

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 work of 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 a quantity denoted $M(P)$, depending on P , which is related to the Tamagawa number of E and 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.

Date: November 1, 2011.

2010 Mathematics Subject Classification. Primary: 11G05, 11G07; Secondary: 11D25, 11B37, 11B39, 11Y55, 11G50, 14H52.

Key words and phrases. elliptic divisibility sequence, Lang’s conjecture, height functions.

The author’s research has been supported by NSERC PDF-373333 and NSF MSPRF 080291.

In this paper, we obtain a version of this result in which the constant depends only on the ratio of heights $h(E)/\widehat{h}(P)$. See Section 10 for the definitions of the heights.

Theorem 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*

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

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

The restriction to minimal elliptic curves is necessary, since otherwise there exist methods of constructing examples with arbitrarily many integral points. The bound becomes uniform if one assumes a well-known conjecture of Lang.

Lang's Height Conjecture ([20, p. 92]). *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 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 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).

Another conjecture of Hall and Lang posits an upper bound on the height of an integral point in terms of the height of the curve.

Hall-Lang Conjecture ([21, 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,*

$$(1) \quad \widehat{h}(P) < C_{HL} h(E).$$

This conjecture generalises a conjecture of Hall for elliptic curves of the form $y^2 = x^3 + b$ [15]. In [21], Lang used a different definition of $h(E)$ than we use here; see Section 10. The conjecture seems out of reach; the best known bounds with a uniform constant are exponential in $h(E)$ [2, 24, 32, 34], but see also [23].

A corollary of Theorem 1 can be seen as progress toward the Hall-Lang Conjecture.

Corollary 2. *There are uniform constants c and c' such that for any elliptic curve E/\mathbb{Q} in minimal Weierstrass form, and integral 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

$$\widehat{h}(P) \leq ch(E).$$

There is another way in which Theorem 1 can be viewed as progress toward the Hall-Lang Conjecture. If the form of the bound could be improved to

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

then the bound on all but one sufficiently large n would become

$$\widehat{h}([n]P) \leq Ch(E).$$

In other words, all but one sufficiently large integral multiple of the generator of a rank 1 curve would satisfy a Hall-Lang bound.

Unfortunately, the constants C and C' in Theorem 1, while effective, are quite large. More details can be found in Section 10.

Theorem 1 is proven using the following estimate for integral points (Proposition 30):

$$\widehat{h}(P) \leq \log n + \frac{11}{2}h(E).$$

Ingram's argument depends upon a similar estimate, which in turn depends upon 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 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, 12], primitive divisors [11, 19, 37], squares and powers [10, 14, 22] 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 Theorem

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.

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 which has become a sort of ‘folk theorem,’ although its first appearance in print is due to Cheon and Hahn [3, 4] (but see Remark 16).

Theorem 3 (Theorem 12, Introductory Form; see Section 5 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 12, 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 4 (Theorems 8, 12, 17, 24 and 25, Combination Introductory Form). *Let K be an unramified extension of \mathbb{Q}_p , $p \neq 2$. Let W_n be an EDS, associated to an elliptic curve E/K in Weierstrass form, and non-torsion $P \in E(K)$. There exist integers $a, \ell, c_1, c_2, c_3, c_4, c_5$ 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 7.

For P such that $[n]P \not\equiv \mathcal{O}$ modulo p , the valuations of W_n are connected to Néron-Tate local heights by the following relationship [28, Exercise VI.6.4(e)]:

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

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

In the case of good reduction in minimal Weierstrass form, Theorem 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 (5)), 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

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

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 32 improves the error term on this estimate to $O(\log n)$; see Section 11.1.

For any torsion point P , the W_n are supported only on primes of bad reduction (see Remark 14). 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 11.2.

Throughout the paper (except in the last three sections, 10 through 12), 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 to E and P .

Sections 2 and 3 provide background. Section 4 generalises the central lemma on formal groups that lies at the core of Theorem 3. Sections 5, 6, 8 and 9 describe the valuation sequence $v(W_n)$ for each type of reduction. Section 7 considers the properties of elliptic troublemaker sequences. Section 10 proves Theorem 1, while Section 11 examines a few other connections and applications. Finally, Section 12 gives some detailed examples of elliptic divisibility sequences and their sequences of valuations.

Acknowledgements. The author would like to thank Patrick Ingram, Joseph H. Silverman and Jonathan Wise for helpful suggestions.

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], [29, Exercise III.3.7]. Suppose the elliptic curve E is 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

$$\begin{aligned}\Psi_1 &= 1, \\ \Psi_2 &= 2y + a_1x + a_3, \\ \Psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\ \Psi_4 &= \Psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 \\ &\quad + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),\end{aligned}$$

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

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

The n -th division polynomial vanishes at all non-trivial n -torsion points: it has divisor $\sum_{Q \in E[n]}(Q) - n^2\mathcal{O}$.

Proposition 5. *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

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

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

$$(3) \quad w(x) = 2, \quad w(y) = 3, \quad w(a_i) = i,$$

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

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

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 6. *The division polynomials Ψ_n have the following properties.*

(i) *Using the natural weights (3), 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 ,*

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

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

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

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

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

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) can be obtained as special cases [33, Theorem 3.7].

Finally, using the Weierstrass σ -function and the usual complex uniformization \mathbb{C}/Λ of an elliptic curve over \mathbb{C} , Ward showed that [36, Theorem 12.1],

$$(4) \quad \Psi_n(z, \Lambda) = \frac{\sigma(nz, \Lambda)}{\sigma(z, \Lambda)^{n^2}}.$$

3. PRELIMINARIES ON ELLIPTIC DIVISIBILITY SEQUENCES

Definition 1. An *elliptic divisibility sequence*, or EDS, is a sequence W_n satisfying

$$(5) \quad W_{n+m}W_{n-m}W_r^2 + W_{m+r}W_{m-r}W_n^2 + W_{r+n}W_{r-n}W_m^2 = 0.$$

The connection between EDS and elliptic curves is described by Ward in his original memoir on the subject. We let Ψ_n denote the n -th division polynomial. We state an updated version of Ward’s theorem which applies to fields of characteristic zero in general (it follows from his proof):

Theorem 7 (Ward [36, Theorem 12.1]). *Let E be an elliptic curve defined over a field K of characteristic zero, and let $P \in E(K)$. Then $W_n = \Psi_n(P)$ is an elliptic divisibility sequence. Furthermore, if $W_n \in K$ is an elliptic divisibility sequence, then there exists a constant $C \in K$, an elliptic curve E/K and $P \in E(K)$ so that $W_n = C\Psi_n(P)$.*

In other words, each EDS over K appears as the sequence of division polynomials for some elliptic curve E/K evaluated at a point $P \in E(K)$.

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 to E and P . If we change the Weierstrass equation for E , we may 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 6(iv). This immediately gives the following result, which will be important enough for the later results that we include it as a theorem.

Theorem 8. *Let E be an elliptic curve defined over K and let $\mathcal{O} \neq P \in E(K)$. Let W_n be the associated elliptic divisibility sequence. Then there exists an isomorphism $\phi : E \rightarrow E'$, defined over K , to an elliptic curve E' in minimal Weierstrass form. Let W'_n be the elliptic divisibility sequence associated to $\phi(P)$. Then there exists an $r_P \in \mathbb{Z}$ such that*

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

4. 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 (6) below is quite complicated, in most cases we encounter, $j = 0$, whereupon it simply reduces to $v(z) + v(n)$. For background on formal groups, see [29, Chapter IV].

Lemma 9. *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 ,*

$$(6) \quad v([n]z) = \begin{cases} b^j v(z) + \frac{b^j - 1}{b - 1} h + v(n) - jv(p) + w & \text{if } v(n) > jv(p) \\ b^{v(n)/v(p)} v(z) + \frac{b^{v(n)/v(p)} - 1}{b - 1} h & \text{if } v(n) \leq jv(p) \end{cases}.$$

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

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

- (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 10. 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 (6) 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

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

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

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

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

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 34 and 37.

Proof of Lemma 9. 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 $[m_1 m_2]T = [m_1]([m_2]T)$, 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

$$(7) \quad [p]T = pf(T) + g(T^p),$$

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 that $g \equiv 0$, so that we have $p \mid b$ and $b \geq p > 1$. Define j to be the smallest non-negative integer such that

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

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

From (7),

$$(8) \quad v([p]z) \geq \min\{v(z) + v(p), bv(z) + h\}$$

Suppose that $j > 0$. Then, since $v(p) > (b-1)v(z) + h$, the second option determines the minimum in (8), in which the inequality is an equality, and so

$$a_1 = ba_0 + h$$

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

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

For $k = j + 1$, we again obtain (8) (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

$$a_{j+1} = a_j + v(p) = b^j a_0 + \frac{b^j - 1}{b - 1} h + v(p).$$

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

$$a_k = b^j a_0 + \frac{b^j - 1}{b - 1} h + (k - j)v(p),$$

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 (8) for $k = j + 1$. In this case, the minimum in (8) 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

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

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, (8) is replaced with

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

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

The formula in Lemma 9 being somewhat cumbersome, we set some notation for the class of such sequences.

Definition 2. Suppose $p \in \mathbb{Z}$ is a prime, and let u be the valuation on \mathbb{Q} associated to 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

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

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 11. (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 , $S_n(p, b, d, h, s, w) = O(\log n)$.

5. 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 16), [4, Lemma], [5, Lemma 2.6], [30, Lemma 5], [35, Lemma 3.4]. Loosely speaking, in most cases one expects that for non-torsion points with non-singular reduction of order $n_P > 1$,

$$(9) \quad v(W_n) = \begin{cases} v(W_{n_P}) + v(n/n_P) & \text{if } n_P \mid n \\ 0 & \text{if } n_P \nmid n \end{cases}.$$

There are exceptions, however. Lemma 9 on formal groups allows us to prove a somewhat stronger, more general statement. Please refer to Definition 2 for the sequence S_n , which generalises (9).

Theorem 12. *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 $\widetilde{[n_P]P} = \tilde{\mathcal{O}}$ in \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

$$(10) \quad v(W_n) = \min \left\{ 0, \frac{v(x(P))}{2} \right\} n^2 + \begin{cases} S_{n/n_P}(p, b_P, v(p), h_P, s_P, w_P) & \text{if } n_P \mid n \\ 0 & \text{if } n_P \nmid n \end{cases}.$$

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

Corollary 13. *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 14. This corollary implies that the non-zero terms of an elliptic divisibility sequence associated to 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 35.

Corollary 15. *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 three below listed conditions,*

$$(11) \quad v(W_n) = \begin{cases} v(W_{n_P}) + v(n/n_P) & \text{if } n_P \mid n \\ 0 & \text{if } n_P \nmid n \end{cases}.$$

- (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 for $p \geq 3$.

Remark 16. The statement of [3, Theorem 1] corresponding to this paper's Theorem 12 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 (11) 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 12 and its corollaries.

Proof of Theorem 12. There is a standard isomorphism of groups (see [29, Proposition VII.2.2])

$$\Theta : E_1(K) \rightarrow \hat{E}(\mathcal{M}), \quad (x, y) \mapsto -\frac{x}{y},$$

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

$$(12) \quad [n]P = \left(\frac{\phi_n}{\Psi_n^2}, \frac{\omega_n}{\Psi_n^3} \right)$$

as in Section 2.

We begin with the case that $n_P = 1$, i.e. $\tilde{P} = \tilde{\mathcal{O}}$. 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 6(iii), $v(\phi_n) = 2n^2v_0$, from which we obtain

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

Then,

$$(13) \quad v(\Psi_n) = \frac{v(x(P))}{2}n^2 + v(\Theta([n]P)).$$

Now suppose that $\tilde{P} \neq \tilde{\mathcal{O}}$ 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 (12) and the form of the Weierstrass equation. Therefore for all integers k ,

$$(14) \quad v(\Theta([kn_P]P)) = v(-\phi_{kn_P}\Psi_{kn_P}/\omega_{kn_P}) = v(\Psi_{kn_P}).$$

Now, in both cases ($n_P = 1$ and $n_P \neq 1$), Lemma 9, written in terms of Definition 2, says

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

for some b_P, h_P , and w_P . If $n_P \nmid n$, then $v(\Psi_n) = 0$. This, combined with (13) and (14), completes the proof. \square

Proof of Corollary 13. 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 5. \square

Proof of Corollary 15. In all three parts, we use the notation of Theorem 12 and Lemma 9.

Condition (1). 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 (1) implies that $j = 0$ (since $h \geq 0$) in Definition 2 (since this is immediate if $b_P = 1$, while otherwise $b_P \geq p$ from which it follows). Condition (1) also implies $w_P = 0$ by Lemma 9(iii). By Proposition 11(i),

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

Condition (2). 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 (1) and we are done) except possibly in the

case that $p = 2$ and $v(W_{n_P}) = 1$. Either way, $j = 0$. Then, according to Lemma 9 and the proof of Theorem 12,

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

where $z = \Theta([n_P]P)$. If $w_P = 0$, we are done as in condition (1). For an elliptic curve, the formal group law is

$$[2]z = 2z - a_1z^2 - 2a_2z^3 + O(z^4)$$

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

$$v([2]z/2z) > 0 \iff v(1 - a_1z/2) > 0 \iff v(a_1) = 0.$$

(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 (3). 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 (1) is satisfied. \square

6. SINGULAR REDUCTION ON A CURVE OF POTENTIAL GOOD REDUCTION

In the case that 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 $v(W_n)$. In short, there is some positive integer d dividing 24 such that $dv(W_n)$ is of the form (10) given in Theorem 12. The statement is made precise as follows.

Theorem 17. *Assume that E has potential good reduction. There exists an isomorphism $\phi : E \rightarrow E'$ 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 to $\phi(P)$. Then,*

$$(15) \quad dv(W_n) = (n^2 - 1)dv(\Delta_E)/12 + v_1(W'_n)$$

where $v_1(W'_n)$ is of the form (10) of Theorem 12, since $\phi(P)$ has non-singular reduction.

Proof of Theorem 17. 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 to E and P considered over L . Changing coordinates, using Theorem 8, we obtain

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

for some $r \in \mathbb{Z}$. 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. The valuation of Δ_E in L is d times greater; r must be chosen to change this to 0. Hence $r = dv(\Delta_E)/12$. \square

Remark 18. 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 37.

The following proposition gives some restrictions on the parameters used in Theorem 17.

Proposition 19. *Under the hypotheses and notations of Theorem 17, with reference to the parameters of (10), let*

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

Then,

- (i) If $d' = 2, 4, 8$, then $n_P \in \{1, 2\}$.
- (ii) If $d' = 3$, then $n_P \in \{1, 3\}$.
- (iii) If $d' \neq 1, 2, 3, 4, 8$, then $n_P = 1$.

For Proposition 19, we require an elementary number theoretical lemma.

Lemma 20. *Let $a, b \in \mathbb{Z}^{>0}$. Suppose that for all integers n ,*

$$(16) \quad n \not\equiv 0 \pmod{a} \implies n^2 \equiv 1 \pmod{b}.$$

Then

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

where $*$ represents any positive integer.

Proof. The statement (16) holds vacuously if $a = 1$ and trivially if $b = 1$. Suppose $a = 2$. Setting $n = 2k + 1$ we find that $n^2 - 1 = 4k(k - 1)$, so

$$a = 2 \implies b \in \{2, 4, 8\}.$$

Suppose $a = 3$. Taking $n = 3k \pm 1$, we find that $n^2 - 1 = 3k(3k \pm 2)$, so

$$a = 3 \implies b \in \{3\}.$$

Claim: If $a, b > 1$, then $a \mid b$. For, if not, let p be a prime satisfying $p \mid a$, $p \nmid b$. Then $n \not\equiv 0 \pmod{p}$ implies $n \not\equiv 0 \pmod{a}$, so we can replace a in the statement (16) with p . Thus we may assume without loss of generality that a and b are coprime. But if so, then the condition $n \not\equiv 0 \pmod{a}$ is satisfied by at least one element in every equivalence class of integers modulo b . But $n^2 \equiv 1 \pmod{b}$ is not satisfied by every such equivalence class, a contradiction.

Now, suppose $a > 3$. Then, since $a \mid b$, in particular,

$$n \not\equiv 0 \pmod{a} \implies n^2 \equiv 1 \pmod{a}$$

But for $a > 3$, there is more than one equivalence class of non-zero squares. \square

Proof of Proposition 19. Write $r = dv(\Delta_E)/12$, and $g = \gcd(d, r)$. Since $v(W_n) \in \mathbb{Z}$, we find that for n divisible by n_P ,

$$S_{n/n_P}(p, b_P, dv(p), h_P, s_P, w_P) \equiv -(n^2 - 1)r \equiv 0 \pmod{g}.$$

If $n = n_P$, we find that $g \mid s_P$, and from this we deduce that $g \mid h_P$ (if $j = 0$ we may simply change h without changing the function S_{n/n_P} ; otherwise take n satisfying $v(n/n_P) = 1$). Then $g \mid w_P$ by taking n having $v(n/n_P)$ large enough. Therefore, by Proposition 11(ii),

$$S_{n/n_P}(p, b_P, dv(p), h_P, s_P, w_P) = gS_{n/n_P}(p, b_P, dv(p)/g, h_P/g, s_P/g, w_P/g).$$

So we can replace the parameters in equation (10) and (15) as follows:

$$d' = d/g, \quad h'_P = h_P/g, \quad s'_P = s_P/g, \quad r' = r/g, \quad w'_P = w_P/g,$$

and in particular, $\gcd(d', r') = 1$ (the notation $d' = d/g$ agrees with the statement of the theorem).

Since $v(W_n)$ is an integer, (10) now implies that if $n_P > 1$, then

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

Since r' is coprime to d' , Lemma 20 implies that the implication only holds if

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

□

7. ELLIPTIC TROUBLEMAKER SEQUENCES

In this section we define a class of integer sequences which 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 3. To 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

$$(17) \quad R_n(a, \ell) = \left\lfloor \frac{n^2 \widehat{a}(\ell - \widehat{a})}{2\ell} \right\rfloor - \left\lfloor \frac{\widehat{na}(\ell - \widehat{na})}{2\ell} \right\rfloor,$$

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 21. *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 , $R_n(ka, k\ell) = kR_n(a, \ell)$.
- (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 $0 < n < \ell/a$,

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

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

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

$$(18) \quad R_n(a, \ell) = \left\lfloor \frac{n^2 a (\ell - a)}{2\ell} \right\rfloor.$$

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

$$(19) \quad R_n(a, \ell) = \frac{\ell}{2} \left(\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right)^2 - \left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right) - n^2 \left(\frac{a}{\ell} - \left\lfloor \frac{a}{\ell} \right\rfloor \right)^2 + n^2 \left(\frac{a}{\ell} - \left\lfloor \frac{a}{\ell} \right\rfloor \right) \right).$$

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

$$(20) \quad R_n(a, \ell) = \frac{\ell}{2} \left(\left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right)^2 - \left(\frac{na}{\ell} - \left\lfloor \frac{na}{\ell} \right\rfloor \right) + \frac{n^2 a (\ell - a)}{\ell^2} \right).$$

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

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

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

$$(21) \quad R_n(a, \ell) = \frac{n^2 - n}{2} a + \left(\sum_{k=1}^{\left\lfloor \frac{na}{\ell} \right\rfloor} k\ell - na \right) - n^2 \left(\sum_{k=1}^{\left\lfloor \frac{a}{\ell} \right\rfloor} k\ell - a \right).$$

(xiii) We have

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

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

$$(22) \quad 0 \leq \frac{b(\ell - b)}{2\ell} \leq \ell/8.$$

For any A and B ,

$$(23) \quad [A] + [B] \leq [A + B], \quad [A] + [-A] = -1.$$

From the definition, (22) and (23),

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

Part (x) We will show that (20) is equal to (17), under the assumption that $0 \leq a < \ell$.

We consider the case $\ell \mid na$ separately. In this case, using (20), to show (17) (or actually (18)), we need only check that $\frac{n^2 a(\ell - a)}{\ell}$, 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

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

where X, Y, Z are integers and $0 < x, y < 1$ and $0 \leq z < 1$. 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 may 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

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

which is what was required to prove.

Part (ix) If $0 \leq a < \ell$, it is immediate that (19) reduces to (20). Therefore, using parts (iii) and (x), it suffices to check that (19) is independent of the choice of residue of a modulo ℓ . But this is a direct calculation (compare the formula (19) for $R_n(a, \ell)$ and $R_n(a + \ell, \ell)$).

Parts (iv) and (xi) Direct calculations from (19) 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 (19) 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 (19) 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 $[0, 1]$. \square

Remark 22. By Proposition 21, 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 $\mathbb{Q} \cap [0, \frac{1}{2}]$.

8. 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 4. For any elliptic curve E/K with non-integral j -invariant, and any $P \in E(K)$, let $\phi : E \rightarrow E_q$ 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

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

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

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

$a_P = v(u)$ 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 24. *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 4. Let n_P be the smallest positive integer such that $\widehat{[n_P]P} = \tilde{\mathcal{O}}$ in \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 ,

$$(24) \quad v(W_n) = R_n(a_P, \ell_P) + \begin{cases} S_{n/n_P}(p, p, v(p), 0, s_P, w_P) & n_P \mid n \\ 0 & n_P \nmid n \end{cases}.$$

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

$$(25) \quad E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

in which case, the point u corresponds to $(X(u, q), Y(u, q))$ where X and Y are defined in [28, Theorem V.3.1]. We can define $\Psi_n(u, q)$ as the usual polynomial in X and Y for (25). 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

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

(To see this, use (4), together with the standard change of coordinates to eliminate $2\pi i$, for example in [28, Section V.1].) Therefore, over \mathbb{C} ,

$$(26) \quad \Psi_n(u, q) = u^{(n^2-n)/2} \frac{\theta(u^n, q)}{\theta(u, q)^{n^2}}.$$

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 to (25) and the point $(X(u, q), Y(u, q))$). We wish to discover the form of $v(W_n)$. Note that (25) 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 to 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 $a, n, \ell \geq 0$),

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

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 (26) and (21), 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 $k_0\ell = n_0a$, 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 $\widehat{[n_P]P} = \widetilde{\mathcal{O}}$ in $E(k)$. But it is a property of division polynomials that $\widehat{[n]P} = \widetilde{\mathcal{O}}$ 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 $k_P\ell = n_Pa$, 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 $K^* \rightarrow \mathbf{k}^*$. Let \mathbb{G}_m be the formal multiplicative group. By the theory of formal groups, we have an isomorphism

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

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

$$\Theta : E_{q,1}(K) \longrightarrow \hat{E}_q(\mathcal{M}), \quad (x, y) \mapsto -x/y,$$

as in the proof of Theorem 12, we obtain a chain of isomorphisms

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

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

Lemma 9 for $\mathbb{G}_m(\mathcal{M})$ implies

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

for some $w_P \in \mathbb{Z}^{\geq 0} \cup \{\infty\}$. (Note that $b = p$ and $h = 0$ in Lemma 9 by Remark 10.) Thus, we have shown (24), 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 (24).

In the case that W_n is associated to 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). □

9. 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, 5, 6, 8 and 9 combine to give Theorem 4.

Theorem 25. *Assume that E does not have potential good reduction. There exists an isomorphism $\phi : E \rightarrow E'$ 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 to $\phi(P)$. Then,*

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

where $v_1(W'_n)$ is of the form (10) of Theorem 12, if $\phi(P)$ has non-singular reduction, or the form (24) of Theorem 24, 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

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

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, $r = dv(c_4(E))/4$. □

10. 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

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

This differs by a factor of 2 from the definitions of some authors.

Lang, [21, 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

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

which is always at least $2 \log 2$. The statement of Theorem 1 is the same no matter which height is used, thanks to the following proposition, which says the two heights are equivalent.

Proposition 26. $h_I(E) \asymp h_0(E)$

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

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

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 $h_I(E) \leq 4h_0(E)$. \square

Lang [21, 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 26, 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 [21].

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. Ingram's result is as follows.

Theorem 27 ([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.*

The quantity $M(P)$ depends on P and is related to the Tamagawa number. The proof of this result depends on a lemma about valuations of division polynomials, restated here.

Lemma 28 ([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 $n \geq 1$,*

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

Ingram's proof of Lemma 28 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 29. *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 $n \geq 1$,*

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

Ingram's proof of Theorem 27 depends upon $M(P)$ in two places: first, in the Lemma we are replacing; and second, in the constant C_λ of the bound

$$\widehat{h}(P) \geq C_\lambda h(E)$$

of [17, Lemma 5], based on work of Silverman [25] and Hindry and Silverman [16]. In our version of Ingram's proof, we simply track the dependence on $\widehat{h}(P)/h(E)$ explicitly, and we obtain Theorem 1. If we wish to assume Lang's conjecture, the quantity $\widehat{h}(P)/h(E)$ is uniformly bounded below, and all the constants become uniform.

In what follows, we use the main theorems of this paper to prove Lemma 29, and then list the modifications to [17] necessary to obtain Theorem 1. It should be pointed out that, once the lemma is in place, the remaining modifications are straightforward and partially follow unpublished notes of Ingram [18].

Proof of Lemma 29. 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 valuation $v = v_p$ associated to 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. 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

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

as in the proof of Theorem 24. We conclude that

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

Consider an isomorphism, $\phi : E \rightarrow E'$ such that $\phi(P) = P'$. There is a u such that $\Delta' := \Delta_{E'} = u^{12}\Delta$, $W'_n := \Psi_n(\phi(P), E') = u^{n^2-1}W_n$ and $x(\phi(P)) = u^2x(P)$.

Suppose that E is of additive potential multiplicative reduction. In this case, $v(\Delta) > -v(j) \geq 0$. We pass to an extension of degree d over which such a ϕ is defined between E and a minimal E' of multiplicative reduction. From Theorem 25,

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

Recall that

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

We obtain

$$v_1(\Delta') = dv(\Delta) - 3dv(c_4) = -dv(j).$$

We also have

$$v(D'_n) \leq v(D_n) + \frac{1}{4}dv(c_4).$$

Therefore we may compute

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

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 17,

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

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

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

□

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. He shows that 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 modified lemma results in a modified [17, Proposition 4], which becomes

Proposition 30. *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, $n \geq 2$. Then*

$$\widehat{h}(P) \leq \log n + \frac{11}{2}h(E).$$

Proposition 30 only differs from [17, Proposition 4] in that the coefficient of $h(E)$ no longer depends on $M(P)$.

Proof of Proposition 30. The proof is exactly as for [17, Proposition 4], except that we assume $|x(P)| > 240n^2 \exp(3h(E)/2)$ and use Lemma 29 in place of [17, Lemma 3]. The altered proof is included for completeness and because part of it is used later.

A result 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 that

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

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,

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

Therefore,

$$2 \log |\Psi_n| > 2 \log n + (n^2 - 1)(3h(E)/2 + 2 \log n + \log 120)$$

On the other hand, by Lemma 29 and the triangle inequality,

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

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

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

which is a contradiction. Therefore,

$$(27) \quad |x(P)| \leq 240n^2 \exp(3h(E)/2).$$

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,

$$\widehat{h}(P) \leq \frac{1}{2}h(x(P)) + 2h(E) \leq \frac{1}{2} \log 240 + \log n + \frac{7}{2}h(E) \leq \log n + \frac{11}{2}h(E)$$

since $h(E) \geq 2 \log 2$. □

Modifications to the rest of the proof of [17, Theorem 1] consist of the following:

- (1) Ingram's [17, Lemma 5] gives a bound C_λ for $\widehat{h}(P) \geq C_\lambda h(E)$ which depends on $M(P)$. Instead of using the lemma and tracking dependence on $M(P)$, simply track dependence on C_λ . Note that throughout the proof, the lemma is only used for the fixed point P . In the end we may take $C_\lambda = \widehat{h}(P)/h(E)$.
- (2) Use Proposition 30 in place of [17, Proposition 4].

These need to be applied for [17, Proposition 7, Lemma 9, Proposition 11, Lemma 12 and Proposition 13]; this having being accomplished, the constants in their statements and proofs are expressed in terms of their dependence on C_λ . Explicitly:

- (1) [17, **Proposition 7.**] The constant if we follow Ingram's method of proof is $c_0 = \max\{e^2, \frac{169}{4}C_\lambda^{-2}\}$. However, the estimate comes down to [17, **Lemma 6**], which gives a lower bound on x such that $f(x) = x^2 - a \log(x) - b$ is positive. In place of this, we can apply this lemma:

Lemma 31. *Let $a > 0$ be a real number. Let $f(x) = x^2 - a \log x - a$. Then $f(x) \geq 0$ for $x \geq \max\{4, \sqrt{a} \log a\}$.*

Then, we may use $c_0 = \max\{4, 13C_\lambda^{-1} \log(\frac{13}{2}C_\lambda^{-1})\}$.

- (2) [17, **Lemma 9.**] $c_1 = C_\lambda/2$ and $c_2 = \sqrt{6/C_\lambda}$.
(3) [17, **Proposition 11.**] It now suffices to take

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

and we can use $C' = 10^{46}$. For curves with $h(E) \geq 2\pi\sqrt{3}$, we can then use $c_4 = 10^{24}C_\lambda^{-1/2}$, and choosing any $0 < \epsilon < 1$, we can use

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

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 .)

- (4) [17, **Lemma 12.**] We replace Ingram's equation (10) with our (27), which does not depend on $M(P)$. Then we can take $C = \sqrt{5/c_1} = \sqrt{10}/C_\lambda^{1/2}$.
(5) [17, **Proposition 13.**] We use $c_5 = 2/c_1 = 4/C_\lambda$ and $c_6 = \max\{c_0, C, K\}$ where K is an absolute constant.

For clarity, we now present the proof of Theorem 1, following [17, Theorem 1], but using the modified [17, Propositions 7, 11, and 13].

Proof of Theorem 1. Let E/\mathbb{Q} be a quasi-minimal elliptic curve with an integral point $P \in E(\mathbb{Q})$ of infinite order. Let $C_0 = \max\{c_0, c_3, c_6, c_7\}$, where

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

By the modified [17, Propositions 11, and 13], for $n_i > C_0$, 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

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

Recall that

$$c_5 = 4/C_\lambda, \quad c_4 = 10^{24}/C_\lambda^{1/2}$$

and since $n_1 > c_6 \geq \sqrt{10}C_\lambda^{-1/2}$, the first constant 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

$$C'_0 = \sup_{h(E) \leq N} \{n : [n]P \text{ is integral from some } P \in E(\mathbb{Q})\}.$$

The set of $h(E) \leq N$ is finite and can be effectively computed, if N is known. Letting $C = \max\{C_0, C'_0\}$, we have proven the theorem.

It remains to simplify the constant C_0 . Considered as a function of $x = C_\lambda^{-1}$, it is of the form

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

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

$$C_0 = \max\{K'_0, K_1 x \log x\}$$

This proves the theorem. □

11. OTHER CONNECTIONS AND APPLICATIONS

11.1. 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,

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

where $C < 2$ and may depend on P .

This work also allows computation of the constant coefficient of n^2 . For a point of singular reduction on a curve of additive reduction, the constant depends on the behaviour of the point when the field is extended to resolve the additive reduction; see Theorems 17 and 25, and the examples of Section 12.

For multiplicative reduction, the constant is more easily stated. If E is in minimal form, then from Theorem 24, Proposition 21(xiii), and Proposition 11(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 4. 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

Theorem 32. *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 11(iii) and 21(xiii) and Theorems 8, 12, 17, 24 and 25. \square

11.2. 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

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

They go on to give the general term as

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

where

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

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

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.

12. EXAMPLES

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

Example 33. This example demonstrates non-singular reduction fitting the hypotheses of Corollary 15, 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 15,

$$v_3(W_n) = \begin{cases} v(W_5) + v(n/5) & 5 \mid n \\ 0 & 5 \nmid n \end{cases}.$$

The curve has multiplicative reduction at $p = 7$. The point P reduces to a non-singular point of order 6. By Corollary 15,

$$v_7(W_n) = \begin{cases} v(W_6) + v(n/6) & 6 \mid n \\ 0 & 6 \nmid n \end{cases}.$$

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 24, $\ell_P = v_2(\Delta) = 8$. 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 9, $h = 0$ and $b = p$ by Theorem 24. Also, $s_P = v_2(\Theta([6]P)) = 1$ and so $j = 0$. Furthermore, $w_P = v_2(\Theta([12]P)/\Theta([6]P)^2) = 3 - 2 = 1$. Therefore,

$$v_2(W_n) = R_n(4, 8) + \begin{cases} 2 + v(n/6) & v_6(n) > 1 \\ 1 & v_6(n) = 1 \\ 0 & 6 \nmid n \end{cases}.$$

The EDS associated to E and P is

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

with valuations, agreeing with the formulæ above, of

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

Example 34. This example describes a point which 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 12, 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 9, $b = 5$, and $j = h = w = 0$. Therefore, from Theorem 12, 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 12 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 9. We have $w_P = v_\pi(\Theta([6]P)/\Theta([3]P)^2) - h_P = 4 - 2 \cdot 1 - 2 = 0$. Therefore,

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

By Theorem 17, 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

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

and has valuations, agreeing with the formulæ above, of

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

Example 35. 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 12 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

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

and has valuations, agreeing with the formula above, of

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

Example 36. 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,

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

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 24(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 notations of Lemma 9, $b = p$ and $h = 0$ by Theorem 24. 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 to 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 25, 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

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

and has valuations, agreeing with the formula above, of

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

Example 37. This example of potential good reduction exhibits very unusual, complicated behaviour. In particular, we have an example with $j \neq 0$ in Lemma 9. 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

$$\tilde{E} : y^2 = x^3 + x + 1$$

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

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

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

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

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

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

The EDS W'_n associated to 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 to 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 9. Multiplication-by-2 in the formal group for E_D begins

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

and since $v_L(a) = 16$, we get $b = 4$ in Lemma 9, and so we have $t = 2$, $c = 2$, $j = 1$ and $w = 6$ in Definition 2. The sequence $v_L(W'_n) - 2n^2 = S_n(2, 2, 24, 0, 2, 6)$ is

$$\begin{aligned} &2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 80, 2, 8, 2, 32, 2, 8, 2, 56, \\ &2, 8, 2, 32, 2, 8, 2, 104, 2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 80, \\ &2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 128, 2, 8, 2, 32, 2, 8, 2, 56, \\ &2, 8, 2, 32, 2, 8, 2, 80, 2, 8, 2, 32, 2, 8, 2, 56, 2, 8, 2, 32, 2, 8, 2, 104, 2, 8, 2, \dots \end{aligned}$$

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

$$\begin{aligned} &1, 2\beta, -\alpha^2 + 1530\alpha + 250155, \\ &-4\beta\alpha^3 - 5540\beta\alpha^2 + 1277796\beta\alpha + 95764068\beta, \dots \end{aligned}$$

or

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

The valuations $v_2(W_n)$ are,

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

These are exactly equal to

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

REFERENCES

- [1] Mohamed Ayad, *Points S -entiers des courbes elliptiques*, Manuscripta Math. **76** (1992), no. 3-4, 305–324.
- [2] A. Baker, *The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$* , J. London Math. Soc. **43** (1968), 1–9.
- [3] J. Cheon and S. Hahn, *Explicit valuations of division polynomials of an elliptic curve*, Manuscripta Math. **97** (1998), no. 3, 319–328.
- [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] Gunther Cornelissen and Karim Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. **613** (2007), 1–33.
- [6] Sinnou David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) (1995), no. 62, iv+143.

- [7] Manfred Einsiedler, Graham Everest, and Thomas Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1–13 (electronic).
- [8] Torsten Ekedahl, *One semester of elliptic curves*, EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2006.
- [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 (electronic).
- [10] Graham Everest and Helen King, *Prime powers in elliptic divisibility sequences*, Math. Comp. **74** (2005), no. 252, 2061–2071 (electronic).
- [11] Graham Everest, Gerard Mclaren, and Thomas Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), no. 1, 71–89.
- [12] Graham Everest and Thomas Ward, *Primes in divisibility sequences*, Cubo Mat. Educ. **3** (2001), no. 2, 245–259.
- [13] B. Gezer and O. Bizim, *Elliptic divisibility sequences associated to elliptic curves with torsion points*, 2011, [arXiv:1101.3839](https://arxiv.org/abs/1101.3839).
- [14] Betül Gezer and Osman Bizim, *Squares in elliptic divisibility sequences*, Acta Arith. **144** (2010), no. 2, 125–134.
- [15] Marshall Hall, Jr., *The Diophantine equation $x^3 - y^2 = k$* , 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.
- [17] Patrick Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory **129** (2009), no. 1, 182–208.
- [18] Patrick Ingram, personal communication, 2011.
- [19] Patrick Ingram and Joseph H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number theory, Analysis and Geometry (In memory of Serge Lang), Springer-Verlag, 2011, pp. 233–263.
- [20] Serge Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin, 1978.
- [21] ———, *Conjectured Diophantine estimates on elliptic curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 155–171.
- [22] Valéry Mahé, *Prime power terms in elliptic divisibility sequences*, preprint, january 2010.
- [23] Ákos Pintér, *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. **52** (1995), no. 2, 195–199.
- [24] Wolfgang M. Schmidt, *Integer points on curves of genus 1*, Compositio Math. **81** (1992), no. 1, 33–59.
- [25] Joseph H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), no. 3, 633–648.
- [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.
- [28] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [29] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
- [30] Joseph H. Silverman and Katherine E. Stange, *Terms in elliptic divisibility sequences divisible by their indices*, Acta Arith. **146** (2011), no. 4, 355–378.
- [31] Joseph H. Silverman and Nelson Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 1–17.
- [32] Vladimir G. Sprindžuk, *Classical Diophantine equations*, Lecture Notes in Mathematics, vol. 1559, Springer-Verlag, Berlin, 1993, Translated from the 1982 Russian original,

Translation edited by Ross Talent and Alf van der Poorten, With a foreword by van der Poorten.

- [33] Katherine E. Stange, *Elliptic nets and elliptic curves*, preprint, April 2010.
- [34] H. M. Stark, *Effective estimates of solutions of some Diophantine equations*, Acta Arith. **24** (1973), 251–259, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, III.
- [35] Marco Streng, *Divisibility sequences for elliptic curves with complex multiplication*, Algebra Number Theory **2** (2008), no. 2, 183–208.
- [36] Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.
- [37] Minoru Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Experiment. Math. **18** (2009), no. 3, 303–310.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, 450 SERRA MALL, BUILDING 380, STANFORD, CA, 94305, USA

E-mail address: `stange@math.stanford.edu`