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

KENNETH KRAMER

Abstract. We present a family of elliptic curves defined over the rationals \( \mathbb{Q} \) such that each curve admits only good or multiplicative reduction and for every integer \( n \) there is a curve whose Tate-Shafarevitch group over \( \mathbb{Q} \) 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 \( \mathbb{Q} \) and let \( A(\mathbb{Q}) \) 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 \( A(\mathbb{Q}) \) by a "descent" procedure which amounts to piecing together globally the local information obtained by finding \( A(\mathbb{Q}_p) \) for each completion \( \mathbb{Q}_p \) of \( \mathbb{Q} \), including the Archimedean one. The Tate-Shafarevitch group \( \text{III}(A, \mathbb{Q}) \) is defined in Galois cohomology as the kernel of the localization map

\[
H^1(\mathbb{Q}, A) \rightarrow \prod_{p} H^1(\mathbb{Q}_p, A)
\]

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

Cassels [3] first showed that the 3-torsion in \( \text{III}(A, \mathbb{Q}) \) 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, Bolling [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

\[
\sup \{|\text{III}(A, K)_2|: A \in M(j, K)\} = \infty
\]

where \( |\text{III}(A, K)_2| \) is the order of the kernel of multiplication by 2 on \( \text{III}(A, K) \).

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

\[
B: Y^2 + XY = X^3 - (16m)X^2 - (8m)X - m
\]
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

$$\dim \text{III}(B, \mathbb{Q})_2 \geq 2N - 2$$

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

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with integral coefficients $a_i$ chosen to minimize the absolute value of the discriminant $\Delta$. The $j$-invariant is $j = c_4^3/\Delta$ with $c_4 = (a_1^2 + 4a_2)^3 - 24(a_1a_3 + 2a_4)$. 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 $p \not| c_4$). In case of multiplicative reduction it is necessary to distinguish between a Tate curve [6, Theorem 5] over $\mathbb{Q}_p$ for which the tangents to the node on $A$ modulo $p$ are rational over $\mathbb{F}_p$, and a twisted Tate curve for which the tangents lie in a quadratic extension of $\mathbb{F}_p$.

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

$$y^2 + xy = x^3 + a_2x^2 + a_4x$$

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 $\mathbb{Q}_p$ if and only if either $p$ divides $a_4$ and $b_2 \in \mathbb{Q}_p^2$ or $p$ divides $b_2^2 - 64a_4$ and $-2b_2 \in \mathbb{Q}_p^2$. Furthermore all points of order 2 are in $\mathbb{Q}$ 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 $\Delta$ 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 $\mathbb{F}_p$-rational if and only if $b_2 \in \mathbb{Q}_p^2$ if $p$ divides $a_4$ or $-2b_2 \in \mathbb{Q}_p^2$ 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 $\Delta$ 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 $\Delta$ 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 \( \text{char}(K) \neq 2 \), and that \( A \) has a rational point \( T \) of order 2 defined over \( K \). There is an isogeny \( f: A \to B \) with kernel \( \{0, T\} \) and a dual isogeny \( g: B \to A \) such that \( f \circ g = 2 \) and \( g \circ f = 2 \). From the cohomology of the diagram

\[
\begin{array}{c}
0 & \to & A(\overline{K})_2 & \to & A(\overline{K}) & \to & A(\overline{K}) & \to & 0 \\
\downarrow f & & \downarrow f & & \| & & \| & & \\
0 & \to & B(\overline{K})_g & \to & B(\overline{K}) & \to & A(\overline{K}) & \to & 0
\end{array}
\]

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

\[
\begin{array}{c}
A(K)/2A(K) & \xrightarrow{\lambda_K} & H^1(K, A_2) \\
\downarrow & & \downarrow \pi_K \\
A(K)/gB(K) & \xrightarrow{\gamma_K} & H^1(K, B_g)
\end{array}
\]

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

\[
y^2 = (x + t_1)(x + t_2)(x + t_3)
\]

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

\[
\mathfrak{X} = \left\{ (a, b, c) \in \bigoplus_{i=1}^{3} K^*: abc \in K^{*2} \right\}.
\]

The homomorphism \( \lambda_K \) 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 \( \mathfrak{X} \), and \( \pi_K \) 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 \( \lambda_p = \lambda_{\mathbb{Q}_p} \) over the local field \( \mathbb{Q}_p \). 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 \( \lambda_p: A(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, A_2) \). Let \( U_p \) denote the multiplicative group of units of \( \mathbb{Q}_p \). Then \( S_p = T_p/T_p^2 \) where \( T_p \) is as follows:

(i) If \( p \nmid 2A \) then \( T_p = \{(a, b, ab): a, b \in U_p\} \).

(ii) If \( 2 \mid m \) then \( T_p = \{(a, b, ab): a, b \in U_2, ab \equiv 1 \pmod{4}\} \).

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

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

(v) If \( m > 0 \) then \( T_0 = \{(a, a, 1): a \in \mathbb{R}\} \).
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 \(\overline{A}(F_2)\) so the result follows by [2, Lemma 3.5, Proposition 3.6]. In cases (iii) and (iv), \(A\) is a Tate curve over \(\mathbb{Q}_p\). 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 \(\gamma_p\) is \(\pi_p(S_p)\); that is, the projection to \(\mathbb{Q}_p^*/\mathbb{Q}_p^{2}\) of the first coordinate of \(S_p\).

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

\[
S(A/2A) = \{ s \in H^1(\mathbb{Q}, A_2) : \text{res}_{\mathbb{Q}/\mathbb{Q}_p}(s) \in \text{Image}_p \forall_p \}.
\]

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

\[
0 \to A(\mathbb{Q})/2A(\mathbb{Q}) \to S(A/2A) \to \mathbb{III}(A, \mathbb{Q})_2 \to 0.
\]

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

\[
\text{rank } A(\mathbb{Q}) = \dim S(A/2A) - \dim A(\mathbb{Q})_2 - \dim \mathbb{III}(A, \mathbb{Q})_2.
\]

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

\[
S(A/gB) = \{ s \in H^1(\mathbb{Q}, B_2) : \text{res}_{\mathbb{Q}/\mathbb{Q}_p}(s) \in \text{Image}_p \forall_p \}
\]

and we obtain the exact sequence

\[
0 \to A(\mathbb{Q})/gB(\mathbb{Q}) \to S(A/gB) \to \mathbb{III}(B, \mathbb{Q})_g \to 0.
\]

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

\[
\dim \mathbb{III}(B, \mathbb{Q})_2 \geq \dim \mathbb{III}(B, \mathbb{Q})_g = \dim S(A/gB) - \dim A(\mathbb{Q})/gB(\mathbb{Q})
\]

\[
\geq \dim S(A/gB) - \dim A(\mathbb{Q})/2A(\mathbb{Q})
\]

\[
\geq \dim S(A/gB) - \dim S(A/2A)
\]

with the last inequality resulting from (7).

Theorem. Let \(n\) be a positive integer. One can choose integers \(a = a_1 \cdots a_n r\) and \(m = m_1 \cdots m_n s\) with the following properties:

(i) \(a_1, \ldots, a_n, m_1, \ldots, m_n\) are distinct odd primes with \(a_i \equiv 1 \pmod{4}\) for \(1 \leq i \leq n\),

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

(iii) \(a = 16m + 1\),

(iv) the Legendre symbols \((m_i/a_i) = (-1)^{s_i}\) for \(1 \leq i, j \leq n\).

Let \(B\) be the elliptic curve defined over \(\mathbb{Q}\) by the model (1), with \(m\) as above. Then \(\dim \mathbb{III}(B, \mathbb{Q})_2 \geq 2n\).
Proof. To show that the requisite choices are possible, first select distinct primes \( f_j \equiv 1 \pmod{4} \) for \( 1 \leq j \leq n \). Then condition (iv) is satisfied for an arithmetic progression of choices of \( m_i \) with common difference \( f_1 \cdots f_n \), from which we can select \( m_i \) prime with condition (i) also being satisfied. Among the integers \( r \) and \( s \) such that

\[
f_1 \cdots f_n r - 16m_1 \cdots m_n s = 1
\]

we can use the fact that \( f_1 \cdots f_n \) 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 \( r \equiv 1 \pmod{4} \) 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

\[
A: y^2 + xy = x^3 + (8m)x^2 + m(16m + 1)x
\]

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 \( \mathbb{Q} \). There is an isogeny \( f: A \to B \) 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 Vêlu [8] that \( f \) is given explicitly by

\[
f(x, y) = (X, Y) \text{whh}
\]

\[
X = x + a_4/x + 8m, \quad Y = y - \left[ a_4(x + y) \right]/x^2 - 4m.
\]

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 \( \mathcal{L} \) (resp. \( \mathcal{M} \)) be the set of primes dividing \( \ell = 16m + 1 \) (resp. \( m \)). Then \( \mathcal{L} \cup \mathcal{M} \) 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 \( p \in \mathcal{L} \). It follows that viewed as a subgroup of \( \mathbb{Q}^*/\mathbb{Q}^{*2} \), \( S(A/gB) \) is generated by the cosets of \(-1\) and the primes in \( \mathcal{L} \cup \mathcal{M} \). Hence \( \dim S(A/gB) = |\mathcal{L}| + |\mathcal{M}| + 1 \).

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

\[
\{v_p = (p, 1, p): p \in \mathcal{L}\} \cup \{w_q = (q, q, 1): q \in \mathcal{M}\}.
\]

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

\[
s = (-1, -1, 1)^{e_2(\infty)} \prod_{p \in \mathcal{L}} v_p^{e_p(p)} \prod_{q \in \mathcal{M}} w_q^{e_q(q)}
\]

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

\[
(a_p) \quad (-1)^{e_2(\infty)} \prod_{q \in \mathcal{M}} q^{e_q(q)} \in \mathbb{Q}_p^2 \quad \text{for all } p \in \mathcal{L},
\]

\[
(b_q) \quad \prod_{p \in \mathcal{L}} p^{e_p(p)} \in \mathbb{Q}_q^2 \quad \text{for all } q \in \mathcal{M}.
\]
By considering the equations \((a_p)\) for \(p = \ell_i\) with \(1 \leq i \leq n\) and using condition (iv) of the theorem we find \(n\) independent equations over \(\mathbb{F}_2\) of the form
\[
\varepsilon(m_i) + \sum_{q \in \mathbb{M}} c_{iq} \varepsilon(q) = 0, \quad 1 \leq i \leq n,
\]
where \(\mathbb{M}' = \mathbb{M} - \{m_1, \ldots, m_n\}\). From the equations \((b_q)\) for \(q = m_i\) with \(1 \leq i \leq n\) we obtain \(n\) additional independent equations of the form
\[
\varepsilon(\ell_i) + \sum_{p \in \mathbb{L}} d_{ip} \varepsilon(p) = 0, \quad 1 \leq i \leq n,
\]
where \(\mathbb{L}' = \mathbb{L} - \{\ell_1, \ldots, \ell_n\}\). Hence \(\text{dim } S(A/2A) \leq |\mathbb{M}| + |\mathbb{L}| + 1 - 2n\) and by (10), \(\text{dim } \text{III}(B, Q)_2 \geq 2n\) as desired.

**Remark.** If \(r\) is in fact chosen to be prime, then \(\text{dim } \text{III}(B, Q)_2 \geq 2N - 2\), 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 \(A(Q)_{\text{tor}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\) and \(B(Q)_{\text{tor}} = \mathbb{Z}/2\mathbb{Z}\).

**Proof.** It is easy to check that \(|\overline{A}(F_2)| = 4\). 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 \(A(Q)\) has only 2-power torsion. Now \(A\) has a model of the form (5) in which the points of order 2 are \((-t_1,0)\) with \(t_1 = 0\), \(t_2 = 4m\), \(t_3 = \frac{1}{4}(16m + 1)\). By applying the map \(\lambda_Q\) of diagram (4) we see that none of these points is in \(2A(Q)\). It follows that \(A(Q)_{\text{tor}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\).

Because \(A\) and \(B\) are isogenous via an isogeny of degree 2, \(B(Q)\) also has only 2-power torsion. Now \((-1/4, 1/8)\) is easily seen to be the only point of order 2 in \(B(Q)\) on the model (1) because for example \(\Delta_B = m(16m + 1)\) cannot be a square by elementary number theory. Moreover, \(B(Q)\) 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 \(gB(Q)\). But this is impossible because the map \(\gamma_Q\) of diagram (4) is not trivial at these points. Hence \(B(Q)_{\text{tor}} = \mathbb{Z}/2\mathbb{Z}\) 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
\[
\text{dim } S(A/2A) \leq |\mathbb{M}| + |\mathbb{L}| + 1 - 2n = 2.
\]
But \(\text{dim } A(Q)_2 = 2\). Hence \(\text{III}(A, Q)_2\) is trivial and \(\text{rank } A(Q) = 0\) by (8). It follows from Lemma 3 that
\[
A(Q)/gB(Q) = A(Q) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.
\]
Since \(\text{dim } S(A/gB) = |\mathbb{M}| + |\mathbb{L}| + 1 = 4\) we have \(\text{dim } \text{III}(B, Q)_g = 2\) by (9). In general,
\[
0 \to \text{III}(B, Q)_g \to \text{III}(B, Q)_2 \to \text{III}(A, Q)_f
\]
is exact. But \(\text{III}(A, Q)_f \subseteq \text{III}(A, Q)_2 = \{0\}\). Hence \(\text{III}(B, Q)_g = \text{III}(B, Q)_2\) 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 \( \Delta \) in minimal form (2) over \( \mathbb{Z} \), let \( w = dx/(2y + ax^3 + a_3) \) and define \( \alpha = \int_{E(\mathbb{R})} w \). Let \( E_0(\mathbb{Q}_p) \) be the subgroup of \( E(\mathbb{Q}_p) \) consisting of points whose reduction modulo \( p \) is nonsingular and define \( c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)] \). It is conjectured that the \( L \)-series \( L(E, s) \) for \( E \) over \( \mathbb{Q} \) has an analytic continuation to the complex plane and that

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

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

Isogenous curves \( A \) and \( B \) over \( \mathbb{Q} \) 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

\[
|\Sha(B, \mathbb{Q})| = |\Sha(A, \mathbb{Q})| \cdot \frac{|\Sha(\mathbb{Q})|}{|\Sha(\mathbb{Q})_g|} \cdot \frac{|\Sha(\mathbb{Q})/\mathbb{Q}|}{|\Sha(\mathbb{Q})/\mathbb{Q}^g|} \cdot \frac{\alpha(A)}{\alpha(B)} \cdot \prod_{p|\Delta} \frac{c_p(A)}{c_p(B)}
\]

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

\[
0 \to A(\mathbb{Q})_f \to A(\mathbb{Q})_2 \to B(\mathbb{Q})_g \to B(\mathbb{Q})/fA(\mathbb{Q}) \to A(\mathbb{Q})/2A(\mathbb{Q}) \to A(\mathbb{Q})/gB(\mathbb{Q}) \to 0.
\]

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

\[
2^{r+2} |\Sha(B, \mathbb{Q})| = |\Sha(A, \mathbb{Q})| \cdot |\Sha(\mathbb{Q})/fA(\mathbb{Q})|^2 \cdot \frac{\alpha(A)}{\alpha(B)} \cdot \prod_{p|\Delta} \frac{c_p(A)}{c_p(B)}.
\]

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 \( \Delta_A = \Delta_B \). Hence \( c_p(A) = 2^a c_p(B) \) for all \( p \mid \Delta \). By consideration of continuity and the images of the points of order 2, the isogeny \( f: A(\mathbb{R}) \to B(\mathbb{R}) \) 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

\[
2^{r+2} |\Sha(B, \mathbb{Q})| \geq 2^{D+1} |\Sha(A, \mathbb{Q})|
\]

where \( D \) is the number of distinct primes dividing \( D_A \) or \( D_B \). This gives an indication that the rank of \( B(\mathbb{Q}) \) combined with the order of the 2-primary component of \( \Sha(B, \mathbb{Q}) \) 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 \( \Sha(E, \mathbb{Q})_2 \) 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 $\III(E, \mathbb{Q})_2 = 0$. Note that this descent also shows that the curves of conductor 443 treated in [2, Example 2, p. 739] in fact have $\III_2 = 0$, contrary to the remark in that example.

REFERENCES


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