A Generalization of Siegel's Theorem and Hall's Conjecture

Graham Everest and Valéry Mahé

CONTENTS

1. Introduction
2. Special Cases
3. Computational Data
Acknowledgments
References

Consider an elliptic curve defined over the rational numbers and embedded in projective space. The rational points on the curve are viewed as integer vectors with coprime coordinates. What can be said about the rational points for which the number of prime factors dividing a fixed coordinate does not exceed a fixed bound? If the bound is zero, then Siegel's theorem guarantees that there are only finitely many such points. We consider, theoretically and computationally, two conjectures: one is a generalization of Siegel's theorem, and the other is a refinement that resonates with Hall's conjecture.

1. INTRODUCTION

Let C denote an elliptic curve defined over the rational field $\mathbb{Q}$ embedded in projective space $\mathbb{P}^N$ for some N. For background on elliptic curves consult [Cassels 91, Silverman 86, Silverman 94]. The rational points of C can be viewed as vectors

$$[x_0, \ldots, x_N], \quad x_0, \ldots, x_N \in \mathbb{Z}, \tag{1–1}$$

with coprime integer coordinates. Fixing $0 \leq n \leq N$, Siegel's theorem guarantees that only finitely many rational points $Q \in C(\mathbb{Q})$ have $x_n = 1$. The number 1 is divisible by no primes, so we consider how the set of rational points Q might be constrained if the number of distinct primes dividing x_n is restricted to lie below a given positive bound.

Conjecture 1.1. *Let C denote an elliptic curve defined over the rational field $\mathbb{Q}$, embedded in projective space. For any fixed choice of coordinate x_n, as in* (1–1)*, given a fixed bound L, the set $S_n(L)$ of points $Q \in C(\mathbb{Q})$ for which x_n is divisible by fewer than L primes is repelled by $C(\overline{\mathbb{Q}})$. In other words, on any affine piece of C containing a point $D \in C(\overline{\mathbb{Q}})$, there is a punctured neighborhood $N(D)$ of D (with respect to the archimedean topology)*

2000 AMS Subject Classification: 11G05, 11A41

Keywords: Elliptic curve, Hall's conjecture, prime, Siegel's theorem

1058-6458/2009 $ 0.50 per page

such that

$$N(D) \cap S_n(L) = \emptyset.$$

Example 1.2. To show that Conjecture 1.1 implies Siegel's theorem, consider the rational points with $x_n = 1$. The hyperplane $x_n = 0$ intersects $C(\overline{\mathbb{Q}})$ nontrivially. Let D denote any point in the intersection. Fixing $L = 0$, the conjecture implies in particular that each $|x_i/x_n|$, with $i \neq n$, is bounded above. Since $x_n = 1$, this bounds each $|x_i|$ with $i \neq n$. Thus there can be only finitely many such points.

Example 1.3. Consider a homogeneous cubic

$$AX^3 + BY^3 + CZ^3 = 0$$

with all the terms nonzero integers. Consider the coprime integer triples $[X, Y, Z]$ satisfying the equation with one of them, say Z, constrained to be a prime power. Choosing D to be any algebraic point with Z-coordinate zero, the application of Conjecture 1.1 to D predicts that $|X/Z|$ and $|Y/Z|$ are bounded. Notice that the conjecture does not predict that only finitely many such points exist.

If A/B is a rational cube, then only finitely many triples can have Z equal to a prime power. This is essentially the point in [Everest et al. 04, Theorem 4.1]. The condition about A/B enables a factorization to take place. Now the claim follows because essentially all of Z must occur in one of the factors. But the logarithms of the variables are commensurate by a strong form of Siegel's theorem [Silverman 86, p. 250], and this yields a contradiction.

Example 1.4. When the group of rational points has rank 1, we expect a natural generalization of the primality conjecture [Einsiedler et al. 01, Everest et al. 04, Everest and King 05] for elliptic divisibility sequences to hold. This conjecture was stated in [Einsiedler et al. 01] for Weierstrass curves, and it predicts that only finitely many multiples of a fixed nontorsion point have a prime-power denominator in the x-coordinate. Using the same heuristic argument as in [Einsiedler et al. 01, Everest et al. 04], we expect that in rank 1, $S_n(1)$ is finite. More generally, it seems likely that in rank 1, $S_n(L)$ is finite for any fixed L and n.

On a plane curve, Siegel's theorem can be interpreted to say that the point at infinity repels integral points. We can see no reason why infinity should play a special role, and the computations in Section 3 support this view. That is why Conjecture 1.1 is stated in such a general way. For practical purposes, measuring the distance to infinity is natural, and many of our computations concern this distance. Conjecture 1.1 arose from the use of the Weierstrass model, so we now focus on that equation, making a conjecture about an explicit bound on the radius of the punctured neighborhood, one that resonates with Hall's conjecture.

1.1 Weierstrass Equations

Let E denote an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation in minimal form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1\text{–}2)$$

with $a_1, \ldots, a_6 \in \mathbb{Z}$. Given a nonidentity rational point $Q \in E(\mathbb{Q})$, the shape of equation (1–2) forces Q to be in the form

$$Q = \left(\frac{A_Q}{B_Q^2}, \frac{C_Q}{B_Q^3} \right), \qquad (1\text{–}3)$$

where $A_Q, B_Q, C_Q \in \mathbb{Z}$ and $\gcd(B_Q, A_QC_Q) = 1$. Define the *length* of Q, written $L(Q)$, to be the number of distinct primes p such that

$$|x(Q)|_p > 1, \qquad (1\text{–}4)$$

where $|\cdot|_p$ denotes the usual multiplicative p-adic valuation. In other words, the length of Q is the number of distinct prime divisors of B_Q. From the definition, the length-zero rational points are precisely the integral points on E. Conjecture 1.1 implies that bounding $L(Q)$ bounds $|x(Q)|$ independently of Q.

The case $L(Q) = 1$ is much more interesting. The definition of a length-1 point Q means that the denominator of $x(Q)$ is the square of a prime power. It has been argued heuristically [Einsiedler et al. 01, Everest et al. 04, Everest and King 05] that when the rank of $E(\mathbb{Q})$ is 1, then again, only finitely many points Q exist. This is known as the *primality conjecture* for elliptic divisibility sequences. Much data has been gathered in support of the primality conjecture, and it has been proved in many cases. In higher rank, a heuristic argument, together with computational evidence [Everest et al. 02], suggests that in some cases, infinitely many rational points Q can have length 1. In Section 3, many examples appear.

What follows is an explicit form of Conjecture 1.1. To motivate this, consider a Mordell curve

$$E : y^2 = x^3 + d, \quad d \in \mathbb{Z}.$$

Hall's conjecture [Birch et al. 65, Hall 71] predicts an asymptotic bound of $(2 + \varepsilon) \log |d|$ (which is essentially

$(1+\varepsilon)\log|\Delta_E|)$ for $\log|x|$ when $x \in \mathbb{Z}$. Conjecture 1.5 is a simultaneous generalization of a strong form of Siegel's theorem and of Hall's conjecture. Given any rational point D on E, let h_D denote the Weil height from D. In other words,

$$h_D(Q) = \max\{0, \log|x(Q)|\}$$

if $D = O$ is the point at infinity, and

$$h_D(Q) = \max\{0, -\log|x(Q) - x(D)|\}$$

if D is a finite point.

Conjecture 1.5. *Assume that E is in standardized minimal form. Let D denote any rational point on E. If $L(Q) \le L$, then*

$$h_D(Q) < C(L, D)\log|\Delta_E|, \tag{1–5}$$

where $C(L, D)$ depends only on L and D, and Δ_E denotes the discriminant of E.

Note 1.6. The term *standardized* means that $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Every elliptic curve has a unique standardized minimal form. This assumption is necessary in Conjecture 1.5. When $D = O$, the point at infinity, the left-hand side is not invariant under a translation of the x-coordinate, unlike the right-hand side.

Note 1.7. When D is algebraic but not rational, a similar conjecture can be made. Now, though, the constant $C(L, D)$ will also depend on the degree of the field generated by D.

Although strong bounds are known for the number of S-integral points on an elliptic curve [Gross and Silverman 95, Hindry and Silverman 98, Silverman 87], the best unconditional bound on the height of an S-integral point is quite weak [Bilu 97, Bugeaud 97, Hadju and Herendi 98] in comparison with what is expected to be true. Using the ABC conjecture, an explicit bound on the height of an S-integral point can be given [Elkies 91, Surroca 04]. For integral points, the best bound for the logarithm of the x-coordinate of an integral point on a standardized minimal curve is expected to be a multiple of the log-discriminant (or the Faltings height).

What follows are some special cases of Conjecture 1.5.

Theorem 1.8. *Let $N > 0$ denote an integer and consider the curve*

$$E_N : y^2 = x^3 - Nx.$$

Suppose the nontorsion point $Q_1 \in E_N(\mathbb{Q})$ has $x(Q_1) < 0$. Let O denote the point at infinity. Assume that the ABC conjecture holds in $\mathbb{Z}$.

- *If $L(nQ_1) \le 1$, then the following uniform bound holds:*
$$h_O(nQ_1) \ll \log N.$$
- *With Q_1 as before, assume that Q_1 and Q_2 are independent and either Q_2 is twice another rational point or $x(Q_2)$ is a square. Writing $G = \langle Q_1, Q_2\rangle$ for any point $Q \in G$, $L(Q) \le 1$, implies the uniform bound*
$$h_O(Q) \ll \log N.$$

The discriminant of E_N is essentially a power of N, so $\log N$ is commensurate with the log-discriminant, as required by Conjecture 1.5.

As we said before, only finitely many terms nQ_1 are expected to have length 1. Nonetheless, Theorem 1.8 gives nontrivial information about where they are located. Computations, as well as a standard heuristic argument, suggest there could be infinitely many length-1 points in the group $G = \langle Q_1, Q_2\rangle$ in the second part of Theorem 1.8.

Example 1.9. $E_{90} : y^2 = x^3 - 90x$, $Q_1 = [-9, 9]$, $Q_2 = [49/4, -217/8]$. This example occurs as one of a number of similar examples of rank-2 curves appearing Table 6, in Section 3. Note that Q_2 is twice the point $[-6, 18]$.

Example 1.10. $E_{1681} : y^2 = x^3 - 1681x$, $Q_1 = [-9, 120]$, $Q_2 = [841, 24360]$. Note that $x(Q_2) = 29^2$. Also, Q_1 and Q_2 are generators for the torsion-free part of $E_{1681}(\mathbb{Q})$.

An immediate consequence of Theorem 1.8 is a version of Conjecture 1.5 when D is the point $[0, 0]$.

Corollary 1.11. *Assume the ABC conjecture for $\mathbb{Z}$. Let D denote the point $[0, 0]$. With G as in Theorem 1.8, let $G' = D + G$. Suppose Q is a point in G' with a prime-power numerator. Then*

$$h_D(Q) \ll \log N$$

uniformly.

Although there are many curves with a large number of length-1 points, no proof exists of the infinitude of length-1 points for even one curve. We see no way of gathering data about length-2 points, because checking

seems to require the ability to factorize very large integers. All the data gathered in this paper used Cremona's tables [Cremona 02], together with the computing packages MAGMA and PARI-GP.

Theorem 1.8 and Corollary 1.11 are proved in the next section. Section 3 gives data in support of Conjecture 1.5. The introduction concludes with a brief subsection about the situation in which the base field is a function field.

1.2 The Function Field $\mathbb{Q}(t)$

The situation in which the base field is $\mathbb{Q}(t)$ lies at a somewhat obtuse angle to the rational case. On a Weierstrass model, Conjecture 1.1 predicts that over the rational field, length-1 points will have bounded x-coordinate. In the language of local heights [Hindry and Silverman 00], this is equivalent to the archimedean local height being bounded. Over the field $\mathbb{Q}(t)$, Manin [Manin 63] showed that all the local heights, including the one at infinity, are bounded unconditionally. On the other hand, work of Hindry and Silverman [Hindry and Silverman 98, Proposition 8.2] shows that the bound for integral points agrees with the one predicted by Conjecture 1.5.

2. SPECIAL CASES

Before the proof of Theorem 1.8, one lemma is needed.

Lemma 2.1. *Let P denote any nontorsion point in $E_N(\mathbb{Q})$. Assuming the ABC conjecture for $\mathbb{Z}$, if $L(2P) \leq 1$, then*

$$\log|x(P)| \ll \log|N| \text{ and } \log|x(2P)| \ll \log|N|.$$

Proof: Note that $L(2P) \leq 1$ implies $L(P) \leq 1$. If

$$P = \left(\frac{A}{B^2}, \frac{C}{B^3}\right)$$

with $\gcd(B, AC) = 1$, then

$$x(2P) = \left(\frac{A^2 + NB^4}{2CB}\right)^2. \tag{2–1}$$

If $L(P) = 0$, then $\log|x(P)| = \log|A| \ll \log N$ follows from the ABC conjecture. A similar bound for $\log|x(2P)|$ follows from (2–1) with $B = 1$.

If $L(P) = 1$, then $2C$ must cancel in (2–1). That is,

$$C|A^2 + NB^4, \tag{2–2}$$

using the coprimality relations $\gcd(B, C) = \gcd(B, A^2 + NB^4) = 1$. The defining equation gives

$$C^2 = A(A^2 - NB^4). \tag{2–3}$$

Any prime power p^r dividing C divides $2N$ from (2–2) and (2–3). Hence $|C| \leq 2N$. Then equation (2–3) implies $|A| \leq 4N^2$. Rearranging (2–3) bounds B in a similar way. The bound for $x(P)$ follows directly. The bound for $x(2P)$ follows using (2–1). □

Write $E^O(\mathbb{R})$ for the connected component of infinity on the real curve. If $E(\mathbb{R})$ has two connected components, write $E^B(\mathbb{R})$ for the bounded component.

Proof (of Theorem 1.8.): Note first that

$$|x(P)| \leq N, \tag{2–4}$$

for any $P \in E_N^B(\mathbb{Q})$. A proof of the first part of Theorem 1.8 follows: if n is odd, then $nQ_1 \in E_N^B(\mathbb{Q})$, so we are done, and if n is even and $L(nQ_1) \leq 1$, then Lemma 2.1 applies.

For the second part, assume first that Q_2 is twice a rational point. Any $Q \in G$ can be written $Q = n_1Q_1 + n_2Q_2$ with $n_1, n_2 \in \mathbb{Z}$. If $n_2 = 0$, the first part applies. If $n_1 = 0$, Lemma 2.1 applies. If n_1 is odd, then $Q \in E_N^B(\mathbb{Q})$, so (2–4) applies. If n_1 is even, then Lemma 2.1 applies.

Now assume that $x(Q_2)$ is a square. This condition implies [Cassels 91, Chapter 14] that E'_N maps to E_N via a 2-isogeny σ, where

$$E'_N : y^2 = x^3 + 4Nx \text{ and } x(\sigma(Q)) = x(Q) + \frac{4N}{x(Q)}.$$

An analogue of Lemma 2.1 says that if $L(\sigma(Q)) \leq 1$, then

$$\log|x(Q)| \ll \log|N| \text{ and } \log|x(\sigma(Q))| \ll \log|N|. \tag{2–5}$$

To prove (2–5), first write $Q = [a/b^2, c/b^3]$ with $a, b, c \in \mathbb{Z}$ and b coprime to ac. The case $b = 1$ follows from the ABC conjecture as before. If b is a prime power, then $L(\sigma(Q)) \leq 1$ only when $a \mid 4N$. Now using the ABC conjecture on the equation

$$c^2 = a^3 + 4Nab^4,$$

we obtain $\log|b| \ll \log N$. The double of any rational point lies in the image of σ: if $Q = 2Q'$, then Q is the image of $\widehat{\sigma}(Q')$, where $\widehat{\sigma} : E_N \to E'_N$ is the dual isogeny. Therefore, the assumptions on Q_1 and Q_2 guarantee that the elements of G lie either on the bounded component or in the image of σ. The proof follows exactly as before. □

Proof of Corollary 1.11.: Translating by the point $D = [0, 0]$, the conditions and the conclusion of Theorem 1.8 become the corresponding statements for the corollary.

d	x	$\log x$	$\log x/2\log\lvert d\rvert$
1641843	5853886516781223	36.305	1.268
30032270	38115991067861271	38.179	1.108
−1090	28187351	17.154	1.226
−193234265	810574762403977064	41.236	1.080
−17	5234	8.562	1.511
−225	720114	13.487	1.245
−24	8158	9.006	1.417
307	939787	13.753	1.200
207	367806	12.815	1.201
−28024	3790689201	22.055	1.076

TABLE 1. Evidence for Hall's Conjecture.

Note in particular that translation by D essentially inverts the x-coordinate; hence numerators become denominators. Also, the distance between a point and infinity changes places with the distance to D. □

This section concludes with a generalization of (2–4), by giving an explicit bound for the x-coordinate of a point in the bounded component of the real curve in short Weierstrass form, in terms of the height of the curve. Let $h(a/b) = \log\max\{|a|,|b|\}$ denote the usual projective height. Let $j = j_E$ denote the j-invariant of E, $\Delta = \Delta_E$ the discriminant of E, and write $h(E) := \frac{1}{12}\max(h(j)), h(\Delta))$ for the height of E.

Proposition 2.2. *Assume that E is in short Weierstrass form. For every rational point $Q \in E^B(\mathbb{Q})$, the following inequality holds:*

$$\log|x(Q)| \le 4h(E). \tag{2–6}$$

Proof: Denote by $\alpha_1, \alpha_2, \alpha_3$ the three roots of x^3+Ax+B. The proof can be obtained using Hunter's formula [Cohen 93, Theorem 6.4.2].[1] Alternatively, using Cardan's Formula, we see that there are two complex numbers u_i, v_i such that $\alpha_i = u_i + v_i$ and

$$\Delta = -16\times 27\times(B+2u_i^3)^2 = -16\times 27\times(B+2v_i^3)^2.$$

[1]We are indebted to the referee for this observation.

Since $-16\times 27\times B^2 = \frac{(j+1728)\Delta}{1728}$, we have

$$\begin{aligned}
2|u_i|^3 &\le |B| + |B+2u_i^3| \\
&\le e^{6h(E)}\left(\frac{1}{2^4\times 3^3} + \frac{e^{12h(E)}}{2^{10}\times 3^6}\right)^{1/2} + \frac{e^{6h(E)}}{12\sqrt{3}} \\
&\le \frac{e^{6h(E)}}{12\sqrt{3}} + \frac{e^{12h(E)}}{864} + \frac{e^{6h(E)}}{12\sqrt{3}} \\
&\le \frac{e^{12h(E)}}{4\sqrt{3}}.
\end{aligned}$$

In the same way, we prove that $|v_i| \le \frac{e^{4h(E)}}{2\times 3^{1/6}}$. In particular, an upper bound for $|\alpha_i|$ follows: $|\alpha_i| \le \frac{e^{4h(E)}}{3^{1/6}}$. To conclude, notice that $|x(Q)| \le \max_{i=1}^3(|\alpha_i|)$ for every point Q in the bounded real connected component of E. □

3. COMPUTATIONAL DATA

3.1 Data Concerning Hall's Conjecture

To enable a comparison to be made, Table 1 gives some examples in the length-0 case. They are drawn from Elkies' research into Hall's conjecture [Elkies 00, Elkies 08a]. The table shows values of x and d with $E : y^2 = x^3 + d$ with $\log x$ large in comparison to $2\log|d|$ (essentially $\log|\Delta_E|$).

3.2 Some Rank-2 Curves

Table 2 shows data collected for some rank-2 curves taken from a table of thirty curves studied by Peter Rogers [Everest et al. 02, Rogers 08] (the first ten curves and the last three). In rank 2, the available data support the heuristic argument that if P_1, P_2 are a basis for the torsion-free part of $E(\mathbb{Q})$, then the number of length-1 points $n_1P_1+n_2P_2$ having $|n_1|, |n_2| < T$ is asymptotically

E	P	Q	$\lvert\Delta_E\rvert$	$[m,n]$	$\overline{h}$	$\overline{h}/h_E$
$[0,0,1,-199,1092]$	$[-13,38]$	$[-6,45]$	11022011	$[21,26]$	12.809	0.789
$[0,0,1,-27,56]$	$[-3,10]$	$[0,7]$	107163	$[14,5]$	11.205	0.967
$[0,0,0,-28,52]$	$[-4,10]$	$[-2,10]$	236800	$[14,8]$	13.429	1.085
$[1,-1,0,-10,16]$	$[-2,6]$	$[0,4]$	10700	$[29,11]$	9.701	1.045
$[1,-1,1,-42,105]$	$[17,-73]$	$[-5,15]$	750592	$[33,30]$	8.136	0.601
$[0,-1,0,-25,61]$	$[19,-78]$	$[-3,10]$	154368	$[29,69]$	16.592	1.388
$[1,-1,1,-27,75]$	$[11,-38]$	$[-1,10]$	816128	$[22,17]$	12.363	0.908
$[0,0,0,-7,10]$	$[2,2]$	$[1,2]$	21248	$[18,43]$	12.075	1.211
$[1,-1,0,-4,4]$	$[0,2]$	$[1,0]$	892	$[5,17]$	11.738	1.727
$[0,0,1,-13,18]$	$[1,2]$	$[3,2]$	3275	$[4,-3]$	6.511	0.804
$[0,1,0,-5,4]$	$[-1,3]$	$[0,2]$	4528	$[1,-4]$	7.377	0.876
$[0,1,1,-2,0]$	$[1,0]$	$[0,0]$	389	$[5,8]$	9.707	1.627
$[1,0,1,-12,14]$	$[12,-47]$	$[-1,5]$	2068	$[16,19]$	9.819	1.286

TABLE 2. Rank 2 length 1.

E	P	Q	$\lvert\Delta_E\rvert$	$[m,n]$	$\overline{h}$	$\overline{h}/h_E$
$[0,0,1,-199,1092]$	$[-13,38]$	$[-6,45]$	11022011	$[65,48]$	7.476	0.461
*$[0,0,1,-27,56]$	$[-3,10]$	$[0,7]$	107163	$[4,1]$	1.945	0.168
$[0,0,0,-28,52]$	$[-4,10]$	$[-2,10]$	236800	$[14,8]$	13.429	1.085
*$[1,-1,0,-10,16]$	$[-2,6]$	$[0,4]$	10700	$[1,-1]$	3.135	0.337
$[1,-1,1,-42,105]$	$[17,-73]$	$[-5,15]$	750592	$[21,12]$	8.923	0.659
$[0,-1,0,-25,61]$	$[19,-78]$	$[-3,10]$	154368	$[9,13]$	5.976	0.500
$[1,-1,1,-27,75]$	$[11,-38]$	$[-1,10]$	816128	$[8,5]$	9.843	0.723
$[1,-1,0,-4,4]$	$[0,2]$	$[1,0]$	892	$[3,3]$	2.772	0.408
$[0,0,1,-13,18]$	$[1,2]$	$[3,2]$	3275	$[68,8]$	15.496	4.408

TABLE 3. Rank 2 prime numerators.

E	P	Q	R	$[m,n,l]$	$\overline{h}$	$\overline{h}/h_E$
$[0,0,1,-7,6]$	$[-2,3]$	$[-1,3]$	$[0,2]$	$[27,32,-23]$	14.079	1.650
$[1,-1,1,-6,0]$	$[-2,1]$	$[-1,2]$	$[0,0]$	$[-45,36,41]$	15.934	1.709
$[1,-1,0,-16,28]$	$[-3,8]$	$[-2,8]$	$[-1,7]$	$[12,35,29]$	21.260	2.114
$[0,-1,1,-10,12]$	$[-3,2]$	$[-2,4]$	$[-1,4]$	$[1,32,3]$	13.960	1.328
$[1,0,1,-23,42]$	$[-5,8]$	$[-1,8]$	$[0,6]$	$[10,7,4]$	18.721	1.613
$[0,1,1,-30,60]$	$[4,4]$	$[-5,10]$	$[-4,11]$	$[18,27,40]$	14.463	1.133
$[0,0,1,-147,706]$	$[4,13]$	$[-13,20]$	$[-11,31]$	$[-39,20,30]$	15.800	0.968
$[0,0,0,-28,148]$	$[4,10]$	$[-6,10]$	$[-4,14]$	$[-77,69,55]$	19.720	1.240
$[1,-1,0,-324,-896]$	$[23,47]$	$[-15,28]$	$[-13,38]$	$[93,27,17]$	22.899	1.075
$[1,-1,0,-142,616]$	$[-12,28]$	$[-11,33]$	$[-10,36]$	$[21,23,20]$	18.494	1.058

TABLE 4. Rank 3 length 1.

$c_1 \log T$, where $c_1 > 0$ is a constant that depends only on E.

In the table, E is a minimal elliptic curve given by a vector $[a_1, \ldots, a_6]$ in Tate's notation; P and Q denote independent points in $E(\mathbb{Q})$; $|\Delta_E|$ denotes the absolute value of the discriminant of E; $[m,n]$ denote the indices yielding the maximum absolute value of an x-coordinate with a prime square denominator, where $|m|, |n| \leq 150$; $\overline{h}$ denotes that absolute value; the final column compares $\overline{h}$ with $h_E = \log |\Delta_E|$.

E	P	$\lvert\Delta_E\rvert$	n	$\overline{h}/h_E$
$[1,1,1,-125615,61203197]$	$[7107,594946]$	1494113863691104200	39	0.361
$[1,0,0,-141875,18393057]$	$[-386,-3767]$	36431493120000000	32	0.216
$[1,-1,1,-3057,133281]$	$[591,-14596]$	5758438400000	33	0.388
$[1,1,1,-2990,71147]$	$[27,-119]$	553190400000	43	0.319
$[0,0,0,-412,3316]$	$[-18,-70]$	274400000	37	0.484
$[1,0,0,-4923717,4228856001]$	$[1656,-25671]$	87651984035481255936	197	0.331
$[1,0,0,-13465,839225]$	$[80,485]$	148827974400000	34	0.254
$[1,0,0,-21736,875072]$	$[-154,-682]$	325058782980096	36	0.245
$[1,-1,1,-1517,26709]$	$[167,-2184]$	76204800000	41	0.223
$[1,0,0,-8755,350177]$	$[14,473]$	10245657600000	79	0.255
$[1,-1,1,-180,1047]$	$[-1,35]$	62720000	31	0.451
$[1,0,0,-59852395,185731807025]$	$[12680,1204265]$	1180977565620646379520000	28	0.277
$[1,0,0,-10280,409152]$	$[304,-5192]$	3093914880000	41	0.283
$[0,1,1,-310,3364]$	$[-19,52]$	3281866875	59	0.309
$[1,0,0,-42145813,105399339617]$	$[31442,5449079]$	8228050444183680000000	47	0.206
$[1,0,0,-25757,320049]$	$[-116,-1265]$	1048775180673024	40	0.269
$[1,0,0,-350636,80632464]$	$[352,748]$	51738305261094144	34	0.287
$[1,0,0,-23611588,39078347792]$	$[-3718,-272866]$	182691077679728640000000	26	0.264

TABLE 5. Elliptic divisibility sequences.

E	P	Q	$\lvert\Delta_E\rvert$	$[m,n]$	$\overline{h}_D$	$\overline{h}_D/h_E$
$[0,0,0,150,0]$	$[10,50]$	$[24,132]$	216000000	$[4,-19]$	6.436	0.335
$[0,0,0,-90,0]$	$[-9,9]$	$[-6,18]$	46656000	$[1,30]$	3.756	0.212
$[0,0,0,-132,0]$	$[-11,11]$	$[-6,24]$	147197952	$[1,2]$	4.470	0.237
$[0,1,0,-648,0]$	$[-24,48]$	$[-9,72]$	17420977152	$[1,-6]$	0.602	0.025
$[0,0,0,34,0]$	$[8,28]$	$[32,184]$	2515456	$[12,-19]$	2.107	0.143
$[0,0,0,-136,0]$	$[-8,24]$	$[153,1887]$	160989184	$[17,2]$	0.279	0.014
$[0,1,0,-289,0]$	$[-17,17]$	$[-16,28]$	1546140752	$[11,0]$	5.712	0.269

TABLE 6. Distance to $[0,0]$.

In Table 3, similar computations are shown, except that the numerator of $x(mP+nQ)$ is tested for primality and a resulting bound for the x-coordinate is shown. For the curves marked with an asterisk, it seems likely that only finitely many points have a prime numerator in the x-coordinate.

3.3 Some Rank-3 Curves

In rank 3, it is expected [Everest et al. 02] that asymptotically, c_2T values $x(n_1P_1+n_2P_2+n_3P_3)$, with index bounded by T, will have length 1, where $c_2>0$ depends only on E. As before, elliptic curves E are listed, now with generators P, Q, and R. The index set is bounded by 100 in each variable. For the eighth and ninth curves in Table 4, although the largest values occur at large indices, the increment is noteworthy. For the eighth curve, $[-30,47,22]$ yields a point whose x-coordinate has logarithm 19.244. For the ninth curve, $[10,1,-1]$ yields a point whose x-coordinate has logarithm 20.586.

3.4 Some Elliptic Divisibility Sequences

Table 5 shows data collected for some elliptic divisibility sequences generated by rational points with small height [Elkies 08b, Everest et al. 08]. Although the curves themselves do not necessarily have rank 1, the data are interesting because some of the discriminants are very large. Also, the primes occurring are extreme in a sense. The notation remains as before, but this time, n denotes the index yielding the maximum absolute value of an x-coordinate with a prime square denominator, where $n\le 3500$.

3.5 Other Repelling Points

Table 6 gives examples of rank-2 curves with generators P and Q and a rational 2-torsion point equal to $D=[0,0]$.

We computed the smallest value of $x(mP + nQ)$ when $L(mP + nQ) = 1$, assuming that the bound on $|m|$ and $|n|$ was 100. For consistency with the definitions given, the largest value

$$\overline{h}_D = -\log|x(mP + nQ) - x(D)| = -\log|x(mP + nQ)|$$

with $L(mP + nQ) = 1$ and $|m|, |n| \leq 100$ is recorded.

ACKNOWLEDGMENTS

The second author's research was supported by a postdoctoral grant from EPSRC. Both authors thank the referee for several helpful comments.

REFERENCES

[Bilu 97] Y. Bilu. "Quantitative Siegel's Theorem for Galois Coverings." *Compositio Math.* 106:2 (1997), 125–158.

[Birch et al. 65] B. Birch, S. Chowla, M. Hall, and A. Schinzel. "On the Difference $x^3 - y^2$." *Norske Vid. Selsk. Forh.* 38 (1965), 65–69.

[Bugeaud 97] Y. Bugeaud. "Bounds for the Solutions of Superelliptic Equations." *Compositio Math.* 107:2 (1997), 187–219.

[Cassels 91] J. W. S. Cassels. *Lectures on Elliptic Curves*, London Mathematical Society Student Texts 24. Cambridge: Cambridge University Press, 1991.

[Cohen 93] H. Cohen. *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138. Berlin: Springer-Verlag, 1993.

[Cremona 02] J. E. Cremona. "Elliptic Curve Data," updated 14 January 2002. Available online (http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html).

[Einsiedler et al. 01] M. Einsiedler, G. Everest, and T. Ward. "Primes in Elliptic Divisibility Sequences." *LMS J. Comp. Math.* 4 (2001), 1–13.

[Elkies 91] N. D. Elkies. "ABC implies Mordell." *Intern. Math. Research Notices* 7 (1991), 99–109.

[Elkies 00] N. D. Elkies. "Rational Points near Curves and Small Nonzero $|x^3 - y^2|$ via Lattice Reduction." In *Algorithmic Number Theory (Leiden, 2000)*, pp. 33–63, Lecture Notes in Comput. Sci. 1838. Berlin: Springer, 2000.

[Elkies 08a] N. D. Elkies. "Hall's Conjecture: Small Non-zero Values of $|x^3 - y^2|$." Available online (http://www.math.harvard.edu/~elkies/hall.html), 2008.

[Elkies 08b] N. D. Elkies. "Rational Points with Small Height." Available online (www.math.harvard.edu/~elkies/low_height.html), 2008.

[Everest and King 05] G. Everest and H. King. "Prime Powers in Elliptic Divisibility Sequences." *Math. Comp.* 74 (2005), 2061–2071.

[Everest et al. 02] G. Everest, P. Rogers, and T. Ward. "A Higher Rank Mersenne Problem." In *ANTS V Proceedings*, pp. 95–107, Springer Lecture Notes in Computer Science 2369. New York: Springer, 2002.

[Everest et al. 04] G. Everest, V. Miller, and N. Stephens. "Primes Generated by Elliptic Curves." *Proc. Amer. Math. Soc.* 132 (2004), 955–963.

[Everest et al. 08] G. Everest, P. Ingram, V. Mahé, and S. Stevens. "The Uniform Primality Conjecture for Elliptic Curves." To appear in *Acta Arithmetica*, 2008.

[Gross and Silverman 95] R. Gross and J. Silverman. "S-Integer Points on Elliptic Curves." *Pacific J. Math.* 167 (1995), 263–288.

[Hadju and Herendi 98] L. Hadju and T. Herendi. "Explicit Bounds for the Solutions of Elliptic Equations with Rational Coefficients." *J. Symbolic Comp.* 25:3 (1998), 361–366.

[Hall 71] M. Hall. "The Diophantine Equation $x^3 - y^2 = k$." In *Computers in Number Theory*, edited by A. Atkin and B. Birch. New York: Academic Press, 1971.

[Hindry and Silverman 98] M. Hindry and J. Silverman. "The Canonical Height and Integral Points on Elliptic Curves." *Invent. Math.* 93:2 (1998), 419–450.

[Hindry and Silverman 00] M. Hindry and J. Silverman. *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics 201. New York: Springer-Verlag, 2000.

[Manin 63] Yu V. Manin. "Rational Points on an Algebraic Curve over Function Fields." *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963), 1395–1440; translated in *Amer. Math. Soc. Transl. (2)* 50 (1966), 189–234.

[Rogers 08] P. Rogers. "Prime Appearance in Some Rank-2 Curves." Available online (http://www.mth.uea.ac.uk/~h090/2deds.htm), 2008.

[Silverman 86] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106. New York: Springer-Verlag, 1986.

[Silverman 87] J. H. Silverman. "A Quantitative Version of Siegel's Theorem: Integral Points on Elliptic Curves and Catalan Curves." *J. Reine Angew. Math.* 378 (1987), 60–100.

[Silverman 94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151. New York: Springer-Verlag, 1994.

[Surroca 04] A. Surroca "Siegel's Theorem and the ABC Conjecture." *Riv. Mat. Univ. Parma* (7) 3* (2004), 323–332.

Graham Everest, School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK (g.everest@uea.ac.uk)

Valéry Mahé, Institut de Mathématiques et de Modélisation de Montpellier, Case Courrier 051,
Place Eugène Bataillon, 34095 Montpellier, Cedex, France (vmahe@math.univ-montp2.fr)

Received March 11, 2008; accepted in revised form July 3, 2008.