BULL. AUSTRAL. MATH. SOC. 11G40, 11G05
VOL. 61 (2000) [319–327]

ARITHMETIC ON CERTAIN FAMILIES OF ELLIPTIC CURVES

ANDRZEJ DĄBROWSKI AND MAŁGORZATA WIECZOREK

Consider a family of elliptic curves $E_{(B)} : y^2 = x^3 + d_0^2 A_0 x + d_0^3 B$ (A, A_0, d_0 fixed integers). We prove that, under certain conditions on A_0 and d_0, the rational torsion subgroup of $E_{(B)}$ is either cyclic of order ≤ 3 or non-cyclic of order 4. Also, assuming standard conjectures, we establish estimates for the order of the Tate-Shafarevich groups as B varies.

INTRODUCTION

Let $E : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z},\ 4A^3 + 27B^2 \neq 0)$ be a fixed elliptic curve over $\mathbb{Q}$. For each $d \neq 0$ let E_d be the elliptic curve $E_d : y^2 = x^3 + d^2 Ax + d^3 B$.

One can prove that for all but finitely many square-free integers $d \neq 0$, the torsion subgroup of $E_d(\mathbb{Q})$ is one of (0), $\mathbb{Z}/2$, $\mathbb{Z}/2 \oplus \mathbb{Z}/2$, and a necessary condition that E_d posseses $\mathbb{Q}$-rational point of order greater than 2 is $d \mid 4A^3 + 27B^2$ [**10**].

We shall prove that the $\mathbb{Q}$-torsion subgroup of $E_{(B)} : y^2 = x^3 + d_0^2 A_0 x + d_0^3 B$ (A_0, d_0 fixed) is, under certain conditions on A_0 and d_0, one of (0), $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ (Section 1). Let N_B, R_B, and $Ш(E_{(B)})$ denote respectively the conductor, the regulator, and the Tate-Shafarevich group (conjecturally finite) of $E_{(B)}$. Assuming the Birch and Swinnerton-Dyer conjecture for all $E_{(B)}$ we prove that

$$N_B^{1/12-\varepsilon} \ll R_B \cdot \sharp Ш(E_{(B)}) \ll N_B^{1/12+\varepsilon}$$

for infinitely many B (the lower bound is actually valid for all B) (Section 2). We also comment on the behaviour of the order of Ш in other families of elliptic curves. In section 3 we give some evidence for Mazur's conjecture on the variation of the rank in a family in a special case.

1. TORSION POINTS ON CERTAIN FAMILIES OF ELLIPTIC CURVES

1.1. CONSTRUCTION OF CERTAIN FAMILIES OF ELLIPTIC CURVES. We start with the following well known result.

Received 15th July, 1999

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/00 $A2.00+0.00.

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

PROPOSITION 1.1.1. [**12**, Ex. 8.13(a), p.238] Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ with a rational torsion point of order ≥ 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 easily be rewritten into the following equivalent form:

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

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. For each $0 \neq d \in \mathbb{Z}$ consider its quadratic twist

$$E_d: y^2 = x^3 + d^2Ax + d^3B.$$

E_d has a rational point of order ≥ 4 if and only if it is of the form (2) with some $u, v \in \mathbb{Q}$. In particular, we have

$$16v^2 + \left(8u^2 - 24u\right)v + \left(u^4 + 48Ad^2\right) = 0.$$

Now

$$\Delta_v = \left(8u^2 - 24u\right)^2 - 4 \cdot 16 \cdot \left(u^4 + 48Ad^2\right) = 2^6\left(-6u^3 + 9u^2 - 48Ad^2\right).$$

Hence $\Delta_v \in \mathbb{Q}^2$ if and only if $-6u^3 + 9u^2 - 48Ad^2 = y^2$ with certain $y \in \mathbb{Q}$ if and only if $E(A;d): y^2 = x^3 - 27x - 54\left(32Ad^2 - 1\right)$ has solution in $x, y \in \mathbb{Q}$.

Note that $E(A;d)$ is an elliptic curve if and only if $A \neq 0$.

PROPOSITION 1.1.2. *Assume $A \neq 0$. Then $E(A;d)(\mathbb{Q}) = (0)$ implies that the torsion part $E(A,B)_d(\mathbb{Q})_{\text{tors}}$ is one of (0), $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.*

PROOF: Combine the above construction with Mazur's theorem [**9**]. ∎

1.2. TORSION PART OF $E(A;d)(\mathbb{Q})$. Assume that $E(\mathbb{Q})_{\text{tors}} \neq (0)$; then we know [**9**] that $E(\mathbb{Q})_{\text{tors}}$ contains only points of orders 2 or 3 or 5 or 7.

(a) Non-existence of point of order 5.

By [**5**] we know that $E(A;d)(\mathbb{Q})$ contains a point of order 5 if and only if $E(A;d)$ is of the form

$$y^2 + (1-c)xy - cy = x^3 - cx^2, \quad \text{with some } c \in \mathbb{Q},$$

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

which is equivalent to

$$y^2 = x^3 + \left[-\frac{1}{3}c^2 + \frac{1}{6}c(c-1)^2 - \frac{1}{48}(c-1)^4 + \frac{1}{2}c(c-1)\right]x + \left[\frac{2}{27}\left(-c + \frac{1}{4}(c-1)^2\right)^3 - \frac{1}{6}c(c-1)\left(-c + \frac{1}{4}(c-1)^2\right) + \frac{1}{4}c^2\right].$$

Comparing the coefficients we obtain

$$-(c-1)^4 + 8c(c-1)^2 + 8c^2 - 24c + 2^4 3^4 = 0.$$

The above equation has no solution in $c \in \mathbb{Q}$, hence $E(A;d)(\mathbb{Q})$ contains no points of order 5.

(b) Non-existence of point of order 7.

We know [5] that $E(A;d)(\mathbb{Q})$ contains a point of order 7 if and only if $E(A;d)$ is of the form

$$y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2, \quad \text{with some } t \in \mathbb{Q},$$

which is equivalent to

$$y^2 = x^3 + \left[-\frac{1}{3}\left(\frac{1}{4}(1+t-t^2)^2 + (t^2-t^3)\right)^2 + \frac{1}{2}(1+t-t^2)(t^2-t^3)\right]x + \left[\frac{2}{27}\left(\frac{1}{4}(1+t-t^2)^2 + (t^2-t^3)\right)^3 - \frac{1}{6}\left(\frac{1}{4}(1+t-t^2)^2 + (t^2-t^3)\right)(1+t-t^2)(t^2-t^3) + \frac{1}{4}(t^2-t^3)^2\right].$$

Comparing the coefficients we obtain

$$(1+t-t^2)^4 + 8(1+t-t^2)^2(t^2-t^3) + 16(t^2-t^3)^2 - 24(1+t-t^2)(t^2-t^3) - 2^4 3^4 = 0.$$

The above equation has no integer (hence rational) solutions.

(c) Points of order 3.

We have, similarly to [5], that $E(A;d)(\mathbb{Q})$ contains a point of order 3 if and only if $E(A;d)$ is of the form

$$y^2 + axy + by = x^3 \quad (a, b \in \mathbb{Q}),$$

which is equivalent to

$$y^2 = x^3 + \left(-\frac{1}{48}a^4 + \frac{1}{2}ab\right)x + \left(\frac{1}{27 \cdot 32}a^6 - \frac{1}{24}a^3 b + \frac{1}{4}b^3\right).$$

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

Comparing the coefficients we obtain an equation in a:

$$a^{12} - 2^5a^9 - 2^4 3^5 a^8 + 2^9 3^5 a^5 + 2^8 3^9 a^4 - 2^{12}3^6\big(1 - 2^5 d^2 A\big)a^3 - 2^{12}3^{12} = 0.$$

In the case $A = 1$ one checks the above equation has no rational solutions.

(d) Points of order 2.

$E(A;d)(\mathbb{Q})$ contains a point of order 2 if and only if $x^3 - 27x - 54\big(32Ad^2 - 1\big) = 0$ has solutions in $x \in \mathbb{Z}$. Certainly this is not the case for $A = 1$, $d \equiv 2 (\mathrm{mod}\ 5)$.

1.3. FREE PART OF $E(A;d)(\mathbb{Q})$. It is not difficult to calculate finite products of the type $f(x) = \prod_{p<x} \big(p^{-1}\sharp E(A;d)(\mathbb{F}_p)\big)$, x big enough. One expects that the rank of $E(A;d)(\mathbb{Q})$ is zero if $f(x)$ is bounded. To calculate the rank exactly one can use, say, (pseudo)algorithms described in Cremona's book [**1**], or an executable version of the program from his ftp server. For example: $rank\ E(1;2)(\mathbb{Q}) = 0$, $rank\ E(1;7)(\mathbb{Q}) = 1$.

1.4. AN EXAMPLE. Take $A_0 = 1$, $d_0 = 2$, and consider the family $E_{(B)} : y^2 = x^3 + 4x + 8B$. Considering the reduction modulo 5, and applying Proposition 1.1.2 and [**10**], we conclude that

$$\begin{aligned}
&E_{(2B)}(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/3 \text{ for } B \equiv 2,3 (\mathrm{mod}\ 5),\\
&E_{(2B)}(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/2 \oplus \mathbb{Z}/2 \text{ for } B \equiv 0,1,4 (\mathrm{mod}\ 5),\\
&E_{(2B+1)}(\mathbb{Q})_{\mathrm{tors}} = (0) \text{ for } B \equiv 0,4 (\mathrm{mod}\ 5),\\
&E_{(2B+1)}(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/2 \oplus \mathbb{Z}/2 \text{ for } B \equiv 1,2,3 (\mathrm{mod}\ 5).
\end{aligned}$$

Note however (by the Lutz-Nagell theorem) that $E_{(B)}(\mathbb{Q})$ contains a point of order 2 if and only if $B = k\big(k^2 + 1\big)$, $k \in \mathbb{Z}$.

2. BOUNDS ON THE SIZE OF THE ORDER OF THE TATE-SHAFAREVICH GROUP

In this section we shall establish estimates for the orders of $Ш\big(E_{(B)}\big)$ as B varies (Theorem 2.4.1).

2.1. BOUNDS ON THE REAL PERIOD. Let $\pi_\infty(E)$ denote the real period of E.

LEMMA 2.2.1. *We have* $\pi_\infty\big(E(A_0,B)_{d_0}\big) \gg\ll B^{-\frac{1}{6}}$.

PROOF: Note that

$$\pi_\infty\big(E(A_0,B)_{d_0}\big) = d_0^{1/2}\pi_\infty\big(E(A_0,B)\big).$$

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

Now

$$\pi_\infty\big(E(A_0,B)\big) = \int_{-\infty}^{\infty} \frac{dx}{\sqrt{x^3+A_0x+B}} = \int_1^{\infty} + \int_{-1}^{1} + \int_{-\infty}^{-1}.$$

$$\int_1^{\infty} \frac{dx}{\sqrt{x^3+A_0x+B}} \ll \int_1^{\infty} \frac{dx}{\sqrt{x^3+B}} \ll \int_1^{\infty} \frac{dx}{\big(x+B^{1/3}\big)^{3/2}} \ll B^{-1/6}.$$

$$\int_{-1}^{1} \frac{dx}{\sqrt{x^3+A_0x+B}} \ll \int_{-1}^{1} \frac{dx}{\sqrt{B}} \ll B^{-1/2}.$$

$$\int_{-\infty}^{-1} \frac{dx}{\sqrt{x^3+A_0x+B}} = \left(\int_{-\infty}^{-B^{1/3}} + \int_{-B^{1/3}}^{-1}\right) \frac{dx}{\sqrt{x^3+A_0x+B}} \ll B^{-1/6}.$$

The above proves the "$\ll$" part. For the "$\gg$" part see [**6**, p.159]. □

2.2. BOUNDS ON THE CONDUCTOR. Let

$$E(A_0,B)_{d_0}: \quad y^2 = x^3 + d_0^2A_0 + d_0^3B.$$

We have

$$\Delta = -2^4\big(4d_0^6A_0^3 + 27d_0^6B^2\big) \ll B^2.$$

Hence $N_B = N_{E(A_0,B)_{d_0}} \ll B^2$.

Now assume $A_0d_0 \neq 0$.

LEMMA 2.2.1. *For infinitely many integers B we have $N_B \gg B^2$.*

PROOF: Indeed, by Iwaniec's work [**4**] we know that the polynomial $27x^2 + a$ (a fixed odd integer) takes infinitely many values of the form p_1p_2, (p_1,p_2 different rational primes). The assertion follows. □

2.3. AN UPPER BOUND FOR $\prod \pi_p$.

LEMMA 2.3.1. *We have*

$$\prod_{p \mid N_B} \pi_p = O(B^\epsilon).$$

PROOF: Take a rational prime $p \mid N_B$. We obtain, using Tate's algorithm [**13**], that the corresponding Kodaira symbol is never of type I_ν ($\nu > 0$). Hence $\pi_p \leq 4$, and the assertion follows. □

2.4. ESTIMATES ON THE ORDER OF Ш.

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

THEOREM 2.4.1. *Fix integers A_0, d_0 ($A_0 d_0 \neq 0$). Assume the Birch and Swinnerton–Dyer conjecture holds for all $E_{(B)} = E(A_0, B)_{d_0}$. Then*

(a)
$$R_B \cdot \sharp Ш(E_{(B)}) \gg N_B^{1/12-\varepsilon}.$$

(b) *Assume additionally the generalised Lindelöf conjecture* [**3**] *for the family $E(A_0, B)_{d_0}$. Then there exist infinitely many B such that*

$$R_B \cdot \sharp Ш(E_{(B)}) \ll N_B^{1/12+\varepsilon}.$$

PROOF:

(a) Using the above bounds and the Birch and Swinnerton-Dyer conjecture for all $E(A_0, B)_{d_0}$, we have

$$R_B \cdot \sharp Ш(E_{(B)}) \gg B^{1/6-\varepsilon} \gg N_B^{1/12-\varepsilon}.$$

(b) The generalised Lindelöf hypothesis for $L(E, s)$ implies $L^{(r)}(E, 1) = O(N_E^{\varepsilon})$ (see [**3,** p.154]). On the other hand $\pi_\infty\big(E(A_0, B)_{d_0}\big) \ll B^{-1/6}$. Also we have $\sharp E(A_0, B)_{d_0}(\mathbb{Q})_{\text{tors}} \leq 16$ by [**9**], and $\prod_{p|N_B} c_p \geq 1$.

The above estimates and the Birch and Swinnerton-Dyer conjecture for all the $E(A_0, B)_{d_0}$ imply $R_B \cdot \sharp Ш(E_{(B)}) \ll B^{1/6+\varepsilon}$. By Iwaniec's result we have $N_B \gg B^2$ for infinitely many B. The assertion follows. ∎

2.5. REMARK. Assuming additionally the Lang conjecture $R_E \gg N_E^{-\varepsilon}$, one can state the result in the form:

$$N_B^{1/12-\varepsilon} \ll \sharp Ш(E_{(B)}) \ll N_B^{1/12+\varepsilon}$$

for infinitely many B.

2.6. EXAMPLE. Consider the family $E(B) : y^2 = x^3 + 12x + 16B$, ($B \in \mathbb{Z}$). Here $\Delta = 2^8 3^3 (1 + B^2)$, and one checks that the reduction is split multiplicative at all primes $p \neq 2, 3$. On the other hand, it is classical that every odd prime divisor of $1 + B^2$ is of the type $4k + 1$. Hence, using [**11,** Propositions 1 and 3] we conclude that for infinitely many B's the root number $\varepsilon\big(E(B)\big)$ depends only on the local root numbers at 2 and 3. As a consequence we obtain that, at least conjecturally, the rank is even (maybe zero) for infinitely many B's.

2.7. REMARKS.

(i) Part (b) of the theorem is consistent with the following conjecture of Lang. Write $E : y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$; let $H(E) = \max\big(|a|^3, |b|^2\big)$. Lang [**6**] conjectures that

$$R_E \cdot \sharp Ш(E) \ll H(E)^{1/12} N^{\varepsilon(N)} c^r (\log N)^r,$$

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

with some universal constant c, and $\varepsilon(N) \to 0$ as $N \to \infty$.

(ii) The case $A = 0$. Note that $E(0;d)$ is not an elliptic curve. Hence the family $E(0,B)_{d_0}$ cannot be treated by our method. Such a family was studied from an analytic point of view in [7]; consequences for the order of Ш (in a case $E(d): x^3 + y^3 = d$, d cubic-free) are as follows:

$$N_{E(d)}^{1/6-\varepsilon} \ll \sharp Ш(E(d)) \ll N_{E(d)}^{1/3+\varepsilon}$$

for infinitely many d.

(iii) The family $E(A_0;d)$ $(d \in \mathbb{Z})$ also has interesting properties. Take, say, $A_0 = 1$, and denote $E(d) = E(1;d)$. One can show that for all $d \in \mathbb{Z}$

$$N_{E(d)}^{1/12-\varepsilon} \ll \sharp Ш(E(d)) \cdot R_{E(d)} \ll N_{E(d)}^{1/9+\varepsilon}.$$

(iv) Consider the family $E(p): y^2 = x^3 + px$ (p prime $\equiv 7, 11 (\mathrm{mod}\ 16)$). Then $rank\ E(p)(\mathbb{Q}) = 0$ [**12**, p.311], and one can show (assuming the Birch and Swinnerton-Dyer conjecture) that

$$N_{E(p)}^{1/8-\varepsilon} \ll \sharp Ш(E(p)) \ll N_{E(p)}^{1/8+\varepsilon}$$

for all such primes.

(v) Denote by E_d (d square-free integer) the quadratic twist of E. Mai and Murty [8] proved, assuming the Birch and Swinnerton-Dyer conjecture for all E_d's, that there exist infinitely many d such that E_d has rank zero and

$$\sharp Ш(E_d) \gg N_{E_d}^{1/4-\varepsilon}.$$

As for the upper bound, one can prove [2] (assuming additionally the generalised Lindelöf hypothesis) that for the same family E_d (of rank zero) one has

$$\sharp Ш(E_d) \ll N_{E_d}^{1/4+\varepsilon}.$$

2.8. NUMERICAL OBSERVATION. Let $E(d): y^2 = x^3 - d^2x$ ($d \geq 1$ an odd square-free integer) denote the congruent number elliptic curve. Let

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \qquad \Theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2},$$

$$f(z) := \eta(8z)\eta(16z)\Theta(2z) = \sum_{n=1}^{\infty} a(n) q^n.$$

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

For $E(d)$'s of rank zero (assuming the Birch and Swinnerton-Dyer conjecture) we have (see [14]):

$$\sqrt{\sharp Ш(E(d))} = \frac{|a(d)|}{\tau(d)},$$

where $\tau(d)$ denotes the number of divisors of d.

We have tabulated all odd square-free d's ($d \leq 20000$) such that $\operatorname{rank} E(d) = 0$ and $\sharp Ш(E(d)) = 1$. The calculations led us to the following observation. Let

$$A := \left\{d \in \mathbb{N} : \ d \text{ odd square-free, } \operatorname{rank} E(d) = 0, \ \sharp Ш(E(d)) = 1\right\},$$
$$B := \left\{n \in \mathbb{N} : \ n \text{ is a sum of digits of a certain } d \in A\right\}.$$

CONJECTURE. *Let n be a positive integer. Then $n \in B$ if and only if $9 \nmid n$.*

3. Evidence for Mazur's conjecture

In this section we check Mazur's conjecture in a special case, which concerns the variation of *rank* $E(1;t)(\mathbb{Q})$ with $t \in \mathbb{Q}$: either there are only finitely many $t \in \mathbb{Q}$ such that the rank of $E(1;t)(\mathbb{Q})$ is positive, or else the set of all such t is dense in $\mathbb{R}$.

First, it is plain that $(x,y) = (-2,5)$ is a point of infinite order on $E(1;5/24) : y^2 = x^3 - 27x - 21$. Also, $(-2,5/24)$ is a point of infinite order on $E : 54 \cdot 32y^2 = x^3 - 27x + 29$. Therefore, $E(\mathbb{Q}) \cap E(\mathbb{R})^0$ is dense in $E(\mathbb{R})^0$, and hence $E(\mathbb{Q})$ contains points of infinite order of the form $(q, k/l)$ with $q \in \mathbb{Q}$, $k, l \in \mathbb{Z}$, $(k,l) = 1$. Since the curves $E(1;t)$ have no rational torsion points for a dense set of $t \in \mathbb{Q} \subset \mathbb{R}$ (use Section 1.2), we obtain the following result.

THEOREM 3.1. *The set of all rational t such that $E(1,t)(\mathbb{Q})$ has positive rank is dense in $\mathbb{R}$.*

QUESTION. It would be interesting to have any information concerning the behaviour of *rank* $E(A_0;d)(\mathbb{Q})$ as $d \in \mathbb{Z}$ varies. One possible way is to study the variation of the root number in such a family using ideas from [11].

References

[1] J.E. Cremona, *Algorithms for modular elliptic curves* (Cambridge University Press, Cambridge, 1992).

[2] A. Dąbrowski and J. Pomykała, 'On the order of the Tate-Shafarevich group in a quadratic family of elliptic curves', (submitted).

[3] D. Goldfeld, J. Hoffstein and S.J. Patterson, 'On automorphic functions of half-integral weight with applications to elliptic curves', in *Number Theory Related to Fermat's Last Theorem* (Birkhäuser, Boston, MA, 1982), pp. 153–193.

https://doi.org/10.1017/S0004972700022322 Published online by Cambridge University Press

[4] H. Iwaniec, 'Almost-primes represented by quadratic polynomials', *Invent. Math.* **47** (1978), 171–188.

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

[6] S. Lang, 'Conjectured diophantine estimates on elliptic curves', in *Arithmetic and Geometry - Papers dedicated to I.R. Shafarevich* **1** (Birkhäuser, Boston, MA, 1983), **pp.** 155–171.

[7] D. Lieman, 'Nonvanishing of L-series associated to cubic twists of elliptic curves', *Ann. Math.* **140** (1994), 81–108.

[8] L. Mai and M.R. Murty, 'A note on quadratic twists of an elliptic curve', in *CRM Proc. Lecture Notes* **4** (American Mathematical Society, Providence, RI, 1994), **pp.** 121–124.

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

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

[11] D.E. Rohrlich, 'Variation of the root number in families of elliptic curves', *Compositio Math.* **87** (1993), 119–151.

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

[13] J. Tate, 'Algorithms for determining the type of a singular type in an elliptic pencil', in *Modular Functions of One Variable IV*, Lecture Notes in Mathematics **476** (Springer-Verlag, Berlin, Heidelberg, New York, 1972), **pp.** 33–52.

[14] J. Tunnell, 'A classical diophantine problem and modular forms of weight 3/2', *Invent. Math.* **72** (1983), 323–334.

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/S0004972700022322 Published online by Cambridge University Press