ACTA ARITHMETICA
131.1 (2008)

Approximating algebraic numbers by j-invariants of elliptic curves

by

Patrick Ingram (Toronto)

Consider elliptic curves of the form $E_{A,B} : y^2 = x^3 + Ax + B$, where A and B are integers. It was demonstrated by Bennett and the author in [2] that for any fixed $\varepsilon > 0$, all but finitely many curves of this form with a rational point of order at least 5 satisfy

$$|A| \leq |B|^{1+\varepsilon}.$$

Notice that if $E_{A,B}$ is a curve whose coefficients are large and do not satisfy the above inequality, then the j-invariant

$$j(E_{A,B}) = 1728\left(\frac{4A^3}{4A^3 + 27B^2}\right)$$

is very close to 1728. Viewed in another light, then, this result says that $j(E_{A,B})$ cannot be "too close" to 1728 (relative to the sizes of A and B) if $E_{A,B}(\mathbb{Q})$ contains a torsion point of order at least 5. In [5], the author proved similar results bounding $|B|$ by a power of $|A|$, again for $E_{A,B}$ with certain torsion/isogeny structure. One may similarly view these results as saying that $j(E_{A,B})$ cannot be "too close" to 0 for curves $E_{A,B}$ with given torsion structure. This prompts us to formulate here a general result on the approximation of a fixed algebraic number by the j-invariants of elliptic curves with certain torsion structure. The main results are stated over arbitrary number fields and contain, as special cases, most of the results in [2, 5].

It is easy to show that for each N,

$$\{j(E) : E/\mathbb{Q} \text{ admits a rational } N\text{-isogeny}\}$$

is either empty or dense in $\mathbb{Q}$. When one has a dense subset of a larger set of numbers, one might ask how well elements in the larger set may be

2000 *Mathematics Subject Classification*: 11G05, 11J68.

Key words and phrases: elliptic curve, j-invariant.

The author was supported in part by a grant from NSERC of Canada.

approximated by members of the smaller set. Fixing $\varepsilon > 0$, our main result (applied to $\mathbb{Q}$) states that if r is a fixed rational number other than 0 or 1728, and $p/q = j(E)$ for an elliptic curve $E/\mathbb{Q}$ admitting a non-trivial $\mathbb{Q}$-rational isogeny, then

$$|r - p/q| \geq q^{-2/3-\varepsilon},$$

with at most finitely many exceptional values of p/q. If $p/q = j(E)$ for an elliptic curve $E/\mathbb{Q}$ admitting a $\mathbb{Q}$-rational isogeny of degree at least 4 or 6, respectively, we have in addition

$$|1728 - p/q| > q^{-2/3-\varepsilon} \quad \text{and} \quad |p/q| > q^{-3/4-\varepsilon},$$

respectively, again with at most finitely many exceptions. The proof of the general result uses three pillars of diophantine approximation, namely Roth's theorem, Siegel's theorem, and Faltings' theorem; as these results are available over number fields, ours will be too.

Although the results of [2, 5] focus on the archimedean absolute value, the tools used have p-adic analogues and, making use of these, we may provide local versions of the above results. For example, it is shown in Section 3 that for any finite set of primes S there are, up to quadratic twisting, at most finitely many elliptic curves $E_{A,B}$ with $A, B \in \mathbb{Z}$ admitting $\mathbb{Q}$-isogenies of degree at least 4 such that B is an S-unit. As twisting by an S-unit will produce another curve with the same properties, the qualifier "up to twisting" is crucial.

Our notation is, in general, selected to coincide with [8]. If $K/\mathbb{Q}$ is a number field, then we let M_K denote the set of standard absolute values on K, and for $v \in M_K$, we let n_v denote the local degree $[K_v : \mathbb{Q}_v]$ (where K_v and $\mathbb{Q}_v$ are the completions of K and $\mathbb{Q}$ at v). The absolute value corresponding to $v \in M_K$ will be normalized so that $|\cdot|_v$ extends $|\cdot|_p^{n_v}$ if p is the prime above v, for non-archimedean valuations, or $|\cdot|^{n_v}$ for archimedean ones. As such, we define the K-height of

$$P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$$

by

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}$$

and, when $x \in K$, we will use $H_K(x)$ as an abbreviation of $H_K([x, 1])$. If $a/b \in \mathbb{Q}$ is a fraction in lowest terms, this corresponds to our usual conception of height:

$$H_{\mathbb{Q}}(a/b) = \max\{|a|, |b|\}.$$

For convenience, we will also identify the non-archimedean absolute values in M_K with the primes which define them.

THEOREM 1. *Let $N \geq 2$ and $\varepsilon > 0$. Fix a number field $K/\mathbb{Q}$, a finite set of places $S \subseteq M_K$ containing all infinite places, and some $r \in K$. Then unless*

$$(N, r) \in \{(2, 1728), (3, 1728), (2, 0), (3, 0), (4, 0), (5, 0)\},$$

there is a constant $\mu_0 = \mu_0(N, r) < 1$ such that for every elliptic curve E/K admitting a K-rational isogeny of degree N, either $j(E) = r$ or

$$\prod_{v \in S} \min\{|r - j(E)|_v, 1\} \gg H_K(j(E))^{-\mu_0 - \varepsilon}.$$

Here the implied constant depends only on N, ε, and r. Furthermore, we may take $\mu_0 = 0$ if $X_0(N)$ has positive genus, and $\varepsilon = 0$ if this genus is at least 2.

In fact, when $X_0(N)$ has genus 0, we may take

$$\mu_0(N, r) = \frac{2e_r}{N \prod_{p|N}(1 + 1/p)}, \quad \text{where} \quad e_r = \begin{cases} 3 & \text{if } r = 0, \\ 2 & \text{if } r = 1728, \\ 1 & \text{otherwise.} \end{cases}$$

Notice that, as $X_0(N)$ has genus 0 for only finitely many values of N, we may make a uniform statement on the approximation of a fixed r by an elliptic curve with any non-trivial isogeny (excepting the cases excluded in the theorem).

It is worth noting that, for $x, y \in K$ and $v \in M_K$,

$$\prod_{v \in S} |y - x|_v \gg H_K(x)^{-1}$$

rather trivially, so the substance of the result is that $\mu_0 < 1$. Indeed, the inequality in the theorem holds as well in the exceptional cases listed, but in these cases $\mu_0(N, r) \geq 1$, and so the trivial bound supersedes the bound above. For simplicity in the statements of later results, we set $\mu_0(N, r) = 1$ for the exceptional cases mentioned in the theorem.

Theorem 1, of course, implies results for j-invariants of curves with K-rational points of order N, as each such curve admits the K-rational isogeny (of degree N) which annihilates the point of order N (explicit formulae for such an isogeny may be found in [10]). In general, however, the existence of torsion affords us something slightly stronger.

THEOREM 2. *Let $N \geq 2$ and $\varepsilon > 0$. Fix a number field $K/\mathbb{Q}$, a finite set of places $S \subseteq M_K$ containing all infinite places, and some $r \in K$. Then unless*

$$(N, r) \in \{(2, 1728), (3, 1728), (2, 0), (3, 0), (4, 0)\},$$

there is a constant $\mu_1 = \mu_1(N, r) < 1$ such that for every elliptic curve E/K

with a K-rational point of order N, either $j(E) = r$ or

$$\prod_{v\in S} \min\{|r - j(E)|_v, 1\} \gg H_K(j(E))^{-\mu_1-\varepsilon},$$

where the implied constant depends only on N, ε, and r. Furthermore, we may take $\mu_1 = 0$ if $X_1(N)$ has positive genus, and $\varepsilon = 0$ if this genus is at least 2.

When $X_1(N)$ has genus 0, we may take

$$\mu_1(N,r) = \begin{cases} 2e_r/3 & \text{if } N = 2, \\ \dfrac{4e_r}{N^2\prod_{p|N}(1-1/p^2)} & \text{otherwise,} \end{cases}$$

where e_r is as above. Again, we will set $\mu_1(N,r) = 1$ in the exceptional cases.

The gist of the proof of the main result is as follows. Let K be a number field, C/K a non-singular curve, and $\mathcal{E} \to C$ an elliptic surface over K (see [9]). For each $t \in C$ such that the fibre $\mathcal{E}_t$ of $\mathcal{E}$ above t is non-singular, let $j_{\mathcal{E}}(t) = j(\mathcal{E}_t)$. Then the map $j_{\mathcal{E}}$ extends to a morphism $j_{\mathcal{E}} : C \to \mathbb{P}^1$. The question of how well a value $j_{\mathcal{E}}(t)$, for $t \in C(K)$, approximates some $r \in \mathbb{P}^1(K)$ can be lifted to an approximation question on C, namely how well t approximates the preimages of r by $j_{\mathcal{E}}$, which are points in $C(L)$ for some algebraic extension L/K depending on r. So we may apply Roth's theorem, Siegel's theorem, or Faltings' theorem depending on the genus of C. Theorem 1 is deduced in this way, with $C = X_0(N)$ and $\mathcal{E} \to X_0(N)$ a surface parametrizing curves admitting isogenies of degree N. Theorem 2 is nearly identical, with $C = X_1(N)$.

Section 1 contains the proof of Theorem 1, following the above outline. In Section 2 we show how many of the results of [2, 5] can be deduced directly from Theorems 1 and 2, while Section 3 focusses on local versions of these results. The results in Section 1 are presented in full generality, but for the sake of simplicity, the results in the later sections are shown only over $\mathbb{Q}$.

Acknowledgements. The author would like to thank J. H. Silverman for comments on [2] suggesting the present line of inquiry, and the anonymous referee for pointing out several mistakes in the draft of this paper.

1. The proof of the main result. As mentioned, the proof breaks down into three cases, according as $X_0(N)$ has genus 0, 1, or greater.

When $X_0(N)$ has genus 0. In this case, our result is a consequence of Roth's theorem on approximation of algebraic numbers by rationals [7], and later variants thereof that apply to number fields and various absolute values.

Fix $\delta > 0$ to be specified later, and N such that $X_0(N)$ has genus 0. We let j denote the morphism mentioned in the introduction (dropping the subscript). As $X_0(N) \cong \mathbb{P}^1$, we may consider j to be a morphism $\mathbb{P}^1 \to \mathbb{P}^1$ which sends the point at infinity to itself. In particular, we may restrict attention to the affine map $j : \overline{K} \to \overline{K}$. Let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be the roots of $j(x) - r$, and let $e_j(x)$ denote the ramification index of j at x. Factoring $j(x) - r$ over $K(\alpha^{(i)})$, for each i, we see that

$$|r - j(x)|_v \gg \min_i \{|\alpha^{(i)} - x|_v^{e_j(\alpha^{(i)})}, 1\},$$

where the implied constant depends just on r, K, and N. Thus, by Roth's theorem (and later generalisations),

$$\prod_{v\in S} \min\{|r - j(x)|_v, 1\} \gg H_K(x)^{-(2+\delta)e_r},$$

where e_r is the largest $e_j(\alpha^{(i)})$ as i varies, and the implied constant now depends on δ as well. On the other hand, j is a morphism, and so

$$H_K(x)^{\deg(j)} \gg H_K(j(x)),$$

from which we obtain

$$\prod_{v\in S} \min\{|r - j(x)|_v, 1\} \gg H_k(j(x))^{-(2+\delta)e_r/\deg(j)}.$$

Now note that $j : X_0(N) \to \mathbb{P}^1$ is a morphism of degree

$$\deg(j) = N \prod_{p|N} (1 + 1/p)$$

(see, for example, [9]; in particular exercises on page 86) which is unramified except possibly at points above 0 and 1728. Above these points, the ramification index is 3 (or 1) and 2 (or 1), respectively. By letting $\delta = \varepsilon \deg(j)/e_r$, we have our result. Similarly, for Theorem 2, we note that $j : X_1(N) \to \mathbb{P}^1$ is a morphism of degree

$$\deg(j) = \begin{cases} 3 & \text{if } N = 2, \\ N^2 \prod_{p|N} (1 - 1/p^2) & \text{otherwise,} \end{cases}$$

with similar ramification.

When $X_0(N)$ has genus 1. In this case, we apply Siegel's theorem for diophantine approximation on curves of genus 1 (see, for example, [8, IX.3]). By a standard construction, there exists an elliptic curve E_r/K such that $j(E_r) = r$, and there is a finite extension L/K over which E_r admits an isogeny of degree N (for example, let L be the splitting field of the N-division polynomial of E_r). Thus E_r corresponds to some $Q \in X_0(N)(L)$.

Set, for $v \in S$,

$$d_v(P, Q) = \min\{|j(P) - j(Q)|_v^{1/e_j(Q)}, 1\},$$

where $e_j(Q)$ is again the ramification index of j at Q. Then by Siegel's theorem [8, p. 247], for any $\delta > 0$ we have

$$\frac{\log d_v(P, Q)}{\log H_K(j(P))} \geq -\delta$$

for all but finitely many $P \in X_0(N)(L)$. Thus

$$|r - j(P)|_v = |j(P) - j(Q)|_v \gg H_L(j(P))^{-e_j(Q)\delta}$$

as P ranges over $X_0(N)(K)$ (or, more generally, over $X_0(N)(L)$). As before, we have $e_j(Q) = 1$ unless $j(Q) = 0$ or 1728, in which case we may have $e_j(Q) = 3$ or 2, respectively. Note that $H_L(x) = H_K(x)^{[L:K]}$, and so by selecting

$$\delta = \frac{\varepsilon}{e_j(Q)[L:K](\#S)},$$

we get

$$\prod_{v \in S} \min\{|r - j(E)|_v, 1\} \gg H_K(j(E))^{-\varepsilon}$$

for elliptic curves E/K admitting K-rational isogenies of degree N.

When $X_0(N)$ has genus at least 2. By Faltings' theorem [4], $X_0(N)(K)$ is finite when the genus of $X_0(N)$ is at least 2. So for each $v \in S$ and each $P \in X_0(N)(K)$, either $j(P) = r$ or $|r - j(P)|_v$ is bounded below by some positive value that depends only on v, N, and K. The result is immediate.

2. From j to A and B. In this section we show how many of the results of [2, 5] follow from Theorems 1 and 2. For simplicity, and in keeping with the focus of the aforementioned papers, we restrict our attention to $K = \mathbb{Q}$ and S containing just the place at infinity. From this point forward, we will denote by $E_{A,B}$ the elliptic curve

$$E_{A,B} : y^2 = x^3 + Ax + B,$$

where A and B will always be taken to lie in $\mathbb{Z}$. If we set $H(E_{A,B}) = \max\{|A|^3, |B|^2\}$, then

$$H(j(E_{A,B})) \leq 54 H(E_{A,B}).$$

LEMMA 3. *Suppose that $\kappa > 2/3$, and that $E_{A,B}$ satisfies $|A| > |B|^\kappa$. Then*

$$|1728 - j(E_{A,B})| \ll H(j(E_{A,B}))^{-1+2/3\kappa},$$

where the implied constant is absolute.

Proof. As $\kappa > 2/3$, we have $|4A^3+27B^2| > |A|^3$ for sufficiently large $|A|$. Thus

$$|1728 - j(E_{A,B})| = 6^6\left|\frac{B^2}{4A^3+27B^2}\right| \le 6^6|A|^{2/\kappa-3} \ll H(j(E_{A,B}))^{(2/\kappa-3)/3},$$

as $H(E_{A,B}) = |A|^3$. ∎

LEMMA 4. *Suppose $E_{A,B}$ is as above, with $|B| > |A|^\kappa$ and $\kappa > 3/2$. Then*

$$|j(E_{A,B})| \ll H(j(E_{A,B}))^{-1+3\kappa/2},$$

where the implied constant is absolute.

The following proposition is the conjunction of Theorems 1 and 2 and Lemmas 3 and 4.

PROPOSITION 5. *Let $N \ge 2$ and $\varepsilon > 0$. Then for all but finitely many pairs of integers $A, B \in \mathbb{Z}$ with $|B| \ge 2$ such that $E_{A,B}$ admits a $\mathbb{Q}$-rational isogeny of degree N (respectively, contains a $\mathbb{Q}$-rational point of order N), we have*

$$\frac{2}{3}(1-\mu_i(N,0)) - \varepsilon < \frac{\log|A|}{\log|B|} < \frac{2}{3(1-\mu_i(N,1728))} + \varepsilon$$

with $i = 0$ (respectively, with $i = 1$).

In cases where $\mu_i(N,0) = 1$ or $\mu_i(N,1728) = 1$, the bounds are trivial (interpreting the pole as an infinite bound). Note that the non-trivial bounds correspond precisely to those appearing in [5]. It should also be pointed out that the condition $|B| \ge 2$ is entirely an artifact of the form of the proposition. One may easily describe the torsion/isogeny structure of curves with $|B| \le 1$ (see [5]).

3. Local results. Suppose $E_{A,B}$ is a curve admitting a $\mathbb{Q}$-rational isogeny of degree N, and suppose that B (respectively A) is an S-unit, that is, an integer whose prime divisors all lie in S. Then it is easy to construct infinitely many other curves with the same property merely by twisting $E_{A,B}$ by S-units. As it betides, this is the only way to construct an infinite family of such curves.

We will say that the elliptic curve $E_{A,B}$ is *quasi-minimal* if there does not exist a curve $E_{A',B'}$ isomorphic to $E_{A,B}$ over $\mathbb{Q}$ with $|A'| < |A|$ and $A', B' \in \mathbb{Z}$. Equivalently, $E_{A,B}$ is quasi-minimal if there is no prime p with $p^4 \mid A$ and $p^6 \mid B$. Curves that are quasi-minimal might not be minimal, in the traditional sense, at 2 or 3. We will say that $E_{A,B}$ is *twist-minimal* if there is no $E_{A',B'}$ isomorphic to $E_{A,B}$ over $\mathbb{C}$ with $|A'| < |A|$ and $A', B' \in \mathbb{Z}$.

Equivalently, $E_{A,B}$ is twist-minimal if there is no prime p with $p^2 \mid A$ and $p^3 \mid B$.

THEOREM 6. *Let S be a finite set of primes. Then there are at most finitely many twist-minimal curves $E_{A,B}$ such that*

(i) *A is an S-unit and $E_{A,B}$ admits a $\mathbb{Q}$-rational isogeny of degree at least 6, or*
(ii) *B is an S-unit and $E_{A,B}$ admits a $\mathbb{Q}$-rational isogeny of degree at least 4.*

There are at most finitely many minimal curves $E_{A,B}$ such that

(iii) *A is an S-unit and $E_{A,B}(\mathbb{Q})$ contains a point of order at least 5, or*
(iv) *B is an S-unit and $E_{A,B}(\mathbb{Q})$ contains a point of order at least 4.*

Our proof will make use of the following lemma.

LEMMA 7. *Let S be a finite set of places (containing the infinite place), and fix $\mu < 1$ and $m, n, C > 0$. If a and b are integers such that*

(i) *a is an S-unit,*
(ii) *for every prime p, either $\operatorname{ord}_p(a) \le m$ or $\operatorname{ord}_p(b) \le n$,*
(iii) *the inequality*

$$\prod_{v \in S} \min\{|a/b|_v, 1\} \ge C H(a/b)^{-\mu} \tag{1}$$

holds,

then $|a|$ and $|b|$ are bounded in terms of S, μ, C, m, and n.

Proof. Suppose $p \mid a$. Then by (ii), either $\operatorname{ord}_p(a) \le m$ or $\operatorname{ord}_p(a/b) \ge \operatorname{ord}_p(a) - n$. In particular,

$$\operatorname{ord}_p(a) \le n + m + \max\{\operatorname{ord}_p(a/b), 0\},$$

and so

$$|a|_p^{-1} \le p^{n+m} \min\{|a/b|_p, 1\}^{-1}.$$

As a is divisible only by primes in S, we have

$$\prod_{v \in S} \min\{|a/b|_v, 1\} \le \min\{|a/b|, 1\} \prod_{p \in S \setminus \{\infty\}} p^{n+m}|a|_p$$
$$= \min\{|a/b|, 1\} s^{n+m}|a|^{-1},$$

where s is the product of the finite primes in S. From (1), we now have

$$\min\{|a/b|, 1\} \ge C s^{-n-m}|a| H(a/b)^{-\mu}.$$

Suppose that $|a| \le |b|$. Then the above becomes

$$|a/b| \ge C s^{-n-m}|a|\,|b|^{-\mu},$$

which in turn yields $|a| \le |b| \le (s^{n+m}C^{-1})^{1/(1-\mu)}$. If, on the other hand, $|a| > |b|$, then we obtain

$$1 \ge Cs^{-n-m}|a|^{1-\mu},$$

whence $|b| < |a| \le (s^{n+m}C^{-1})^{1/(1-\mu)}$. ■

Proof of Theorem 6. The theorem is certainly not weakened if we enlarge the set of primes, so we will assume without loss of generality that $2, 3 \in S$. We will first treat the case (i), where A is an S-unit and $E_{A,B}$ admits a rational isogeny of degree at least 6. Suppose that $E_{A,B}$ is twist-minimal, and note that

$$j(E_{A,B}) = \frac{6912A^3}{4A^3 + 27B^2}.$$

Let $a = 6912A^3 = 2^8 3^3 A^3$ and $b = 4A^3 + 27B^2$. Then if $p \ge 5$ is a prime and $p^6 \mid a$, we have $p^2 \mid A$. If $p^6 \mid b$, then $p^6 \mid 1728b - a = 6^6 B^2$, and so $p^3 \mid B$. This contradicts the twist-minimality of $E_{A,B}$, so either $\mathrm{ord}_p(a) \le 5$ or $\mathrm{ord}_p(b) \le 5$. Similarly, if $2^{14} \mid a$, then $2^2 \mid A$. If we also have $2^{12} \mid b$, then $2^{12} \mid 1728b - a = 6^6 B^2$, and so $2^3 \mid B$. Under the hypothesis that $E_{A,B}$ is twist-minimal we have either $\mathrm{ord}_2(a) \le 13$ or $\mathrm{ord}_2(b) \le 11$. By a similar argument, $\mathrm{ord}_3(a) \le 8$ or $\mathrm{ord}_3(b) \le 5$.

If $E_{A,B}$ admits a $\mathbb{Q}$-rational isogeny of degree at least 6 we have, after applying Theorem 1 with $\varepsilon = 1/8$,

$$\prod_{v \in S} \min\{|a/b|_v, 1\} \ge CH(a/b)^{-7/8}$$

for some $C > 0$. Note that, as $2, 3 \in S$, a is an S-unit if A is, and so we may apply Lemma 7 with $m = 13$, $n = 11$, $\mu = 7/8$, and C and S as above. We see that $|a|$ and $|b|$ are bounded by some expression depending only on S, and so $|A|$ and $|B|$ are as well.

The proofs of the other three cases are straightforward modifications of the above argument, applying Theorem 1 or Theorem 2 with $r = 0$ or $r = 1728$ as appropriate. The only subtle point is that we may replace "twist-minimal" with "minimal" for curves with a $\mathbb{Q}$-rational point of the appropriate order. One way to see that this is true is to consider that an elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order $N \ge 3$ may have at most one (non-trivial) quadratic twist with a $\mathbb{Q}$-rational point of order N. If E and its twist over $\mathbb{Q}(\sqrt{D})$ both contain $\mathbb{Q}$-rational points of order N, then $E(\mathbb{Q}(\sqrt{D}))$ contains full N-torsion. As the Weil pairing of any two generators of the full N-torsion on E is a primitive Nth root of unity, the above situation can occur only for the twist of E over $\mathbb{Q}(\sqrt{-3})$ when $N = 3$, the twist of E over $\mathbb{Q}(i)$ when $N = 4$, and not at all when $N \ge 5$. ■

For example, it follows from Theorem 6 that there are only finitely many minimal $E_{A,B}$ with a $\mathbb{Q}$-rational point of order 5 such that B is a $\{2, 3\}$-unit.

Although perhaps only a curiosity, a much stronger statement holds in this special setting.

PROPOSITION 8. *Let A and B be integers such that $E_{A,B}$ is minimal, $E_{A,B}(\mathbb{Q})$ contains a point of order* 5, *and B is not divisible by any prime $p \equiv 1 \pmod 4$. Then $A = -432$ and $B = 8208$.*

Proof. If $E_{A,B}$ is minimal, and $E_{A,B}(\mathbb{Q})$ contains a point of order 5, then for some coprime integers s and t,

$$\begin{aligned} A &= -27(s^4 - 12s^3t + 14s^2t^2 + 12st^3 + t^4), \\ B &= 54(s^2+t^2)(s^4 - 18s^3t + 74s^2t^2 + 18st^3 + t^4) \end{aligned} \tag{2}$$

(see, for example, [2]). If B is not divisible by any prime $p \equiv 1 \pmod 4$, then neither is s^2+t^2. But clearly s^2+t^2 is not divisible by any prime $p \equiv 3 \pmod 4$ either, and thus $s^2+t^2 = 2^n$ for some n. As $\gcd(s,t) = 1$, we need only consider the values of s^2+t^2 in $\mathbb{Z}/4\mathbb{Z}$ to see that $n \in \{0,1\}$, and so

$$(s,t) \in \{(\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1), (\pm 1, \mp 1)\}.$$

The only non-singular curve that results is $E_{-432,8208}$. ■

We note, with a view to Theorem 6, that if S is a finite set of primes, $E_{A,B}(\mathbb{Q})$ contains a point of order 5, and B is an S-unit, then (2) defines a Thue–Mahler equation. This gives us not only a more direct verification of the relevant case of Theorem 6, but also, through theorems of Baker and Coates [1, 3], an effective method for finding all such $E_{A,B}$. Indeed, Theorem 6 can be made computationally effective in all cases by a similar reduction to the solution of Thue–Mahler equations.

4. Analogous results over function fields. Many of the above results have analogues over function fields. In many cases, we can make effective statements in this context that are stronger than those in [2, 5]. Rather than pursue these slight improvements here, we present an unconditional analogue of a result from [2] which used the *abc* Conjecture.

Recall that in [2] it was shown that there exists, for each $\varepsilon > 0$, a constant $C_\varepsilon > 0$ such that if $E_{A,B}(\mathbb{Q})$ contains a point of order 3, where $A, B \in \mathbb{Z}$, then

$$\log|A| \le (2+\varepsilon)\log|B| + C_\varepsilon.$$

(À propos of the analogy below, note that $\log|A| = h(A)$.) We will prove the analogous result for elliptic curves defined over function fields of genus and characteristic 0. The analogue of the *abc* Conjecture is known to be true in this setting (see [6]). To see the analogy between the two results, let k be an algebraically closed field of characteristic 0, let $t \in k \cup \{\infty\}$, and let $f \in k(T)$. We denote by $\mathrm{ord}_t(f)$ the order of vanishing of f at t, in the usual sense, and define a valuation and an absolute value by

$$v_t(f) = \mathrm{ord}_t(f), \qquad |f|_t = e^{-\mathrm{ord}_t(f)}.$$

We see that f is integral with respect to these valuations if and only if $f \in k[T]$ (that is, f is a polynomial), and that in this case the height of f is

$$h(f) = \deg(f).$$

PROPOSITION 9. *Let k be an algebraically closed field of characteristic 0, and let $K = k(T)$ be the field of rational functions in T over k. Then for all $A, B \in k[T]$ such that $E_{A,B}$ contains a K-rational point of order 3, we have*

$$\deg(A) \le 2\deg(B).$$

Proof. The proof follows almost exactly as in [2]. Suppose $(x, y) \in E_{A,B}(K)$ is a point of order 3. Then, examining duplication on $E_{A,B}$, we obtain both

$$\left(\frac{3x^2 + A}{2y}\right)^2 = 3x \quad \text{and} \quad 3x^4 + 6Ax^4 + 12Bx = A^2.$$

Note from the second equation that $x \in k[T]$, for any pole of x is as well a pole of A. By the first equation, we have $3x = s^2$, say, for $s \in k[T]$. If we write $A = st$, the second equation becomes

$$3s^6 + 6s^3t + 12B = t^2.$$

Solving the quadratic equation in t, we obtain

$$t = 3s^3 \pm \sqrt{12(s^6 + B)}.$$

Hence $s^6 + B$ is a square in $k[T]$, say $M^2 = s^6 + B$. Applying the *abc* Theorem for K (see [6]), we have

$$6\deg(s) \le \deg(BMs) - 1.$$

If, on the one hand, we have $2\deg(M) = \deg(B)$, then this implies

$$5\deg(s) \le \tfrac{3}{2}\deg(B) - 1.$$

If, on the other hand, $\deg(B) < 2\deg(M)$, then $\deg(M) = 3\deg(s)$. If this is the case, we derive

$$6\deg(s) \le \deg(B) + \deg(Ms) - 1 \le \deg(B) + 4\deg(s) - 1.$$

Finally, if $2\deg(M) < \deg(B)$, then $6\deg(s) = \deg(B)$. In any case, we have

$$\deg(A) \le 4\deg(s) \le 2\deg(B).$$

Note that for $\deg(B) \ge 2$, we have actually shown

$$\deg(A) \le 2\deg(B) - 2. \ \blacksquare$$

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers. I, II, III*, Mathematika 13 (1966), 204–216; 14 (1967), 102–107; 14 (1967), 220–228.

[2] M. A. Bennett and P. Ingram, *Torsion subgroups of elliptic curves in short Weierstrass form*, Trans. Amer. Math. Soc. 357 (2005), 3325–3337.

[3] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1968/1969), 279–305.

[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[5] P. Ingram, *Diophantine analysis and torsion on elliptic curves*, Proc. London Math. Soc. 94 (2007), 137–154.

[6] R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, Cambridge, 1984.

[7] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20; corrigendum, ibid. 168.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[9] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[10] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B 273 (1971), A238–A241.

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 2E4, Canada
E-mail: pingram@math.utoronto.ca

Received on 2.4.2007
and in revised form on 24.9.2007 (5423)