Bull. Austral. Math. Soc. 11G05
Vol. 62 (2000) [303–306]

FAMILIES OF ELLIPTIC CURVES WITH TRIVIAL MORDELL-WEIL GROUP

Andrzej Dąbrowski and Małgorzata Wieczorek

Fix an elliptic curve $y^2 = x^3 + Ax + B$, satisfying $A, B \in \mathbb{Z}$, $A \geqslant |B| > 0$. We prove that the associated quadratic family contains infinitely many elliptic curves with trivial Mordell-Weil group.

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 [**5**] tells us that $E(A,B)(\mathbb{Q})_{\text{tors}}$ (the torsion subgroup of the $\mathbb{Q}$-points) is one of the 15 groups: $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, \dots, 10, 12)$, $\mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ $(n = 1, 2, 3, 4)$. In any particular case, it is not difficult to determine $E(A,B)(\mathbb{Q})_{\text{tors}}$ explicitly. In some cases one can calculate the torsion part for infinitely many given curves at once (see [**8**]).

Our first observation (Proposition 2) is that the torsion part $E(A,B)(\mathbb{Q})_{\text{tors}}$ $(A \geqslant 0)$ contains no point of order 5 or 7. It easily generates new examples of quadratic families of elliptic curves (without complex multiplication) with prescribed torsion subgroups.

Our second application is the existence of infinitely many elliptic curves with trivial Mordell-Weil group in a wide class of quadratic families (Corollary 2). It is a pretty combination of our calculations, with recent results of Kolyvagin [**3**], Bump-Friedberg-Hoffstein-Iwaniec-Murty-Murty [**2**], and the modularity conjecture completely settled by Wiles-Taylor-Diamond-Breuil-Conrad [**1**]. The result should be compared with [**6**], where the authors proved the existence of infinitely many elliptic curves (with complex multiplication) with no rational points except the origin.

1. Elliptic curves with no rational torsion point of orders 5 and 7

The following result is well known (see [**9**, Exercise 8.13a]).

Received 8th February, 2000
The first author was partially supported by KBN Grant No. 2PO3A02318.

https://doi.org/10.1017/S0004972700018773 Published online by Cambridge University Press

PROPOSITION 1. *Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ with a rational torsion point of order $\geqslant 4$. Then E has an equation of the form*

$$y^2 + uxy + vy = x^3 + vx^2 \tag{1}$$

with $u, v \in \mathbb{Q}$.

The family (1) can be rewritten into the following form:

$$\begin{aligned} E(u,v): \quad y^2 = x^3 &+ \left(-\frac{1}{3}v^2 + \left(-\frac{1}{6}u^2 + \frac{1}{2}u\right)v - \frac{1}{48}u^4\right)x \\ &+ \left(\frac{2}{27}\left(v + \frac{1}{4}u^2\right)^3 - \frac{1}{6}uv\left(v + \frac{1}{4}u^2\right) + \frac{1}{4}v^2\right). \end{aligned} \tag{2}$$

Let $E = E(A,B) : y^2 = x^3 + Ax + B$ ($A, B \in \mathbb{Z}$, $4A^3 + 27B^2 \neq 0$) be an elliptic curve over the rationals. Our first observation is the following

PROPOSITION 2. *Assume that $A \geqslant 0$. Then the torsion part $E(A,B)(\mathbb{Q})_{\text{tors}}$ contains no point of order 5 or 7.*

PROOF: The proof is based on the parametrisation of torsion structures [**4**, Table 3]. Namely, elliptic curves (over $\mathbb{Q}$) having the specified torsion subgroup all lie in a 1-parameter family. We know [4], that $E(A,B)(\mathbb{Q})$ contains a point of order 5 if and only if $E(A,B)$ is of the form (2) with $u = 1 - v$. Comparing the coefficients we obtain

$$v^4 + 12v^3 + 14v^2 - 12v + 1 + 48A = 0$$

and

$$v^6 + 18v^5 + 75v^4 + 75v^2 + 18v + 1 - 2^5 3^3 B = 0.$$

Take $A \gg 1$. Then the first equation has no integer (hence rational) solutions in v. Now $E(A,B)$ is isomorphic to $E\left(Ad^4, Bd^6\right)$ ($d = 1, 2, \dots$), hence we can replace $A \gg 1$ by $A \geqslant 0$.

Elliptic curves having the torsion subgroup $\mathbb{Z}/7\mathbb{Z}$ lie in a family

$$y^2 + \left(1 - t - t^2\right)xy + \left(t^2 - t^3\right)y = x^3 + \left(t^2 - t^3\right)x^2,$$

and the same method shows that $E(A,B)(\mathbb{Q})$ has no rational torsion point of order 7 for $A \geqslant 0$. $\square$

https://doi.org/10.1017/S0004972700018773 Published online by Cambridge University Press

2. Families of elliptic curves with trivial Mordell-Weil group

Let, as usual, $E = E(A, B) : y^2 = x^3 + Ax + B$ be an elliptic curve. For each $0 \neq d \in \mathbb{Z}$ consider its quadratic twist

$$E_d = E(A, B)_d : y^2 = x^3 + d^2Ax + d^3B.$$

If $E_d(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then, using [4] we see that E_d has an equation of the form $y^2 = x^3 + ax^2 + bx$, or equivalently, we have

$$b - \frac{1}{3}a^2 = Ad^2, \quad \frac{2}{27}a^3 - \frac{1}{3}ab = Bd^3.$$

It leads to the following equation in a:

$$a^3 + 9Ad^2a + 27Bd^3 = 0. \tag{3}$$

Our next observation is the following

Proposition 3. *Fix integers A, B, satisfying $A \geqslant |B| > 0$. Also fix a non-zero integer d. Then the equation (3) has no rational solutions in a.*

Proof: The substitution $a \mapsto 3dx$ leads to the equation $x^3 + Ax + B = 0$ with no real solution (when $A \geqslant |B| > 0$, of course). $\square$

Corollary 1. *Fix non-zero integers A, B satisfying $A \geqslant |B| > 0$, and a positive integer r. There are infinitely many square-free integers d having exactly r prime factors such that $E(A, B)_d(\mathbb{Q})_{\text{tors}} = (0)$.*

Proof: Combine Propositions 2 and 3, and remark that $E(A, B)_d$ possesses $\mathbb{Q}$-rational points of order 3 only for a finitely many d's (see [7]). $\square$

Corollary 2. *Fix an elliptic curve $E(A, B)$, with $A \geqslant |B| > 0$. There are infinitely many d's for which $E(A, B)_d(\mathbb{Q}) = (0)$.*

Proof: Combine Corollary 1, and a recent result that there are infinitely many d's such that $L\big(E(A, B)_d, 1\big) \neq 0$ (see, for example, [2] and references there), Kolyvagin's result [3], and Wiles-Taylor-Diamond-Breuil-Conrad's result [1]. $\square$

Example. $E : y^2 = x^3 + 5x + 1$. Here $\Delta = 527 = 17 \cdot 31$. One easily checks that $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$ $(= \{(0, 1), (0, -1), \infty\})$. Proposition 3 implies that $E_d(\mathbb{Q})$ has no point of order 2. Now E_d (d square free) may possess a rational torsion point of order greater than 2 only for $d = \pm 17, \pm 31, \pm 527$. Again, using Proposition 2, we see that is has no point of order 5. Reducing modulo 5 we conclude that $E_d(\mathbb{Q})_{\text{tors}} \subset \mathbb{Z}/3\mathbb{Z}$ in all these cases, and a short calculation shows $E_d(\mathbb{Q})_{\text{tors}}$ are all trivial.

https://doi.org/10.1017/S0004972700018773 Published online by Cambridge University Press

References

[1] C. Breuil, B. Conrad, F. Diamond and R. Taylor, 'On the modularity conjecture for all elliptic curves', (article in preparation).

[2] D. Bump, S. Friedberg and H. Hoffstein, 'On some applications of automorphic forms to number theory', *Bull. Amer. Math. Soc. (New Series)* **33** (1996), 157–175.

[3] V.A. Kolyvagin, 'Finitness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves', *Izv. Akad. Nauk SSSR Ser. Mat.* **52** (1988), 522–540.

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

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

[6] J. Nakagawa and K. Horie, 'Elliptic curves with no rational points', *Proc. Amer. Math. Soc.* **104** (1988), 20–24.

[7] L.D. Olson, 'Torsion points on elliptic curves with given j-invariant', *Manuscripta Math.* **16** (1975), 145–150.

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

[9] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106** (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

University of Szczecin
Institute of Mathematics
ul. Wielkopolska 15
70-451 Szczecin
Poland
e-mail: dabrowsk@sus.univ.szczecin.pl

https://doi.org/10.1017/S0004972700018773 Published online by Cambridge University Press