PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 89, Number 3, November 1983

A FAMILY OF SEMISTABLE ELLIPTIC CURVES WITH LARGE TATE-SHAFAREVITCH GROUPS[1]

KENNETH KRAMER

ABSTRACT. We present a family of elliptic curves defined over the rationals $\mathbf{Q}$ such that each curve admits only good or multiplicative reduction and for every integer n there is a curve whose Tate-Shafarevitch group over $\mathbf{Q}$ has more than n elements of order 2. Previously known examples of large Tate-Shafarevitch groups were constructed by forcing many places of additive reduction.

1. Introduction. Let A be an elliptic curve defined over the rational numbers $\mathbf{Q}$ and let $A(\mathbf{Q})$ denote the Mordell-Weil group of points on A with rational coordinates. One obtains a bound for the rank of the finitely generated abelian group $A(\mathbf{Q})$ by a "descent" procedure which amounts to piecing together globally the local information obtained by finding $A(\mathbf{Q}_p)$ for each completion $\mathbf{Q}_p$ of $\mathbf{Q}$, including the Archimedean one. The Tate-Shafarevitch group $Ш(A, \mathbf{Q})$ is defined in Galois cohomology as the kernel of the localization map

$$H^1(\mathbf{Q}, A) \to \prod_p H^1(\mathbf{Q}_p, A)$$

where we let $H^1(K, A) = H^1(\mathrm{Gal}(\bar{K}/K), A(\bar{K}))$ with $\bar{K}$ an algebraic closure of the field K. The group $Ш(A, \mathbf{Q})$ may be thought of as a measure of the error between the actual rank of $A(\mathbf{Q})$ and the bound obtained from all the local information. For the precise statement, see (8).

Cassels [3] first showed that the 3-torsion in $Ш(A, \mathbf{Q})$ can be arbitrarily large, beginning with the curve A whose j-invariant is $j = 0$ and introducing arbitrarily many new places of additive reduction while keeping $j = 0$. Similarly, Bölling [1] has shown that if K is an algebraic number field and if $M(j, K)$ consists of the elliptic curves defined over K with fixed j-invariant equal to j, then

$$\sup\{|Ш(A, K)_2| : A \in M(j, K)\} = \infty$$

where $|Ш(A, K)_2|$ is the order of the kernel of multiplication by 2 on $Ш(A, K)$.

One may ask whether there can be growth in the order of Ш without additive reduction or the phenomenon of "twisting" used above. The purpose of this note is to present such an example. Consider the curve

$$B: Y^2 + XY = X^3 - (16m)X^2 - (8m)X - m \tag{1}$$

Received by the editors February 5, 1982 and, in revised form, March 10, 1983; presented to the Society, March 17, 1982.

1980 *Mathematics Subject Classification.* Primary 14G25, 14K07.

[1] Research partially supported by a grant from the National Science Foundation.

0002-9939/83 $1.00 + $.25 per page

of discriminant $\Delta_B = m(16m + 1)$. The curve B has multiplicative reduction at each prime of bad reduction. Under suitable assumptions on the quadratic characters of the prime factors of $16m + 1$ modulo those of m (see the theorem of §5) we show that

$$\dim Ш(B, \mathbf{Q})_2 \geqslant 2N - 2$$

where N is the number of distinct prime factors of $16m + 1$ and dim is vector space dimension over the 2-element field $\mathbf{F}_2$.

2. Semistability. An elliptic curve A over $\mathbf{Q}$ has a minimal Weierstrass model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

with integral coefficients a_i chosen to minimize the absolute value of the discriminant Δ. The j-invariant is $j = c_4^3/\Delta$ with $c_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4)$. See [**6**] for all such formulae. We begin with a lemma which will be used to guarantee that our examples are semistable curves. That is, for each prime p they admit either good reduction ($p \nmid \Delta$) or multiplicative reduction ($p \mid \Delta$ but $p \nmid c_4$). In case of multiplicative reduction it is necesssary to distinguish between a Tate curve [**6**, Theorem 5] over $\mathbf{Q}_p$ for which the tangents to the node on A modulo p are rational over $\mathbf{F}_p$, and a twisted Tate curve for which the tangents lie in a quadratic extension of $\mathbf{F}_p$.

LEMMA 1. *Let A be an elliptic curve defined over $\mathbf{Q}$ having a height one formal group over $\mathbf{Q}_2$ and a point of order 2 with integral coordinates. Then A has a minimal model over $\mathbf{Z}$ of the form*

$$y^2 + xy = x^3 + a_2x^2 + a_4x \tag{3}$$

with $b_2 = 1 + 4a_2$ and discriminant $\Delta = a_4^2(b_2^2 - 64a_4)$. This model is semistable if and only if g.c.d.$(b_2, a_4) = 1$. *If so, A is a Tate curve over $\mathbf{Q}_p$ if and only if either p divides a_4 and $b_2 \in \mathbf{Q}_p^2$ or p divides $b_2^2 - 64a_4$ and $-2b_2 \in \mathbf{Q}_p^2$. Furthermore all points of order 2 are in $\mathbf{Q}$ if and only if there is an integer m such that $a_4 = (b_2 - 16m)m$.*

PROOF. By translating the integral point of order 2 to $(0, 0)$ we force $a_6 = a_3 = 0$ in the model (2). Since A has height 1 reduction modulo 2, the coefficient a_1 is odd [**6**, (19)] and we may replace y by $y + \frac{1}{2}(a_1 - 1)x$ to obtain a model of the form (3). This assumption guarantees semistability for $p = 2$. Using the fact that A is multiplicative modulo p if and only if p divides Δ but does not divide $c_4 = b_2^2 - 48a_4$ we obtain the criterion g.c.d. $(b_2, a_4) = 1$ for semistability when p is odd. When there is a node modulo p, an easy computation shows that the slopes of the tangents are $\mathbf{F}_p$-rational if and only if $b_2 \in \mathbf{Q}_p^2$ if p divides a_4 or $-2b_2 \in \mathbf{Q}_p^2$ if p divides $b_2^2 - 64a_4$. Finally, given the existence of one rational point of order 2, the others are rational precisely when the discriminant Δ is a square. If $b_2^2 - 64a_4 = t^2$ then the sign of t may be chosen so that 32 divides $b_2 - t$. Hence $b_2 - t = 32m$ and $a_4 = (b_2 - 16m)m$. Conversely, it is clear that Δ is a square when $a_4 = (b_2 - 16m)m$, so that all points of order 2 are rational in that case.

3. Algebraic preliminaries. Suppose for the moment that A is an elliptic curve defined over a field K with $\mathrm{char}(K) \neq 2$, and that A has a rational point T of order 2 defined over K. There is an isogeny $f\colon A \to B$ with kernel $\{0, T\}$ and a dual isogeny $g\colon B \to A$ such that $f \circ g = 2$ and $g \circ f = 2$. From the cohomology of the diagram

$$\begin{array}{ccccccccc} 0 & \to & A(\bar{K})_2 & \to & A(\bar{K}) & \overset{2}{\to} & A(\bar{K}) & \to & 0 \\ & & \downarrow f & & \downarrow f & & \| & & \\ 0 & \to & B(\bar{K})_g & \to & B(\bar{K}) & \underset{g}{\to} & A(\bar{K}) & \to & 0 \end{array}$$

we obtain the commutative diagram below, in which the horizontal arrows are injective:

$$\begin{array}{ccc} A(K)/2A(K) & \overset{\lambda_K}{\to} & H^1(K, A_2) \\ \downarrow & & \downarrow \pi_K \\ A(K)/gB(K) & \underset{\gamma_K}{\to} & H^1(K, B_g) \end{array} \tag{4}$$

If we assume further that all points of order 2 are K-rational, we may obtain for A a model of the form

$$y^2 = (x + t_1)(x + t_2)(x + t_3) \tag{5}$$

with $t_1, t_2, t_3 \in K$ and $T = (-t_1, 0)$. Then $H^1(K, B_g) = K^*/K^{*2}$ and $H^1(K, A_2) = \mathcal{H}/\mathcal{H}^2$ with

$$\mathcal{H} = \left\{(a, b, c) \in \bigoplus_{i=1}^{3} K^*\colon abc \in K^{*2}\right\}. \tag{6}$$

The homomorphism λ_K is induced almost everywhere by the map which sends a point $P = (x, y)$ in $A(K)$ to $(x + t_1, x + t_2, x + t_3)$ in $\mathcal{H}$, and π_K is projection to the first coordinate. These facts may be verified by direct computation as in [**5**, p. 142] or else see [**2**, §2].

4. Local information. Suppose now that A is the curve of Lemma 1, with $a_4 = (b_2 - 16m)m$. It has a model of the form (5) with $t_1 = 0$, $t_2 = 4m$, $t_3 = \frac{1}{4}(b_2 - 16m)$. The following lemma provides a description of the image of $\lambda_p = \lambda_{\mathbf{Q}_p}$ over the local field $\mathbf{Q}_p$. The cases not treated in the lemma can be worked out by the same techniques, but will not be needed later.

LEMMA 2. *Let S_p be the image of $\lambda_p\colon A(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, A_2)$. Let U_p denote the multiplicative group of units of $\mathbf{Q}_p$. Then $S_p = T_p/T_p^2$ where T_p is as follows*:

(i) *If $p \nmid 2\Delta$ then $T_p = \{(a, b, ab)\colon a, b \in U_p\}$.*

(ii) *If $2 \nmid m$ then $T_2 = \{(a, b, ab)\colon a, b \in U_2, ab \equiv 1\ (4)\}$.*

(iii) *If p odd and $p \mid m$ and $b_2 \in \mathbf{Q}_p^2$ then $T_p = \{(a, a, 1)\colon a \in \mathbf{Q}_p^*\}$.*

(iv) *If $p \mid b_2 - 16m$ and if $b_2 \in \mathbf{Q}_p^2$ then $T_p = \{(a, 1, a)\colon a \in \mathbf{Q}_p^*\}$.*

(v) *If $m > 0$ then $T_\infty = \{(a, a, 1)\colon a \in \mathbf{R}\}$.*

PROOF. In case (i) we have good reduction and odd residue characteristic. The result follows for example by [2, Corollary 3.3]. In case (ii), the point of order 2 given by $(-t_3, 0)$ in the model (5) is distinguished by the fact that it reduces to the identity element of $\bar{A}(\mathbf{F}_2)$ so the result follows by [2, Lemma 3.5, Proposition 3.6]. In cases (iii) and (iv), A is a Tate curve over $\mathbf{Q}_p$. We apply [2, Proposition 4.1], noting that the point of order 2 distinguished by the fact that its reduction is nonsingular is $(-t_3, 0)$ in case (iii) and $(-t_2, 0)$ in case (iv). Case (v) is covered by [2, Proposition 3.7] once we observe that if $m > 0$ then $-t_3$ is the smallest root of the cubic on the right side of (5).

REMARK. Since the vertical arrow on the left of diagram (4) is surjective, the image of γ_p is $\pi_p(S_p)$; that is, the projection to $\mathbf{Q}_p^*/\mathbf{Q}_p^{*2}$ of the first coordinate of S_p.

5. The descent. The Selmer group for multiplication by 2 on A over $\mathbf{Q}$ is defined to be

$$S(A/2A) = \left\{ s \in H^1(\mathbf{Q}, A_2) : \operatorname{res}_{\mathbf{Q}/\mathbf{Q}_p}(s) \in \text{Image } \lambda_p \ \forall_p \right\}.$$

It is easy to check that the following sequence is exact:

$$0 \to A(\mathbf{Q})/2A(\mathbf{Q}) \to S(A/2A) \to Ш(A, \mathbf{Q})_2 \to 0. \tag{7}$$

Since the elements of $S(A/2A)$ are unramified almost everywhere (Lemma 2(i)), the Selmer group is finite and by (7)

$$\text{rank } A(\mathbf{Q}) = \dim S(A/2A) - \dim A(\mathbf{Q})_2 - \dim Ш(A, \mathbf{Q})_2. \tag{8}$$

In a similar fashion, the Selmer group for the isogeny g is defined to be

$$S(A/gB) = \left\{ s \in \hat{H}^1(\mathbf{Q}, B_g) : \operatorname{res}_{\mathbf{Q}/\mathbf{Q}_p}(s) \in \text{Image } \gamma_p \ \forall_p \right\}$$

and we obtain the exact sequence

$$0 \to A(\mathbf{Q})/gB(\mathbf{Q}) \to S(A/gB) \to Ш(B, \mathbf{Q})_g \to 0. \tag{9}$$

Since $Ш(B, \mathbf{Q})_2 \supseteq Ш(B, \mathbf{Q})_g$ and $2A(\mathbf{Q}) = g \circ fA(\mathbf{Q}) \subseteq gB(\mathbf{Q})$ we have

$$\begin{aligned} \dim Ш(B, \mathbf{Q})_2 &\geqslant \dim Ш(B, \mathbf{Q})_g = \dim S(A/gB) - \dim A(\mathbf{Q})/gB(\mathbf{Q}) \\ &\geqslant \dim S(A/gB) - \dim A(\mathbf{Q})/2A(\mathbf{Q}) \\ &\geqslant \dim S(A/gB) - \dim S(A/2A) \end{aligned} \tag{10}$$

with the last inequality resulting from (7).

THEOREM. *Let n be a positive integer. One can choose integers $\ell = \ell_1 \cdots \ell_n r$ and $m = m_1 \cdots m_n s$ with the following properties*:

(i) *$\ell_1, \ldots, \ell_n, m_1, \ldots, m_n$ are distinct odd primes with $\ell_i \equiv 1 \pmod 4$ for $1 \leqslant i \leqslant n$,*

(ii) *r and s are positive odd integers and each prime factor of r is $1 \pmod 4$,*

(iii) *$\ell = 16m + 1$,*

(iv) *the Legendre symbols $(m_i/\ell_j) = (-1)^{\delta_{ij}}$ for $1 \leqslant i, j \leqslant n$.*

Let B be the elliptic curve defined over $\mathbf{Q}$ by the model (1), with m as above. Then $\dim Ш(B, \mathbf{Q})_2 \geqslant 2n$.

PROOF. To show that the requisite choices are possible, first select distinct primes $\ell_j \equiv 1 \pmod 4$ for $1 \leqslant j \leqslant n$. Then condition (iv) is satisfied for an arithmetic progression of choices of m_i with common difference $\ell_1 \cdots \ell_n$ from which we can select m_i prime with condition (i) also being satisfied. Among the integers r and s such that

$$\ell_1 \cdots \ell_n r - 16 m_1 \cdots m_n s = 1$$

we can use the fact that $\ell_1 \cdots \ell_n$ is odd to choose s odd and we can make r sufficiently large to guarantee $s > 0$. From the arithmetic progression of possible r's we can always arrange that r is in fact prime (with $r \equiv 1$ (4) forced) to ensure that condition (ii) holds.

Consider the curve A obtained by putting $a_2 = 8m$ and $a_4 = m(16m + 1)$ in (3) to arrive at a model

$$A\colon y^2 + xy = x^3 + (8m)x^2 + m(16m + 1)x \tag{11}$$

with discriminant $\Delta_A = m^2(16m + 1)^2$. By Lemma 1, A is semistable and all of its points of order 2 are defined over $\mathbf{Q}$. There is an isogeny $f\colon A \to B$ whose kernel is generated by the point of order 2 given by $(0, 0)$ on the model (11). Using the model (1) for B, it follows for example from Vélu [**8**] that f is given explicitly by $f(x, y) = (X, Y)$ with

$$X = x + a_4/x + 8m, \qquad Y = y - \big[a_4(x + y)\big]/x^2 - 4m. \tag{12}$$

The curve A satisfies the conditions of §4, so that Lemma 2 and the subsequent remark can be applied to determine the Selmer group $S(A/gB)$ as follows. Let $\mathfrak{L}$ (resp. $\mathfrak{M}$) be the set of primes dividing $\ell = 16m + 1$ (resp. m). Then $\mathfrak{L} \cup \mathfrak{M}$ contains precisely the primes of bad reduction for A. Clearly $b_2 = 1 + 32m = 2\ell - 1$ is a square modulo each of these primes, using the fact that $p \equiv 1 \pmod 4$ for $p \in \mathfrak{L}$. It follows that viewed as a subgroup of $\mathbf{Q}^*/\mathbf{Q}^{*2}$, $S(A/gB)$ is generated by the cosets of -1 and the primes in $\mathfrak{L} \cup \mathfrak{M}$. Hence $\dim S(A/gB) = |\mathfrak{L}| + |\mathfrak{M}| + 1$.

We now find an upper bound for $\dim S(A/2A)$. Viewed as a subgroup of $\mathcal{K}/\mathcal{K}^2$ as in (6), $S(A/2A)$ is contained in the span of the cosets of $(-1, -1, 1)$ and

$$\{v_p = (p, 1, p)\colon p \in \mathfrak{L}\} \cup \{w_q = (q, q, 1)\colon q \in \mathfrak{M}\}.$$

However, further descent criteria apply on the second and third coordinates; namely, for an element

$$s = (-1, -1, 1)^{\varepsilon(\infty)} \prod_{p \in \mathfrak{L}} v_p^{\varepsilon(p)} \prod_{q \in \mathfrak{M}} w_q^{\varepsilon(q)}$$

to represent a coset in $S(A/2A)$ it is necessary and sufficient that all of the following hold:

$$(\mathrm{a}_p) \qquad (-1)^{\varepsilon(\infty)} \prod_{q \in \mathfrak{M}} q^{\varepsilon(q)} \in \mathbf{Q}_p^2 \quad \text{for all } p \in \mathfrak{L},$$

$$(\mathrm{b}_q) \qquad \prod_{p \in \mathfrak{L}} p^{\varepsilon(p)} \in \mathbf{Q}_q^2 \quad \text{for all } q \in \mathfrak{M}.$$

By considering the equations (a_p) for $p = \ell_i$ with $1 \leqslant i \leqslant n$ and using condition (iv) of the theorem we find n independent equations over $\mathbf{F}_2$ of the form

$$\varepsilon(m_i) + \sum_{q \in \mathfrak{M}'} c_{iq}\varepsilon(q) = 0, \qquad 1 \leqslant i \leqslant n,$$

where $\mathfrak{M}' = \mathfrak{M} - \{m_1, \ldots, m_n\}$. From the equations (b_q) for $q = m_i$ with $1 \leqslant i \leqslant n$ we obtain n additional independent equations of the form

$$\varepsilon(\ell_i) + \sum_{p \in \mathfrak{L}'} d_{ip}\varepsilon(p) = 0, \qquad 1 \leqslant i \leqslant n,$$

where $\mathfrak{L}' = \mathfrak{L} - \{\ell_1, \ldots, \ell_n\}$. Hence $\dim S(A/2A) \leqslant |\mathfrak{M}| + |\mathfrak{L}| + 1 - 2n$ and by (10), $\dim Ш(B, \mathbf{Q})_2 \geqslant 2n$ as desired.

REMARK. If r is in fact chosen to be prime, then $\dim Ш(B, \mathbf{Q})_2 \geqslant 2N - 2$, where N is the number of prime factors of $16m + 1$, as claimed in the introduction.

LEMMA 3. *Let A be the curve* (11) *and B the isogenous curve* (1). *Assume only that m is a positive odd integer. Then the torsion subgroups of A and B are $A(\mathbf{Q})_{\text{tor}} = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ and $B(\mathbf{Q})_{\text{tor}} = \mathbf{Z}/2\mathbf{Z}$.*

PROOF. It is easy to check that $|\bar{A}(\mathbf{F}_2)| = 4$. It follows from [**6**, Theorem 3, Corollary 1] that reduction mod p is injective on torsion points of order prime to p at places of good reduction. Hence $A(\mathbf{Q})$ has only 2-power torsion. Now A has a model of the form (5) in which the points of order 2 are $(-t_i, 0)$ with $t_1 = 0$, $t_2 = 4m$, $t_3 = \frac{1}{4}(16m + 1)$. By applying the map $\lambda_{\mathbf{Q}}$ of diagram (4) we see that none of these points is in $2A(\mathbf{Q})$. It follows that $A(\mathbf{Q})_{\text{tor}} = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Because A and B are isogenous via an isogeny of degree 2, $B(\mathbf{Q})$ also has only 2-power torsion. Now $(-1/4, 1/8)$ is easily seen to be the only point of order 2 in $B(\mathbf{Q})$ on the model (1) because for example $\Delta_B = m(16m + 1)$ cannot be a square by elementary number theory. Moreover, $B(\mathbf{Q})$ cannot contain a point P of order 4. Otherwise, $2P = (-1/4, 1/8) = f(-t_i, 0)$ for $i = 2, 3$. Hence at least one of the points $(-t_i, 0)$ would have to be in $gB(\mathbf{Q})$. But this is impossible because the map $\gamma_{\mathbf{Q}}$ of diagram (4) is not trivial at these points. Hence $B(\mathbf{Q})_{\text{tor}} = \mathbf{Z}/2\mathbf{Z}$ as claimed.

EXAMPLE. The inequality in the theorem may be exact. Consider for example the case with $m = 9$, $m_1 = 3$, $\ell = 145$, $\ell_1 = 5$, $n = 1$. Then

$$\dim S(A/2A) \leqslant |\mathfrak{M}| + |\mathfrak{L}| + 1 - 2n = 2.$$

But $\dim A(\mathbf{Q})_2 = 2$. Hence $Ш(A, \mathbf{Q})_2$ is trivial and $\operatorname{rank} A(\mathbf{Q}) = 0$ by (8). It follows from Lemma 3 that

$$A(\mathbf{Q})/gB(\mathbf{Q}) = A(\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

Since $\dim S(A/gB) = |\mathfrak{M}| + |\mathfrak{L}| + 1 = 4$ we have $\dim Ш(B, \mathbf{Q})_g = 2$ by (9). In general,

$$0 \to Ш(B, \mathbf{Q})_g \to Ш(B, \mathbf{Q})_2 \xrightarrow{g} Ш(A, \mathbf{Q})_f$$

is exact. But $Ш(A, \mathbf{Q})_f \subseteq Ш(A, \mathbf{Q})_2 = \{0\}$. Hence $Ш(B, \mathbf{Q})_g = Ш(B, \mathbf{Q})_2$ is 2 dimensional, as desired.

6. Implications of the conjectures of Birch and Swinnerton-Dyer. It is interesting to examine some consequences of the conjectures of Birch and Swinnerton-Dyer in the situation studied above. For an elliptic curve E with discriminant Δ in minimal form (2) over $\mathbf{Z}$, let $w = dx/(2y + a_1x + a_3)$ and define $\alpha = \int_{E(\mathbf{R})} |w|$. Let $E_0(\mathbf{Q}_p)$ be the subgroup of $E(\mathbf{Q}_p)$ consisting of points whose reduction modulo p is nonsingular and define $c_p = [E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$. It is conjectured that the L-series $L(E, s)$ for E over $\mathbf{Q}$ has an analytic continuation to the complex plane and that

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\alpha \cdot \prod_{p|\Delta} c_p \cdot R(E,\mathbf{Q}) \cdot |Ш(E,\mathbf{Q})|}{|E(\mathbf{Q})_{\text{tor}}|^2}$$

where r is the rank of $E(\mathbf{Q})$ and $R(E, \mathbf{Q})$ is a "regulator" which involves the height pairing on a set of generators for $E(\mathbf{Q})$ modulo torsion. See [**6**, §8] for more details and further references.

Isogenous curves A and B over $\mathbf{Q}$ have the same rank and L-function. One might therefore expect to be able to compare the orders of their Tate-Shafarevitch groups as predicted by the above conjecture. In fact, Cassels [**4**, Theorem 1.3] has shown unconditionally that

$$(13)\quad |Ш(B,\mathbf{Q})| = |Ш(A,\mathbf{Q})| \cdot \frac{|B(\mathbf{Q})/fA(\mathbf{Q})|}{|A(\mathbf{Q})/gB(\mathbf{Q})|} \cdot \frac{|B(\mathbf{Q})_g|}{|A(\mathbf{Q})_f|} \cdot \frac{\alpha(A)}{\alpha(B)} \cdot \prod_{p|\Delta} \frac{c_p(A)}{c_p(B)}$$

in the sense that if either Tate-Shafarevitch group is finite, then so is the other and (13) holds. If in particular $g \circ f = 2$, we have the exact sequence

$$0 \to A(\mathbf{Q})_f \to A(\mathbf{Q})_2 \xrightarrow{f} B(\mathbf{Q})_g \to B(\mathbf{Q})/fA(\mathbf{Q}) \xrightarrow{g} A(\mathbf{Q})/2A(\mathbf{Q}) \to A(\mathbf{Q})/gB(\mathbf{Q}) \to 0.$$

Furthermore, $|A(\mathbf{Q})/2A(\mathbf{Q})| = 2^r |A(\mathbf{Q})_2|$ and $|A(\mathbf{Q})_f| = |B(\mathbf{Q})_g| = 2$. It follows that

$$2^{r+2}|Ш(B,\mathbf{Q})| = |Ш(A,\mathbf{Q})| \cdot |B(\mathbf{Q})/fA(\mathbf{Q})|^2 \cdot \frac{\alpha(A)}{\alpha(B)} \cdot \prod_{p|\Delta} \frac{c_p(A)}{c_p(B)}.$$

It is easy to see that the models (1) and (11) above are minimal using for example an algorithm of Tate [**7**, p. 47, case 2]. It follows from this algorithm or from the parametrization by p-adic theta functions [**6**, Theorem 5] that $c_p = \text{ord}_p(\Delta)$. But $\Delta_A = \Delta_B^2$. Hence $c_p(A) = 2c_p(B)$ for all $p | \Delta$. By consideration of continuity and the images of the points of order 2, the isogeny f: $A(\mathbf{R}) \to B(\mathbf{R})$ is a double covering. It follows, using the change of variables given by (12), that $\alpha(A) = 2\alpha(B)$. Therefore, for the curves A and B given by (11) and (1) we have

$$2^{r+2}|Ш(B,\mathbf{Q})| \geq 2^{D+1}|Ш(A,\mathbf{Q})|$$

where D is the number of distinct primes dividing Δ_A or Δ_B. This gives an indication that the rank of $B(\mathbf{Q})$ combined with the order of the 2-primary component of $Ш(B, \mathbf{Q})$ grows with the number of places of bad reduction. This result is of course weaker than the theorem of §5.

It would be interesting to examine the order of $Ш(E, \mathbf{Q})_2$ when the number of places of bad reduction for E is limited. For curves of prime conductor $p < 1000$ the

descent in [2] shows that $Ш(E, \mathbf{Q})_2 = 0$. Note that this descent also shows that the curves of conductor 443 treated in [2, Example 2, p. 739] in fact have $Ш_2 = 0$, contrary to the remark in that example.

REFERENCES

1. R. Bölling, *Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig gross werden*, Math. Nachr. **67** (1975), 157–179.

2. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. (4) **44** (1977), 715–743.

3. J. W. S. Cassels, *Arithmetic on curves of genus* 1 (VI). *The Tate-Šafarevič group can be arbitrarily large*, J. Reine Angew. Math. **214/215** (1964), 65–70.

4. _____, *Arithmetic on curves of genus* 1 (VIII). *On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.

5. L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969.

6. J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

7. _____, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Lecture Notes in Math., vol. 476, Springer, Berlin and New York, 1975, pp. 33–52.

8. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A **273** (1971), 238–241.

DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE (CUNY), FLUSHING, NEW YORK 11367