On the torsion group of elliptic curves induced by $D(4)$-triples

Andrej Dujella and Miljen Mikić

Abstract

A $D(4)$-m-tuple is a set of $m$ integers such that the product of any two of them increased by 4 is a perfect square. A problem of extendibility of $D(4)$-m-tuples is closely connected with the properties of elliptic curves associated with them. In this paper we prove that the torsion group of an elliptic curve associated with a $D(4)$-triple can be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, except for the $D(4)$-triple $\{-1, 3, 4\}$ when the torsion group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Keywords: $D(4)$-triples, elliptic curves, torsion group
Mathematics Subject Classification: (2010) 11G05

1 Introduction

Let $n$ be a given nonzero integer. A set of $m$ nonzero integers $\{a_1, a_2, \ldots, a_m\}$ is called a $D(n)$-m-tuple (or a Diophantine m-tuple with the property $D(n)$) if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Diophantus found the $D(256)$-quadruple $\{1, 33, 68, 105\}$, while the first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat (see [1], [2]).

One of the most interesting questions in the study of $D(n)$-m-tuples is how large these sets can be. In this paper we will examine sets with the property $D(4)$. Mohanty and Ramasamy [17] were first to achieve a significant result on the nonextendibility of $D(4)$-m-tuples. They proved that a $D(4)$-quadruple $\{1, 5, 12, 96\}$ cannot be extended to a $D(4)$-quintuple. Kedlaya [14] later proved that if $\{1, 5, 12, d\}$ is a $D(4)$-quadruple, then $d$ has to be 96. Dujella and Ramasamy [9] generalized this result to the parametric family of $D(4)$-quadruples $\{F_{2k}, 5F_{2k}, 4F_{2k+2}, 4L_{2k}F_{4k+2}\}$ involving Fibonacci and Lucas numbers. Other generalization to a two-parametric family of $D(4)$-triples can be found in [13]. Dujella [6] proved that there does not exist a
\[
D(1)\text{-sextuple and that there are only finitely many } D(1)\text{-quintuples. By observing congruences modulo 8, it is not hard to conclude that a } D(4)\text{-m-tuple can contain at most two odd numbers (see [9, Lemma 1]). Thus, the results from [6] imply that there does not exist a } D(4)\text{-8-tuple and that there are only finitely many } D(4)\text{-7-tuples. Filipin [10, 11] significantly improved these results by proving that there does not exist a } D(4)\text{-sextuple and that there are only finitely many } D(4)\text{-quintuples.}
\]

Let \( \{a, b, c\} \) be a \( D(4)\)-triple. Then there exist nonnegative integers \( r, s, t \) such that
\[
ab + 4 = r^2, \quad ac + 4 = s^2, \quad bc + 4 = t^2.
\]
In order to extend this triple to a quadruple, we have to solve the system
\[
ax + 4 = \Box, \quad bx + 4 = \Box, \quad cx + 4 = \Box.
\]
We assign to the system (2) the elliptic curve
\[
E : y^2 = (ax + 4)(bx + 4)(cx + 4).
\]
The purpose of this paper is to examine possible forms of torsion groups of elliptic curves obtained in this manner. Additional motivation for this paper is a gap found in the proof of [4, Lemma 1] concerning torsion groups of elliptic curves induced by \( D(1)\)-triples. Namely, if \( \{a', b', c'\} \) is a \( D(1)\)-triple, then \( \{2a', 2b', 2c'\} \) is a \( D(4)\)-triple. Thus, the proof of Lemma 2 in present paper also provides a valid proof of [4, Lemma 1].

### 2 Torsion group of \( E \)

The coordinate transformation
\[
x \mapsto \frac{x}{abc}, \quad y \mapsto \frac{y}{abc}
\]
applied on the curve \( E \) leads to the elliptic curve
\[
E' : y^2 = (x + 4bc)(x + 4ac)(x + 4ab).
\]
There are three rational points on \( E' \) of order 2:
\[
A' = (-4bc, 0), \quad B' = (-4ac, 0), \quad C' = (-4ab, 0),
\]
and also other obvious rational points
\[
P' = (0, 8abc), \quad S' = (16, 8rst).
\]
It is not so obvious, but it is easy to verify that $S' \in 2E'(\mathbb{Q})$. Namely, $S' = 2R'$, where
\[ R' = (4rs + 4rt + 4st + 16(r + s)(r + t)(s + t)). \]

In this section we will first examine one special case and after that we may assume without the loss of generality that $a, b, c$ are positive integers such that $a < b < c$. Since $\{-a, -b, -c\}$ induces the same curve as $\{a, b, c\}$, a problem may arise only when there are mixed signs. It is easily seen that the only such possible $D(4)$-triple is $\{-1, 3, 4\}$ (and the equivalent one $\{-4, -3, 1\}$). The elliptic curve associated with this $D(4)$-triple has rank 0 and the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In this special case $B' \in 2E'(\mathbb{Q})$, more precisely $B' = 2P'$, so the point $P'$ is of order 4. Note that in this case the point $R'$ is also of order 4 since $R' = P' + A'$ and thus $2R' = 2P'$.

Thus, we assume from now on that $a, b, c$ are positive integers such that $a < b < c$.

**Lemma 1.** If $\{a, b, c\}$ is $D(4)$-triple, then $c = a + b + 2r$ or $c > ab + a + b + 1 > ab$.

**Proof.** By [5, Lemma 3], there exists an integer
\[ e = 4(a + b + c) + 2(abc - r st) \]  \hspace{1cm} (4)
and nonnegative integers $x, y, z$ such that
\[ ae + 16 = x^2, \] \hspace{1cm} (5)
\[ be + 16 = y^2, \] \hspace{1cm} (6)
\[ ce + 16 = z^2 \] \hspace{1cm} (7)
and $c = a + b + \frac{r}{4} + \frac{1}{8}(abe + rxy)$. From (7), it follows that $e \geq 0$ (the case $e = -1$ implies $c \leq 16$, but the only such $D(4)$-triple $\{1, 5, 12\}$ does not satisfy (5) and (6)). For $e = 0$ we get $c = a + b + 2r$, while for $e \geq 1$ we have $c > \frac{1}{4}abe + a + b + \frac{e}{8}$. By observing congruences modulo 8, we can easily prove that at most two of the integers $a, b, c$ are odd, which implies that $abc - r st$ is even. Hence, from (4) we conclude that $e \equiv 0 \pmod{4}$. It follows $e \geq 4$ and thus $c > ab + a + b + 1$.

**Remark 1.** Filipin (see [12, Lemma 4]) proved that $c = a + b + 2r$ or $c > \frac{1}{4}abe$. Lemma 1 may be considered as a slight improvement of that result.
Remark 2. Lemma 1 implies $c \geq a + b + 2r$. Indeed, the inequality $ab + a + b + 1 \geq a + b + 2r$ is equivalent to $(r - 3)(r + 1) \geq 0$, and this is satisfied for all $D(4)$-triples with positive elements.

Remark 3. The statement of Lemma 1 is sharp in the sense that the inequality $c > ab$ cannot be replaced by $c > (1 + \varepsilon)ab$ for any fixed $\varepsilon > 0$. Indeed, for an integer $k \geq 3$, if we put $a = k^2 - 4, b = k^2 + 2k - 3, c = k^4 + 2k^3 - 3k^2 - 4k$, then $\{a, b, c\}$ is a $D(4)$-triple and $\lim_{k \to \infty} \frac{c}{ab} = 1$.

In the next lemma we show that $E'$ cannot have a point of order 4. We follow the strategy of the proof of an analogous result for $D(1)$-triples [4, Lemma 1]. However, we have noted a serious gap in the proof of [4, Lemma 1]. Namely, [4, formula (7)] should be $(\beta^2 - 1)^2 = b(4c\beta^2 - a^2b - 2a(1 + \beta^2))$, instead of $(\beta^2 - 1)^2 = b(4c - a^2b - 2a(1 + \beta^2))$, so later arguments are not accurate in the case $\beta \neq 1$. Here we will prove more general result, but by taking $a, b, c$ to be even, in the same time we fill the mentioned gap in the proof of [4, Lemma 1].

Lemma 2. $A', B', C' \notin 2E'(Q)$

Proof. If $A' \in 2E'(Q)$, then the 2-descent Proposition [15, 4.2, p.85] implies that $c(a - b)$ is a square. But $c(a - b) < 0$, a contradiction. Similarly, $B' \notin 2E'(Q)$. If $C' \in 2E'(Q)$, then
\begin{align*}
a(c - b) &= X^2, \\
b(c - a) &= Y^2,
\end{align*}
for integers $X$ and $Y$.

If $\{a, b, c\}$ is a $D(4)$-triple where $a < b < c$, then $c = a + b + 2r$ or $c > ab + a + b + 1$ by Lemma 1.

Assume first that $c = a + b + 2r$. From (8) and (9), we get that $a = kx^2, c - b = ky^2, b = lx^2, c - a = lu^2$, where $k, l, x, y, z, u$ are positive integers.

We have $c = kx^2 + lu^2 = ky^2 + lz^2$, and from $c = a + b + 2r$ we get
\begin{equation}
2r = k(y^2 - x^2) = l(u^2 - z^2).
\end{equation}

By squaring (10), we obtain
\begin{equation*}
4r^2 = 16 + 4ab = 16 + 4kx^2z^2 = k^2(y^2 - x^2)^2 = l^2(u^2 - z^2)^2,
\end{equation*}
which implies that $k \in \{1, 2, 4\}$ and $l \in \{1, 2, 4\}$. Since $kl$ is not a perfect square (otherwise $(2r)^2 = 16 + (2xz\sqrt{kl})^2$ which implies $2r = 5$), we may
take without loss of generality \( k = 1, \ l = 2 \) or \( k = 2, \ l = 4 \). For \( k = 1, \ l = 2 \), we have \( 4r^2 = 16 + 8x^2z^2 \), which implies \( r^2 = 4 + 2x^2z^2 \), which leads to the conclusion that \( r \) is even and \( xz \) is even. Therefore, \( r^2 \equiv 4 \pmod{8} \) and \( r \equiv 2 \pmod{4} \). But from \( 2r = 2(u^2 - z^2) \) we conclude \( u^2 - z^2 \equiv 2 \pmod{4} \), and that is impossible. If \( k = 2, \ l = 4 \), then \( 4r^2 = 16 + 32x^2z^2 \), which implies \( r^2 = 4 + 8x^2z^2 \), thus \( r^2 \equiv 4 \pmod{8} \) and \( r \equiv 2 \pmod{4} \). But from \( 2r = 2(y^2 - x^2) \) we conclude \( y^2 - x^2 \equiv 2 \pmod{4} \), and that is impossible.

Assume now that \( c > ab + a + b + 1 > ab \).

Let us write the conditions (8) and (9) in the form

\[
\begin{align*}
ac - ab &= s^2 - r^2 = (s - \alpha)^2, \\
b\sqrt{c} - ab &= t^2 - r^2 = (t - \beta)^2,
\end{align*}
\]

where \( 0 < \alpha < s \), \( 0 < \beta < t \). Then we have

\[
r^2 = 2s\alpha - \alpha^2 = 2t\beta - \beta^2.
\]

From (13) we get

\[
4(bc + 4)\beta^2 = (ab + 4 + \beta^2)^2
\]

and

\[
(\beta^2 - 4)^2 = b(4c\beta^2 - a^2b - 2a(4 + \beta^2)).
\]

From (14) we conclude that either \( \beta = 1 \) or \( \beta = 2 \) or \( \beta^2 \geq \sqrt{b} + 4 \).

If \( \beta = 1 \), then

\[
b(4c - a^2b - 10a) = 9
\]

which implies \( b \mid 9 \), but that is possible only for \( b = 9 \) (there are no \( D(4) \)-triplies with \( b < 4 \)). This implies \( a = 5 \), but (15) then gives \( c = 69 \) and \( \{5, 9, 69\} \) is not a \( D(4) \)-triple.

If \( \beta = 2 \), then from (14) we find that

\[
c = \frac{a^2b + 16a}{16}.
\]

Now we have

\[
s^2 = ac + 4 = \frac{1}{16}(a^3b + 16a^2 + 64) = \frac{1}{16}(a^2r^2 + 12a^2 + 64).
\]

Hence \( s^2 > \left( \frac{2r}{a} \right)^2 \) and \( s^2 < \left( \frac{ar + 8}{4} \right)^2 \). Therefore we have to consider several cases:
1. \( s^2 = (\frac{ar+n}{4})^2 \), where \( n \) is odd. That is equivalent to

\[ 2a(rn - 6a) = 64 - n^2. \] (17)

The left hand side of (17) is even and the right hand side is odd, a contradiction.

2. \( s^2 = (\frac{ar+2}{4})^2 \), or equivalently \( a(r - 3a) = 15 \). The cases \( a \leq 3 \) and (16) imply that \( c < b \). The case \( a = 5 \) gives the triple \( \{5, 64, 105\} \) that does not satisfy \( c > ab \) (\( c \) equals \( a + b + 2r \)), and \( a = 15 \) leads to \( 15b + 4 = 46^2 \) which has no integer solutions.

3. \( s^2 = (\frac{ar+4}{4})^2 \), or equivalently \( a(2r - 3a) = 12 \). We conclude that \( a \) must be even and we get triples: \( \{2, 16, 6\} \) (with \( c < b \)) and \( \{6, 16, 42\} \) (with \( c = a + b + 2r \)), so we can eliminate this case.

4. \( s^2 = (\frac{ar+6}{4})^2 \) is equivalent to \( 3a(r-a) = 7 \), which is clearly impossible.

Thus, we may assume that \( \beta^2 \geq \sqrt{b} + 4 \), which implies

\[ \beta > \max\{\sqrt{b}, 2\} \] (18)

The function \( f(\beta) = t^2 - (t - \beta)^2 \) is increasing for \( 0 < \beta < t \). Thus we have

\[ ab = t^2 - (t - \beta)^2 - 4 > 2t \sqrt{b} - \sqrt{b} - 4 > 2\sqrt{bc} \sqrt{b} - \sqrt{b} - 4, \]

which implies \( ab > \sqrt{bc} \sqrt{b} \), because \( \sqrt{b}(\sqrt{c} \sqrt{b} - 1) > 4 \) (since \( b \geq 4 \) and \( c \geq 12 \), which follows from the fact that \( \{3, 4, 15\} \) and \( \{1, 5, 12\} \) are \( D(4) \)-triples with smallest \( b \) and \( c \) respectively). This further gives

\[ c < a^2 \sqrt{b}. \] (19)

We will use (4) to define the integer \( d_- \) as

\[ d_- = \frac{e}{4} = a + b + c + \frac{abc - rst}{2} \]

Then \( d_- \neq 0 \) (since \( c \neq a + b + 2r \)) and \( \{a, b, c, d_-\} \) is a \( D(4) \)-quadruple. In particular,

\[ ad_- + 4 = \left( \frac{rs - at}{2} \right)^2. \] (20)

Moreover,

\[ c = a + b + d_- + \frac{1}{2}(abd_- + \sqrt{(ab + 4)(ad_- + 4)(bd_- + 4)}) > abd_- \] (21)
(see the proof of Lemma 1). By comparing this with (19), we get
\begin{equation}
    d_- < \frac{a}{\sqrt{b}}.
\end{equation}
Therefore, we have \(d_- < a < b\) which implies that \(b\) is the largest element in the \(D(4)\)-triple \(\{a, b, d_-\}\). Thus, by Remark 2, \(b \geq a + d_- + 2\sqrt{ad_- + 4}\) or equivalently \(d_- \leq a + b - 2r\). Let us define also
\[
c' = a + b + d_- + \frac{1}{2}(abd_- - \sqrt{(ab + 4)(ad_- + 4)(bd_- + 4)}).
\]
We have
\[
cc' = (a + b + d_- + \frac{1}{2}abd_-)^2 - \frac{1}{4}(ab + 4)(ad_- + 4)(bd_- + 4)
\]
\[
= (a + b + d_-)^2 - 4ab - 4ad_- - 4bd_- - 16
\]
\[
= (a + b - d_-)^2 - 4r^2 = (a + b + 2r - d_-)(a + b - 2r - d_-) \geq 0.
\]
This implies
\begin{equation}
    c < 2(a + b + d_- + \frac{1}{2}abd_-) < 4b + abd_- < 2abd_-.
\end{equation}
(we use here \(ad_- > 4\) which is true because \(\{a, d_-\}\) is a \(D(4)\)-pair). Let us denote \(p = \frac{rs - at}{2}\). Then \(p > 0\) and, by (20), we have \(ad_- + 4 = p^2\). In order to estimate the size of \(p\), we also define \(p' = \frac{rs + at}{2}\). Then
\[
pp' = \frac{1}{4}(a^2bc + 4ac + 4ab + 16 - a^2bc - 4a^2) = a(b + c - a) + 4,
\]
and
\[
p < \frac{2(a(c + b)}{2at} < \frac{c + b}{\sqrt{bc}} = \frac{\sqrt{c}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{c}},
\]
\[
p > \frac{2(ac + 4)}{2rs} = \frac{s}{r}.
\]
Furthermore, we have
\[
\frac{\sqrt{c}}{\sqrt{b}} - \frac{s}{r} = r\sqrt{c} - s\sqrt{b} = \frac{4c - 4b}{r\sqrt{b}(r\sqrt{c} + s\sqrt{b})} < \frac{4c}{2rsb} < \frac{2\sqrt{c}}{ab\sqrt{b}},
\]
and thus
\begin{equation}
    p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{2\sqrt{c}}{ab\sqrt{b}}.
\end{equation}
The inequality (19) implies that \( c < \frac{ab^2}{2} \), and this is equivalent to

\[
\frac{\sqrt{b}}{\sqrt{c}} \geq \frac{2\sqrt{c}}{ab\sqrt{b}}
\]

which gives

\[
p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{\sqrt{b}}{\sqrt{c}}.
\]

By comparing both estimates for \( p \), we get

\[
\left| p - \frac{\sqrt{c}}{\sqrt{b}} \right| < \frac{\sqrt{b}}{\sqrt{c}}.
\]  

Let us now define an integer \( \alpha \) by

\[
2d_\beta - \beta = p + \alpha.
\]

Assume that \( \alpha = 0 \). Then (20) implies that \( d_\beta - (4\beta^2d_\beta - a) = 4 \), thus \( d_\beta \in \{1, 2, 4\} \). We have three cases:

1. \( d_\beta = 1 \), which implies \( 2\beta = p \). With this assumption, (12) gives

\[
r^2 + \frac{p^2}{4} = tp,
\]

while \( c \) satisfies the inequalities

\[
ab < ab + a + b + 1 < c < ab + 2a + 2b + 2 < ab + 4b < 2ab
\]

(see Lemma 1 and (23) with \( d_\beta = 1 \)). The left hand side of (27) is

\[
< ab + 4 + \frac{c^2 + 2bc + b^2}{4bc} = ab + 4 + \frac{a}{4} + 1 + \frac{1}{2} + \frac{1}{4a} < ab + \frac{a}{4} + 6.
\]

On the other hand, by (24), the right hand side of (27) is

\[
> \sqrt{bc} \left( \frac{\sqrt{c}}{\sqrt{b}} - \frac{2\sqrt{c}}{ab\sqrt{b}} \right) = c - \frac{2c}{ab} > ab + a + b + 1 - 4 = ab + a + b - 3.
\]

By comparing these two estimates for (27), we get

\[
b + \frac{3}{4}a < 9,
\]

but this is in contradiction with \( b \geq 12 \) (\( b \) is the largest element in the \( D(4) \)-triple \( \{d_\beta, a, b\} \)).

We treat similarly the other two cases.
2. $d_- = 2$, which implies $4\beta = p$, and this leads to
\[
\frac{b}{2} + \frac{3}{8}a < 8,
\]
which is in contradiction with $b \geq 16$ ($D(4)$-triple of the form $\{2, a, b\}$ with the smallest $b$ is $\{2, 6, 16\}$).

3. $d_- = 4$ is equivalent to $8\beta = p$, which leads to
\[
\frac{b}{4} + \frac{3}{16}a < 8,
\]
but the only $D(4)$-triple of the form $\{4, a, b\}$ with $b < 35$ is $\{4, 8, 24\}$, which does not satisfy (22), so we have a contradiction here as well.

Therefore, we may now assume that $\alpha \neq 0$. We will estimate $2d_\gamma t\beta$ and compare it with $c$. First we will prove
\[
\beta^2 < \frac{a^2b}{c}. \tag{28}
\]
Since $\beta < t$, and the case $\beta = t - 1$ gives $b(c - a) = 1$, which is impossible, we conclude that $t \geq \beta + 2$. This implies $t\beta \geq \beta^2 + 2\beta$, and $ab - t\beta \geq 2\beta - 4 > 0$ because of (18). Hence, we get $t\beta < ab$, and this clearly implies (28).

Therefore,
\[
0 < d_- \beta^2 < \frac{d_- a^2b}{c} < a.
\]
From $2t\beta = r^2 + \beta^2 > ab + 4$, we get $2d_-t\beta > abd_- + 4d_-$. On the other hand,
\[
d_- \beta^2 < \frac{d_- a^2b}{c} \iff 2d_-t\beta < abd_- + 4d_- + \frac{d_- a^2b}{c} < abd_- + 4d_- + a.
\]
By combining these two estimates, we get
\[
abd_- + 4d_- < 2d_-t\beta < abd_- + 4d_- + a. \tag{29}
\]
By comparing (29) with (21) and (23), we conclude that
\[
|2d_-t\beta - c| < 4b. \tag{30}
\]
By combining the estimate (26) for $p$ with the trivial estimate for $\alpha$, namely $|\alpha| \geq 1$, we get
\[
\left|2d_-\beta - \sqrt{c}\right| = \left|p + \alpha - \sqrt{c}\right| \geq 1 - \frac{\sqrt{b}}{\sqrt{c}}.
\]
Note that \( ad_\geq 26 \). Namely, only \( D(4) \)-pairs such that \( ad_\leq 26 \) are \( \{1, 5\}, \{1, 12\}, \{1, 21\}, \{2, 6\}, \{3, 4\} \) and \( \{3, 7\} \). From first three pairs, respecting (21) and (22), we find triples

\[
\{1, 5, 96\}, \{1, 12, 320\}, \{1, 21, 1365\}, \{2, 6, 780\}, \{2, 12, 7392\}
\]

that do not satisfy (8) nor (9). From the last three pairs we cannot obtain a \( D(4) \)-triple because of (22).

Finally, we obtain

\[
|2d_\cdot t\beta - c| = |2d_\cdot t\beta - t\sqrt{\frac{c}{b}} + t\sqrt{\frac{a_2}{b}} - c| \geq \frac{t}{\sqrt{c}} \left| 2d_\cdot \beta - \sqrt{\frac{c}{b}} - \frac{t}{\sqrt{c}} \right| \geq \frac{t}{\sqrt{c}} \left( 1 - \sqrt{\frac{c}{b}} \right) > b(\sqrt{ad_\geq} - 1 - \frac{1}{\sqrt{2}}) > 4b
\]

which contradicts (30).

**Theorem 3.** \( E'(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \).

**Proof.** By Mazur’s theorem [16] which characterizes all possible torsion groups for elliptic curves over \( \mathbb{Q} \), since \( E' \) has three points of order 2, the only possibilities for \( E'(\mathbb{Q})_{\text{tors}} \) are \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z} \) with \( k = 1, 2, 3, 4 \). But Lemma 2 shows that the cases \( k = 2, 4 \) are not possible for an elliptic curve induced by a \( D(4) \)-triple with positive elements.

**Corollary 4.** Let \( \{a, b, c\} \) be a \( D(1) \)-triple. Then the torsion group of the elliptic curve \( y^2 = (ax + 1)(bx + 1)(cx + 1) \) is either \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \).

**Remark 4.** We note that an analogue of Theorem 3 and Corollary 4 is not valid for general \( D(n^2) \)-triples and their induced elliptic curves

\[
y^2 = (ax + n^2)(bx + n^2)(cx + n^2).
\]

For example, for the \( D(9) \)-triple \( \{8, 54, 104\} \) the torsion group of the induced elliptic curve is \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \). Also, there are examples with torsion group \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \), e.g. for the \( D(5220840540435206419201940^2) \)-triple

\[
\{3871249317729019929807383, 101862056999203416732147408, 217448139952121636379025175\}
\]
(there are much simpler examples with triples with mixed signs, see e.g. [7]).

We should also mention that we do not know any example of $D(1)$ or $D(4)$-triples inducing elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Indeed, it is known that this torsion group cannot appear for certain families of $D(1)$-triples (see [3, 4, 8, 18]). Again, there are examples of such curves for general $D(n^2)$-triples. For example, the $D(294^2)$-triple $\{32, 539, 1215\}$ induces an elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

**Acknowledgements.** A.D. was supported by the Croatian Science Foundation under the project no. 6422.

**References**


