MATHEMATICS OF COMPUTATION
Volume 74, Number 252, Pages 2061–2071
S 0025-5718(05)01737-0
Article electronically published on March 1, 2005

PRIME POWERS IN ELLIPTIC DIVISIBILITY SEQUENCES

GRAHAM EVEREST AND HELEN KING

Abstract. Certain elliptic divisibility sequences are shown to contain only finitely many prime power terms. In some cases the methods prove that only finitely many terms are divisible by a bounded number of distinct primes.

1. Introduction

Let E denote an elliptic curve that is defined over $\mathbb{Q}$. See [1] or [10] for background on elliptic curves. The curve E is given by a Weierstrass equation

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with $a_1, \dots a_6 \in \mathbb{Z}$. Suppose E has a non-torsion point $Q \in E(\mathbb{Q})$. Throughout the paper, when Q denotes a point on an elliptic curve given in the form (1), the expression $x(Q)$ will denote the x-coordinate. For any non-zero $n \in \mathbb{Z}$, write

$$x(nQ) = \frac{A_n}{B_n^2}, \tag{2}$$

in lowest terms, with A_n and B_n in $\mathbb{Z}$. The sequence B is a divisibility sequence, meaning that $B_m | B_n$ whenever $m|n$ (a proof is supplied later). Since the sequence arises from an elliptic curve, it seems natural to call B an *elliptic divisibility sequence*. In the literature (see [15] for example) this term has been used for a related sequence (to be discussed at the end of the introduction), one that is also defined using a rational point on an elliptic curve. The sequence B divides the other sequence term by term and in many cases coincides with it. Silverman [11] has proposed that the definition be extended to cover both cases; his proposal is adopted in this paper.

In [3], Chudnovsky and Chudnovsky considered the likelihood that the sequences B might be a source of "large" primes. They gave some impressive examples of prime values of B_n.

Example 1.1.

$$E: \quad y^2 = x^3 + 26, \quad Q = [-1, 5]$$

The term B_{29} is a prime with 286/285 decimal digits.

$$E: \quad y^2 = x^3 + 15, \quad Q = [1, 4]$$

The term B_{41} is a prime with 510/509 decimal digits.

Received by the editor March 30, 2004 and, in revised form, April 26, 2004.
2000 *Mathematics Subject Classification.* Primary 11G05, 11A41.
Key words and phrases. Elliptic curve, isogeny, prime, elliptic divisibility sequence.
The second author was supported by an EPSRC Doctoral Training Award. Both authors thank the referee for several comments leading to improvements in the text.

In [5], further numerical work suggested that for fixed E and Q, the sequence B should only contain finitely many primes. A probabilistic argument, coupled with an affirmative answer to the elliptic Lehmer problem, suggested the number of prime terms should be uniformly bounded; see [5], [6].

An *isogeny* between elliptic curves is a group homomorphism defined by rational functions on the coordinates. Such a map has a degree d, essentially the degree of the polynomials involved in the rational map, and we say the map is a d-isogeny. The most basic example is multiplication $Q \mapsto mQ$ where m is an integer. The degree of this isogeny is m^2. Any such map factorizes as a composition of two isogenies, each of degree m. In [7], it was proved that only finitely many prime power terms B_n appear if Q is the image under a non-trivial isogeny of a rational point. In [7] we defined such a point Q to be *magnified*.[1] This definition will now be generalized.

Suppose K denotes an algebraic number field and $Q \in E(K)$ is non-torsion. We say that Q is *magnified* if the following items exist:

(1) a finite extension L/K,
(2) an elliptic curve F defined over L,
(3) an isogeny $\sigma : F \to E$ of degree $\deg(\sigma) > [L : K]$,
(4) a point $R \in F(L)$ such that $\sigma(R) = Q$.

The key point is (3), that the degree of the isogeny is strictly greater than the degree of the field extension. We say Q is *magnified from* R to indicate the dependence upon R. This definition clearly generalizes the one in [7] because the definition in that paper applied only when $L = K = \mathbb{Q}$. Furthermore, we say Q is *Galois magnified* if we are able to take for L the Galois closure of $K(R)/K$. For example, every magnified point is Galois magnified if $[L : K] = 1$ or, more generally, if L/K is an abelian extension. In the appendix to the paper an alternative way of generalizing the definition of magnified will be discussed.

Let the set of valuations on K be denoted by M_K, similarly for L. (See section 2 for the definition of valuation.)

Definition 1.2. For any number field K, and any point $Q \in E(K)$, let $S_K(Q)$ denote the non-Archimedean valuations v in M_K for which $|x(Q)|_v > 1$. The definition of $S_K(Q)$ depends upon the Weierstrass equation (1). So we assume this equation has been fixed.

Theorem 1.3. *Let E denote an elliptic curve that is defined over $\mathbb{Q}$ and let $Q \in E(K)$ denote a non-torsion, K-rational, Galois magnified point. Then there are only finitely many $n \in \mathbb{N}$ for which $S_K(nQ)$ consists of a single valuation.*

Corollary 1.4. *Let E denote an elliptic curve that is defined over $\mathbb{Q}$ and let $Q \in E(\mathbb{Q})$ denote a non-torsion rational Galois magnified point. Let B denote the associated elliptic divisibility sequence as in* (2)*. Then only finitely many terms B_n are prime powers.*

Theorem 1.3 clearly generalizes the main result in [7] and it will be proved using different methods. We expect Theorem 1.3 is true in general. It is possible to prove that only finitely many terms B_n are prime if Q is a magnified point (without the Galois condition). Later we present many examples of rational points magnified from points generating quadratic extensions. So the Galois condition comes free

[1]The term was chosen because the height of a point increases under such a map.

for such examples. Later we will also prove that sometimes a K-rational Galois magnified point is the image of a K-rational point under an isogeny.

Our generalization of the result in [7] will be applied in two ways. The first application gives a hint as to what might be ultimately true. For each positive integer l we say the point $Q \in E(K)$ is *l-magnified* if it is the image of a point under the composition of l magnifications. We say it is *Galois l-magnified* if each of the composite magnifications are Galois magnifications. For example, being magnified is the same as being 1-magnified. For $1 \leq n \in \mathbb{N}$, write

$$\nu(n) = \sum_{p|n} 1,$$

the sum running over the prime divisors of n.

Theorem 1.5. *Let E denote an elliptic curve and let $Q \in E(K)$ denote a non-torsion, K-rational, Galois l-magnified point. Then there are only finitely many $n \in \mathbb{N}$ for which $S_K(nQ)$ consists of l valuations.*

Corollary 1.6. *Let E denote an elliptic curve and let $Q \in E(\mathbb{Q})$ denote a non-torsion, rational, Galois l-magnified point. Let B denote the associated elliptic divisibility sequence as in (2). Then only finitely many terms B_n have $\nu(B_n) \leq l$.*

Example 1.7. Consider the elliptic curve

$$y^2 = x^3 - x^2 - 4x - 2.$$

The point $Q = [3, 2]$ lies on E. Let $a^2 - 4a - 4 = 0$. Then either point R with $x(R) = a$ satisfies $2R = Q$. Thus Q is a Galois magnified point. Now let $b^4 - 16b^3 - 24b^2 - 16b - 8 = 0$. Then either point S with $x(S) = b$ satisfies $2S = R$; hence R is itself Galois magnified. In both cases the Galois condition is satisfied because the extensions are quadratic. Theorem 1.5 shows that the equation $B_n = p^e q^f$ with p and q both primes has only finitely many solutions.

Conjecture. Suppose E denotes an elliptic curve and Q denotes a non-torsion rational point on E. We conjecture that for any constant C the set

$$B(C) = \{n \in \mathbb{N} : \nu(B_n) \leq C\}$$

is finite. Initially we supposed the elliptic curve E is defined over $\mathbb{Q}$: provided E is in minimal form, we conjecture further that $|B(C)|$, the number of elements in $B(C)$, satisfies

$$|B(C)| < M = M(C),$$

where $M(C)$ is a bound that depends upon C only and not Q or E. In the terms of Theorem 1.3, we expect that if $|S_K(nQ)|$ is bounded, then n is bounded without any assumptions about L/K.

The probabilistic arguments used in [5] (see also [6]) apply to support this conjecture. On the other hand, it is not easy to obtain convincing numerical evidence. Efficient tests can be applied for primality (at least for "probable primality" in the usual sense of computational number theory). However, no such tests can be applied, for example, to decide if an integer is divisible by only two primes. This appears to require the factorization of the integer and, given the rapid growth rate of the sequences B, is impractical.

The second application of Theorem 1.3 is the following. For any elliptic curve, and any integer $k \in \mathbb{Z}$, consider the algebraic point Q with $x(Q) = k$. The x-coordinates $x(nQ)$ for $n \in \mathbb{N}$ are all rational (assuming Q is non-torsion) and so

an integral sequence B can be defined, just as in (2). Theorem 1.3 applies in this situation, and later examples are provided of (singly and multiply) magnified points Q.

Example 1.8. Suppose E denotes the elliptic curve

$$y^2 + xy + y = x^3 - 36x - 70.$$

The point Q with $x(Q) = -5$ gives rise to an integral sequence B as in (2). It is doubly magnified, in one step by times 2 and in the other by times 3, from points generating respectively a quadratic and a cubic extension. The Galois closure of the second extension over the first has degree at most 6 (< 9). Hence both steps are Galois magnifications. Theorem 1.5 implies that the equation $B_n = p^e q^f$ with p and q both primes bounds n.

Nomenclature. Morgan Ward used the term *elliptic divisibility sequence* (see [9], [13] or the papers [5], [15]) for sequences u that satisfy

$$u_{n+k}u_{n-k} = u_{n-1}u_{n+1}u_k^2 - u_{k-1}u_{k+1}u_n^2$$

for all $n \geq k \in \mathbb{N}$. These sequences are intimately connected with the theory of elliptic curves. Given E and Q we can associate a divisibility sequence $\psi_n(Q)$ using the division polynomials, which satisfy the recurrence relation above; see [5] for details. Assuming without loss of generality that Q is integral, $\psi_n(Q)$ is an integral sequence with $B_n | \psi_n(Q)$. It follows that if only finitely many terms B_n have length bounded by l, the same result follows for $\psi_n(Q)$ a fortiori.

2. Valuations and heights

The valuations on $\mathbb{Q}$ consist of the usual Archimedean absolute value together with the non-Archimedean, p-adic valuations, written $|.|_p$, one for each prime p. Let v denote a valuation on K. Then either v corresponds to an embedding of K into $\mathbb{C}$ or it corresponds to a prime ideal $\mathfrak{p}$ that is a factor of a rational prime. Again, these are called Archimedean and non-Archimedean valuations. Write K_v for the completion of K with respect to v. If v is Archimedean, corresponding to the embedding $\phi : K \to \mathbb{C}$, then

$$|\alpha|_v = |\phi(\alpha)|^{1/[K:\mathbb{Q}]}.$$

If v is non-Archimedean, then it corresponds to the prime ideal $\mathfrak{p}$ dividing the rational prime p. Now

$$|\alpha|_v = |\alpha|_{\mathfrak{p}}^{e_v/[K:\mathbb{Q}]},$$

where $e_v = [K_v : \mathbb{Q}_p]$. Given any $0 \neq \alpha \in K$, the product formula holds:

$$\prod_{v \in M_K} |\alpha|_v = 1,$$

where the product runs over all valuations for K, both Archimedean and non-Archimedean. Write

$$h_v(\alpha) = \log \max\{1, |\alpha|_v\}, \tag{3}$$

for the local (logarithmic) height at v. The naïve global logarithmic height of Q is defined to be

$$h(\alpha) = \sum_{v \in M_K} h_v(\alpha) = \sum_{v \in M_K} \log \max\{1, |\alpha|_v\},$$

the sum running over all the valuations of K. The global height is insensitive to the field of definition of α in the sense that we can replace K by any extension field in which α lies and the result will be the same. If Q denotes any K-rational point on an elliptic curve, we write $h_v(Q)$ and $h(Q)$ for the above, when $\alpha = x(Q)$. Usually in the literature, the global height is further normalized by dividing by 2.

Suppose Q denotes a K-rational point of E. The theory of heights gives an estimate for

$$h(Q) = \widehat{h}(Q) + O(1),$$

where $\widehat{h}(Q)$ denotes the canonical height of Q. The canonical height enjoys the additional property that $\hat{h}(mQ) = m^2\hat{h}(Q)$ for any $m \in \mathbb{Z}$. More generally, if $\sigma : F \to E$ denotes a d-isogeny, then for $R \in F(L)$,

$$\hat{h}(\sigma(R)) = d\hat{h}(R). \tag{4}$$

Lemma 2.1. *Suppose $Q \in E(K)$ denotes a non-torsion K-rational point. Then*

$$h_v(nQ) = O(\log n \log\log n),$$

for any Archimedean valuation v.

Proof of Lemma 2.1. The estimate in Lemma 2.1 follows from an appropriate upper bound for $|x(nQ)|_v$. The Archimedean valuations correspond to the embeddings of K into $\mathbb{C}$. We assume such a valuation has now been fixed and work with the usual absolute value on $\mathbb{C}$. Putting the model (1) into the usual Weierstrass equation only translates x by a constant c_0. Let z_Q correspond to Q under an analytic isomorphism $E(\mathbb{C}) \simeq \mathbb{C}/L$, for some lattice L. Thus we may assume that the x-coordinate of a point is given using the Weierstrass $\wp$-function with Laurent expansion in even powers of z,

$$x = x(Q) = \wp_L(z_Q) + c_0 = \frac{1}{z_Q^2} + c_0 + c_2 z_Q^2 + \dots.$$

Write $\{nz_Q\}$ for nz_Q modulo L. When the quantity $|x(nQ)|$ is large it means nz_Q is close to zero modulo L; thus the quantities $|x(nQ)|$ and $1/|\{nz_Q\}|^2$ are commensurate. On the complex torus, this means that the elliptic logarithm is close to zero. So it is sufficient to supply a lower bound for $\{nz_Q\}$, and this can be given by elliptic transcendence theory (see [4]). We use Théorème 2.1 in [4] but see also [12] where an explicit version of David's Theorem appears on page 20. The nature of the bound is

$$\log|x(nQ)| \ll \log n \log\log n, \tag{5}$$

where the implied constant depends upon E, the valuation v and the point Q. □

We will need some theory of elliptic curves over local fields; see [10]. For every non-Archimedean valuation w, write L_w for the completion of L with respect to w. Write ord_w for the corresponding order function defined in terms of the prime ideal associated to w. There is a subgroup of the group of L_w-rational points:

$$E_1(L_w) = \{O\} \cup \{P \in E(L_w) : \mathrm{ord}_w(x(P)) < 0\}.$$

In [10], Silverman proves the following.

Proposition 2.2. *For all $P \in E_1(L_w)$ and all $m \in \mathbb{Z}$:*

$$\log|x(mP)|_w = \log|x(P)|_w - \log|m|_w. \tag{6}$$

This important result yields several corollaries. The first is a simple consequence of (6).

Corollary 2.3. *The sequence B is a divisibility sequence, meaning that $B_m|B_n$ whenever $m|n$.*

For finitely many prime ideals $\mathfrak{p}$ the reduction of E or F is not an elliptic curve because the reduced curve is singular. Write S for the set of valuations in M_L corresponding to all such prime ideals.

Corollary 2.4. *Suppose $\sigma : F \to E$ denotes an isogeny and $R \in F_1(L_w)$. If $w \notin S$, then $h_w(\sigma(R)) \geq h_w(R)$. The local heights are related by the formula*

$$h_w(\sigma(R)) = h_w(R) + O(1), \tag{7}$$

where the implied constant depends only upon the isogeny and is independent of R.

Proof of Corollary 2.4. Any isogeny factorizes as a composition of isogenies of prime degree. Without loss of generality, assume σ is an isogeny of prime degree m. Suppose w corresponds to the prime ideal $\mathfrak{p}$. Provided $w \notin S$ both curves and the isogeny can be reduced modulo powers of $\mathfrak{p}$ and the first statement in the Corollary follows. Applying the dual isogeny gives a similar inequality $h_w(\sigma^*(Q)) \geq h_w(Q)$ for all $Q \in E_1(L_w)$. However, composing σ with its dual gives multiplication by m on F. Now (6) applies to prove (7). □

Corollary 2.5. *Suppose S denotes any fixed, finite set of valuations of L. Then*

$$\sum_{w \in S} h_w(nR) = O((\log n)^2). \tag{8}$$

Proof. This is an immediate consequence of Lemma 2.1, for the Archimedean valuations in S and (6) for the non-Archimedean valuations in S. □

Proof of Theorem 1.3. Suppose there is an L-rational point R with $\sigma(R) = Q$, where $\sigma : F \to E$ denotes a d-isgoeny. From (4), $\hat{h}(Q) = d\hat{h}(R)$, where $\hat{h}$ denotes the canonical height of the algebraic points on E and F. The canonical height differs from the naïve height by a bounded amount; hence we are justified in using only the naïve height in the sequel. Begin by noting that

$$O(1) = dh(nR) - h(nQ). \tag{9}$$

Suppose $S_K(nQ)$ consists of the single valuation v. We may assume $v \notin S$ by Corollary 2.5. From Lemma 2.1,

$$h(nQ) - h_v(nQ) = O((\log n)^2) = h(nR) - \sum_{w \in S_L(nR)} h_w(nR),$$

recalling that $S_L(nR)$ denotes those $w|v$ with $h_w(nR) > 0$. It follows from (9) that

$$O((\log n)^2) = d \sum_{w \in S_L(nR)} h_w(nR) - h_v(nQ).$$

The right-hand side is

$$d \sum_{w \in S_L(nR)} h_w(nR) - \sum_{w \in S_L(nQ)} h_w(nQ). \tag{10}$$

The Galois assumption implies that the local height $h_w(nR)$ is the same for each $w \in S_L(nR)$ and similarly for $h_w(nQ)$. Fix $w \in S_L(nR) \subset S_L(nQ)$ by the first part of Lemma 2.4. Write $e = |S_L(nR)|$ and $f = |S_K(nQ)|$. By the Galois assumption,

$$e \quad | \quad f \quad | \quad [L_w : K_v] \quad | \quad [L : K]. \tag{11}$$

Hence (10) becomes

$$deh_w(nR) - fh_w(nQ). \tag{12}$$

Now (7) implies

$$h_w(nQ) = h_w(nR) + O(1).$$

Thus (12) can be written

$$(de - f)h_w(nQ) + O(1). \tag{13}$$

It follows from (11) that $(de - f) > 0$ if $d > [L : K]$. This is enough to bound n because $h_w(nQ)$ is quadratic in n while the expression in (13) is meant to be $O((\log n)^2)$. □

Proof of Theorem 1.5. This follows by induction using the methods in the proof of Theorem 1.3. Suppose that $Q = \sigma(R)$ is magnified via a d-isogeny σ, where R generates a Galois extension L. For a contradiction, assume the only valuations in $S_K(nQ)$ consist of those that are extended by those in $S_L(nR)$. As before, the expression (10) is $O((\log n)^2)$. Suppose there are g conjugacy classes of valuations in $S_L(nR)$ and choose representatives $w_1, \ldots, w_g$. The Galois assumption implies that the local height is the same for each valuation in a fixed class. Write e_i and f_i, as before, corresponding to each fixed class. Then, by the Galois assumption,

$$e_i \quad | \quad f_i \quad | \quad [L : K]. \tag{14}$$

Hence (10) becomes

$$\sum_{i=1}^{g} [de_i h_{w_i}(nR) - f_i h_{w_i}(nQ)]. \tag{15}$$

As before, using (7) allows (15) to be written as

$$\sum_{i=1}^{g} (de_i - f_i) h_{w_i}(nQ) + O(1). \tag{16}$$

From (14), $(de_i - f_i) > 0$ if $d > [L : K]$. As before, this is enough to bound n because the expression in (16) is meant to be $O((\log n)^2)$. This contradiction shows that each time a point is Galois magnified, a new class of non-Archimedean valuations ultimately appears in the computation of the height. □

3. Examples of magnified points

Recall Velu's formulae for isogenies [14]. Every isogeny factorizes as a product of isogenies of prime degree. So consider m to be prime in what follows. Fix notation in the following way: an isogeny $\sigma : F \to E$ will be described, where F is given in Weierstrass form:

$$F : y^2 + a'_1 xy + a'_3 y = x^3 + a'_2 x^2 + a'_4 x + a'_6.$$

Firstly, when $m = 2$, there must be a rational 2-torsion point $T = [x_1, y_1]$ on F. Write

$$\begin{aligned} t &= 3x_1^2 + 2a_2'x_1 + a_4' - a_1'y_1, \\ u &= 4x_1^3 + b_2'x_1^2 + 2b_4'x_1 + b_6', \\ w &= u + x_1 t. \end{aligned}$$

Of course $u = 0$; this is simply a device to unify the presentation. Then there is a 2-isogeny σ to a curve E taking $R = [x, y]$ to $\sigma(R) = Q$, where

$$x(Q) = x + t/(x - x_1).$$

The isogenous curve E has the form

$$[a_1, a_2, a_3, a_4, a_6] = [a_1', a_{2,}', a_{3,}' a_4' - 5t, a_6' - b_2't - 7w]. \tag{17}$$

For odd m, let $T = [x_1, y_1]$ denote a point of order m on the curve and write its multiples as $kT = (x_k, y_k)$, for $1 < k < m$. The point T may or may not have coordinates in the base field $\mathbb{Q}$. However, the formulae, when applied to a point R on a curve F over $\mathbb{Q}$, yield an isogenous curve E and a point Q. The formulae for t, u, w are given as follows. Define, for each k with $1 \le k \le (m-1)/2$,

$$\begin{aligned} t_k &= 6x_k^2 + b_2'x_k + b_4', \\ u_k &= 4x_k^3 + b_2'x_k^2 + 2b_4'x_k + b_6', \\ w_k &= u_k + x_k t_k. \end{aligned}$$

Then with

$$t = \sum t_k, \qquad u = \sum u_k, \qquad \text{and} \qquad w = \sum w_k,$$

the formula for E is exactly as in (17) and $x(Q)$ is given by

$$x(Q) = x + \sum_{k=1}^{(m-1)/2} \left\{ \frac{t_k}{(x - x_k)} + \frac{u_k}{(x - x_k)^2} \right\}. \tag{18}$$

Proposition 3.1. *Suppose $Q \in E(K)$ is a non-torsion point and $mR = Q$, where R generates a Galois extension L/K. Suppose that for all the points R', which are Galois conjugates of R, $R - R'$ is a K-rational m-torsion point. Then Q is the image of a K-rational point under an isogeny.*

When $m = 2$, the hypothesis about $R - R'$ is always satisfied. This is because $R + R'$ is a K-rational point that doubles to $2Q$; hence it differs from Q by a K-rational torsion point. Write $R + R' + T = Q$: T is non-trivial because if $R + R' = Q = 2R$, then $R = R'$ and hence R is K-rational. Finally, $R + R' + T = Q = 2R$ implies $R - R' = T$.

Proof of Proposition 3.1. If R is K-rational, we are done. Otherwise, let R' denote any conjugate of R not equal to R. Then $R - R' = T$ is a K-rational m-torsion point on the curve F. Use this point to construct an m-isogeny to an elliptic curve defined over K as above. Plainly $\sigma(T) = \mathcal{O}$. Hence $\mathcal{O} = \sigma(R - R') = \sigma(R) - \sigma(R') = \sigma(R) - \sigma(R)'$, which shows that $\sigma(R) \in E(K)$. Now the dual isogeny $\sigma^* : F \to E$ has $\sigma^*\sigma$ equal to multiplication by m on E. Hence $\sigma(R)$ is a K-rational point that maps to Q under the isogeny σ^*. □

TABLE 1.

m	E	Q	Torsion Order	Magnification
2	$[1,-1,1,4,6]$	[0, 2]	4	2
	$[0,-1,0,-4,-2]$	[3, 2]	2	2
	$[1,-1,1,20,22]$	[8, 21]	4	3
	$[1,-1,1,-23,-34]$	[-2, 1]	2	3
	$[1,-1,1,-37,124]$	[2, -9]	4	2
	$[1,-1,1,-67,226]$	[14, 36]	4	2
	$[1,1,0,4,0]$	[1, 2]	2	2
	$[1,0,0,-10,-13]$	[7, 13]	2	2
	$[1,-1,1,7,-8]$	[2, 2]	2	2
	$[1,1,1,-63,156]$	[6, 3]	4	2
	$[[1,0,1,12,-14]$	[2, 3]	2	2
	$[0,0,0,9,0]$	[4, 10]	2	2
	$[1,-1,0,-990,-11745]$	[238, 3513]	2	3
	$[0,1,0,-39,-108]$	[12, 36]	2	2
	$[1,-1,0,90,436]$	[12, 50]	2	2
3	$[0,1,1,-7,5]$	[-1, 3]	3	2
	$[0,-1,1,-65,-204]$	[12, 24]	1	2

Proposition 3.1 is provable under even weaker hypotheses. If all the points $R-R'$ can be written as multiples of a single m-torsion point, then that m-torsion point can be used in Velu's formula to construct an m-isogeny σ with the same property as above, i.e., that $\sigma(R)$ is a K-rational point with image Q under the dual isogeny. Note however that the isogenous curve is not necessarily defined over K.

TABLE 2.

m	E	k	Torsion Order	Magnification
2	$[1,0,1,-36,-70]$	8	6	1
		7		1
		-5		2
	$[1,0,1,-171,-874]$	-8	2	1
	$[1,0,1,-11,12]$	-4	6	1
	$[1,1,1,-10,-10]$	-4	8	2
3	$[1,0,1,4,-6]$	-1	6	1
		-3		1
		-19		1
3	$[1,0,1,-36,-70]$	9	6	1
		4		1
		-5		2
		-1		1
		-3		1
		-9		1
3	$[1,0,1,-1,0]$	-9	6	2
3	$[1,0,1,-11,12]$	-5	6	1
		-7		1
4	$[1,1,1,-10,-10]$	-13	8	1
5	$[0,-1,1,0,0]$	-1	5	1

The interest in this paper is that we can construct points that are multiply magnified. Table 1 shows elliptic curves with multiply magnified generators Q under some multiplication by an m map. The curves are recorded in the form $[a_1, a_2, a_3, a_4, a_6]$ to agree with (1). The examples were found among the first 500 rank-1 curves on Cremona's tables [2] using the wonderful PARI-GP computing package [8]. For each curve, we computed a factorization of the polynomial of degree m^2 whose roots are the x-coordinates of the points R with $mR = Q$. If the order of magnification is 2, there is a point S with $mS = R$ that generates a field of degree m^2. Order 3 indicates the point S is itself magnified from a point that generates a field of degree m^3. Note that when $m = 3$, Theorem 1.3 is satisfied because the Galois closure of each extension has degree at most 6.

Table 2 shows algebraic points Q with $x(Q) = k$ associated to the first few elliptic curves by a conductor. In every case we searched for $k = x(Q)$ with $|k| \leq 20$. The table shows the curve E together with x-coordinates of algebraic points magnified from another algebraic point by a multiplication by an m map. Line 3 is repeated at line 13 because the point shown is doubly magnified via multiplication by 2 and 3.

Appendix

All of the main conclusions in the paper can be given under an alternative generalization of the definition of the term *magnified*. We could define the term to mean that Q is the image of an L-rational point under an isogeny of degree $d \geq 2$, where d is coprime to $[L : K]$. This condition can certainly be fulfilled. On the other hand, in all the examples we have found, a magnified point according to this definition is simultaneously magnified from a rational point. We believe the definition could have some value, i.e., a magnification in this sense could form part of a chain of maps comprising a multiple magnification.

Table 3 shows rank-1 elliptic curves E together with generators Q. In each case there is a 3-isogeny that maps a point R to Q, where R generates a quadratic extension. Besides this, there is a 3-isogeny that maps a rational point to Q. These

Table 3.

E	Q	Torsion Order
$[0, 1, 1, -7, 5]$	[-1, 3]	3
$[0, 0, 1, -24, 45]$	[-3, 9]	3
$[0, -1, 0, 8, -16]$	[4, 8]	1
$[0, 1, 1, -27, 55]$	[-5, 9]	3
$[1, 0, 0, -2, 4]$	[-2, 2]	3
$[0, 1, 1, 3, 2]$	[2, 4]	3
$[1, 0, 0, 3, 1]$	[0, 1]	1
$[0, 1, 0, -5, -5]$	[-2, 1]	2
$[0, -1, 0, 2, -1]$	[1, 1]	1
$[1, 0, 0, 4, 16]$	[-2, 0]	3
$[1, 1, 0, 3, 1]$	[0, 1]	1
$[1, -1, 1, 46, 209]$	[-3, 7]	3
$[0, 0, 1, -42, 105]$	[5, 4]	3
$[0, -1, 0, -53, -131]$	[-4, 1]	1
$[0, 1, 0, -101, 359]$	[2, 13]	3

were computed using Velu's formulae as above. The table also shows the order of the rational torsion on E.

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves,* London Math. Soc. Student Texts 24, Cambridge Univ. Press, 1991. MR1144763 (92k:11058)

[2] J. E. Cremona, *Elliptic Curve Data* up-dated 14-1-02, http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html

[3] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Adv. in Appl. Math. 7 (1986), 385–434. MR0866702 (88h:11094)

[4] Sinnou David, *Minorations de formes linéaires de logarithmes elliptiques,* Mém. Soc. Math. France (N.S.) (1995), no. 62, iv+143. MR1385175 (98f:11078)

[5] Manfred Einsiedler, Graham Everest and Thomas Ward, *Primes in elliptic divisibility sequences,* LMS J. Comp. Math. 4 (2001), 1–13. MR1815962 (2002e:11181)

[6] Graham Everest, Alf van der Poorten, Igor Shparlinski and Thomas Ward, *Recurrence Sequences,* Mathematical Surveys and Monographs 104, Amer. Math. Soc., 2003. MR1990179 (2004c:11015)

[7] Graham Everest, Victor Miller and Nelson Stephens, *Primes generated by elliptic curves,* Proc. Amer. Math. Soc. 32 (2004), 955–963. MR2045409

[8] PARI-GP, http://www.parigp-home.de

[9] Rachel Shipsey, *Elliptic divisibility sequences,* Ph.D. thesis, Univ. of London, 2000.

[10] Joseph H. Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag, New York, 1986. MR0817210 (87g:11070)

[11] Joseph H. Silverman, *Common divisors of elliptic divisibility sequences over function fields,* Manuscripta Math. 114 (2004), 431–446.

[12] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms,* Acta. Arith., 67 (1994), 177–196. MR1291875 (95m:11056)

[13] Christine Swart, *Elliptic divisibility sequences,* Ph.D. thesis, Univ. of London, 2003.

[14] J. Velu, *Isogénies entre courbes elliptiques,* C. R. Acad. Sci. Paris, 273 (1971), 238-241. MR0294345 (45:3414)

[15] Morgan Ward, *Memoir on elliptic divisibility sequences,* Amer. J. Math., 7 (1948), 31–74. MR0023275 (9:332j)

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom

E-mail address: g.everest@uea.ac.uk

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom

E-mail address: h.king@uea.ac.uk