Canad. Math. Bull. Vol. **46** (1), 2003 pp. 157–160

Torsion Points on Certain Families of Elliptic Curves

Małgorzata Wieczorek

Abstract. Fix an elliptic curve $y^2 = x^3 + Ax + B$, satisfying $A, B \in \mathbb{Z}$, $A \geq |B| > 0$. We prove that the $\mathbb{Q}$-torsion subgroup is one of (0), $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$. Related numerical calculations are discussed.

1 Introduction

Let $E(A,B) : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z}, 4A^3 + 27B^2 \neq 0)$ be a fixed elliptic curve over $\mathbb{Q}$. The deep theorem of Mazur [4] tells us that $E(A,B)(\mathbb{Q})_{\mathrm{tors}}$ (the torsion subgroup of the $\mathbb{Q}$-points) is one of the 15 groups: $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, \dots, 10, 12)$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ $(m = 1, 2, 3, 4)$. In any particular case, it is not difficult to determine $E(A,B)(\mathbb{Q})_{\mathrm{tors}}$ explicitly. In some cases we can calculate the torsion part for infinitely many given curves at once [1], [5].

We shall prove that the torsion subgroup of $E(A,B)(\mathbb{Q})$ is, under the assumption $A \geq |B| > 0$, one of (0), $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ (Proposition 3.2). The proof is based on the parametrisation of torsion structures [3, Table 3]. Numerical calculations suggest that all non-trivial groups $E(A,B)(\mathbb{Q})_{\mathrm{tors}}$ $(0 < |B| \leq A)$ are isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

2 General Observations

We start with the following elementary observation.

Proposition 2.1 *Fix integers A, B satisfying $3 \nmid 4A^3 + 27B^2$.*

(i) *Assume $A \equiv 1 \pmod 3$. Then $E(A,B)(\mathbb{Q})_{\mathrm{tors}}$ is one of (0), $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*
(ii) *Assume $A \equiv 2 \pmod 3$. Then $B \equiv 2 \pmod 3$ implies $E(A,B)(\mathbb{Q})_{\mathrm{tors}} = (0)$, $E(A,B)(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/7\mathbb{Z}$ if $B \equiv 1 \pmod 3$, and $E(A,B)(\mathbb{Q})_{\mathrm{tors}}$ is one of (0), $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if $3|B$.*

Proof Consider the reduction modulo 3 of $E(A,B)$. ∎

Remark One checks that $E(-43, 166)(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$ $(= \{[0:1:0], [11:-32:1], [11:32:1], [3:-8:1], [3:8:1], [-5:-16:1], [-5:16:1]\})$. This is the only elliptic curve $E(A,B)$, $0 < |A|, |B| \leq 10^4$, $A \equiv 2 \pmod 3$, $B \equiv 1 \pmod 3$, satisfying $E(A,B)(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$.

Received by the editors April 25, 2001.
AMS subject classification: 11G05.

https://doi.org/10.4153/CMB-2003-016-6 Published online by Cambridge University Press

Remark There are only 29 elliptic curves $E(A, B)$ $(0 < A < 10^4, A \equiv 0 \pmod 3,$ $0 \le |B| \le 10^4)$ with $\mathbb{Q}$-torsion of order 4. All of them are cyclic. Here are all such pairs (A, B):

$(6, -7)$,	$(6, 6973)$,	$(33, 34)$,	$(33, 5474)$,	$(54, 189)$,
$(54, 4185)$,	$(69, 470)$,	$(69, 3094)$,	$(78, 889)$,	$(78, 2189)$,
$(81, 1458)$,	$(96, -448)$,	$(213, -3674)$,	$(213, -434)$,	$(324, 0)$,
$(429, 866)$,	$(486, -5103)$,	$(528, 2176)$,	$(621, 3942)$,	$(708, 6176)$,
$(753, -5614)$,	$(789, 8890)$,	$(1014, -5195)$,	$(1269, -3834)$,	$(1518, -1519)$,
$(1761, 1762)$,	$(1998, 6021)$,	$(4749, -9506)$,	$(5184, 0)$.	

Now consider an algebraic curve $E(A) : y^2 = x^3 - 27x - 54(32A - 1)$. Note that $E(A)$ is an elliptic curve if and only if $A \neq 0$. Let us recall the following criterion [2, Proposition 1.1.2].

Proposition 2.2 *Assume $A \in \mathbb{Z} \setminus \{0\}$. Then $E(A)(\mathbb{Q}) = (0)$ implies that the torsion subgroup $E(A, B)(\mathbb{Q})_{\text{tors}}$ is one of* (0), $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

We have used an executable version of the program from Cremona's ftp server to tabulate all the integers A $(0 < |A| < 1065)$ such that $E(A)(\mathbb{Q}) = (0)$. Here are all such A's with $0 < |A| \le 50$:

-50,	-49,	-46,	-43,	-40,	-38,	-36,	-32,	-31,	-26,
-24,	-22,	-18,	-15,	-14,	-13,	-11,	-10,	-9,	-6,
-5,	-4,	-2,	2,	3,	4,	5,	13,	16,	18,
19,	20,	21,	22,	23,	24,	25,	29,	36,	37,
39,	47,	48,	50.						

3 The Case $0 < |B| \le A$

Lemma 3.1 *Fix integers A, B, satisfying $A \ge |B| > 0$. Then $E(A, B)(\mathbb{Q})_{\text{tors}}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and contains no point of order* 5 *or* 7.

Proof Combine Propositions 2 and 3 in [1]. ■

Proposition 3.2 *Fix integers A, B, satisfying $A \ge |B| > 0$. Then $E(A, B)(\mathbb{Q})_{\text{tors}}$ is one of* (0), $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$.

Proof Elliptic curve E with $E(\mathbb{Q})_{\text{tors}} \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ may be assumed to have the equation $y^2 = x(x + M)(x + N)$ $(M, N \in \mathbb{Z})$, or equivalently

$$y^2 = x^3 + 3^3(MN - M^2 - N^2)x + 3^3(M + N)(2M^2 + 2N^2 - 5MN).$$

Now $MN - M^2 - N^2 < 0$, hence $E(A, B)(\mathbb{Q})_{\text{tors}}$ $(A \ge |B| > 0)$ is cyclic.

From the theorem of Mazur it follows that $E(A, B)(\mathbb{Q})_{\text{tors}}$ is cyclic with even order if and only if $E(A, B)(\mathbb{Q})$ has just one non-trivial rational point of order 2. It means that $E(A, B)$ can be defined by the equation

$$y^2 = x(x + M)(x + N),$$

https://doi.org/10.4153/CMB-2003-016-6 Published online by Cambridge University Press

or equivalently,

$$(*) \qquad y^2 = x^3 - 3^3(m^2 + 3Dn^2)x - 3^3 2m(m^2 - 9Dn^2),$$

where $M = m + n\sqrt{D}$, $N = m - n\sqrt{D}$, D, m, n are square-free integers, $D \neq 1$, $n \neq 0$.

We shall need the following lemma [6, Theorem 1].

Lemma 3.3 *Let E denote the elliptic curve defined by* $(*)$*.*

(i) $E(\mathbb{Q})_{\mathrm{tors}} \supset \mathbb{Z}/4\mathbb{Z}$ *if and only if* $m = a^2 + b^2 D$, $n = 2ab$, *where* $a, b \in \mathbb{Z}$ *are relatively prime and non-zero.*

(ii) $E(\mathbb{Q})_{\mathrm{tors}} \supset \mathbb{Z}/6\mathbb{Z}$ *if and only if*

$$m = a^2 + 2ac + b^2 D, \quad n = 2b(a + c), \quad a^2 - b^2 D = c^2,$$

where $a, b, c \in \mathbb{Z}$ *are relatively prime and non-zero.*

We return to the proof of Proposition 3.2. Write

$$A = -3^3(m^2 + 3Dn^2), \quad B = -3^3 2m(m^2 - 9Dn^2).$$

If $D > 1$, then, of course $A < 0$. Now assume $D < 0$. If $E(A, B)(\mathbb{Q})_{\mathrm{tors}}$ contains $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$, then Lemma 3.3 implies $m \neq 0$, and we obtain $A < |B|$.

We conclude that $E(A, B)(\mathbb{Q})$ $(A \geq |B| > 0)$ contains no point of even order. Now let us mention Lemma 3.1. The assertion follows. ■

It is plain to check that the x-coordinate of a point of order 3 on $E(A, B)$ satisfies $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$. In particular $3|A$, and $2|A$ implies $4|A$. Also note that, fixed $A \in \mathbb{Z} \setminus \{0\}$, there exist at most finitely many $B \in \mathbb{Z}$ satisfying $E(A, B)(\mathbb{Q}) \supset \mathbb{Z}/3\mathbb{Z}$.

Numerical calculations show that all non-trivial $E(A, B)(\mathbb{Q})_{\mathrm{tors}}$ $(0 < |B| \leq A \leq 10^4)$ are isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Here are all such pairs (A, B):

$(27, -27)$,	$(33, -26)$,	$(39, -23)$,	$(45, -18)$,	$(51, -11)$,
$(57, -2)$,	$(63, 9)$,	$(69, 22)$,	$(75, 37)$,	$(81, 54)$,
$(87, 73)$,	$(804, -767)$,	$(816, -704)$,	$(828, -639)$,	$(840, -572)$,
$(852, -503)$,	$(864, -432)$,	$(876, -359)$,	$(888, -284)$,	$(900, -207)$,
$(912, -128)$,	$(924, -47)$,	$(936, 36)$,	$(948, 121)$,	$(960, 208)$,
$(972, 297)$,	$(984, 388)$,	$(996, 481)$,	$(1008, 576)$,	$(1020, 673)$,
$(1032, 772)$,	$(1044, 873)$,	$(1056, 976)$,	$(4419, -4307)$,	$(4437, -4058)$,
$(4455, -3807)$,	$(4473, -3554)$,	$(4491, -3299)$,	$(4509, -3042)$,	$(4527, -2783)$,
$(4545, -2522)$,	$(4563, -2259)$,	$(4581, -1994)$,	$(4599, -1727)$,	$(4617, -1458)$,
$(4635, -1187)$,	$(4653, -914)$,	$(4671, -639)$,	$(4689, -362)$,	$(4707, -83)$,
$(4725, 198)$,	$(4743, 481)$,	$(4761, 766)$,	$(4779, 1053)$,	$(4797, 1342)$,
$(4815, 1633)$,	$(4833, 1926)$,	$(4851, 2221)$,	$(4869, 2518)$,	$(4887, 2817)$,
$(4905, 3118)$,	$(4923, 3421)$,	$(4941, 3726)$,	$(4959, 4033)$,	$(4977, 4342)$,
$(4995, 4653)$,	$(5013, 4966)$.			

Question *Assume* $0 < |B| \leq A$. *Is it true that* $E(A, B)(\mathbb{Q})_{\mathrm{tors}} \subset \{(0), \mathbb{Z}/3\mathbb{Z}\}$*?*

References

[1] A. Dąbrowski and M. Wieczorek, *Families of elliptic curves with trivial Mordell-Weil group*. Bull. Austral. Math. Soc. **62**(2000), 303–306.

[2] ———, *Arithmetic on certain families of elliptic curves*. Bull. Austral. Math. Soc. **61**(2000), 319–327.

[3] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*. Proc. London Math. Soc. **33**(1976), 193–237.

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

[5] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication*. Manuscripta Math. **14**(1974), 195–205.

[6] D. Qiu and X. Zhang, *Explicit classification for torsion subgroups of rational points of elliptic curves.* Preprint No **131** (Algebraic number theory archives, September 3, 1998).

University of Szczecin
Institute of Mathematics
ul. Wielkopolska 15
70-451 Szczecin
Poland
email: wieczorek@wmf.univ.szczecin.pl

https://doi.org/10.4153/CMB-2003-016-6 Published online by Cambridge University Press