and $l = 4m-3$ where $m \in \mathbb{N}$.*

*Proof.* We know the exact formulas for $c_1(k)$ and $c_2(k)$, combining them with (2.2) gives the following sequence of congruences modulo 8:

$$\begin{aligned} c_1(k) &\equiv 4k \pmod 8\\ c_2(k) &\equiv 4k \pmod 8,\\ c_3(k) &\equiv 0 \pmod 8,\\ c_4(k) &\equiv 0 \pmod 8,\\ c_5(k) &\equiv 4k \pmod 8,\\ c_6(k) &\equiv 4k \pmod 8,\\ &\cdots. \end{aligned}$$

Hence, we conclude that

$$c_{4m-2}(k) \equiv c_{4m-3}(k) \equiv 4k \pmod 8, \tag{2.11}$$

$$c_{4m}(k) \equiv c_{4m-1}(k) \equiv 0 \pmod 8, \tag{2.12}$$

for $m \in \mathbb{N}$. From (2.1), with the coordinate transformation $x \mapsto x-(k-1)c_l(k)$, we get the following curve:

$$E_l(k)'' : y^2 = x(x+(k-1)(k+1-c_l(k)))(x+2c_l(k)).$$

As in the proofs of the two previous theorems, we will assume the opposite, that the torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. This brings the system of equations:

$$M = (k-1)(k+1-c_l(k)) = d^2(a^4+2a^3b), \tag{2.13}$$

$$N = 2c_l(k) = d^2(b^4+2ab^3). \tag{2.14}$$

From (2.14), it follows that at least one of $b$ or $d$ is even.

(i) $b$ is even and $d$ is odd. The right hand side of (2.14) is divisible by 16, so the left hand side must be divisible by 16 as well, which implies that $k$ is even (see (2.11)). Then, from (2.13), it follows that $a$ is odd. By adding (2.13) and (2.14), we get

$$k^2-1+(3-k)c_l(k) = d^2\left((a^2+ab+b^2)^2-3a^2b^2\right). \tag{2.15}$$

Since $d$ is odd, it must be $d^2 \equiv 1 \pmod 8$, which implies that the right hand side of (2.15) is congruent to 1 or 5 modulo 8. On the left hand side there is $c_l(k) \equiv 0 \pmod 8$ and $k$ is even, so the left hand side is congruent to 3 or 7 modulo 8, a contradiction.

(ii) $b$ is odd and $d$ is even. From (2.13), it follows that $k$ is odd. It means that the left hand side of (2.14) is divisible by 8 but is not divisible by 16. This is a contradiction with the right hand side which is, depending on $d$, either divisible by 4 or 16.

(iii) Both $b$ and $d$ are even. From (2.13), it follows that $k$ is odd and from (2.14) that $k$ is even, which is obviously impossible. □

**Remark 2.4.** For other $l$, the torsion group can still be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, even though we have not found any example of the latter. Namely, the proof provided is not valid when $l \equiv 0$ or $3 \pmod 4$, because then we have unconditionally $c_l(k) \equiv 0 \pmod 8$ and thus we cannot eliminate cases (ii) and (iii) in the proof like we did when $l \equiv 1$ or $2 \pmod 4$ and $c_l(k) \equiv 4k \pmod 8$.

**3. Rank of $E_l(k)$.** Beside the points $A'$, $B'$, $C'$, there are also two additional rational points on $E_l(k)'$:

$$\begin{aligned} P' &= \big(0,\ (k^2-1)c_l(k)\big), \\ R' &= \big(s_l(k)t_l(k) + k(s_l(k)+t_l(k)) + 1, \\ &\qquad (s_l(k)+k)(t_l(k)+k)(s_l(k)+t_l(k))\big). \end{aligned}$$

We will prove that $P'$ and $R'$ are independent for all $l \geq 2$, which, together with the fact that torsion group can be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ consequently gives that the rank of $E_l(k)'$ over $\mathbb{Q}$ is greater than or equal to two for all $l \geq 2$.

**Lemma 3.1.** *$P', P'+A', P'+B', P'+C' \notin 2E_l(k)'(\mathbb{Q})$.*

*Proof.* We have:

$$\begin{aligned} x(P') &= 0, \\ x(P'+A') &= c_l(k)^2 - 2kc_l(k), \\ x(P'+B') &= 2k+2-(k+1)c_l(k), \\ x(P'+C') &= -2k+2-(k-1)c_l(k). \end{aligned}$$

If $P' \in 2E_l(k)'(\mathbb{Q})$, then the 2-descent proposition [**10,** Proposition 4.2, page 85] (we will use it through the rest of the paper without mentioning it explicitly) implies that $k^2-1$ is a square, which is impossible. Similarly, if $P'+B' \in 2E_l(k)'(\mathbb{Q})$, then $x(P'+B')+k^2-1 = (k+1)(k+1-c_l(k)) = \square$, and if $P'+C' \in 2E_l(k)'(\mathbb{Q})$, then $x(P'+C')+k^2-1 = (k-1)(k-1-c_l(k)) = \square$. Because of $k \geq 2$ and $c_l(k) \geq c_1(k) = 4k$, both expressions are negative and thus cannot be a square. Finally, if $P'+A' \in 2E_l(k)'(\mathbb{Q})$, then $x(P'+A')+k^2-1 = (c_l(k)-k)^2-1 = \square$, which is impossible as well. □

**Lemma 3.2.** *$R', R'+A', R'+B', R'+C' \notin 2E_l(k)'(\mathbb{Q})$ for $l \geq 2$.*

*Proof.* We have:

$$\begin{aligned} x(R') &= s_l(k)t_l(k) + k(s_l(k) + t_l(k)) + 1, \\ x(R' + A') &= s_l(k)t_l(k) - k(s_l(k) + t_l(k)) + 1, \\ x(R' + B') &= (t_l(k) + k)(t_l(k) - s_l(k)) - (k + 1)c_l(k), \\ x(R' + C') &= (s_l(k) + k)(s_l(k) - t_l(k)) - (k - 1)c_l(k). \end{aligned}$$

If $R' + B' \in 2E_l(k)'(\mathbb{Q})$, then $x(R' + B') + k^2 - 1 = (t_l(k) + k)(k - s_l(k)) = \square$, and if $R' + C' \in 2E_l(k)'(\mathbb{Q})$, then $x(R' + C') + k^2 - 1 = (s_l(k) + k)(k - t_l(k)) = \square$. Because $k \geq 2$, $s_l(k) \geq s_1(k) = 2k - 1$ and $t_l(k) \geq t_1(k) = 2k + 1$, both expressions are negative and thus cannot be a square.

If $R' \in 2E_l(k)'(\mathbb{Q})$, we have the following system of equations:

$$\begin{aligned} (s_l(k) + k)(t_l(k) + k) &= \square, \\ (s_l(k) + t_l(k))(s_l(k) + k) &= \square, \\ (s_l(k) + t_l(k))(t_l(k) + k) &= \square. \end{aligned}$$

Let $d = \gcd(s_l(k)+t_l(k), t_l(k)+k, s_l(k)+k)$. Then, $d \mid t_l(k)+k+s_l(k)+k - (s_l(k) + t_l(k))$, or $d \mid 2k$. If $d \mid k$, then also $d \mid s_l(k)$ and $d \mid t_l(k)$, but from (1.3) and (1.4) we have $c_l(k) = \frac{1}{2}(t_l(k) - s_l(k))(t_l(k) + s_l(k))$, which implies $d \mid c_l(k)$. However, $d \mid c_l(k)$, $d \mid s_l(k)$ and (1.3) give $d = 1$, therefore $d \in \{1, 2\}$. This implies

$$s_l(k) + k = \square, \qquad t_l(k) + k = \square, \qquad s_l(k) + t_l(k) = \square$$

or

$$s_l(k) + k = 2\square, \qquad t_l(k) + k = 2\square, \qquad s_l(k) + t_l(k) = 2\square.$$

Let us define a new sequence $\{a_l(k)\}$ as $s_l(k) + t_l(k) = 2a_{l+1}(k)$. Because of the recurrence relations (1.7) and (1.8), it follows that

$$a_l(k) = 2ka_{l-1}(k) - a_{l-2}(k), \quad a_0(k) = 0, \ a_1(k) = 1.$$

It is easy to prove that the explicit formula of the sequence $\{a_l(k)\}$ is

$$a_l(k) = \frac{(k + \sqrt{k^2 - 1})^l - (k - \sqrt{k^2 - 1})^l}{2\sqrt{k^2 - 1}}. \tag{3.1}$$

$a_l(k)$ is obviously of the form

$$\frac{\alpha^l - \beta^l}{\alpha - \beta},$$

where

$$\alpha = \frac{1}{2}(2k + \sqrt{(2k)^2 - 4})$$

and

$$\beta = \frac{1}{2}(2k - \sqrt{(2k)^2 - 4}).$$

Together with $k \geq 2$, this implies that the sequence $\{a_l(k)\}$ satisfies the conditions of the theorem of Mignotte and Pethő **[13]** and thus $a_l(k) = \square, 2\square, 3\square$ or $6\square$ implies $l < 4$. Cases $l \in \{2, 3\}$ were checked in **[14]**, so we conclude that, if $s_l(k) + t_l(k) = 2\square$ or $s_l(k) + t_l(k) = \square$, then $l = 1$. Otherwise, we have a contradiction and $R' \notin 2E_l(k)'(\mathbb{Q})$.

If $R' + A' \in 2E_l(k)'(\mathbb{Q})$, we have the following system of equations:

$$\begin{aligned}(s_l(k) - k)(t_l(k) - k) &= \square,\\ (s_l(k) + t_l(k))(s_l(k) - k) &= \square,\\ (s_l(k) + t_l(k))(t_l(k) - k) &= \square.\end{aligned}$$

Using the same reasoning, it follows that $s_l(k) + t_l(k) = 2\square$ or $s_l(k) + t_l(k) = \square$, which is only possible for $l = 1$, and thus $R' + A' \notin 2E_l(k)'(\mathbb{Q})$ for $l \geq 2$. □

**Proposition 3.3.** *$t_{2l}(k) - s_{2l}(k) = c_l(k) - c_{l-1}(k) = 2a_{2l}(k)$.*

*Proof.* From (1.5) and (1.6), we find that $t_{2l}(k) - s_{2l}(k)$ equals to:

$$\begin{aligned}&\frac{(k + \sqrt{k^2 - 1})^{2l+1}(2k - 2\sqrt{k^2 - 1})}{2\sqrt{k^2 - 1}}\\ &\qquad + \frac{(k - \sqrt{k^2 - 1})^{2l+1}(-2k - 2\sqrt{k^2 - 1})}{2\sqrt{k^2 - 1}}\\ &\qquad = \frac{(k + \sqrt{k^2 - 1})^{2l} - (k - \sqrt{k^2 - 1})^{2l}}{\sqrt{k^2 - 1}}.\end{aligned}$$

Because of (3.1), this is equal to $2a_{2l}(k)$. On the other hand, from (1.2) we calculate $c_l(k) - c_{l-1}(k)$:

$$\begin{aligned}
&\frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1}}{2(k^2-1)} \\
&\quad - \frac{(k+\sqrt{k^2-1})^{2l-1} - (k-\sqrt{k^2-1})^{2l-1}}{2(k^2-1)} \\
&= \frac{(k+\sqrt{k^2-1})^{2l+1}(1-(k-\sqrt{k^2-1})^2)}{2(k^2-1)} \\
&\quad + \frac{(k-\sqrt{k^2-1})^{2l+1}(1-(k+\sqrt{k^2-1})^2)}{2(k^2-1)} \\
&= \frac{(k+\sqrt{k^2-1})^{2l+1}(k-\sqrt{k^2-1})-(k-\sqrt{k^2-1})^{2l+1}(k+\sqrt{k^2-1})}{\sqrt{k^2-1}} \\
&= \frac{(k+\sqrt{k^2-1})^{2l} - (k-\sqrt{k^2-1})^{2l}}{\sqrt{k^2-1}}. \qquad \square
\end{aligned}$$

**Proposition 3.4.**

$$t_{2l}(k) + k = (k+1)\left(c_l(k) - \frac{c_l(k)+c_{l-1}(k)}{2k} + 1\right).$$

*Proof.* We will calculate

$$-k + (k+1)(c_l(k) - \frac{c_l(k)+c_{l-1}(k)}{2k} + 1) :$$

$$\begin{aligned}
&-k + \frac{k+1}{2k}(c_l(k)(2k-1) - c_{l-1}(k) + 2k) \\
&= \frac{4k-4k^2+(k+\sqrt{k^2-1})^{2l+1}(2k-1-(k-\sqrt{k^2-1})^2)}{4k(k-1)} \\
&\quad + \frac{(k-\sqrt{k^2-1})^{2l+1}(2k-1-(k+\sqrt{k^2-1})^2)}{4k(k-1)} + 1 \\
&= \frac{(k+\sqrt{k^2-1})^{2l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k-1}} \\
&\quad - \frac{(k-\sqrt{k^2-1})^{2l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k-1}} \\
&= t_{2l}(k). \qquad \square
\end{aligned}$$

**Remark 3.5.** Both factors on the right hand side of the equality in Proposition 3.3 are integers. Namely, from the first two elements of $\{c_l(k)\}$ and (2.2) it follows that $c_l(k)$ is divisible by $2k$ for all $k$ and $l$.

Along the same lines as in the proof of Proposition 3.4, we can prove the next three identities:

**Proposition 3.6.**

$$s_{2l}(k) - k = (k-1)\left(c_l(k) + \frac{c_l(k) + c_{l-1}(k)}{2k} - 1\right).$$

**Proposition 3.7.**

$$s_{2l+1}(k) - k = (k-1)\left(\frac{c_{l+1}(k) + c_l(k)}{2k} + c_l(k) - 1\right).$$

**Proposition 3.8.**

$$t_{2l+1}(k) - k = (k+1)\left(\frac{c_{l+1}(k) + c_l(k)}{2k} - c_l(k) - 1\right).$$

From Propositions 3.7 and 3.8, we get:

$$t_{2l+1}(k) - s_{2l+1}(k) = \frac{c_{l+1}(k) + c_l(k)}{k} - 2kc_l(k) - 2, \tag{3.2}$$

$$t_{2l+1}(k) + k = k - 1 + \frac{(k+1)(c_{l+1}(k) + (1-2k)c_l(k))}{2k}, \tag{3.3}$$

$$s_{2l+1}(k) + k = k + 1 + \frac{(k-1)(c_{l+1}(k) + (1+2k)c_l(k))}{2k}. \tag{3.4}$$

To prove Lemma 3.10, we will need three more sequences, $\{d_l(k)\}$, $\{e_l(k)\}$ and $\{f_l(k)\}$, defined as:

$$d_l(k) = \frac{c_l(k)}{k}(k-1) + 1, \tag{3.5}$$

$$e_l(k) = \frac{c_l(k)}{k}(k+1) - 1, \tag{3.6}$$

$$f_l(k) = \frac{c_l(k)}{2k}(k^2 - 1). \tag{3.7}$$

From (2.2), it follows that

$$\begin{aligned} d_{l+2}(k) &= (4k^2-2)d_{l+1}(k) - d_l(k) + 4k - 4k^2, \\ e_{l+2}(k) &= (4k^2-2)e_{l+1}(k) - e_l(k) + 4k + 4k^2, \\ f_{l+2}(k) &= (4k^2-2)f_{l+1}(k) - f_l(k) + 2(k^2-1). \end{aligned} \tag{3.8}$$

Additionally, like the Fibonacci sequence satisfies the famous Cassini identity, there are also four identities that connect two consecutive elements of $\{c_l(k)\}$, $\{d_l(k)\}$, $\{e_l(k)\}$ and $\{f_l(k)\}$:

**Proposition 3.9.**

$$\begin{aligned} d_{l+1}(k)^2 - (4k^2-2)d_{l+1}(k)d_l(k) + d_l(k)^2& \\ + (4k^2-4k)(d_{l+1}(k)+d_l(k)) - 4(k-1)^2 &= 0, \end{aligned}$$

$$\begin{aligned} e_{l+1}(k)^2 - (4k^2-2)e_{l+1}(k)e_l(k) + e_l(k)^2& \\ - (4k^2+4k)(e_{l+1}(k)+e_l(k)) - 4(k+1)^2 &= 0, \end{aligned}$$

$$c_{l+1}(k)^2 - (4k^2-2)c_{l+1}(k)c_l(k) + c_l(k)^2 - 4k(c_{l+1}(k)+c_l(k)) = 0,$$

$$f_{l+1}(k)^2 - (4k^2-2)f_{l+1}(k)f_l(k) + f_l(k)^2 - (2k^2-2)(c_{l+1}(k)+c_l(k)) = 0.$$

*Proof.* We will prove only the first identity with the induction on $l$; the other proofs go analogously. We have:

$$\begin{aligned} d_1(k) &= 4k-3, \\ d_2(k) &= 16k^3 - 16k^2 - 4k + 5. \end{aligned}$$

Thus,

$$d_2(k)^2 - (4k^2-2)d_2(k)d_1(k) + d_1(k)^2 + (4k^2-4k)(d_2(k)+d_1(k)) = 4(k-1)^2,$$

as desired. Suppose $d_{l+1}(k)^2 - (4k^2-2)d_{l+1}(k)d_l(k) + d_l(k)^2 + (4k^2 -$

$4k)(d_{l+1}(k)+d_l(k))=4(k-1)^2$. It follows from (3.8) that

$$\begin{aligned}&d_{l+2}(k)^2-(4k^2-2)d_{l+2}(k)d_{l+1}(k)+d_{l+1}(k)^2\\&\quad+(4k^2-4k)(d_{l+2}(k)+d_{l+1}(k))\\&=((4k^2-2)d_{l+1}(k)-d_l(k)+4k-4k^2)^2+d_{l+1}(k)^2+(4k^2-4k)d_{l+1}(k)\\&\quad+((4k^2-2)d_{l+1}(k)-d_l(k)+4k-4k^2)(4k^2-4k-(4k^2-2)d_{l+1}(k))\\&=4(k-1)^2.\end{aligned}$$ □

**Lemma 3.10.** *$R'+P', R'+P'+A', R'+P'+B', R'+P'+C' \notin 2E_l(k)'(\mathbb{Q})$ for $l\geq 2$.*

*Proof.* $R'+P'\in 2E_l(k)'(\mathbb{Q})$ if and only if $x(R'+P')+k^2-1=\square$, $x(R'+P')+(k+1)c_l(k)=\square$ and $x(R'+P')+(k-1)c_l(k)=\square$. But, with some algebraic manipulation it is not hard to verify that:

$$\begin{aligned}x(R'+P')+k^2-1&=(s_l(k)+k)(t_l(k)+k)(k^2-1)\\&\quad\times\frac{(c_l(k)-t_l(k)-s_l(k))^2}{(s_l(k)t_l(k)+k(s_l(k)+t_l(k))+1)^2},\end{aligned}$$

or, equivalently,

$$x(R'+P')+k^2-1=(s_l(k)+k)(t_l(k)+k)(k^2-1)\square. \tag{3.9}$$

Similarly, we get

$$x(R'+P')+(k+1)c_l(k)=2(k+1)(t_l(k)-s_l(k))(t_l(k)+k)\square, \tag{3.10}$$

$$x(R'+P')+(k-1)c_l(k)=2(k-1)(t_l(k)-s_l(k))(s_l(k)+k)\square. \tag{3.11}$$

(i) $l$ is even. Using Propositions 3.3 and 3.4, we can write (3.10) for even $l$ ($l=2i$) as

$$\begin{aligned}x(R'+P')+(k+1)c_{2i}(k)&=2(c_i(k)-c_{i-1}(k))\\&\quad\times(c_i(k)-\frac{c_i(k)+c_{i-1}(k)}{2k}+1)\square.\end{aligned}\tag{3.12}$$

We will show that the right hand side of (3.12) cannot be a square, which will imply that $R'+P'\notin 2E_l(k)'(\mathbb{Q})$ for all even $l$. Let

$$g=\gcd\left(c_i(k)-c_{i-1}(k), c_i(k)-\frac{c_i(k)+c_{i-1}(k)}{2k}+1\right).$$

It can be proved inductively that $\gcd(t_{2i}(k)+k, 2k) = 1$ and that is equivalent to $\gcd(g, 2k) = 1$. Therefore,

$$g \mid \frac{c_i(k) - c_{i-1}(k)}{2k}, \qquad g \mid c_i(k) - \frac{c_i(k) + c_{i-1}(k)}{2k} + 1,$$

which implies

$$g \mid \frac{c_i(k)}{k}(k-1) + 1, \qquad g \mid \frac{c_{i-1}(k)}{k}(k-1) + 1.$$

With $d_l(k)$ defined in (3.5), it follows that $g \mid d_i(k)$, $g \mid d_{i-1}(k)$. Our next step is to verify that $g = 1$. From Proposition 3.9, $g \mid d_i(k)$ and $g \mid d_{i-1}(k)$, it follows that $g \mid 4(k-1)^2$. Formula (3.5) and the fact that $\gcd(g, 2) = 1$ imply that $g = 1$. Back to (3.10) and (3.12), we now conclude that $t_l(k) - s_l(k) = \square$ or $t_l(k) - s_l(k) = 2\square$, but Proposition 3.3 and the theorem of Mignotte and Pethő **[13]** eliminate that possibility, as in the proof of Lemma 3.2. Hence, $R' + P' \notin 2E_l(k)'(\mathbb{Q})$ for all even $l$.

(ii) $l$ is odd and $k$ is even. We shall prove from (3.10) and (3.11) that $t_l(k) + k$ and $s_l(k) + k$ both have to be squares. Combining that with (3.9) will then require $k^2 - 1$ to be a square, which is a contradiction. Because of (3.3) and (3.4), we can write the formulas (3.10) and (3.11) for odd $l$ ($l = 2i + 1$) as:

$$\begin{aligned} &x(R'+P') + (k+1)c_{2i+1}(k) \\ &\quad = 2(k+1)\left(\frac{c_{i+1}(k) + c_i(k)}{k} - 2kc_i(k) - 2\right) \tag{3.13} \\ &\qquad \times \left(k - 1 + \frac{(k+1)(c_{i+1}(k) + (1-2k)c_i(k))}{2k}\right), \tag{3.14} \end{aligned}$$

$$\begin{aligned} &x(R'+P') + (k-1)c_{2i+1}(k) \\ &\quad = 2(k-1)\left(\frac{c_{i+1}(k) + c_i(k)}{k} - 2kc_i(k) - 2\right) \tag{3.15} \\ &\qquad \times \left(k + 1 + \frac{(k-1)(c_{i+1}(k) + (1+2k)c_i(k))}{2k}\right). \tag{3.16} \end{aligned}$$

It can be inductively verified from the definition of $c_i(k)$ (see (1.2)) that

$$\frac{(k+1)(c_{i+1}(k) + (1-2k)c_i(k))}{2k}$$

is even. Since $k$ is also even, it follows that $t_{2i+1}(k)+k$ is odd. It is obvious that $t_{2i+1}(k)+k \equiv 2 \pmod{k+1}$; hence, $\gcd(t_{2i+1}(k)+k,\ 2(k+1))=1$. Now we prove that $\gcd(t_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k))=1$, as well. Let

$$m=\gcd\Bigg(\frac{c_{i+1}(k)+c_i(k)}{k}-2kc_i(k)-2,\\ k-1+\frac{(k+1)(c_{i+1}(k)+(1-2k)c_i(k))}{2k}\Bigg).$$

Then $\gcd(m,2k)=1$ because $m \mid t_{2i+1}(k)+k$ and $\gcd(t_{2i+1}(k)+k,k)=1$ (the latter follows inductively from the definition of $t_l(k)$). Furthermore,

$$m \mid (k^2-1)c_i(k)+2k,$$

which is equivalent to

$$m \mid \frac{k^2-1}{2k}c_i(k)+1.$$

Similarly, we get

$$m \mid \frac{k^2-1}{2k}c_{i+1}(k)+k^2.$$

Using the definition of $f_l(k)$ (see (3.7)) this implies $m \mid f_l(k)+1$ and $mf_{l+1}(k)+k^2$. Proposition 3.9 further gives that $m \mid (k^2-1)^2$, which is because of the definition of $f_l(k)$ and the fact that $m \mid f_l(k)$ are possible only for $m=1$. With the exact same reasoning we obtain that $\gcd(s_{2i+1}(k)+k,\ 2(k-1))=1$ and $\gcd(s_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k))=1$. Hence, for even $k$, both $t_{2i+1}(k)+k$ and $s_{2i+1}(k)+k$ are squares of integers. From (3.9), it follows that $k^2-1$ needs to be a square as well, which is impossible.

(iii) $l$ and $k$ are odd. Both $t_{2i+1}(k)+k$ and $s_{2i+1}(k)+k$ are now even. Let us denote

$$S=\{\gcd\left(t_{2i+1}(k)+k,\ 2(k+1)\right),\\ \gcd\left(t_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k)\right),\\ \gcd\left(s_{2i+1}(k)+k,\ 2(k-1)\right),\\ \gcd\left(s_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k)\right)\}.$$

Based on previous observations, we conclude that all elements of $S$ have to be powers of 2. Depending on $k$ and $i$, we get the following from (2.11), (2.12), (3.2), (3.3) and (3.4):

| $k$ | $t_{2i+1}(k) - s_{2i+1}(k)$ | $t_{2i+1}(k) + k$ | $s_{2i+1}(k) + k$ |
|---|---|---|---|
| 1 | 2 | 4 | 2 |
| 3 | 2 | 2 | 0 |
| 5 | 2 | 0 | 6 |
| 7 | 2 | 6 | 4 |

TABLE 1. Remainders modulo 8 for $i \equiv 0$ or $2 \pmod 4$

| $k$ | $t_{2i+1}(k) - s_{2i+1}(k)$ | $t_{2i+1}(k) + k$ | $s_{2i+1}(k) + k$ |
|---|---|---|---|
| 1 | 6 | 0 | 2 |
| 3 | 6 | 2 | 4 |
| 5 | 6 | 4 | 6 |
| 7 | 6 | 6 | 0 |

TABLE 2. Remainders modulo 8 for $i \equiv 1$ or $3 \pmod 4$

From Tables 1 and 2 it follows that $S = \{2, 4, 8\}$. Because the right hand sides of both (3.14) and (3.16) have to be squares, this implies that either $t_{2i+1}(k) + k = 2\square$ and $s_{2i+1}(k) + k = 2\square$ or $t_{2i+1}(k) + k = 2\square$ and $s_{2i+1}(k) + k = \square$ (and vice versa). If $t_{2i+1}(k) + k = 2\square$ and $s_{2i+1}(k) + k = 2\square$, then $k^2 - 1 = \square$ because the right hand side of (3.9) needs to be a square, and that is impossible. On the other hand, if $t_{2i+1}(k) + k = 2\square$ and $s_{2i+1}(k) + k = \square$ (or vice versa), then $k^2 - 1 = 2\square$ and that is possible if and only if $k - 1 = \square$, $k + 1 = 2\square$ or $k - 1 = 2\square$, $k + 1 = \square$. Putting that back in (3.10) and (3.11) gives that $t_l(k) - s_l(k) = \square$ or $t_l(k) - s_l(k) = 2\square$ for odd $l$. Because $t_l(k) - s_l(k) = 2a_l(k)$ (it can be proved as in the proof of Proposition 3.3) this leads to $a_l(k) = \square$ or $a_l(k) = 2\square$, which is again eliminated by the theorem of Mignotte and Pethő **[13]**. Thus, $R' + P' \notin 2E_l(k)'(\mathbb{Q})$ for all $l \geq 2$.

Next, we have

$$\begin{aligned} &x(R'+P'+A')+(k^2-1) \\ &\quad =(k^2-1)(t_l(k)-k)(s_l(k)-k)\square, \end{aligned} \tag{3.17}$$

$$x(R'+P'+A')+(k+1)c_l(k)=2(k+1)(t_l(k)-s_l(k))(t_l(k)-k)\square, \tag{3.18}$$

$$x(R'+P'+A')+(k-1)c_l(k)=2(k-1)(t_l(k)-s_l(k))(s_l(k)-k)\square. \tag{3.19}$$

$R'+P'+A' \in 2E_l(k)'(\mathbb{Q})$ if and only if all the right hand sides of this system of equations are squares. Again, we will have separate strategies depending on parity of $l$.

(i) $l$ is even. Propositions 3.3 and 3.6 imply that (3.19) for even $l$ ($l=2i$) becomes:

$$x(R'+P'+A')+(k-1)c_{2i}(k)$$

$$=2(c_i(k)-c_{i-1}(k)) \tag{3.20}$$

$$\times\left(c_i(k)+\frac{c_i(k)+c_{i-1}(k)}{2k}-1\right)\square. \tag{3.21}$$

Following exactly the same steps as in the proof of $R'+P' \notin 2E_l(k)'(\mathbb{Q})$ for even $l$, let

$$h=\gcd\left(c_i(k)-c_{i-1}(k),\ c_i(k)+\frac{c_i(k)+c_{i-1}(k)}{2k}-1\right).$$

Then

$$h \mid \frac{c_i(k)}{k}(k+1)-1,\ h \mid \frac{c_{i-1}(k)}{k}(k+1)-1.$$

With $e_l(k)$ defined in (3.6), it follows that $h \mid e_i(k)$ and $h \mid e_{i-1}(k)$. Proposition 3.9 implies $h \mid 4(k+1)^2$, and that is impossible from the definition of $e_i(k)$ and because all of $e_i(k)$ are odd. Hence, $h=1$ and consequently $t_l(k)-s_l(k)=\square$ or $t_l(k)-s_l(k)=2\square$, which we have already shown is not possible.

(ii) $l$ is odd. From Propositions 3.7 and 3.8, equation (3.17) for odd $l$ ($l = 2i+1$) becomes:

$$\begin{aligned} &x(R' + P' + A') + (k^2 - 1) \\ &\quad = \left(\frac{c_{i+1}(k) + (1-2k)c_i(k) - 2k}{2k}\right) \\ &\quad\quad \times \left(\frac{c_{i+1}(k) + (1+2k)c_i(k) - 2k}{2k}\right)\square. \end{aligned}$$

Let

$$\begin{aligned} n = \gcd\Bigg(&\frac{c_{i+1}(k) + (1-2k)c_i(k) - 2k}{2k}, \\ &\qquad \frac{c_{i+1}(k) + (1+2k)c_i(k) - 2k}{2k}\Bigg). \end{aligned}$$

It is easy to verify from the definition of $c_l(k)$ that

$$2k \mid \frac{c_{i+1}(k) + (1-2k)c_i(k)}{2k}, \; 2k \mid \frac{c_{i+1}(k) + (1+2k)c_i(k)}{2k}.$$

Thus, we conclude that $n$ and $2k$ are coprime. Furthermore, $n \mid c_{i+1}(k) + c_i(k) - 2k$ and $n \mid 2c_i(k)$, and because $n$ is odd it follows that $n \mid c_i(k)$. Moreover, we have $n \mid c_{i+1}(k) - 2k$. Because of $n \mid c_i(k)$ and Proposition 3.9 it follows that $n \mid c_{i+1}(k)(c_{i+1}(k) - 4k)$, so we conclude that $n \mid 4k^2$ and that is impossible for $n > 1$ since $n$ and $2k$ are coprime. Therefore,

$$\frac{c_{i+1}(k) + (1-2k)c_i(k) - 2k}{2k}$$

and

$$\frac{c_{i+1}(k) + (1+2k)c_i(k) - 2k}{2k}$$

are coprime, so they must be squares of integers. Again, from

Propositions 3.7 and 3.8, the equations (3.18) and (3.19) become:

$$\begin{aligned}&x(R'+P'+A')+(k+1)c_{2i+1}(k)\\&\quad=2(t_{2i+1}(k)-s_{2i+1}(k))\\&\quad\quad\times\left(\frac{c_{i+1}(k)+(1-2k)c_i(k)-2k}{2k}\right)\square,\\&x(R'+P'+A')+(k-1)c_{2i+1}(k)\\&\quad=2(t_{2i+1}(k)-s_{2i+1}(k))\\&\quad\quad\times\left(\frac{c_{i+1}(k)+(1+2k)c_i(k)-2k}{2k}\right)\square.\end{aligned}$$

We conclude that, for odd $l$, $t_l(k)-s_l(k)=2\square$, which implies that $a_l(k)=\square$ and that is impossible for $l\geq 2$ by a theorem of Mignotte and Pethő **[13]**. Thus, $R'+P'+A'\notin 2E_l(k)'(\mathbb{Q})$ for all $l\geq 2$.

Finally, we have

$$x(R'+P'+B')+(k^2-1)=(k^2-1)(t_l(k)+k)(k-s_l(k))\square, \tag{3.22}$$

$$x(R'+P'+B')+(k+1)c_l(k)=2(k+1)(t_l(k)+s_l(k))(t_l(k)+k)\square, \tag{3.23}$$

$$x(R'+P'+B')+(k-1)c_l(k)=2(k-1)(t_l(k)+s_l(k))(k-s_l(k))\square. \tag{3.24}$$

and

$$x(R'+P'+C')+(k^2-1)=(k^2-1)(s_l(k)+k)(k-t_l(k))\square, \tag{3.25}$$

$$x(R'+P'+C')+(k+1)c_l(k)=2(k+1)(t_l(k)+s_l(k))(t_l(k)-k)\square, \tag{3.26}$$

$$x(R'+P'+C')+(k-1)c_l(k)=2(k-1)(t_l(k)+s_l(k))(s_l(k)+k)\square. \tag{3.27}$$

The right hand sides of (3.22) and (3.25) are negative and cannot be squares; therefore, $R'+P'+B'\notin 2E_l(k)'(\mathbb{Q})$ and $R'+P'+C'\notin 2E_l(k)'(\mathbb{Q})$. □

**Theorem 3.11.** *The rank of $E_l(k)'$ over $\mathbb{Q}$ is greater than or equal to two for all $l\geq 2$.*

*Proof.* We will prove that $P'$ and $R'$ generate a subgroup of rank 2 in $E_l(k)'(\mathbb{Q})/E_l(k)'(\mathbb{Q})_{\text{tors}}$ for all $l \geq 2$. Assume the opposite. Then $aP' + bR' \in E_l(k)'(\mathbb{Q})_{\text{tors}}$ implies that $a$ and $b$ are not both zero. We know that $E_l(k)'(\mathbb{Q})_{\text{tors}}$ is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Let us first consider the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $E_l(k)'(\mathbb{Q})_{\text{tors}} = \{A', B', C', \mathcal{O}\}$. Let $aP' + bR' = T' \in E_l(k)'(\mathbb{Q})_{\text{tors}}$. If $a$ and $b$ are not both even, then we have one of the following cases: $P' + T' \in 2E_l(k)'(\mathbb{Q})$, $R' + T' \in 2E_l(k)'(\mathbb{Q})$, $P' + R' + T' \in 2E_l(k)'(\mathbb{Q})$. Neither of these cases is possible because of Lemmas 3.1, 3.2 and 3.10. Thus, both $a$ and $b$ have to be even: $a = 2a_1, b = 2b_1$ and $2a_1P' + 2b_1R' \in E_l(k)'(\mathbb{Q})_{\text{tors}}$. Because all $A', B', C'$ have the order two and thus cannot have the form $2T'$, and $E_l(k)'(\mathbb{Q})_{\text{tors}} = \{A', B', C', \mathcal{O}\}$, it follows that $2a_1P' + 2b_1R' = \mathcal{O}$, so $a_1P' + b_1R' \in E_l(k)'(\mathbb{Q})_{\text{tors}}$. Hence, the method of infinite descent gives us $a = b = 0$, a contradiction.

The case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ can be handled in the same way as the previous case, due to the fact that any torsion point $T'$ satisfies $T' \equiv \mathcal{O}, A', B'$ or $C' \pmod{2E_l(k)'(\mathbb{Q})}$. □

**Acknowledgments.** I would like to thank Professor Andrej Dujella and Professor Filip Najman for many valuable suggestions and advice during the preparation of this paper. I would also like to thank the referee for many helpful comments and suggestions that improved the previous version of the paper.

## REFERENCES

**1**. Y. Bugeaud, A. Dujella and M. Mignotte, *On the family of Diophantine triples* $\{k-1, k+1, 16k^3-4k\}$, Glasgow Math. J. **49** (2007), 333–344.

**2**. L.E. Dickson, *A history of the theory of numbers*, Volume 2, Chelsea, New York, 1966.

**3**. A. Dujella, *There are only finitely many Diophantine quintuples*, J. reine angew. Math. **566** (2004), 183–214.

**4**. ______, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.

**5**. ______, *Diophantine m-tuples and elliptic curves*, J. Th. Nomb. Bord. **13** (2001), 111–124.

**6**. A. Dujella and M. Mikić, *On the torsion group of elliptic curves induced by* $D(4)$*-triples*, An. Stiint. Univ. "Ovidius" Constanta Mat. **22** (2014), 79–90.

**7**. A. Dujella and J.C. Peral, *High rank elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *induced by Diophantine triples*, LMS J. Comp. Math. **17** (2014), 282–288.

**8**. A. Dujella and A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debr. **56** (2000), 321–335.

**9**. Y. Fujita, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, J. Num. Theor. **128** (2008), 322–353.

**10**. A. Knapp, *Elliptic curves*, Princeton University Press, Princeton, 1992.

**11**. S. Kwon, *Torsion subgroups of elliptic curves over quadratic extensions*, J. Num. Theor. **62** (1997), 144–162.

**12**. B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

**13**. M. Mignotte and A. Pethő, *Sur les carres dans certaines suites de Lucas*, J. Th. Nomb. Bord. **5** (1993), 333–341.

**14**. F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debr. **75** (2009), 401–418.

**15**. K. Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), 101–123.

**16**. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

Kumičićeva 20, 51000 Rijeka, Croatia
**Email address**: **miljen.mikic@gmail.com**