Canad. J. Math. Vol. **68** (5), 2016 pp. 1120–1158
http://dx.doi.org/10.4153/CJM-2015-005-0

Integral Points on Elliptic Curves and Explicit Valuations of Division Polynomials

Katherine E. Stange

Abstract. Assuming Lang's conjectured lower bound on the heights of non-torsion points on an elliptic curve, we show that there exists an absolute constant C such that for any elliptic curve $E/\mathbb{Q}$ and non-torsion point $P \in E(\mathbb{Q})$, there is at most one integral multiple $[n]P$ such that $n > C$. The proof is a modification of a proof of Ingram giving an unconditional, but not uniform, bound. The new ingredient is a collection of explicit formulæ for the sequence $v(\Psi_n)$ of valuations of the division polynomials. For P of non-singular reduction, such sequences are already well described in most cases, but for P of singular reduction, we are led to define a new class of sequences called *elliptic troublemaker sequences*, which measure the failure of the Néron local height to be quadratic. As a corollary in the spirit of a conjecture of Lang and Hall, we obtain a uniform upper bound on $\widehat{h}(P)/h(E)$ for integer points having two large integral multiples.

1 Introduction

A famous theorem of Siegel states that there are only finitely many integral points on any elliptic curve $E/\mathbb{Q}$. Of course, this implies that among the multiples $[n]P$ of any particular point P, only finitely many may be integral. In this context there are two natural ways to give a bound: on the number of such points, and on the size of n. If one assumes either the *abc* Conjecture of Masser and Oesterlé or Szpiro's Conjecture and restricts attention only to elliptic curves in minimal Weierstrass form, then the *number* of integral points among the multiples of P is bounded uniformly according to Hindry and Silverman [16]. This is also known unconditionally for curves of integral j-invariant [26].

The best known result bounding the *size* of n is due to Ingram [17], who uses lower bounds on linear forms in elliptic logarithms to bound n in terms of the height of E, and the quantity $M(P)$, defined as the smallest m such that $[m]P$ has non-singular reduction modulo all primes (note that $M(P)$ can be bounded above in terms of E alone). Using a gap principle, Ingram goes on to find a constant C, depending only on $M(P)$ (and not the height of E) such that at most one multiple $[n]P$ is integral for $n > C$. At the moment, analogous results bounding integral points among linear combinations $[n]P + [m]Q$ seem to be out of reach.

In this paper, we obtain a similar result in which the constant depends only on the ratio of heights $h(E)/\widehat{h}(P)$, defined as follows. The canonical height of a point P is

Received by the editors August 13, 2013; revised January 5, 2015.
Published electronically July 14, 2016.
The author's research has been supported by NSERC PDF-373333 and NSF MSPRF 080291.
AMS subject classification: **11G05**, 11G07, 11D25, 11B37, 11B39, 11Y55, 11G50, 11H52.
Keywords: elliptic divisibility sequence, Lang's conjecture, height functions.

given by

$$\widehat{h}(P) := \frac{1}{2}\lim_{n\to\infty}\frac{h([2^n]P)}{4^n},$$

where $h(P) := h(x(P))$, the logarithmic height of the x-coordinate. The height of E is

$$h(E) := \max\{h(j), \log|\Delta|, 1\}.$$

See Section 11 for more detail.

Theorem 1.1 *There are uniform constants C and C' such that for all elliptic curves $E/\mathbb{Q}$ in minimal Weierstrass form, and non-torsion points $P \in E(\mathbb{Q})$, there is at most one value of*

$$n > \max\left\{C\frac{h(E)}{\widehat{h}(P)}\log\left(\frac{h(E)}{\widehat{h}(P)}\right), C'\right\} \tag{1.1}$$

such that $[n]P$ is integral. Furthermore, this one value is prime.

The bulk of the proof consists of giving complete closed formulæ for the valuations of elliptic divisibility sequences at primes of bad reduction, which ingredient is combined with established methods of Ingram [17]. The formulæ themselves are considered a principal goal of this paper, but we will first discuss the implications of Theorem 1.1.

The restriction to minimal elliptic curves is necessary, since otherwise there exist methods of constructing examples with arbitrarily many integral points. Throughout the paper we compare this result to [17, Theorem 1], which differs only in that the bound (1.1) is replaced by $n > CM(P)^{16}$. These bounds are quite different. For example, one does not expect curves of large height necessarily to have large $M(P)$. The quantity $M(P)$ divides the least common multiple of the Tamagawa numbers of E, which measure the number of components in the fibres of the Néron model.

Unfortunately, the constants C and C' in Theorem 1.1, while effective, are quite large. More details can be found in Section 11.

The bound becomes uniform if one assumes a well-known conjecture of Lang, given here in a slightly strengthened form (for details, see Section 11).

Lang's Height Conjecture ([19, p. 92], [29, Conjecture 9.9]) *There is a uniform constant C_L such that for any elliptic curve $E/\mathbb{Q}$ in minimal Weierstrass form, and point $P \in E(\mathbb{Q})$ of infinite order,*

$$\widehat{h}(P) > C_L h(E).$$

Lang's conjecture follows from the *abc* Conjecture, via Szpiro's Conjecture [16]. The bound on n in Theorem 1.1 becomes uniform if we assume any of these conjectures. In particular, the bound is uniform if we restrict to elliptic curves of integral j-invariant, or curves for which the denominator of the j-invariant is divisible by a bounded number of primes, for which Lang's conjecture is known to hold [16, 25]. The uniformity of the bound in Theorem 1.1 in the case of integral j-invariant is already a result of Ingram's original argument [17] (but this does not extend to curves whose j-invariant is divisible by a bounded number of primes).

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

The following is an immediate corollary to the main result.

Corollary 1.2 *There are uniform constants c and c' such that for any elliptic curve $E/\mathbb{Q}$ in minimal Weierstrass form, and point $P \in E(\mathbb{Q})$ of infinite order having at least two integral multiples $[n]P$ and $[m]P$ satisfying $n > m > c'$, then $\widehat{h}(P) \leq ch(E)$.*

Call a triple (P, n, m) satisfying the hypotheses of Corollary 1.2 *far-out* for the constant c'. Then the theorem and corollary state that Lang's Height Conjecture is incompatible with the existence of far-out triples for arbitrarily large c'; in essence, sufficiently far-out triples would generate examples of points P with large ratio $h(E)/\widehat{h}(P)$ (*i.e.*, extreme examples for Lang's Height Conjecture).

Compare to another conjecture of Hall and Lang, which posits an upper bound on the height of an integral point in terms of the height of the curve. Note that any P with integral multiples is necessarily integral.

Hall-Lang Conjecture ([20, Conjecture 5]) *There is a uniform constant C_{HL} such that for any elliptic curve $E/\mathbb{Q}$ in minimal Weierstrass form, and integral point $P \in E(\mathbb{Q})$ of infinite order, $\widehat{h}(P) < C_{HL}h(E)$.*

This conjecture generalises a conjecture of Hall for elliptic curves of the form $y^2 = x^3 + b$ [15]. In [20], Lang used a slightly different definition of $h(E)$ than we use here; see Section 11 for a justification that they are equivalent. The conjecture seems out of reach; the best known bounds with a uniform constant are exponential in $h(E)$ ([2, 23, 32, 34], but see also [22]).

In this light, Corollary 1.2 states roughly that far-out triples satisfy a Hall-Lang bound (even if Lang's Height Conjecture holds, it may allow "moderately" far-out triples). More interestingly, a strengthening of Theorem 1.1 would lead to a Hall-Lang result in cyclic subgroups. Specifically, if (1.1) could be strengthened to

$$n > \max\left\{ C\left(\frac{h(E)}{\widehat{h}(P)}\right)^{\frac{1}{2}}, C' \right\},$$

then one would obtain the following statement: There are uniform constants D_1 and D_2 such that for any integral point P, all integral multiples $Q = [n]P$ of P satisfying $n > D_1$, except at most one, satisfy $h(E)/\widehat{h}(Q) > D_2$. To derive this, one uses the fact that $h([n]P) = n^2h(P) + O(1)$ (see, for example, [29, §VIII.6].

Theorem 1.1 is proved using the following estimate for P such that $[n]P$ is integral (Proposition 11.6):

$$\widehat{h}(P) \leq \log n + \tfrac{16}{3}h(E).$$

Ingram's argument depends upon a similar estimate, which in turn depends upon an examination of the division polynomials Ψ_n of an elliptic curve. In particular, for a point P, he bounds the size $|\Psi_n(P)|$ in relation to the denominator D_n of $[n]P$, by considering the valuations $v_p(\Psi_n(P))$ for each prime. The sequence $W_n = \Psi_n(P)$ is called an *elliptic divisibility sequence*, or EDS.

As one might expect, the arithmetic geometry of the underlying curve and point shows itself in the number theory of the elliptic divisibility sequence, which is a subject of interest in its own right. In fact, if one pursues an analogy to the relationship

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

between an EDS and its underlying curve, replacing the elliptic curve with a twist of the multiplicative group, then one obtains, instead of an EDS, a Lucas sequence of the first kind such as the Mersenne or Fibonacci numbers. The centuries-old number theoretic questions about Lucas sequences such as the prime factorisation of their terms, when asked about elliptic divisibility sequences, translate to questions about the arithmetic geometry of P and E such as the orders of P under reduction to finite fields. A great many of these questions have been studied for EDS: appearance of prime terms [7, 10], primitive divisors [12, 18, 38], squares and powers [11, 14, 21], and the sign of terms [31], to name a few.

In this paper, we give a full, explicit description of the possible sequences of valuations $v(W_n)$ for an EDS over a p-adic field or a number field. Ingram's result depends on work of Cheon and Hahn on such sequences of valuations [3], and it is here that the dependence on $M(P)$ arises. Cheon and Hahn describe the sequence of valuations recursively, determining a growth rate. In contrast, this paper provides a closed form whose parameters depend on the reduction properties of P and E. It is this that allows us to prove the estimate of Proposition 11.6 and therefore Theorem 1.1. However, it is the intention of this paper to give a complete description of these valuation sequences for its own sake, and this work makes up the bulk of the paper.

Proposition 11.6 is obtained from Lemma 11.4, which is the moment at which the EDS results are used to feed into the proof of Theorem 1.1. It came to the author's attention after this paper was written that the same result appears in Mahe [21, Proposition 4.2.3], with a proof by different methods.

For primes of good reduction for the associated elliptic curve, the sequence of valuations at a prime place is well understood and has a simple, pleasing description that has become a sort of "folk theorem", although its first appearance in print is due to Cheon and Hahn [3, 4] (but see Remark 6.5).

Theorem 1.3 (Introductory form of Theorem 6.1; see Section 6 for references to other versions appearing in the literature) *Let E be an elliptic curve with good reduction over a p-adic field K with valuation v. Let $n_P > 1$ be the order of $P \in E_0(K)/E_1(K)$. Suppose that E is a minimal Weierstrass model and that $v(W_{n_P}) > \frac{v(p)}{p-1}$. Then*

$$v(W_n) = \begin{cases} v(W_{n_P}) + v(n/n_P) & n_P \mid n, \\ 0 & n_P \nmid n. \end{cases}$$

In Theorem 6.1, we give a more complete characterisation than has, to our knowledge, appeared in the literature. In particular, we remove the assumption that $v(W_{n_P}) > \frac{v(p)}{p-1}$ at the cost of some extra complication to the formula.

In contrast to the good reduction case, the primes of bad reduction often pop up in great quantity in an EDS, in frequency depending on the reduction of P on the Néron model. We now state an introductory theorem combining all types of reduction (each treated separately in the paper).

Theorem 1.4 (Introductory combination of Theorems 3.3, 6.1, 7.1, 9.3 and 10.1) *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. Let W_n be an EDS associated with an elliptic curve E/K in Weierstrass form and non-torsion $P \in E(K)$. There exist integers*

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

$a, \ell, c_1, c_2, c_3, c_4, c_5$ such that

$$v(W_n) = \frac{1}{c_1}\left(R_n(a,\ell) + c_2 n^2 + c_3 + \begin{cases} c_4 + v(n) & c_5 \mid n \\ 0 & c_5 \nmid n \end{cases} \right),$$

where

$$R_n(a,\ell) = \left\lfloor \frac{n^2 \widehat{a}(\ell - \widehat{a})}{2\ell} \right\rfloor - \left\lfloor \frac{\widehat{na}(\ell - \widehat{na})}{2\ell} \right\rfloor,$$

and $\widehat{x}$ denotes the least non-negative residue of x modulo ℓ.

Furthermore,

$$a = 0 \iff R_n(a,\ell) \equiv 0 \iff \left\{ \begin{array}{l} E \text{ has potential good reduction or} \\ P \text{ has non-singular reduction} \end{array} \right\}.$$

The full results in this paper apply to all p-adic fields and to torsion points at the cost of some complication to the final term of the formula. They also provide much more detail about the significance and possible values of the parameters. The sequences $R_n(a,\ell)$, here dubbed *elliptic troublemaker sequences*, satisfy a host of properties examined in Section 8.

For P such that $[n]P \neq \mathcal{O}$, the valuations of W_n are connected to Néron–Tate local heights by the following relationship [28, Exercise VI.6.4(e)]:

$$\lambda_v\big([n]P\big) = n^2 \lambda_v(P) - \log|W_n|_v + \frac{n^2-1}{12}\log|\Delta|_v.$$

Some portions of the results in this paper can be viewed as results about local heights and could be proved by recourse to the established theory of such.

In the case of good reduction in minimal Weierstrass form, Theorem 1.3 implies that $v(W_n)$ is asymptotically equal to $v(n)$ as a function of n (on the non-zero terms). Cheon and Hahn show, using a recurrence relation for EDS (see (3.1)), that for P non-torsion having singular reduction, $v(W_n)$ is asymptotically equal to Cn^2 for some constant C [3]. Everest and Ward use the elliptic Jensen formula to give a growth rate in this situation of

$$\log|\Psi_n(P)|_v = \big(\lambda_v(P) + \log|\Delta|_v/12\big)\, n^2 + O(n^C),$$

for some constant $0 < C < 2$, which may depend on P [9, Theorem 3]. Here, $\lambda_v(P)$ is the Néron local height (note that [9] uses a different normalisation than ours; we follow Silverman [28, Chapter VII]). Everest and Ward use this result to give an algorithm for computing the canonical height of a point. Theorem 12.1 improves the error term on this estimate to $O(\log n)$; see Section 12.1.

For any torsion point P, the W_n are supported only on primes of bad reduction (see Remark 6.3). Gezer and Bizim give some explicit descriptions of these valuations over $\mathbb{Q}$ for $N < 13$ [13, Theorem 2.2]. Their formulæ can be restated in terms of elliptic troublemaker sequences. See Section 12.2.

Sections 2 and 3 provide background. Section 5 generalises the central lemma on formal groups that lies at the core of Theorem 1.3. Sections 6, 7, 9, and 10 describe the valuation sequence $v(W_n)$ for each type of reduction. Section 8 considers the properties of elliptic troublemaker sequences. Section 11 proves Theorem 1.1, while Section 12 examines a few other connections and applications. Finally, Section 13

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

gives some detailed examples of elliptic divisibility sequences and their sequences of valuations.

2 Preliminaries on Division Polynomials

In this section, we briefly catalogue some of the standard properties of division polynomials. The proofs are largely computational, and are omitted. For background, see especially [1, Section 2], but also [8, Chapter 9] and [29, Exercise III.3.7]. Division polynomials are usually defined for elliptic curves, but here we will suppose only a cubic curve E (possibly singular) given in standard Weierstrass form

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

The division polynomials $\Psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ for the curve E are defined recursively using the initial values

$$\begin{aligned}
\Psi_1 &= 1,\\
\Psi_2 &= 2y + a_1x + a_3,\\
\Psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\Psi_4 &= \Psi_2 \cdot \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2\right.\\
&\qquad\qquad \left. + (b_2b_8 - b_4b_6)x + (b4b_8 - b_6^2)\right),
\end{aligned}$$

(here b_i are the usual quantities [29, Section III.1]) and the recurrences

$$\begin{aligned}
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, && \text{for } m \geq 2\\
\Psi_{2m}\Psi_2 &= \Psi_{m-1}^2\Psi_m\Psi_{m+2} - \Psi_{m-2}\Psi_m\Psi_{m+1}^2, && \text{for } m \geq 3.
\end{aligned} \tag{2.1}$$

If $\Psi_2 = 0$, then let $\Psi_{2m} = 0$ for all m. For an elliptic curve E, the n-th division polynomial vanishes at all non-trivial n-torsion points: it has divisor $\sum_{Q\in E[n]}(Q) - n^2(\mathcal{O})$. (We will use $\mathcal{O}$ for the identity of an elliptic curve.)

Proposition 2.1 *Let E be an elliptic curve. Then P is a non-trivial n-torsion point if and only if $\Psi_n(E, P) = 0$.*

There exist $\phi_n, \omega_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ such that the multiplication-by-n formulæ for an elliptic curve are given by

$$[n]P = \left(\frac{\phi_n}{\Psi_n^2}, \frac{\omega_n}{\Psi_n^3}\right).$$

In fact, ϕ_n and ω_n can be given by the following relations:

$$\begin{aligned}
\phi_n &= x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1},\\
4y\omega_n &= \Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2.
\end{aligned}$$

If we assign the natural weights

$$w(x) = 2, \quad w(y) = 3, \quad w(a_i) = i, \tag{2.2}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

then the Weierstrass equation is homogeneous of weight 6. Any change of coordinates between Weierstrass equations of the form

$$x' = u^2 x, \quad y' = u^3 y$$

changes the coefficients according to $a_i' = u^i a_i$ and $\Delta' = u^{12}\Delta$. These weights are useful in determining the valuations of division polynomials.

Proposition 2.2 *The division polynomials Ψ_n have the following properties.*

(i) *Using the natural weights (2.2), Ψ_n, ϕ_n, and ω_n are homogeneous of weight n^2-1, $2n^2$, and $3n^2$, respectively.*

(ii) *As polynomials in x,*

$$\Psi_n^2 = n^2 x^{n^2-1} + (\textit{lower order terms}) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x],$$
$$\phi_n = x^{n^2} + (\textit{lower order terms}) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x].$$

(iii) *If E is given by a v-integral Weierstrass equation, where v is a non-archimedean valuation, and $v(x), v(y) < 0$, then $v(\phi_n) = n^2 v(x)$.*

(iv) *The change of variables $x' = u^2 x + r$ and $y' = u^3 y + sx + t$ from E to E' gives*

$$\Psi_n(x', y', E') = u^{n^2-1}\Psi_n(x, y, E).$$

(v) *Whenever $n \mid m$ for $n, m \geq 1$, we have $\Psi_n \mid \Psi_m$.*

The division polynomials satisfy the more general recurrence equation

$$\Psi_{n+m+s}\Psi_{n-m}\Psi_{r+s}\Psi_r + \Psi_{m+r+s}\Psi_{m-r}\Psi_{n+s}\Psi_n + \Psi_{r+n+s}\Psi_{r-n}\Psi_{m+s}\Psi_m = 0,$$

from which the recurrences (2.1) can be obtained as special cases [33, Theorem 3.7].

Finally, using the Weierstrass σ-function and the usual complex uniformization $\mathbb{C}/\Lambda$ of an elliptic curve over $\mathbb{C}$, Ward showed that [37, Theorem 12.1],

$$\Psi_n(z, \Lambda) = \frac{\sigma(nz, \Lambda)}{\sigma(z, \Lambda)^{n^2}}. \tag{2.3}$$

3 Preliminaries on Elliptic Divisibility Sequences

Definition 3.1 An *elliptic divisibility sequence*, or EDS, is a sequence W_n in an integral domain[1] satisfying

$$W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0. \tag{3.1}$$

The connection between EDS and elliptic curves is described by Ward in his original memoir on the subject. We next state an updated version of Ward's theorem that applies to fields of characteristic zero and cubic curves.

Theorem 3.2 (Ward [37, Theorem 12.1], Shipsey [24, Theorem 4.5.3], S. [33]) *Let E be a cubic curve defined over a field K of characteristic zero, given by Weiestrass form, and let $P \in E(K)$. Then $W_n = \Psi_n(P)$ is an elliptic divisibility sequence. Furthermore,*

[1] One could define such sequences in a more general context, but we will be concerned only with local and global fields.

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

if $W_n \in K$ is an elliptic divisibility sequence with $W_2W_3 \neq 0$, $W_1 = 1$, then there exists a cubic Weierstrass curve E/K and $P \in E(K)$ so that $W_n = \Psi_n(P)$.

In other words, any non-degenerate EDS over K appears as the sequence of division polynomials for some cubic Weierstrass curve E/K evaluated at a point $P \in E(K)$. (As (3.1) is homogeneous, we may first scale so that $W_1 = 1$.) The term "divisibility" in "elliptic divisibility sequence" refers to Proposition 2.2(v). In particular, any EDS arising from a rational point on an elliptic curve $E/\mathbb{Q}$ in minimal Weierstrass form is an integer sequence with the property that $n \mid m \implies W_n \mid W_m$.

Let E be an elliptic curve defined over K (by this we will always mean that E is given by a Weierstrass equation), and let $\mathcal{O} \neq P \in E(K)$. Let W_n be the elliptic divisibility sequence associated with E and P. If we change the Weierstrass equation for E, we can change the elliptic divisibility sequence. For example, it will be convenient to change the equation to one in minimal Weierstrass form, so we can consider the reduction type. Fortunately, the associated elliptic divisibility sequence changes in a simple fashion, as described by Proposition 2.2(iv). This immediately gives the following result, which will be important enough for the later results that we include it as a theorem.

Theorem 3.3 *Let E be an elliptic curve defined over a p-adic field K with valuation v, given by Weierstrass form, and let $\mathcal{O} \neq P \in E(K)$. Let W_n be the associated elliptic divisibility sequence. Then there exists an isomorphism $\phi\colon E \to E'$, defined over K, to an elliptic curve E' in minimal Weierstrass form. Let W'_n be the elliptic divisibility sequence associated with $\phi(P)$. Then there exists an $r_P \in \mathbb{Z}$ such that*

$$v(W_n) = (n^2 - 1)r_P + v(W'_n).$$

4 Notation

Throughout the remainder of the paper (except for Sections 11–13), let p be a prime, let K be a finite extension of $\mathbb{Q}_p$, and let R be the ring of integers of K, with maximal ideal $\mathcal{M}$. Let v be a valuation for K, let π be a uniformizer, and let $\mathbf{k}$ be the residue field. Let E be an elliptic curve defined over K, let $P \in E(K)$, and let W_n be the EDS associated with E and P.

5 Central Lemma on Formal groups

For a point of non-singular reduction, the sequence of valuations $v(W_n)$ is controlled by the formal group of the elliptic curve. For points of singular reduction, the sequence of valuations is partially controlled by the formal group of either the elliptic curve, or the multiplicative group, depending on the type of reduction. In both cases, the results rely on a lemma describing the valuations of the multiples of a point in an abstract formal group. Although the formula (5.1) below is quite complicated in most cases we encounter, the variable j takes the value 0, whereupon (5.1) simply reduces to $v(z) + v(n)$. For background on formal groups, see [29, Chapter IV].

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Lemma 5.1 *Let $\mathcal{F}$ be a one-parameter formal group defined over R, and let $z \in \mathcal{F}(\mathcal{M})$. There exist integers b, j, h, and $w \in \mathbb{Z}^{\geq 0} \cup \{\infty\}$ such that for all integers n,*

$$v([n]z) = \begin{cases} b^j v(z) + \frac{b^j - 1}{b-1} h + v(n) - jv(p) + w & \text{if } v(n) > jv(p), \\ b^{v(n)/v(p)} v(z) + \frac{b^{v(n)/v(p)} - 1}{b-1} h & \text{if } v(n) \leq jv(p). \end{cases} \tag{5.1}$$

Furthermore:

(i) *b is the smallest power of T with a coefficient not divisible by p in the series $[p]T$, and h is the valuation of said coefficient. If no such integer exists, then $b = 1$ and $h = 0$. Otherwise, $p \mid b$ and $b > 1$.*

(ii) *If $b = 1$, then $j = 0$. If $b \neq 1$, then j is the smallest non-negative integer such that*

$$v(p) \leq b^j \big((b-1)v(z) + h \big).$$

(iii) *$w = 0$ unless $b > 1$ and $v(p) = b^j((b-1)v(z) + h)$, in which case*

$$w = v\left(\frac{[p^{j+1}]z}{([p^j]z)^p} \right) - h,$$

which may be equal to ∞.

Remark 5.2 For the formal additive group, given by $f(X, Y) = X + Y$, the series for multiplication-by-m is $[m]T = mT$, so $b = 1$, $h = j = w = 0$, and therefore (5.1) simplifies to $v([n]z) = v(z) + v(n)$.

For the formal multiplicative group, given by $f(X, Y) = (X + 1)(Y + 1) - 1$, multiplication-by-$m$ is

$$[m]T = (T+1)^m - 1 = T^m + mT^{m-1} + \binom{m}{2} T^{m-2} + \cdots + mT,$$

so $b = p$ and $h = 0$.

The formal group of an elliptic curve in standard Weierstrass form is given by

$$\begin{aligned} f(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) \\ + 2a_3(X^3Y + XY^3) + (a_1a_2 - 3a_3)X^2Y^2 + \cdots . \end{aligned}$$

In particular, it may occur that one or more of the conditions $h > 0$, $b > p$, and $j \neq 0$ may hold, for example, over a highly ramified 2-adic field. See Examples 13.2 and 13.5.

Proof of Lemma 5.1 By [29, Proposition IV.2.3(a)], multiplication-by-n has the form

$$[n]T = nT + O(T^2).$$

Suppose n is coprime to p. Since $v(z) > 0$, we obtain $v([n]z) = v(z)$. Since $[m_1m_2]T = [m_1]([m_2]T)$, it therefore suffices to consider only n equal to a power of p. Let $a_k = v([p^k]z)$ for all non-negative k.

By [29, Corollary IV.4.4], the formal group law for $[p]$ has the form

$$[p]T = pf(T) + g(T^p), \tag{5.2}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

where f and g have no constant term. We may also assume that the coefficients in g are not divisible by p. By [29, Proposition IV.2.3(a)],

$$f(T) = T + O(T^2).$$

Let $b \in \mathbb{Z}$ be the smallest power of T in $g(T^p)$ with a non-zero coefficient, and let h be the valuation of that coefficient (so, in particular, $0 \leq h < v(p)$). Let us momentarily skip the case where $g \equiv 0$, so that we have $p \mid b$ and $b \geq p > 1$. Define j to be the smallest non-negative integer such that

$$v(p) \leq b^j\big((b-1)v(z) + h\big).$$

For the moment, let us also assume that the inequality is not an equality.

From (5.2),

$$v([p]z) \geq \min\big\{v(z) + v(p), bv(z) + h\big\}. \tag{5.3}$$

Suppose that $j > 0$. Then, since $v(p) > (b-1)v(z) + h$, the second option determines the minimum in (5.3), in which the inequality is an equality, and so $a_1 = ba_0 + h$.

Repeating this argument for all $k \leq j$, we find

$$a_1 = ba_0 + h \implies a_2 = b^2a_0 + bh + h \implies \cdots \implies a_j = b^ja_0 + \frac{b^j - 1}{b-1}h.$$

For $k = j+1$, we again obtain (5.3) (where we replace z with $[p^j]z$), but $v(p) < b^j((b-1)v(z) + h)$, so the first option determines the minimum, again where inequality is equality, which implies that

$$a_{j+1} = a_j + v(p) = b^ja_0 + \frac{b^j - 1}{b-1}h + v(p).$$

Repeating this argument, we find that for all $k > j$,

$$a_k = b^ja_0 + \frac{b^j - 1}{b-1}h + (k-j)v(p),$$

from which the result follows with $w = 0$.

Now suppose that $v(p) = b^j((b-1)v(z) + h)$. This gives $v(p) = (b-1)a_j + h$. The only place in which this affects the proof is the application of (5.3) for $k = j+1$. In this case, the minimum in (5.3) compares two equal values, and we obtain instead the alternate form

$$a_{j+1} = a_j + v(p) + w,$$

for w either ∞ (if $[p^{j+1}]z = 0$) or a non-negative integer. If $w \neq \infty$, then we find that

$$w = a_{j+1} - a_j - v(p) = a_{j+1} - a_j - (b-1)a_j - h = v([p^{j+1}]z) - bv([p^j]z) - h.$$

For $k > j+1$, $a_k = a_{k-1} + v(p)$ as before. Combining this with the other cases yields the general formula.

Finally, we return to the case that $g \equiv 0$. In this case, (5.3) is replaced with

$$v\big([p]z\big) = v(z) + v(p),$$

and we obtain the formula with $b = 1$, $h = 0$, $j = 0$, and $w = 0$. ∎

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

The formula in Lemma 5.1 being somewhat cumbersome, we set some notation for the class of such sequences.

Definition 5.3 Suppose $p \in \mathbb{Z}$ is a prime, and let u be the valuation on $\mathbb{Q}$ associated with p. Suppose

$$b \in p\mathbb{Z}^{>0} \cup \{1\}, \quad d \in \mathbb{Z}^{>0}, \quad h \in \mathbb{Z}^{\geq 0}, \quad s \in \mathbb{Z}^{>0} \cup \{\infty\}, \quad w \in \mathbb{Z}^{\geq 0} \cup \{\infty\}.$$

If $b = 1$, set $j = 0$. Otherwise, let j to be the smallest non-negative integer such that

$$d \leq b^j\big((b-1)s + h\big).$$

Define a sequence in $\mathbb{Z} \cup \{\infty\}$,

$$S_n(p,b,d,h,s,w) = \begin{cases} b^j s + \frac{b^j-1}{b-1}h + d(u(n) - j) + w & u(n) > j, \\ b^{u(n)}s + \frac{b^{u(n)}-1}{b-1}h & u(n) \leq j. \end{cases}$$

We record a few properties whose proofs are immediate.

Proposition 5.4 (i) *If $j = 0$, then $S_n(p,b,d,h,s,0) = s + du(n)$.*
(ii) *For any integer k, $S_n(p,b,kd,kh,ks,kw) = kS_n(p,b,d,h,s,w)$.*
(iii) *For fixed integers p, b, d, h, s, and w, $S_n(p,b,d,h,s,w) = O(\log n)$.*

6 Non-singular Reduction

The sequence $v(W_n)$ for a point of non-zero non-singular reduction has been described in various contexts in [3, Theorem 1] (but see Remark 6.5), [4, Lemma], [5, Lemma 2.6], [30, Lemma 5], [36, Lemma 3.4]. Loosely speaking, in most cases one expects that for non-torsion points with non-singular reduction of order $n_P > 1$,

$$v(W_n) = \begin{cases} v(W_{n_P}) + v(n/n_P) & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases} \tag{6.1}$$

There are exceptions, however. Lemma 5.1 on formal groups allows us to prove a somewhat stronger, more general statement. Please refer to Definition 5.3 for the sequence S_n, which generalises (6.1).

Theorem 6.1 *Assume that E is in minimal Weierstrass form, P has non-singular reduction, and let n_P be the smallest non-negative integer such that $[n_P]P = \widetilde{\mathcal{O}}$ over the residue field $\mathbf{k}$. There exist*

$$b_P \in p\mathbb{Z}^{>0} \cup \{1\}, \quad h_P \in \mathbb{Z}^{\geq 0}, \quad s_P \in \mathbb{Z}^{>0} \cup \{\infty\}, \quad w_P \in \mathbb{Z}^{\geq 0} \cup \{\infty\},$$

such that

$$v(W_n) = \min\left\{0, \frac{v(x(P))}{2}\right\} n^2 + \begin{cases} S_{n/n_P}(p, b_P, v(p), h_P, s_P, w_P) & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases} \tag{6.2}$$

Furthermore, $v(x(P)) < 0$ if and only if $n_P = 1$.

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Corollary 6.2 *Assume that P is a non-trivial* torsion *point with non-singular reduction to a point of order $n_P > 1$. Suppose that E is a minimal Weierstrass model. Then*

$$v(W_n) = \begin{cases} \infty & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases}$$

Remark 6.3 This corollary implies that the non-zero terms of an elliptic divisibility sequence associated with an integral torsion point P are supported only on the primes of bad reduction. If P is a non-integral torsion point (necessarily of order 2), then the non-zero terms of the EDS are supported on primes of bad reduction, and 2. See Example 13.3.

Corollary 6.4 *Assume that P is a* non-torsion *point with non-singular reduction to a point of order $n_P > 1$. Suppose that E is a minimal Weierstrass model. Under any of the conditions* (i)–(iii) *below, we have*

$$v(W_n) = \begin{cases} v(W_{n_p}) + v(n/n_P) & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases} \tag{6.3}$$

(i) $v(p) < (p-1)v(W_{n_p})$.
(ii) $K = \mathbb{Q}_p$, *and we are not in the special case that* $p = 2$, $v(W_{n_p}) = 1$ *and* E *has ordinary or multiplicative reduction.*
(iii) K *is unramified over* $\mathbb{Q}_p$ *and* $p \geq 3$.

Remark 6.5 The statement of [3, Theorem 1] corresponding to Theorem 6.1 is incorrect, in that it holds only under the missing assumption that E is in minimal Weierstrass form. This assumption is required when applying [29, Proposition VII.2.2] during the proof of their Lemma 1. Furthermore, they give the simpler form (6.3) while neglecting to include the assumption that $v(p) < (p-1)v(W_{n_p})$ or an equivalent. These omissions are corrected in the later paper [4].

We now prove Theorem 6.1 and its corollaries.

Proof of Theorem 6.1 There is a standard isomorphism of groups (see [29, Proposition VII.2.2])

$$\Theta\colon E_1(K) \longrightarrow \widehat{E}(\mathcal{M}), \quad (x, y) \mapsto -\frac{x}{y},$$

where $\widehat{E}(\mathcal{M})$ is the formal group of E. Write

$$[n]P = \left(\frac{\phi_n}{\Psi_n^2}, \frac{\omega_n}{\Psi_n^3} \right) \tag{6.4}$$

as in Section 2.

We begin with the case that $n_P = 1$, *i.e.*, $\widetilde{P} = \widetilde{\mathcal{O}}$. Writing $P = (x, y)$, we have $n_P = 1$ if and only if $v(x) < 0$. From the minimal Weierstrass equation for E, we obtain $2v(x) = 3v(y)$. Let $v_0 = v(y) - v(x) = \frac{1}{2}v(x)$. Then $v(x) = 2v_0$ and $v(y) = 3v_0$. Since $v_0 < 0$, by Proposition 2.2(iii), $v(\phi_n) = 2n^2 v_0$, from which we obtain

$$v\big(\Theta([n]P)\big) = v(x/y) = -1/2v(x) = v(\Psi_n) - n^2 v_0.$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Then

$$v(\Psi_n) = \frac{v(x(P))}{2} n^2 + v\big(\Theta([n]P)\big). \tag{6.5}$$

Now suppose that $\widetilde{P} \neq \widetilde{\mathcal{O}}$ instead. Then we have $v(\Psi_n), v(\phi_n), v(\omega_n) \geq 0$ (by the definition of the division polynomials). A theorem of Ayad [1, Theorem A] implies that since P has non-zero non-singular reduction, at least one of $v(\Psi_n)$ and $v(\phi_n)$ is zero for each n. It follows that $n = n_P$ is the smallest positive n such that $v(\Psi_n) > 0$, and that $v(\phi_{kn_P}) = 0$. This implies $v(\omega_{kn_P}) = 0$ by (6.4) and the form of the Weierstrass equation. Therefore, for all integers k,

$$v\big(\Theta([kn_P]P)\big) = v(-\phi_{kn_P}\Psi_{kn_P}/\omega_{kn_P}) = v(\Psi_{kn_P}). \tag{6.6}$$

Now, in both cases ($n_P = 1$ and $n_P \neq 1$), Lemma 5.1, written in terms of Definition 5.3, says

$$v\big(\Theta([kn_P]P)\big) = S_k\big(p, b_P, v(p), h_P, v(\Theta([n_P]P)), w_P\big)$$

for some b_P, h_P, and w_P. If $n_P \nmid n$, then $v(\Psi_n) = 0$. This, combined with (6.5) and (6.6), completes the proof. ∎

Proof of Corollary 6.2 Since $n_P > 1$, we have $v(W_n) = 0$ whenever $n_P \nmid n$. Furthermore, $s_P = v(W_{n_P}) = \infty$ since $W_{n_P} = 0$ by Proposition 2.1. ∎

Proof of Corollary 6.4 In all three parts, we use the notation of Theorem 6.1 and Lemma 5.1.

Condition (i) Since P is non-torsion, $v(W_{n_P}) \neq \infty$. Since $n_P > 1$,

$$v(W_n) = \begin{cases} S_{n/n_P}(p, b_P, v(p), h_P, v(W_{n_P}), w_P) & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases}$$

Condition (i) implies that $j = 0$ (since $h \geq 0$) in Definition 5.3 (since this is immediate if $b_P = 1$, while otherwise $b_P \geq p$ from which it follows). Condition (i) also implies $w_P = 0$ by Lemma 5.1(iii). By Proposition 5.4(i),

$$S_k\big(p, b_P, v(p), h_P, v(W_{n_P}), 0\big) = v(W_{n_P}) + v(p)u(k) = v(W_{n_P}) + v(k).$$

Condition (ii) For $\mathbb{Q}_p$, $h_P = 0$ by definition. We have $v(p) = 1$, and so

$$(p-1)v(W_{n_P}) \geq p - 1 \geq 1 = v(p).$$

Furthermore, the overall inequality between leftmost and rightmost is strict (and hence we are in Condition (i) and we are done) except possibly in the case where $p = 2$ and $v(W_{n_P}) = 1$. Either way, $j = 0$. Then, according to Lemma 5.1 and the proof of Theorem 6.1,

$$w_P = v([2]z/2z),$$

where $z = \Theta([n_P]P)$. If $w_P = 0$, we are done as in Condition (i). For an elliptic curve, the formal group law is

$$[2]z = 2z - a_1 z^2 - 2a_2 z^3 + O(z^4),$$

so that in the case that $a_i \in R$, $p = 2$ and $v(z) = 1$,

$$v([2]z/2z) > 0 \iff v(1 - a_1 z/2) > 0 \iff v(a_1) = 0.$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

(Recall that the residue field $\mathbf{k}$ has only one unit since $p = 2$.) As remarked in the proof of [30, Lemma 5],

$$v(a_1) = 0 \iff E \text{ has ordinary or multiplicative reduction.}$$

Condition (iii) Since $p \geq 3$, and K is unramified over $\mathbb{Q}_p$,

$$v(p) \leq v(W_{n_p}) < (p-1)v(W_{n_p})$$

and therefore Condition (i) is satisfied. ∎

7 Singular Reduction on a Curve of Potential Good Reduction

In the case where P has singular reduction but E has potential good reduction, we can extend the field and change coordinates to obtain a minimal Weierstrass equation of good reduction for the curve. Keeping track of the effect this has on the elliptic divisibility sequence allows us to give a formula for the valuations $v(W_n)$.

Theorem 7.1 *Assume that E has potential good reduction, and $P \in E(K)$ has EDS W_n. There exists an isomorphism $\phi : E \to E'$ to an elliptic curve in minimal Weierstrass form with good reduction such that ϕ is defined over a finite extension L of K, with ramification degree $d \mid 24$. Let v_1 be a valuation of L lying over v, such that $v_1(z) = dv(z)$ for $z \in K$, and let W'_n be the EDS associated with $\phi(P)$. Then*

$$dv(W_n) = (n^2-1)dv(\Delta_E)/12 + v_1(W'_n),$$

where $v_1(W'_n)$ is of the form (6.2) of Theorem 6.1, since $\phi(P)$ has non-singular reduction. Furthermore, $12 \mid dv(\Delta_E)$.

Proof of Theorem 7.1 By the theory of reduction types, over some extension L/K, and under an appropriate change of coordinates defined over L, we obtain an isomorphic curve and point E' and P' having good reduction. Let v_1 be the valuation for L lying above v such that $v_1(z) = dv(z)$ for $x \in K$, where d is the degree of ramification of L over K. Then $dv(W_n)$ is the valuation of the sequence associated with E and P considered over L. Changing coordinates, using Theorem 3.3, we obtain

$$dv(W_n) = (n^2-1)r + v_1(W'_n)$$

for some $r \in \mathbb{Z}$ such that $0 = v_1(\Delta_{E'}) = dv(\Delta_E) - 12r$. If E has bad reduction, the extension L/K is ramified, so that $d > 1$ [29, Proposition VII.5.4(a)]. Furthermore, we can choose L so that d divides 12 by changing to Legendre normal form [29, Proofs of Propositions III.1.7(a), VII.5.4(c)], unless $p = 2$, in which case d divides 24 by changing to Deuring normal form [29, Proofs of Propositions A.1.3 and A.1.4(a)]. Even if E/K was minimal, E/L will not be minimal. ∎

Remark 7.2 Ayad shows that a P of non-trivial reduction on a minimal curve has singular reduction if and only if $v(W_n) > 0$ for all $n \geq 2$ [1, Theorem A]. In the above theorem, if P has singular reduction, we do indeed obtain sequences satisfying $v(W_n) > 0$ for all $n \geq 2$. See Example 13.5.

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

The following proposition gives some restrictions on the parameters used in Theorem 7.1.

Proposition 7.3 *Under the hypotheses and notations of Theorem 7.1, let*

$$d' = \frac{12}{\gcd(v(\Delta_E), 12)}.$$

(i) *If* $d' = 2, 4$, *then* $n_P \in \{1, 2\}$.
(ii) *If* $d' = 3$, *then* $n_P \in \{1, 3\}$.
(iii) *If* $d' = 6, 12$, *then* $n_P = 1$.

For Proposition 7.3, we require an elementary number theoretical lemma.

Lemma 7.4 *Let* $a, b \in \mathbb{Z}^{>0}$. *Suppose that for all integers n,*

$$n \not\equiv 0 \pmod{a} \implies n^2 \equiv 1 \pmod{b}. \tag{7.1}$$

Then

$$(a, b) \in \left\{ (1, *), (*, 1), (2, 2), (3, 3), (2, 4), (2, 8) \right\},$$

where $*$ *represents any positive integer.*

Proof The statement (7.1) holds vacuously if $a = 1$ and trivially if $b = 1$. If $a = 2$, choosing $n = 3$ implies $b \in \{1, 2, 4, 8\}$. If $a = 3$, choosing $n = 2$ implies $b \in \{1, 3\}$. If $a > 3$, choosing $n = 2$ and $n = 3$ implies that $b = 1$. ∎

Proof of Proposition 7.3 We can assume that $n_P > 1$. By Theorems 7.1 and 6.1, there are parameters d, b, h, s, w such that

$$dv(W_n) = (n^2 - 1)dv(\Delta_E)/12 + \begin{cases} S_{n/n_P}(p, b, dv(p), h, s, w) & \text{if } n_P \mid n, \\ 0 & \text{if } n_P \nmid n. \end{cases} \tag{7.2}$$

Write $r = dv(\Delta_E)/12 \in \mathbb{Z}$, and $g = \gcd(d, r)$. It is an exercise in elementary number theory to see that $d/g = \gcd(v(\Delta_E), 12)$. The exercise is as follows: if $y \mid dv$, then $d/\gcd(d, dv/y) = y/\gcd(v, y)$.

The first claim is that without loss of generality, we can assume (7.2) holds for some (possibly different) d, b, h, s, w having $g = 1$. Since $v(W_n) \in \mathbb{Z}$, we find that for n divisible by n_P,

$$S_{n/n_P}(p, b, dv(p), h, s, w) \equiv 0 \pmod{g}.$$

If $n = n_P$, we find that $g \mid s$, and from this we deduce that $g \mid h$ (if $j = 0$, we can simply change h without changing the function S_{n/n_P}; otherwise, take n satisfying $v(n/n_P) = 1$). Then $g \mid w$ by taking n having $v(n/n_P)$ large enough. Therefore, by Proposition 5.4(ii),

$$S_{n/n_P}\left(p, b, dv(p), h, s, w\right) = gS_{n/n_P}\left(p, b, dv(p)/g, h/g, s/g, w/g\right).$$

Therefore, we can divide (7.2) by g, *i.e.,* replace d by $d/g = \gcd(12, v(\Delta_E))$, and parameters h, s, w replaced by their own quotients with g. This is the proof of the claim. Therefore, without loss of generality let us assume that $\gcd(d, r) = 1$ and $d = \gcd(12, v(\Delta_E))$.

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Table 1: Elliptic troublemaker sequences $R_n(a,\ell)$ for various (a,ℓ).

n:	1	2	3	4	5	6	7	8	9	10	11	12	13
$R_n(1,2)$:	0	1	2	4	6	9	12	16	20	25	30	36	42
$R_n(1,3)$:	0	1	3	5	8	12	16	21	27	33	40	48	56
$R_n(2,3)$:	0	1	3	5	8	12	16	21	27	33	40	48	56
$R_n(1,4)$:	0	1	3	6	9	13	18	24	30	37	45	54	63
$R_n(2,4)$:	0	2	4	8	12	18	24	32	40	50	60	72	84
$R_n(1,5)$:	0	1	3	6	10	14	19	25	32	40	48	57	67
$R_n(2,5)$:	0	2	5	9	15	21	29	38	48	60	72	86	101
$R_n(1,6)$:	0	1	3	6	10	15	20	26	33	41	50	60	70
$R_n(2,6)$:	0	2	6	10	16	24	32	42	54	66	80	96	112
$R_n(3,6)$:	0	3	6	12	18	27	36	48	60	75	90	108	126
$R_n(1,7)$:	0	1	3	6	10	15	21	27	34	42	51	61	72
$R_n(2,7)$:	0	2	6	11	17	25	35	45	57	71	86	102	120
$R_n(3,7)$:	0	3	7	13	21	30	42	54	69	85	103	123	144
$R_n(1,11)$:	0	1	3	6	10	15	21	28	36	45	55	65	76

Since $v(W_n)$ is an integer and $r = dv(\Delta_E)/12$ is an integer,

$$n \not\equiv 0 \pmod{n_P} \implies (n^2-1)r \equiv 0 \pmod{d}.$$

Since r is coprime to d, Lemma 7.4 implies that the implication only holds if

$$(n_P, d) \in \big\{(1,*),(*,1),(2,2),(2,4),(2,8),(3,3)\big\}. \qquad \blacksquare$$

8 Elliptic Troublemaker Sequences

In this section we define a class of integer sequences that will be needed to describe $v(W_n)$ for points P of singular reduction on an elliptic curve E with multiplicative or potential multiplicative reduction.

Definition 8.1 With any pair (a,ℓ) of integers satisfying $\ell \neq 0$, we associate an integer sequence called the *elliptic troublemaker sequence*, defined for $n \geq 0$ by

$$R_n(a,\ell) = \left\lfloor \frac{n^2\widehat{a}(\ell-\widehat{a})}{2\ell} \right\rfloor - \left\lfloor \frac{\widehat{na}(\ell-\widehat{na})}{2\ell} \right\rfloor, \tag{8.1}$$

where $\widehat{x}$ denotes the least non-negative residue of x modulo ℓ.

Some examples are given in Table 1. We devote the rest of this section to properties of these sequences.

Proposition 8.2 *The function $R_n(a,\ell)$ has the following properties.*

(i) $R_n(0,\ell) = 0$.
(ii) $R_0(a,\ell) = R_1(a,\ell) = 0$.
(iii) $R_n(a,\ell) = R_n(\ell \pm a, \ell)$.
(iv) *For any positive integer k, $R_n(ka,k\ell) = kR_n(a,\ell)$.*

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

(v) *For positive integers n and m,* $R_n(ma,\ell) = R_{nm}(a,\ell) - n^2 R_m(a,\ell)$.

(vi) $R_{n+1}(a,\ell) + R_{n-1}(a,\ell) - 2R_n(a,\ell) < \ell$.

(vii) *For* $0 < n < \ell/a$,

$$R_n(a,\ell) = \frac{n^2-n}{2}a.$$

(viii) *If* $\ell \mid na$ *or if* $0 \le a < \ell \le 7$, *then*

$$R_n(a,\ell) = \left\lfloor \frac{n^2 a(\ell-a)}{2\ell} \right\rfloor. \tag{8.2}$$

(ix) *An alternative formula for* $R_n(a,\ell)$ *is*

$$R_n(a,\ell) = \frac{\ell}{2}\left(\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right)^2 - \left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right) - n^2\left(\frac{a}{\ell} - \left\lfloor \frac{a}{\ell} \right\rfloor \right)^2 + n^2\left(\frac{a}{\ell} - \left\lfloor \frac{a}{\ell} \right\rfloor \right) \right). \tag{8.3}$$

(x) *If* $0 \le a < \ell$, *then an alternate formula for* $R_n(a,\ell)$ *is*

$$R_n(a,\ell) = \frac{\ell}{2}\left(\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right)^2 - \left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right) + \frac{n^2 a(\ell-a)}{\ell^2} \right). \tag{8.4}$$

(xi) *Let* $B_2(t) = t^2 - t + \frac{1}{6}$, *called the* second Bernoulli polynomial, *and let* $\widetilde{B}_2(t) = B_2(t - \lfloor t \rfloor)$, *called the* periodic second Bernoulli polynomial. *Then an alternate formula for* $R_n(a,\ell)$ *is*

$$R_n(a,\ell) = \frac{\ell}{2}\left(\widetilde{B}_2\left(\frac{na}{\ell} \right) - n^2 \widetilde{B}_2\left(\frac{a}{\ell} \right) + \frac{n^2-1}{6} \right).$$

(xii) *An alternate formula for* $R_n(a,\ell)$ *is*

$$R_n(a,\ell) = \frac{n^2-n}{2}a + \left(\sum_{k=1}^{\lfloor \frac{na}{\ell} \rfloor} k\ell - na \right) - n^2\left(\sum_{k=1}^{\lfloor \frac{a}{\ell} \rfloor} k\ell - a \right). \tag{8.5}$$

(xiii) *We have*

$$\left| R_n(a,\ell) - \left(\frac{\widehat{a}(\ell-\widehat{a})}{2\ell} \right) n^2 \right| \le \frac{\ell}{8},$$

where $\widehat{x}$ *denotes the least non-negative residue of* x *modulo* ℓ.

Proof We prove the various parts out of order according to the various interdependencies.

Parts (i), (ii), (iii), *and* (viii): Direct calculations from the definition.

Part (vi): For $0 \le x \le 1$, $0 \le x(1-x)/2 \le 1/8$, so that as b ranges through the least non-negative residues modulo ℓ,

$$0 \le \frac{b(\ell-b)}{2\ell} \le \ell/8. \tag{8.6}$$

For any A and B,

$$\lfloor A \rfloor + \lfloor B \rfloor \le \lfloor A+B \rfloor, \quad \lfloor A \rfloor + \lfloor -A \rfloor = -1. \tag{8.7}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

From the definition, (8.6), and (8.7),

$$R_{n+1}(a,\ell)+R_{n-1}(a,\ell)-2R_n(a,\ell)\le\left\lfloor\frac{a(\ell-a)}{\ell}\right\rfloor-2+2\left(\frac{\ell}{8}\right)<\ell.$$

Part (x): We will show that (8.4) is equal to (8.1), under the assumption $0\le a<\ell$.

We consider the case $\ell\mid na$ separately. In this case, using (8.4), to show (8.1) (or actually (8.2)), we need only check that $\frac{n^2a(\ell-a)}{\ell}$, which is an integer divisible by ℓ, is even. Both cases, $2\mid\ell$ and $2\nmid\ell$, are immediate. Therefore, we assume that $\ell\nmid na$.

We express certain quantities in terms of their integer and fractional parts. Write

$$\frac{na}{\ell}=X+x,\quad \frac{n(\ell-a)}{\ell}=Y+y,\quad \frac{n^2a(\ell-a)}{2\ell}=Z+z,$$

where X,Y,Z are integers and $0<x,y<1$ and $0\le z<1$. We also know that $x+y=1$. Furthermore, x and y are rationals with denominator dividing ℓ. We have

$$Z+z=\frac{\ell}{2}(X+x)(Y+y).$$

Write

$$\frac{\ell}{2}(X+x)(Y+y)=\frac{1}{2}(\ell XY+\ell xY+X\ell y)+\frac{\ell}{2}xy.$$

We wish to show that the first of the two terms on the right is an integer. That is, we want to show the integer $\ell XY+(\ell x)Y+X(\ell y)$ is even (note that x and y are not integers, but ℓx and ℓy are). We do this by cases. If $X\equiv Y\equiv 0\pmod 2$, then the integer is even. If $X\equiv Y\equiv 1\pmod 2$, then

$$\ell XY+(\ell x)Y+X(\ell y)\equiv\ell+\ell x+\ell y\equiv 2\ell\equiv 0.$$

If $X\not\equiv Y$, by symmetry we can assume that $X\equiv 0$ and $Y\equiv 1$. Since $X+Y=n-1$, we discover that $n\equiv 0$. Then, since $na=X\ell+x\ell$,

$$\ell XY+(\ell x)Y+X(\ell y)\equiv naY\equiv 0.$$

Thus, we have discovered that $\frac{1}{2}(\ell XY+\ell xY+X\ell y)$ is an integer.

Hence,

$$Z=\frac{1}{2}(\ell XY+\ell xY+X\ell y)+\left\lfloor\frac{\ell}{2}xy\right\rfloor,\quad z=\frac{\ell}{2}xy-\left\lfloor\frac{\ell}{2}xy\right\rfloor.$$

Write $x=s/\ell$ for some $0<s<\ell$ (in other words, $s=\widehat{na}$). Noting that $xy=x-x^2$, and substituting for the meaning of x, y and z in the second equation, we obtain

$$\left(\left\lfloor\frac{n^2a(\ell-a)}{2\ell}\right\rfloor-\frac{n^2a(\ell-a)}{2\ell}\right)-\frac{\ell}{2}\left(\left(\frac{na}{\ell}-\left\lfloor\frac{na}{\ell}\right\rfloor\right)^2-\left(\frac{na}{\ell}-\left\lfloor\frac{na}{\ell}\right\rfloor\right)\right)=\left\lfloor\frac{s(\ell-s)}{2\ell}\right\rfloor,$$

as required.

Part (ix): If $0\le a<\ell$, it is immediate that (8.3) reduces to (8.4). Therefore, using parts (iii) and (x), it suffices to check that (8.3) is independent of the choice of residue of a modulo ℓ. But this is a direct calculation (compare the formula (8.3) for $R_n(a,\ell)$ and $R_n(a+\ell,\ell)$).

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Parts (iv) *and* (xi): Direct calculations from (8.3) of part ix.

Part (v): Letting

$$S(n) = \frac{\ell}{2}\left(\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor\right)^2 - \left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor\right)\right)$$

we obtain, from the formula (8.3) of part (ix),

$$\begin{aligned} R_n(ma, \ell) &= S(mn) - n^2 S(m), \\ R_{mn}(a, \ell) &= S(mn) - m^2 n^2 S(1), \\ n^2 R_m(a, \ell) &= n^2 S(m) - n^2 m^2 S(1). \end{aligned}$$

Part (xii): Let

$$T(n) = \sum_{k=1}^{\left\lfloor \frac{na}{\ell} \right\rfloor} k\ell - na.$$

A calculation reveals that

$$T(n) = \left(\left\lfloor \frac{na}{\ell} \right\rfloor^2 + \left\lfloor \frac{na}{\ell} \right\rfloor - \frac{2na}{\ell}\left\lfloor \frac{na}{\ell} \right\rfloor\right)\frac{\ell}{2}.$$

Then, expanding formula (8.3) of part (ix), we obtain

$$R_n(a, \ell) = T(n) - n^2 T(1) + \frac{\ell}{2}\left(-\frac{na}{\ell} + \frac{n^2 a}{\ell}\right).$$

Part (vii): Follows immediately from part (xii).

Part (xiii): Immediate from parts (xi) and (iii), together with the observation that $X(1 - X)$ has maximum $1/4$ on the interval $[0, 1]$. ∎

Remark 8.3 By Proposition 8.2, parts (iii) and (iv), it suffices to study sequences satisfying $0 \leq 2a \leq \ell$ with $\gcd(a, \ell) = 1$. We could index the collection of such sequences by $\mathbb{Q} \cap [0, \frac{1}{2}]$.

9 Multiplicative Reduction

We now turn to P having singular reduction on a curve E of multiplicative bad reduction, where we will require the theory of the Tate curve.

Suppose that E does not have potential good reduction, *i.e.*, $v(j_E) < 0$. In this case, there is a unique $q \in K^*$ with $v(q) > 0$ such that the Tate curve E_q is isomorphic to E over a finite extension L of K. The case of multiplicative reduction is the case that L can be taken to be unramified, and split multiplicative reduction corresponds to $L = K$. See [28, Chapter V] for background.

Definition 9.1 For any elliptic curve E/K with non-integral j-invariant, and any $P \in E(K)$, let $\phi\colon E \to E_q$ be an isomorphism to the Tate curve (note that $v(q) > 0$). Analytically, E_q is isomorphic to $K^*/q^{\mathbb{Z}}$, under which $\phi(P)$ corresponds to some $u \in K^*$. As a convention, choose u satisfying $0 \leq v(u) < v(q)$. Define

$$\ell_P = v(q), \quad a_P = v(u).$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Note that, despite the notation, the quantity ℓ_P only depends on the elliptic curve E. It is a standard fact that $\ell_P = v(\Delta(E_q)) = -v(j(E_q)) = -v(j(E))$.

Remark 9.2 Using the standard isomorphisms (see [28, Remark IV.9.6])

$$E(K)/E_0(K) \longrightarrow K^*/q^{\mathbb{Z}}R^* \longrightarrow \mathbb{Z}/\ell_P\mathbb{Z},$$

$a_P = v(u)$ is the component of the Néron model special fibre ($\cong \mathbb{Z}/\ell_P\mathbb{Z}$) containing P. In particular, $a_P = 0$ if and only if P has non-singular reduction.

Theorem 9.3 *Suppose that P has singular reduction, and E is in minimal Weierstrass form with multiplicative reduction. Let a_P and ℓ_P be as in Definition 9.1. Let n_P be the smallest positive integer such that $[n_P]P = \widetilde{\mathcal{O}}$ over the residue field $\mathbf{k}$. Then there exist*

$$s_P \in \mathbb{Z}^{>0} \cup \{\infty\}, \quad w_P \in \mathbb{Z}^{\geq 0} \cup \{\infty\}$$

such that for all positive integers n,

$$v(W_n) = R_n(a_P, \ell_P) + \begin{cases} S_{n/n_P}(p, p, v(p), 0, s_P, w_P) & n_P \mid n \\ 0 & n_P \nmid n. \end{cases} \tag{9.1}$$

Furthermore:

(i) *Letting $g = \gcd(a_P, \ell_P)$, the integers n_P and s_P are given by*

$$n_P = \frac{\ell_P \operatorname{ord}(q^{a_P/g}u^{-\ell_P/g})}{g}, \quad s_P = v(1 - q^{n_P a_P/\ell_P}u^{-n_P}).$$

where ord *denotes the multiplicative order of the image in the residue field* $\mathbf{k}$.

(ii) *If P is a torsion point of order N, then*

$$n_P = \frac{\ell_P}{\gcd(a_P, \ell_P)} = N.$$

Proof We drop the subscripts and write $\ell = \ell_P$ and $a = a_P$. First, we consider the Tate curve E_q, by which we mean (as described in [28, Theorem V.3.1]) the curve given by the model

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q), \tag{9.2}$$

in which case, the point u corresponds to $(X(u, q), Y(u, q))$, where X and Y are defined as in [28, Theorem V.3.1]. We can define $\Psi_n(u, q)$ as the usual polynomial in X and Y for (9.2). As in [28, Proposition V.3.2], define the normalised theta function as

$$\theta(u, q) = (1 - u)\prod_{k\geq 1}\frac{(1 - q^k u)(1 - q^k u^{-1})}{(1 - q^k)^2}.$$

We wish to express $\Psi_n(u, q)$ in terms of the normalised theta function. Over $\mathbb{C}$, we have

$$\Psi_n(u, q) = (-2\pi i)^{1-n^2}\frac{\sigma(u^n, q)}{\sigma(u, q)^{n^2}},$$

where

$$\sigma(u, q) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta(1)z^2}e^{-\pi i z}\theta(u, q).$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

(To see this, use (2.3), together with the standard change of coordinates to eliminate $2\pi i$, in [28, Section V.1].) Therefore, over $\mathbb{C}$,

$$\Psi_n(u,q) = u^{(n^2-n)/2}\frac{\theta(u^n,q)}{\theta(u,q)^{n^2}}. \tag{9.3}$$

Using the same method as the proof of [28, Proposition V.3.2(b)]; this relation also holds over K (in fact [28, Proposition V.3.2(b)] is a special case).

We let $W_n = \Psi_n(u,q)$ (so it is the EDS associated with (9.2) and the point $(X(u,q),Y(u,q))$). We wish to discover the form of $v(W_n)$. Note that (9.2) is always a minimal Weierstrass model in its isomorphism class (this can be verified using [29, Remark VII.1.1] and the q-expansions of Δ and c_4). Therefore, information about $v(W_n)$ for a Tate curve applies to any EDS associated with an elliptic curve E/K in minimal Weierstrass form and having split multiplicative reduction.

For any k satisfying $na + \ell k \neq 0$, we have $v(1-q^k u^n) = \min\{\ell k + na, 0\}$. For $k > 0$, we have $v(1-q^k) = 0$. Therefore (recalling that $a, n, \ell \geq 0$),

$$v(\theta(u^n,q)) = t_P(n) + \left(\sum_{k=1}^{\left\lfloor \frac{na}{\ell}\right\rfloor} k\ell - na\right),$$

where $t_P(n) = v(1-q^k u^{-n})$ for the unique integer k for which $-na + \ell k = 0$, if such an integer exists, and $t_P(n) = 0$, otherwise. Taken together with (9.3) and (8.5), this gives

$$v(W_n) = R_n(a,\ell) + t_P(n) - n^2 t_P(1).$$

However, $t_P(1) = 0$, since we assumed $0 \leq a < \ell$, and there is no integer k with $k\ell = a$.

We will now find an expression for $t_P(n)$. The equation $k\ell = na$ has no solution in k unless

$$n_0 := \frac{\ell}{\gcd(a,\ell)}$$

divides n. Therefore, if $n_0 \nmid n$, then $t_P(n) = 0$. Even if $n_0 \mid n$, and if we let k_0 be such that $k_0\ell = n_0 a$, as long as $q^{k_0}u^{-n_0} \not\equiv 1$ in $\mathbf{k}$, we still have $t_P(n_0) = 0$. Therefore, let $n_P = bn_0$ where b is the order of $q^{k_0}u^{-n_0}$ in $\mathbf{k}$. In other words, n_P is the smallest integer such that $t_P(n_P) \neq 0$, and furthermore, if $t_P(n) \neq 0$, then $n_P \mid n$. This gives the expression for n_P in item (i).

The statement of the theorem requires that we also show that n_P is the smallest positive integer such that $\widetilde{[n_P]P} = \widetilde{\mathcal{O}}$ in $E(k)$. But it is a property of division polynomials that $\widetilde{[n]P} = \widetilde{\mathcal{O}}$ exactly when $W_n \equiv 0$ in $\mathbf{k}$, *i.e.*, when $1 - q^{k(n)}u^{-n}$ vanishes in $\mathbf{k}$. Therefore, this follows from the previous paragraph.

We return to finding an expression for $t_P(n)$. At this point, we are reduced to finding an expression for $t'_P(s) = t_P(sn_P)$. Let k_P be the unique integer such that $k_P\ell = n_P a$, and set $\beta = q^{k_P}u^{-n_P}$. Then $t'_P(s) = v(1-\beta^s)$.

Let $s_P = v(1-\beta)$, which is positive by construction. Let $U(K)$ be the kernel of the reduction map $K^* \to \mathbf{k}^*$. Let $\mathbb{G}_m$ be the formal multiplicative group. By the theory of formal groups, we have an isomorphism

$$U(K) \longrightarrow \mathbb{G}_m(\mathfrak{M}), \quad u \longmapsto 1-u.$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Restricting the isomorphism

$$K^*/q^{\mathbb{Z}} \longrightarrow E_q(K), \quad u \mapsto (X(u), Y(u))$$

to $U(K)$, and recalling the isomorphism

$$\Theta\colon E_{q,1}(K) \longrightarrow \widehat{E}_q(\mathcal{M}), \quad (x, y) \longmapsto -x/y,$$

as in the proof of Theorem 6.1, we obtain a chain of isomorphisms:

$$\begin{array}{ccccccc} \mathbb{G}_m(\mathcal{M}) & \longrightarrow & U(K) & \longrightarrow & E_1(K) & \longrightarrow & \widehat{E}(\mathcal{M}) \\ 1-u & \longmapsto & u & \longmapsto & (X(u), Y(u)) & \longmapsto & -X(u)/Y(u) \end{array}$$

It can be verified by the definitions of $X(u)$ and $Y(u)$ that this chain has the property that

$$v(1-u) = v(X(u)/Y(u)).$$

So $s_P = v(1-\beta) = v\big(X(\beta)/Y(\beta)\big) = v(\Theta([n_P]P))$. (Note that $v(1-u) = v(1-u^{-1})$.)

Lemma 5.1 for $\mathbb{G}_m(\mathcal{M})$ implies

$$t'_P(s) = v(1-\beta^s) = S_s\big(p, p, v(p), 0, s_P, w_P\big),$$

for some $w_P \in \mathbb{Z}^{\geq 0} \cup \{\infty\}$. (Note that $b = p$ and $h = 0$ in Lemma 5.1 by Remark 5.2.) Thus, we have shown (9.1), for any E/K having a minimal Weierstrass equation and split multiplicative reduction. We have also found an expression for s_P and n_P (item (i)) in this case.

Now suppose that E has non-split multiplicative reduction. Then we can let L/K be an unramified extension over which E is isomorphic to E_q. Because the extension is unramified, E is minimal over L, because it is minimal over K. Therefore, E, considered over L, satisfies the assumptions of the previous case of split multiplicative reduction. Letting v_1 be the valuation of L lying over K such that $v_1(z) = v(z)$ for $z \in K$, we find that $v(W_n) = v_1(W_n)$ has the form (9.1).

In the case where W_n is associated with an N-torsion point, $N > 1$; then u must satisfy $u^N = q^s$ for some integer s coprime to N, which implies that $Na_P = s\ell_P$ by considering valuations. Combined with item (i), this shows item (ii). ∎

10 Singular Reduction on a Curve with Additive Potential Multiplicative Reduction

This section covers the last remaining case, after which the accumulated theorems of Sections 3, 6, 7, 9, and 10 combine to give Theorem 1.4. Here, $c_4 := b_2^2 - 24b_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3)$ is the usual quantity defined in terms of the coefficients of the Weierstrass equation.

Theorem 10.1 *Assume that E does not have potential good reduction. There exists an isomorphism $\phi\colon E \to E'$ to an elliptic curve in minimal Weierstrass form with multiplicative reduction, such that ϕ is defined over a finite extension L of K, with ramification degree $d \mid 24$. Let v_1 be a valuation of L lying over v such that $v_1(z) = dv(z)$ for $z \in K$, and let W'_n be the EDS associated with $\phi(P)$. Then*

$$dv(W_n) = (n^2-1)dv\big(c_4(E)\big)/4 + v_1(W'_n)$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

where $v_1(W_n')$ is of the form (6.2) of Theorem 6.1, if $\phi(P)$ has non-singular reduction, or the form (9.1) of Theorem 9.3 if $\phi(P)$ has singular reduction.

Proof Suppose that E has additive reduction. There is some finite extension of K over which E has split multiplicative reduction. So we have, by Theorem 3.3,

$$dv(W_n) = (n^2 - 1)r + v_1(W_n')$$

for some r. The extension L/K must be ramified [29, Proposition VII.5.4], so $d > 1$. The extension needed to obtain (not necessarily split) multiplicative reduction has ramification degree dividing 24 [29, Proofs of Propositions III.1.7, VII.5.4(c), A.1.3, A.1.4(a)]. To obtain split reduction may require a further unramified field extension. Therefore, $d \mid 24$. Although E/K may be minimal, E/L is no longer. The change of variables required to make it minimal must take E to E' having $v_1(c_4(E')) = 0$. Therefore, $r = dv(c_4(E))/4$. ∎

11 Integral Points

We begin with some preliminaries about heights. Let $h(p/q) = \log \max\{|p|, |q|\}$ be the usual logarithmic height on $\mathbb{Q}$. The naive height of a point $P \in E(\mathbb{Q})$ is $h(P) = h(x(P))$. The canonical height of P is

$$\widehat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h(x([2^n]P))}{4^n}.$$

This definition follows [29, §VIII.9] and differs by a factor of 2 from the definitions of some other authors. Lang [20, Theorem 2.1] shows that

$$\left| \frac{h(P)}{2} - \widehat{h}(P) \right| \leq \frac{1}{6} h(E) + O(1).$$

The meaning of the notation $h(E)$, the height of E, in the introduction is

$$h(E) = h_0(E) = \max\{h(j), \log|\Delta|, 1\}.$$

However, in this section, following Ingram, it is convenient to consider elliptic curves in short Weierstrass form,

$$y^2 = x^3 + Ax + B,$$

with integral coefficients, and to use

$$h(E) = h_I(E) = \max\left\{ h(j), \log \max\{4|A|, 4|B|\} \right\},$$

which is always at least $2 \log 2$. The statement of Theorem 1.1 is the same no matter which height is used, thanks to the following proposition, which says that the two heights are equivalent.

Proposition 11.1 $h_I(E) \asymp h_0(E)$

Proof Note that $|X + Y| \leq 2 \max\{|X|, |Y|\}$ and $\max\{4|A|, 4|B|\} \geq 4$. We have

$$\begin{aligned} h_0(E) &= \max\{h(j), \log|\Delta|, 1\} \leq 2 \max\{h(j), \log \max\{|4A^3|, |27B^2|\}, 1\} \\ &\leq 18 \max\{h(j), \log \max\{4|A|, 4|B|\}\} \\ &= 18 h_I(E) \end{aligned}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

For the other direction,

$$\begin{aligned}\log\max\{4|A|,4|B|\} &\leq \log\max\{|4A^3|,|27B^2|\} \leq 2\log\max\{|4A^3|,|\Delta|\}\\ &\leq 4\max\{h(j),\log|\Delta|,1\},\end{aligned}$$

from which we conclude that $h_I(E) \leq 4h_0(E)$. ∎

Lang [20, Conjecture 5] originally stated the Lang–Hall conjecture in terms of the height

$$h_{LH}(E) = \log\max\{|A|,|B|\}$$

and the relationship

$$h(P) < C_1 h_{LH}(E) + C_2.$$

One verifies that $h_{LH}(E) \leq h_I(E)$, that $h_I(E) \geq 2\log 2$, and much as in Proposition 11.1, one has

$$h_0(E) \leq C_1 + C_2 h_{LH}(E).$$

These facts combine to show the Lang–Hall Conjecture as stated in the introduction is equivalent to that given in [20].

Lang originally stated the Height Conjecture in terms of $h_H(E) = \log|\Delta|$. Since $h_H(E) \leq h_0(E)$, the conjecture with h_H follows from that with h_0; the conjecture stated in terms of h_0 is actually a strengthened form (see for example [29, Conjecture VIII.9.9]).

We are now ready to prove Theorem 1.1. Ingram's result is as follows.

Theorem 11.2 ([17, Theorem 1]) *There is an absolute constant C such that for all minimal elliptic curves $E/\mathbb{Q}$, and non-torsion points $P \in E(\mathbb{Q})$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P$ is integral. Furthermore, this one value is prime.*

Recall that $M(P)$ is the smallest integer n such that $[n]P$ has non-singular reduction modulo all primes. The proof of this result depends on a lemma about valuations of division polynomials, restated here. Any point $P \in E(\mathbb{Q})$, where E is in Weierstrass form, can be written uniquely in the form $(\frac{A}{D^2}, \frac{B}{D^3})$ for some $A, B, D \in \mathbb{Z}$ with $\gcd(AB, D) = 1$ and $D > 0$. We will call D the *denominator* of P.

Lemma 11.3 ([17, Lemma 3]) *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form, let $P \in E(\mathbb{Q})$ be an integral point of infinite order, and let W_n be the associated elliptic divisibility sequence. Let D_n be the denominator of $[n]P$. Then, for $n \geq 1$,*

$$\log D_n \leq \log|W_n| \leq \log D_n + n^2 M(P)^2 \log|\Delta|.$$

Ingram's proof of Lemma 11.3 depends on the results of Cheon and Hahn [3] concerning valuations of division polynomials. With the stronger results of this paper, we can replace $M(P)$ with a constant independent of the curve and point. The improved lemma is the following.

Lemma 11.4 *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form, let $P \in E(\mathbb{Q})$ be an integral point of infinite order, and let W_n be the associated elliptic divisibility sequence.*

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Let D_n be the denominator of $[n]P$. Then, for $n \geq 1$,

$$\log D_n \leq \log |W_n| \leq \log D_n + \frac{n^2}{8} \log |\Delta|.$$

Proof Since P is integral, $D_n \mid W_n$, and so we have the first inequality. To prove the second inequality, we assume E is minimal and look locally at each prime, and show that

$$v(W_n) \leq v(D_n) + \frac{n^2}{8} v(\Delta).$$

Write $\phi_n = \phi_n(P)$, $\Psi_n = \Psi_n(P) = W_n$. The second inequality is a statement about the size of $g_n = \gcd(\phi_n, \Psi_n)$. Since E is in minimal form, the quantity g_n is supported only on primes for which P has singular reduction [1, Theorem A]. In other words, $v(g_n) = \min\{v(\phi_n), v(\Psi_n)\} = 0$ for any valuation $v = v_p$ associated with a prime p at which P has non-singular reduction. In this case, $v(W_n) = v(D_n)$.

We consider the reduction type of E case-by-case.

Suppose E has multiplicative reduction. Recall the notation of Section 9, especially Definition 9.1 and Theorem 9.3, as well as the elliptic troublemaker sequence R_n of Section 8. Since P has singular reduction, $n_P > 1$. Since $\ell_P = v(\Delta)$ and $x(1-x) \leq 1/4$ for $0 \leq x \leq 1$,

$$R_n(a_P, \ell_P) \leq \frac{n^2 \widehat{a_P}(\ell_P - \widehat{a_P})}{2\ell_P} \leq \frac{\ell_P n^2}{8} = \frac{n^2}{8} v(\Delta).$$

We know

$$v(W_n) = R_n(a, \ell) + T_n,$$

where

$$T_n = \begin{Bmatrix} v(x([n]P)/y([n]P)) & n_P \mid n \\ 0 & n_P \nmid n \end{Bmatrix} = v(D_n)$$

as in the proof of Theorem 9.3. We conclude that

$$v(W_n) - v(D_n) \leq \frac{n^2}{8} v(\Delta).$$

Now suppose that E is of additive potential multiplicative reduction (refer to Section 10). In this case, $v(\Delta) > -v(j) \geq 0$. We pass to an extension of ramification degree d over which an isomorphism $\phi\colon E \to E'$ is defined between E and a minimal E' of multiplicative reduction (guaranteed by Theorem 10.1). Let $P' = \phi(P)$. Write $\Delta' := \Delta_{E'}$ and $W_n' := \Psi_n(P', E')$. Then by Theorem 10.1 and its proof (recall that v_1 is a valuation lying above the valuation v of $\mathbb{Q}_p$ such that $v_1 = dv$ on $\mathbb{Q}_p$),

$$v_1(D_n') \leq dv(D_n) + \frac{1}{4} dv(c_4),$$

as well as

$$dv(\Delta) = v_1(\Delta') + 3dv(c_4),$$
$$dv(W_n) = v_1(W_n') + (n^2 - 1)dv(c_4)/4.$$

Recall that (from the standard fact that $j = c_4^3/\Delta$),

$$3v(c_4) = v(j) + v(\Delta) > 0.$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

We obtain $v_1(\Delta') = -dv(j)$. Therefore, we may compute

$$\begin{aligned} dv(W_n) - dv(D_n) &\leq \frac{n^2-1}{4} dv(c_4) + v_1(W_n') - v_1(D_n') + \frac{1}{4} dv(c_4) \\ &\leq \frac{n^2}{12}\big(dv(j) + dv(\Delta)\big) + \frac{n^2}{8} v_1(\Delta') \\ &= \frac{n^2}{12}\big(dv(j) + dv(\Delta)\big) - \frac{n^2}{8} dv(j) \\ &= -\frac{n^2}{24} dv(j) + \frac{n^2}{12} dv(\Delta) \leq \frac{n^2}{8} dv(\Delta). \end{aligned}$$

Suppose that E has additive reduction that resolves to good reduction. Then we perform the same sort of computation, but $v_1(W_n') = v_1(D_n')$. From Theorem 7.1,

$$dv(W_n) = (n^2-1) dv(\Delta)/12 + v(W_n').$$

Then

$$\begin{aligned} dv(W_n) - dv(D_n) &\leq \frac{n^2-1}{12} dv(\Delta) + v_1(W_n') - v_1(D_n') + \frac{1}{12} dv(\Delta) \\ &= \frac{n^2}{12} dv(\Delta) \end{aligned}$$

In all cases, we find

$$v(W_n) - v(D_n) \leq \frac{n^2}{8} v(\Delta).$$

The lemma, for minimal curves, follows by combining this result for all primes.

For a curve that is not minimal, we must apply a change of variables ϕ for some u with $v(u) < 0$, where E' is minimal. We have

$$\begin{aligned} v(W_n) - v(D_n) &\leq v(W_n') - (n^2-1)v(u) - v(D_n') - v(u) \\ &\leq -n^2 v(u) + \frac{n^2}{8} v(\Delta') \\ &= -n^2 v(u) + \frac{n^2}{8}\big(v(\Delta) + 12v(u)\big) \\ &= \frac{n^2}{2} v(u) + \frac{n^2}{8} v(\Delta) \leq \frac{n^2}{8} v(\Delta). \end{aligned}$$

■

Ingram's proof of Theorem 11.2 depends upon $M(P)$ in two places: first, in Lemma 11.3 that we are replacing with Lemma 11.4, and second, when Ingram bounds the ratio $h(E)/\widehat{h}(P)$ above in [17, Lemma 5] (the proof of this lemma uses work of Silverman [25] and Hindry and Silverman [16]). In our proof, we simply track the dependence on $\widehat{h}(P)/h(E)$ instead of bounding it.

In what follows, we explain the modifications to [17] necessary to obtain Theorem 1.1. It should be pointed out that once Lemma 11.4 is in place, the remaining modifications are relatively straightforward and partially follow unpublished notes of Ingram. However, Ingram's proof spans 11 pages, 95% of which need not be modified at all. Therefore, rather than giving the full proof again, we provide details outlining the modifications only. Most modifications consists of following slight changes

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

in constants. Where more significant modifications are needed, full proofs of the relevant propositions are given.

Since Ingram considers only short Weierstrass form, he defines *quasi-minimal* to mean a curve with minimal discriminant among short Weierstrass forms with integral coefficients. Such a curve has a discriminant dividing $6^{12}\mathcal{D}$, where $\mathcal{D}$ is the true minimal discriminant [17, Proof of Lemma 5].

The first alteration is to [17, Proposition 4], restated here.

Proposition 11.5 ([17, Proposition 4]) *Let $E/\mathbb{Q}$ be an elliptic curve in quasi-minimal Weierstrass form, let $P \in E(\mathbb{Q})$ be an integral point of infinite order, and suppose that $[n]P$ is integral for some $n \geq 2$. Then*

$$\widehat{h}(P) \leq \log n + \left(\frac{16}{3}M(P)^2 + 2\right) h(E).$$

We will prove the following proposition instead.

Proposition 11.6 *Let $E/\mathbb{Q}$ be an elliptic curve in quasi-minimal Weierstrass form, let $P \in E(\mathbb{Q})$ be an integral point of infinite order, and suppose that $[n]P$ is integral for some $n \geq 2$. Then*

$$\widehat{h}(P) \leq \log n + \frac{16}{3}h(E).$$

Proof The proof is exactly as for [17, Proposition 4], except that we assume $|x(P)| > 240n^2 \exp(3h(E)/2)$ and use Lemma 11.4 in place of [17, Lemma 3]. The altered proof is included for completeness and because part of it is used later.

A lemma of David [6, Lemma 10.1] states that for $\mathcal{O} \neq Q \in E[n]$,

$$|x(Q)| \leq 120n^2 \exp(h(E)).$$

Suppose that $[n]P$ is an integral point, and suppose that

$$|x(P)| > 240n^2 \exp(4h(E)/3).$$

Then $|x(P)| > 2|x(Q)|$, and so $|x(P) - x(Q)| > \frac{1}{2}|x(P)|$, for all $\mathcal{O} \neq Q \in E[n]$. From the definition of division polynomials,

$$\Psi_n^2 = n^2 \prod_{Q \in E[n] \smallsetminus \{\mathcal{O}\}} |x(P) - x(Q)|.$$

Therefore,

$$\begin{aligned} 2\log|\Psi_n| &> 2\log n + (n^2-1)(4h(E)/3 + 2\log n + \log 120) \\ &\geq 2\log n + n^2 h(E) + (n^2-1)(2\log n + \log 120), \end{aligned}$$

since $\frac{4}{3}(n^2-1) \geq n^2$ whenever $n \geq 2$. On the other hand, as $D_n = 1$ (since $[n]P$ is integral), so by Lemma 11.4 and the fact that $\log|\Delta| \leq 4h(E)$,

$$2\log|\Psi_n| < n^2 h(E).$$

Combining these two, for $n \geq 2$, we obtain

$$0 \geq 2n^2 \log n + (n^2-1)\log 120,$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

which is a contradiction. Therefore,

$$|x(P)| \leq 240n^2 \exp(4h(E)/3). \tag{11.1}$$

By Silverman [27, Theorem 1.1], for all $P \in E(\mathbb{Q})$,

$$\left|\widehat{h}(P) - \frac{1}{2}h(x(P))\right| < 2h(E).$$

Since P is integral, $h(x(P)) = \log|x(P)|$. Therefore,

$$\widehat{h}(P) \leq \frac{1}{2}h(x(P)) + 2h(E) \leq \frac{1}{2}\log 240 + \log n + \frac{10}{3}h(E) \leq \log n + \frac{16}{3}h(E),$$

since $h(E) \geq 2\log 2$. ∎

The remaining modifications mainly involve tracking the differences in various constants throughout. We will give each statement and its modification.

Lemma 11.7 ([17, Lemma 6]) *Let $a, b > 0$ be real numbers, and set $f(x) = x^2 - a\log(x) - b$. Then $f(x) \geq 0$ for $x \geq \max\{e, a+b\}$.*

(Note that e is the natural logarithm base.) This is replaced with the following lemma.

Lemma 11.8 *Let $a > 0$ be a real number. Let $f(x) = x^2 - a\log x - a$. Then $f(x) \geq 0$ for $x \geq \max\{9, \sqrt{a\log a}\}$.*

Proof The proof is a straightforward exercise. ∎

We will use the notation $C_P := h(E)/\widehat{h}(P)$ for simplicity.

Proposition 11.9 ([17, Proposition 7]) *For all quasi-minimal $E/\mathbb{Q}$ and non-torsion $P \in E(\mathbb{Q})$, there is a constant c_0 depending only on $M(P)$, such that if $[n]P$ is integral and $n > c_0$, then n is prime. Furthermore, we can choose $c_0 = O(M(P)^{16})$, where the implied constant is absolute.*

Proposition 11.10 *For all quasi-minimal $E/\mathbb{Q}$ and non-torsion $P \in E(\mathbb{Q})$, there is a constant c_0 depending only on C_P, such that if $[n]P$ is integral and $n > c_0$, then n is prime. Furthermore, we can choose $c_0 = O(C_P\log(C_P))$, where the implied constant is absolute.*

Proof The proof mimics that of Ingram. Supposing that n is composite, put $n = qa$ where $2 \leq q \leq \sqrt{n}$ is a prime and $q \leq a$. Supposing that $[n]P = [q]([a]P)$ is integral, we may apply Proposition 11.6:

$$a^2\widehat{h}(P) = \widehat{h}([a]P) \leq \log q + \frac{16}{3}h(E).$$

Therefore, since $q \leq a$,

$$a^2 \leq \frac{\log a}{\widehat{h}(P)} + \frac{16}{3}\frac{h(E)}{\widehat{h}(P)}.$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Then, using the fact that $h(E) \geq 1$ and Lemma 11.8, we have

$$a \leq \max\left\{4, \sqrt{\frac{16}{3}\frac{h(E)}{\widehat{h}(P)}\log\left(\frac{16}{3}\frac{h(E)}{\widehat{h}(P)}\right)}\right\}.$$

The stated bound comes from applying this to $n \leq a^2$. ∎

Ingram uses David's explicit lower bounds for linear forms in elliptic logarithms. Let ω be the real period of E, and let $L_{n,m}(z,\omega) = nz + m\omega$, where z is the principal value of the elliptic logarithm of P and choose m so that $L_{n,m}(z,\omega)$ is the principal value of the elliptic logairthm of $[n]P$. See [17, §2] for details.

Lemma 11.11 ([17, Lemma 9]) *There exist absolute positive constants c_1 and c_2 such that if $[n]P$ is an integral point and $n > c_2$, then*

$$\log|L_{n,m}(z,\omega)| \leq -c_1 n^2 h(E).$$

Furthermore, we may take $c_1^{-1} = O(M(P)^6)$ and $c_2 = O(M(P)^3)$.

This is modified to become the following lemma.

Lemma 11.12 *There exist absolute positive constants c_1 and c_2 such that if $[n]P$ is an integral point and $n > c_2$, then*

$$\log|L_{n,m}(z,\omega)| \leq -c_1 n^2 h(E).$$

Furthermore, we can take $c_1^{-1} = O(C_P)$ and $c_2 = O(\sqrt{C_P})$.

Proof The proof is exactly the same, except that in place of using [17, Lemma 5], we track the dependence on C_P. ∎

Proposition 11.13 ([17, Proposition 11]) *Let $E/\mathbb{Q}$ be a quasi-minimal elliptic curve, and let $P \in E(\mathbb{Q})$ be a point of infinite order. There exist positive constants C_3 and c_4 (depending only on $M(P)$) such that for all $n > c_3$, $[n]P$ integral implies*

$$n < c_4 h(E)^{5/2}.$$

Furthermore, we may choose the constants such that $c_3, c_4 = O(M(P)^5 \log^+(M(P))^{3/2})$.

This we will replace with the following proposition.

Proposition 11.14 *Let $E/\mathbb{Q}$ be a quasi-minimal elliptic curve, and let $P \in E(\mathbb{Q})$ be a point of infinite order. There exist positive constants C_3 and c_4 (depending only on C_P) such that for all $n > c_3$, $[n]P$ integral implies*

$$n < c_4 h(E)^{5/2}.$$

Furthermore, we can choose the constants such that $c_3 = O(C_P)$ and $c_4 = O(C_P^{1/2})$.

Proof The proof is as in Ingram, except that (with reference to the notation there), by Proposition 11.6 (in lieu of [17, Proposition 4]), it now suffices to take

$$\log B = \log V_1 \geq 2\log n + 11h(E),$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

and we can use $C' = 10^{46}$. For curves with $h(E) \geq 2\pi\sqrt{3}$, we can then use the improved constant $c_4 = 10^{24}C_P^{1/2}$ (this depends on Lemma 11.12), and choosing any $0 < \epsilon < 1$, we can use

$$c_3 = \max\left\{ c_\epsilon, \left(10^{24}C_P^{1/2}\right)^{\frac{1}{1-\epsilon}} \right\},$$

where c_ϵ is a constant such that $\log n < n^{\epsilon/3}$ for all $n > c_\epsilon$. For example, if $\epsilon = 1/2$, we can take $c_\epsilon = 10^8$. (Note that Ingram makes an inconsequential error in computing c_3.) ■

Lemma 11.15 ([17, Lemma 12]) *If $E/\mathbb{Q}$ is a quasi-minimal elliptic curve, and $P \in E(\mathbb{Q})$ is a point of infinite order, then there is a constant $C = O(M(P)^4)$ such that the following holds: if z is the principal value of the elliptic logarithm of P, ω is the real period of E and $[n]P$ is an integral point, then either $|nz| > \omega/2$ or $n < C$.*

Lemma 11.16 *If $E/\mathbb{Q}$ is a quasi-minimal elliptic curve, and $P \in E(\mathbb{Q})$ is a point of infinite order, then there is a constant $C = O(C_P^{1/2})$ such that the following holds: if z is the principal value of the elliptic logarithm of P, ω is the real period of E and $[n]P$ is an integral point, then either $|nz| > \omega/2$ or $n < C$.*

Proof The proof is as in Ingram: we replace Ingram's equation (10) with our (11.1), which does not depend on $M(P)$. Then we can take $C = \sqrt{5/c_1} = \sqrt{10}C_P^{1/2}$. The proof depends on the modifications Lemma 11.12 and Proposition 11.6. ■

Proposition 11.17 ([17, Proposition 13]) *Let $E/\mathbb{Q}$ be quasi-minimal, and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose that $[n_2]P$ and $[n_1]P$ are integral points. Then there exist constants $c_5 = O(M(P)^6)$ and $c_6 = O(M(P)^{16})$ such that*

$$n_1^2 h(E) \leq c_5 \log n_2$$

whenever $n_1, n_2 > c_6$.

We replace this with the following proposition.

Proposition 11.18 *Let $E/\mathbb{Q}$ be quasi-minimal, and let $P \in E(\mathbb{Q})$ be a point of infinite order. Suppose that $[n_2]P$ and $[n_1]P$ are integral points. Then there exist constants $c_5 = O(C_P)$ and $c_6 = O(C_P^{1/2})$ such that*

$$n_1^2 h(E) \leq c_5 \log n_2$$

whenever $n_1, n_2 > c_6$.

Proof The proof is as in Ingram; we use $c_5 = 2/c_1 = 4C_P$ and $c_6 = \max\{c_0, C, K\}$, where K is an absolute constant. The proof relies on Lemmas 11.12 and 11.16, and Proposition 11.10. ■

For clarity, we now present the proof of Theorem 1.1, following [17, Theorem 1], but using the modified propositions and lemmas.

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Proof of Theorem 1.1 Let $E/\mathbb{Q}$ be a quasi-minimal elliptic curve with an integral point $P \in E(\mathbb{Q})$ of infinite order (if P were not integral, it would not have any integral multiples). Let $C_0 = \max\{c_0, c_3, c_6, c_7\}$, where

$$c_7 = \sqrt{c_5 \log c_4}$$

If $[n_1]P$ and $[n_2]P$ are integral and $C_0 < n_1, n_2$, then by Propositions 11.14 and 11.18, we have

$$n_1^2 h(E) \leq c_5 \log n_2 \quad \text{and} \quad n_2 \leq c_4 h(E)^{5/2}.$$

Combining these, we have

$$h(E) \leq \frac{5c_5}{2n_1^2} \log h(E) + \frac{c_5}{n_1^2} \log c_4. \tag{11.2}$$

Recall that

$$c_5 = O(C_P), \quad c_4 = O(C_P)^{1/2}$$

and since $n_1 > c_6 \geq O(C_P^{1/2})$, the first constant in (11.2) can be replaced with an absolute constant, and since $n_1 > c_7$, the second can also. We therefore obtain an absolute upper bound $h(E) \leq N$. On those E with $h(E) > N$, there can be at most one $n > C_0$ such that $[n]P$ is integral. Let

$$C_0' = \sup_{h(E) \leq N} \{n : [n]P \text{ is integral for some } P \in E(\mathbb{Q})\}.$$

The set of $h(E) \leq N$ is finite and can be effectively computed if N is known. Letting $C = \max\{C_0, C_0'\}$, and we have shown that there is at most one value of $n > C$ such that $[n]P$ is integral.

It remains to simplify the constant C_0. Considered as a function of $x = C_P$, it is of the form

$$C_0 = \max\left\{ K_0, K_1 x(\log x), K_2 x, K_3 x^{\frac{1}{2}}, K_4 x^{\frac{1}{2}} (\log x)^{\frac{1}{2}} \right\},$$

where the K_i are absolute constants. If we increase the constant K_0 sufficiently, then since $x(\log x)$ grows fastest (as x increases) among all the functions (which are all eventually increasing), we may replace C_0 with

$$C_0 = \max\left\{ K_0', K_1 x(\log x) \right\}.$$

This proves the theorem. ∎

12 Other Connections and Applications

12.1 Growth Rates of Valuations

The main theorems of this paper give growth rates of $v(W_n)$. Cheon and Hahn find that for a non-torsion point over a number field with singular reduction, the growth rate is quadratic [3]. Everest and Ward give more precise growth information in [9, Theorem 3], which says that for any E in minimal Weierstrass form and P of singular reduction,

$$\log |\Psi_n(P)|_v = \left(\log |\Delta_E|_v / 12 + \lambda_v(P) \right) n^2 + O(n^C),$$

where $C < 2$ and may depend on P (here, $\lambda_v(P)$ is a canonical local height; see [28, §VI.2]).

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

The results of this paper allow us to improve this estimate. For a point of singular reduction on a curve of additive reduction, the coefficient of n^2 depends on the behaviour of the point when the field is extended to resolve the additive reduction; see Theorems 7.1 and 10.1, and the examples of Section 13.

For multiplicative reduction, the constant is more easily stated. If E is in minimal form, then from Theorem 9.3, Proposition 8.2(xiii), and Proposition 5.4(iii),

$$v(W_n) = \left(\frac{a_P(\ell_P - a_P)}{2\ell_P}\right) n^2 + O(\log n),$$

where the meaning of a_P and ℓ_P is given in Definition 9.1. In particular,

$$0 < a_P \leq \ell_P = v(\Delta_E).$$

Using [28, Theorem VI.4.2(b)], it is immediate to verify that this constant is in agreement with Everest and Ward's.

In all cases (*i.e.,* all types of bad reduction), our theorem improves Everest and Ward's result. We have the following theorem.

Theorem 12.1 *Let K be a p-adic field with valuation v and residue field of size N_K. Let E be a minimal elliptic curve over K and let $P \in E(K)$ be a point with singular reduction. Let W_n be the associated elliptic divisibility sequence. Then*

$$v(W_n) = \left(\frac{\lambda_v(P)}{\log|N_K|} + \frac{v(\Delta_E)}{12}\right) n^2 + O(\log n).$$

Proof From [9, Theorem 3], all that remains is to show that the error term is correct. This follows from Propositions 5.4(iii) and 8.2(xiii) and Theorems 3.3, 6.1, 7.1, 9.3, and 10.1. ∎

12.2 Torsion Points and Tate Normal Form

Gezer and Bizim use Tate's normal form for an elliptic curve with an N-torsion point to obtain general formulæ for EDS of rank N [13]. For example, the general form of a rank 7 EDS is

$$1, -\alpha^2(\alpha-1), -\alpha^6(\alpha-1)^3, \alpha^{11}(\alpha-1)^6 \cdots$$

They go on to give the general term as

$$W_n = \epsilon\alpha^{(5n^2-p)/7}(\alpha-1)^{(3n^2-q)/7},$$

where

$$\epsilon = \begin{cases} +1 & \text{if } n \equiv 1,4,5 \pmod 7, \\ -1 & \text{if } n \equiv 2,3,6 \pmod 7. \end{cases}$$

$$p = \begin{cases} 5 & \text{if } n \equiv 1,6 \pmod 7, \\ 6 & \text{if } n \equiv 2,5 \pmod 7, \\ 3 & \text{if } n \equiv 3,4 \pmod 7, \end{cases} \quad q = \begin{cases} 3 & \text{if } n \equiv 1,6 \pmod 7, \\ 5 & \text{if } n \equiv 2,5 \pmod 7, \\ 6 & \text{if } n \equiv 3,4 \pmod 7. \end{cases}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

We can now restate this general term as

$$W_n = \epsilon \alpha^{R_n(2,7)} (\alpha - 1)^{R_n(1,7)},$$

where ϵ is as above.

13 Examples

The examples in this section illustrate the main theorems of the paper describing $\nu(W_n)$, both the usual and unusual.

Example 13.1 This example demonstrates non-singular reduction fitting the hypotheses of Corollary 6.4, as well as singular reduction on a curve of multiplicative reduction. Consider the elliptic curve in minimal Weierstrass form and point

$$E : y^2 + xy = x^3 + x^2 - 1652x + 25168, \quad P = (24, -4),$$

having $j = -2^{-8} \cdot 7^{-2} \cdot 11^3 \cdot 89^{-1} \cdot 7211^3$, $\Delta = -2^8 \cdot 7^2 \cdot 89$, and $c_4 = 11 \cdot 7211$.

The curve has good reduction at $p = 3$. The point P reduces to a point of order 5. By Corollary 6.4,

$$\nu_3(W_n) = \begin{cases} \nu(W_5) + \nu(n/5) & 5 \mid n \\ 0 & 5 \nmid n. \end{cases}$$

The curve has multiplicative reduction at $p = 7$. The point P reduces to a non-singular point of order 6. By Corollary 6.4,

$$\nu_7(W_n) = \begin{cases} \nu(W_6) + \nu(n/6) & 6 \mid n, \\ 0 & 6 \nmid n. \end{cases}$$

The curve has multiplicative reduction at $p = 2$. The point P reduces to the singular point. The smallest multiple of P reducing to the identity is $[6]P = (4719/196, -56771/2744)$. In Theorem 9.3, $\ell_P = \nu_2(\Delta) = 8$. Since $[2]P$ has non-singular reduction, P reduces to the component of $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2)$ having order 2, *i.e.*, $a_P = 4$. Using the notations of Lemma 5.1, $h = 0$ and $b = p$ by Theorem 9.3. Also, $s_P = \nu_2(\Theta([6]P)) = 1$, and so $j = 0$. Furthermore, $w_P = \nu_2(\Theta([12]P)/\Theta([6]P)^2) = 3 - 2 = 1$. Therefore,

$$\nu_2(W_n) = R_n(4,8) + \begin{cases} 2 + \nu(n/6) & \nu_6(n) > 1, \\ 1 & \nu_6(n) = 1, \\ 0 & 6 \nmid n. \end{cases}$$

The EDS associated with E and P is

$$1,\ 2^4,\ 2^8,\ 2^{16},\ 2^{24} \cdot 3 \cdot 5,\ 2^{37} \cdot 7,\ -2^{48}, -2^{64} \cdot 211,\ -2^{80} \cdot 23 \cdot 137, \ldots$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

with valuations, agreeing with the formulæ above, of

$$\begin{aligned}
v_2(W_n) &: 0, 4, 8, 16, 24, 37, 48, 64, 80, 100, 120, 147, 168, 196, 224, 256, 288,\\
&\quad 325, 360, 400, 440, 484, 528, 580, 624, 676, 728, 784, 840, 901, 960, \ldots\\
v_3(W_n) &: 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 2, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 2,\\
&\quad 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 3, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, \ldots\\
v_7(W_n) &: 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1,\\
&\quad 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, \ldots
\end{aligned}$$

Example 13.2 This example describes a point that reduces to the identity, as well as a point of singular reduction on a curve of additive, potential good reduction. Consider the elliptic curve in minimal Weierstrass form and point

$$E : y^2 = x^3 + 2471x + 1, \quad P = \left(\frac{1}{5^2}, \frac{1249}{5^3}\right),$$

having $j = 2^8 \cdot 3^3 \cdot 7^3 \cdot 353^3 \cdot 60350132471^{-1}$, $\Delta = -2^4 \cdot 60350132471$, and $c_4 = -2^4 \cdot 3 \cdot 7 \cdot 353$.

This curve has good reduction at $p = 5$, but P reduces to the identity. We are in the case of Theorem 6.1, and $v_5(x(P))/2 = -1$. We have $n_P = 1$. The formal group for this elliptic curve has

$$[5]T = 5T - 3083808T^5 - 33480T^7 + 1574818510720T^9 + O(T^{10}).$$

Therefore, in Lemma 5.1, $b = 5$ and $j = h = w = 0$. Therefore, from Theorem 6.1, we expect

$$v_5(W_n) = -n^2 + 1 + v_5(n).$$

At $p = 2$, this curve has additive reduction, but potential good reduction. If we extend $\mathbb{Q}_2$ by a cube root π of 2 (an extension of ramification degree 3), then E obtains good reduction. The change of coordinates is

$$y' = \pi^{-3}(y + x + 1), \quad x' = \pi^{-2}(x + 1),$$

and the new curve (now in minimal Weierstrass form) and point are

$$E' : y^2 + \pi^2 xy + y = x^3 + \pi x^3 + 618\pi^2 x + 618, \quad P' = \left(-\frac{12\pi}{5^2}, \frac{622}{5^3}\right).$$

The point P' reduces modulo π to the point $(0, 0)$ of order 3 on the reduced curve $y^2 + y = x^3$ over $\mathbb{F}_2$. Applying Theorem 6.1 to W'_n, the elliptic divisibility sequence for E' and P', we have $n_P = 3$, $s_P = v_\pi(\Theta([3]P)) = 1$. The formal group for E' has

$$[2]T = 2T - \pi^2 T^2 - 2\pi^2 T^3 + O(T^{10})$$

so that $b = h = 2$, $v(p) = 3$ and so $j = 0$ in Lemma 5.1. We have $w_P = v_\pi(\Theta([6]P)/\Theta([3]P)^2) - h_P = 4 - 2 \cdot 1 - 2 = 0$. Therefore,

$$v_\pi(W'_n) = \begin{cases} 1 + v_\pi(n/3) & 3 \mid n, \\ 0 & 3 \nmid n. \end{cases}$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

By Theorem 7.1, we have

$$3v_2(W_n) = (n^2-1) + v_\pi(W_n') = n^2 + \begin{cases} 3v_2(n/3) & 3 \mid n, \\ -1 & 3 \nmid n. \end{cases}$$

The elliptic divisibility sequence for E and P begins

$$1,\ \ 2\cdot 5^{-3}\cdot 1249,\ \ -1\cdot 2^3\cdot 5^{-8}\cdot 298135585859,$$
$$-1\cdot 2^5\cdot 5^{-15}\cdot 1249\cdot 460436473420870703,\ldots$$

and has valuations, agreeing with the formulæ above, of

$$\begin{aligned} v_2(W_n) : {} & 0,1,3,5,8,13,16,21,27,33,40,50,56,65,75,85,96,109,120,133,\\ & 147,161,176,195,208,225,243,261,280,301,320,341,363,385,\\ & 408,434,456,481,507,533,560,589,616,645,675,705,736,772,\ldots \\ v_5(W_n) : {} & 0,-3,-8,-15,-23,-35,-48,-63,-80,-98,-120,-143,-168,\\ & -195,-223,-255,-288,-323,-360,-398,-440,-483,-528,\\ & -575,-622,-675,-728,-783,-840,-898,-960,-1023,\ldots \end{aligned}$$

Example 13.3 This example showcases a non-integral torsion point. Consider the elliptic curve, in minimal Weierstrass form, and point

$$E : y^2 + xy + y = x^3 + x^2 - 135x - 660, \quad P = (-29/4, 25/8).$$

The discriminant is $\Delta = 3^8\cdot 5^2$. The point P reduces modulo 2 to the identity. Therefore, Theorem 6.1 applies, with $n_P = 1$. We have $v(x(P)) = -2$, so $s_P = 1$, and in the formal group, we have

$$[2]T = 2T - T^2 - 2T^3 - 6T^4 + O(T^5)$$

so that $b_P = 2$, $h_P = 0$, $j = 0$, and $w_P = \infty$ (since $[2]P$ is the identity on E). We obtain

$$v(W_n) = -n^2 + \begin{cases} \infty & 2 \mid n \\ 1 & 2 \nmid n. \end{cases}$$

The elliptic divisibility sequence for E and P begins

$$1,\ 0,\ -2^{-8}\cdot 3^8,\ 0,\ 2^{-24}\cdot 3^{24},\ 0,\ -2^{-48}\cdot 3^{48},\ldots$$

and has valuations, agreeing with the formula above, of

$$v_2(W_n) : 0,\infty,-8,\infty,-24,\infty,-48,\infty,-80,\infty,-120,\infty,-168,\infty,-224,\ldots$$

Example 13.4 This example illustrates singular reduction on a curve of potential multiplicative reduction. Consider the curve, in minimal Weierstrass form, and point

$$E : y^2 + 49y = x^3 + 14x^2 - 312352901x + 2123335052286, \quad P = (10206, 1176).$$

Modulo 7, the point P reduces to the cusp $(0,0)$ on the reduced curve, $y^2 = x^3$ (additive reduction). If we pass to a ramified quadratic extension of $\mathbb{Q}_7$, say by adjoining a square root π of 7, then the change of coordinates $x' = \pi^{-2}x$, $y' = \pi^{-3}y$ gives a minimal Weierstrass equation,

$$E' : y^2 + \pi y = x^3 + 2x^2 - 6374549x + 6190481202, \quad P' = (1458, 24\pi).$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

having $v_\pi(j) = -10$, $v_\pi(\Delta) = 10$, $v_\pi(c_4) = 0$. Therefore, this curve has multiplicative reduction. The point P' reduces to the node $(2,0)$ on the reduced curve $y^2 = x^3 + 2x^2 + x + 3$. We have $\ell_P = v_\pi(\Delta) = 10$. The points P and $[3]P$ reduce to the node, while $[2]P$ reduces to the point $(1,0)$ of order 2; $[4]P$ reduces to the identity. Therefore, $n_P = 4$. By Theorem 9.3(i), $a_P = 5$. Alternatively, a_P must have order 2 in $\mathbb{Z}/\ell_P\mathbb{Z}$, so it must be $a_P = 5$. Using the notation of Lemma 5.1, $b = p$ and $h = 0$ by Theorem 9.3. We can compute $s_P = v(\Theta([4]P)) = 1$, which tells us that $j = 0$ and $w_P = 0$. Gathering together these parameters, we obtain the sequence of valuations for W'_n, the EDS associated with E' and P':

$$v_\pi(W'_n) = R_n(5,10) + \begin{cases} 1 + v_\pi(n/7) & 7 \mid n \\ 0 & 7 \nmid n. \end{cases}$$

By Theorem 10.1, we have

$$2v_7(W_n) = (n^2 - 1) + R_n(5,10) + \begin{cases} 1 + 2v_7(n/7) & 7 \mid n \\ 0 & 7 \nmid n. \end{cases}$$

The elliptic divisibility sequence W_n begins

$$1,\ 7^4,\ 7^9,\ 7^{18},\ 2 \cdot 3^2 \cdot 7^{27} \cdot 19, \ldots$$

and has valuations, agreeing with the formula above, of

$$\begin{aligned} v_7(W_n) : 0, 4, 9, 18, 27, 40, 54, 72, 90, 112, 135, 162, 189, 220, 252, 288, 324, 364, \\ 405, 450, 495, 544, 594, 648, 702, 760, 819, 883, 945, 1012, 1080, \\ 1152, 1224, 1300, 1377, 1458, 1539, 1624, 1710, 1800, 1890, 1984, \ldots \end{aligned}$$

Example 13.5 This example of potential good reduction exhibits very unusual complicated behaviour. In particular, we have an example with $j \neq 0$ in Lemma 5.1. Let $K = \mathbb{Q}_2$, and R be its ring of integers. Let $\alpha = \sqrt{17} \in R^*$. Then the curve

$$E : y^2 = x^3 + \alpha x + \alpha + 2$$

has $j = 2^8 + 2^{10} + 2^{14} + 2^{17} + O(2^{19}) \in R$, so E has potential good reduction. It is a minimal Weierstrass equation, since $v_2(\Delta) = 4 < 12$. It has additive reduction, since $v_2(c_4) = 4 > 0$.

The reduced curve over $\mathbb{F}_2$ is $\widetilde{E} : y^2 = x^3 + x + 1$, which has a cusp at $(1,1)$.

Let $\beta^2 = (-17)^3 + \alpha(-17) + \alpha + 2$. Then $\beta \in R^*$. Let $P = (-17, \beta) \in E(K)$. The point P has singular reduction to the cusp $(1,1)$, but $[2]P$ reduces to the non-singular two-torsion point $(0,1)$.

We have to pass to a ramified extension $L/\mathbb{Q}_2$ to obtain good reduction for E, which will guarantee non-singular reduction for P. It will suffice to change coordinates to Deuring normal form

$$E_D : y^2 + axy + y = x^3.$$

The change of coordinates required is

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

where $q = s - 1$ is a root of the irreducible polynomial

$$p(x) = (x+1)^8 + 18\alpha(x+1)^4 + 108(\alpha+2)(x+1)^2 - 27\alpha^2,$$

whose constant term, $a_0 = 217 + 126\alpha - 27\alpha^2$ has valuation $v_2(a_0) = 2$. Therefore, q is not a uniformizer (since the polynomial is not Eisenstein), but it has positive valuation. Let $N = \mathbb{Q}_2(s)$ have valuation $v_N = dv_2$, where d is the ramification degree of N over $\mathbb{Q}_2$. Since $v_N(p(q) - q^8 - a_0) > v_N(a_0) = 2d$ (all the intermediate terms of the polynomial are divisible by $4x$), we find that $8v_N(q) = 2d$, *i.e.*, $v_N(q) = d/4$. Hence, the extension is totally ramified ($d = 8$), and $v_N(s-1) = 2$.

We also have $u^3 = (\alpha + s^4/3)/s \in \mathbb{Q}_2(s)$. We can compute the valuation of $3\alpha + s^4$ in N as follows. We have

$$3\alpha = (1+2)\big(1 + 2^3 + O(2^5)\big) = 1 + 2 + 2^3 + O(2^4).$$

Meanwhile,

$$s^4 = 1 + 4q + 6q^2 + 4q^3 + q^4.$$

So, $v(3\alpha + s^4) = 8$. Therefore, $v_N(u^3) = 8$. Hence, u generates a totally ramified extension L of degree 3 over $N = \mathbb{Q}_2(s)$. Therefore, $[L:\mathbb{Q}_2] = 24$.

We have $r = s^2/3$ and $t = u^3/2$. Finally, $a = 2s/u$.

The Deuring normal form is a minimal Weierstrass equation of good reduction. (We could also verify that $v_L(u) = 8$, since $v_L(\Delta_E) = 24v_2(\Delta_E) = 96$ and so $0 = v_L(\Delta_{E_D}) = v_L(u^{-12}\Delta_E) = v_L(\Delta_E) - 12v_L(u) = 96 - 12v_L(u)$. We also find that $v_L(a) = 24 + v_L(s) - v_L(u) = 16$, so a is an integer, which confirms that E_D has good reduction.)

Let $\phi\colon E \to E_D$ represent the change of coordinates to Deuring normal form. Then,

$$v\big(x(\phi(P))\big) = v_L(17 + s^2/3) - 2v_L(u) = 12 - 16 = -4.$$

The EDS W'_n associated with the curve E_D and point $P_D = \phi(P)$ satisfies

$$v_L(W'_n) = 24v_2(W_n) - 8(n^2-1)$$

and is associated with a point of non-singular reduction. In fact, P_D reduces to the point at infinity and has $v(x(P_D)) = -4$. Thus, the sequence

$$v_L(W'_n) + 2n^2 = 24v_2(W_n) - 8(n^2-1) + 2n^2$$

must be of the form $S_n(p,t,d,h,s,w)$ as in Lemma 5.1. Multiplication-by-2 in the formal group for E_D begins

$$[2]T = 2T - aT^2 + (1+a)T^4\ldots,$$

and since $v_L(a) = 16$, we get $b = 4$ in Lemma 5.1, and so we have $t = 2$, $c = 2$, $j = 1$, and $w = 6$ in Definition 5.3. The sequence $v_L(W'_n) - 2n^2 = S_n(2,2,24,0,2,6)$ is

2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 80, 2, 8, 2, 32, 2, 8, 2, 56,

2, 8, 2, 32, 2, 8, 2, 104, 2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 80,

2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 128, 2, 8, 2, 32, 2, 8, 2, 56,

2, 8, 2, 32, 2, 8, 2, 80, 2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 104, 2, 8, 2, ...

https://doi.org/10.4153/CJM-2015-005-0 Published online by Cambridge University Press

Now let us verify this directly. The first few terms of the elliptic divisibility sequence associated with E and P are

$$1,\ 2\beta,\ -\alpha^2 + 1530\alpha + 250155,\\ -4\beta\alpha^3 - 5540\beta\alpha^2 + 1277796\beta\alpha + 95764068\beta,\ \dots$$

or

$$1,\ 2 + 2^6 + 2^9 + 2^{11} + 2^{12} + 2^{13} + 2^{16} + 2^{18} + O(2^{19}),\\ 2^2 + 2^5 + 2^7 + 2^8 + 2^{10} + 2^{11} + 2^{12} + 2^{14} + 2^{17} + O(2^{19}),\\ 2^5 + 2^7 + 2^9 + 2^{10} + 2^{12} + 2^{13} + 2^{15} + 2^{16} + 2^{18} + O(2^{19})\ \dots$$

The valuations $v_2(W_n)$ are

$$0,\ 1,\ 2,\ 5,\ 6,\ 9,\ 12,\ 18,\ 20,\ 25,\ 30,\ 37,\ 42,\ 49,\\ 56,\ 67,\ 72,\ 81,\ 90,\ 101,\ 110,\ 121,\ 132,\ 146,\ 156,\ \dots$$

These are exactly equal to

$$\frac{1}{24}\left(8(n^2-1) - 2n^2 + S_n(2,2,24,0,2,6)\right).$$

Acknowledgments The author would like to thank Patrick Ingram, Dino Lorenzini, Valéry Mahe, Joseph H. Silverman, Paul Voutier, Jonathan Wise, and the anonymous referees for helpful suggestions. The examples in this paper were computed with Sage Mathematics Software [35]; scripts for computing elliptic divisibility sequences in Sage are available on the author's website at http://math.colorado.edu/~kstange/.

References

[1] M. Ayad, *Points S-entiers des courbes elliptiques*. Manuscripta Math. **76**(1992), no. 3–4, 305–324. http://dx.doi.org/10.1007/BF02567763
[2] A. Baker, *The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$*. J. London Math. Soc. **43**(1968), 1–9. http://dx.doi.org/10.1112/jlms/s1-43.1.1
[3] J. Cheon and S. Hahn, *Explicit valuations of division polynomials of an elliptic curve*. Manuscripta Math. **97**(1998), no. 3, 319–328. http://dx.doi.org/10.1007/s002290050104
[4] ———, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*. Acta Arith. **88**(1999), no. 3, 219–222.
[5] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*. J. Reine Angew. Math. **613**(2007), 1–33, http://dx.doi.org/10.1515/CRELLE.2007.089
[6] S. David, *Minorations de formes linéaires de logarithmes elliptiques*. Mém. Soc. Math. France (N.S.) **62**(1995).
[7] M. Einsiedler, G. Everest, T. Ward, *Primes in elliptic divisibility sequences*. LMS J. Comput. Math. **4**(2001), 1–13. http://dx.doi.org/10.1112/S1461157000000772
[8] T. Ekedahl, *One semester of elliptic curves*. EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2006. http://dx.doi.org/10.4171/015
[9] G. Everest and T. Ward, *The canonical height of an algebraic point on an elliptic curve*. New York J. Math. **6**(2000), 331–342.
[10] ———, *Primes in divisibility sequences*. Cubo Mat. Educ. **3**(2001), no. 2, 245–259.
[11] G. Everest and H. King, *Prime powers in elliptic divisibility sequences*. Math. Comp. **74**(2005), 2061–2071. http://dx.doi.org/10.1090/S0025-5718-05-01737-0
[12] G. Everest, G. Mclaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*. J. Number Theory **118**(2006), no. 1, 71–89. http://dx.doi.org/10.1016/j.jnt.2005.08.002

[13] B. Gezer and O. Bizim, *Elliptic divisibility sequences associated to elliptic curves with torsion points*. 2011, arxiv:1101.3839
[14] ———, *Squares in elliptic divisibility sequences*. Acta Arith. **144**(2010), no. 2, 125–134. http://dx.doi.org/10.4064/aa144-2-2 http://dx.doi.org/10.4064/aa144-2-2
[15] M. Hall, Jr., *The Diophantine equation* $x^3 - y^2 = k$. In: Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, London, 1971, pp. 173–198.
[16] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*. Invent. Math. **93**(1988), no. 2, 419–450. http://dx.doi.org/10.1007/BF01394340
[17] P. Ingram, *Multiples of integral points on elliptic curves*. J. Number Theory **129**(2009), no. 1, YEAR = 2009, 182–208. http://dx.doi.org/10.1016/j.jnt.2008.08.001 http://dx.doi.org/10.1016/j.jnt.2008.08.001
[18] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*. In: Number theory, Analysis and Geometry (In memory of Serge Lang), Springer-Verlag, Berlin, pp. 233–263.
[19] S. Lang, *Elliptic curves: Diophantine analysis*. Grundlehren der Mathematischen Wissenschaften, 231, Springer-Verlag, Berlin, 1978.
[20] ———, *Conjectured Diophantine estimates on elliptic curves*. In: Arithmetic and geometry, I, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983, pp. 155–171.
[21] V. Mahé, *Prime power terms in elliptic divisibility sequences*. Math. Comp. **83**(2014), no. 288, 1951–1991. http://dx.doi.org/10.1090/S0025-5718-2013-02790-1 http://dx.doi.org/10.1090/S0025-5718-2013-02790-1
[22] Á. Pintér, *On the magnitude of integer points on elliptic curves*. Bull. Austral. Math. Soc. **52**(1995), no. 2, pp. 195–199. http://dx.doi.org/10.1017/S000497270001460X http://dx.doi.org/10.1017/S000497270001460X
[23] W. M. Schmidt, *Integer points on curves of genus* 1. Compositio Math. **81**(1992), no. 1, 33–59.
[24] R. Shipsey, *Elliptic divisibility sequences*. Ph.D. thesis, Goldsmith's College (University of London), 2000.
[25] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*. Duke Math. J. **48**(1981), no. 3, 633–648. http://dx.doi.org/10.1215/S0012-7094-81-04834-1
[26] ———, *A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves*. J. Reine Angew. Math. **378**(1987), 60–100.
[27] ———, *The difference between the Weil height and the canonical height on elliptic curves*. Math. Comp. **55**(1990), no. 192, 723–743. http://dx.doi.org/10.1090/S0025-5718-1990-1035944-5
[28] ———, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.
[29] ———, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.
[30] J. H. Silverman and K. E. Stange, *Terms in elliptic divisibility sequences divisible by their indices*. Acta Arith. **146**(2011), no. 4, 355–378. http://dx.doi.org/10.4064/aa146-4-4 http://dx.doi.org/10.4064/aa146-4-4
[31] J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*. J. Ramanujan Math. Soc. **21**(2006), no. 1, 1–17.
[32] V. G. Sprindžuk, *Classical Diophantine equations*. Lecture Notes in Mathematics, 1559, Springer-Verlag, Berlin, 1993.
[33] K. Stange, *Elliptic nets and elliptic curves*. Algebra Number Theory **5**(2011), no. 2, 197–229. http://dx.doi.org/10.2140/ant.2011.5.197 http://dx.doi.org/10.2140/ant.2011.5.197
[34] H. M. Stark, *Effective estimates of solutions of some Diophantine equations*. Acta Arith. **24**(1973), 251–259.
[35] W. A. Stein, et. al., The Sage Development Team, *Sage Mathematics Software (Version 4.6.2)*. 2011. http://www.sagemath.org
[36] M. Streng, *Divisibility sequences for elliptic curves with complex multiplication*. Algebra Number Theory **2**(2008), 183–208. http://dx.doi.org/10.2140/ant.2008.2.183. http://dx.doi.org/10.2140/ant.2008.2.183
[37] M. Ward, *Memoir on elliptic divisibility sequences*. Amer. J. Math. **70**(1948), 31–74. http://dx.doi.org/10.2307/2371930
[38] M. Yabuta, *Primitive divisors of certain elliptic divisibility sequences*. Experiment. Math. **18**(2009), no. 3, 303–310. http://dx.doi.org/10.1080/10586458.2009.10129047

Department of Mathematics, University of Colorado Boulder, Campus Box 395, Boulder, CO, 80309, USA
e-mail: kstange@math.colorado.edu