Algebra &
Number
Theory

Volume 2
2008
No. 2

Divisibility sequences for elliptic curves with complex multiplication

Marco Streng

mathematical sciences publishers

Divisibility sequences for elliptic curves with complex multiplication

Marco Streng

Elliptic divisibility sequences arise as sequences of denominators of the integer multiples of a rational point on an elliptic curve. Silverman proved that almost every term of such a sequence has a primitive divisor (that is, a prime divisor that has not appeared as a divisor of earlier terms in the sequence). If the elliptic curve has complex multiplication, then we show how the endomorphism ring can be used to index a similar sequence and we prove that this sequence also has primitive divisors. The original proof fails in this context and will be replaced by an inclusion-exclusion argument and sharper diophantine estimates.

1. Introduction

Consider an elliptic curve E, given by a general Weierstrass model with coefficients in the ring of integers $\mathcal{O}_L$ of a number field L. Fix an L-valued point P of infinite order on E. For $n \in \mathbb{Z}$, define the coprime $\mathcal{O}_L$-ideals A_n and B_n by

$$x(nP)\,\mathcal{O}_L = A_n B_n^{-2}. \tag{1.1}$$

We call the sequence $B_1, B_2, B_3, \ldots$ an *elliptic divisibility sequence*. Such a sequence satisfies the *strong divisibility property*

$$\gcd(B_m, B_n) = B_{\gcd(m,n)} \qquad (m, n \in \mathbb{Z}),$$

which in particular implies the (*weak*) *divisibility property*: if $m \mid n$, then $B_m \mid B_n$.

By a *primitive divisor* of the term B_n, we mean a prime $\mathfrak{p} \mid B_n$ that does not divide any term B_m with $n \nmid m$. Silverman proved that almost every term in an elliptic divisibility sequence has a primitive divisor [Silverman 1988]. This is the elliptic curve analogue of a theorem of Zsigmondy for $\mathbb{Q}^*$ [Bang 1886; Zsigmondy 1892].

MSC2000: primary 14H52; secondary 14K22.

Keywords: complex multiplication, divisibility sequence, elliptic curve, endomorphism, primitive divisor, Zsigmondy.

If the curve E has complex multiplication, then (1.1) makes sense for all n in the endomorphism ring $\mathcal{O} = \mathrm{End}_L(E)$ and hence we get a sequence indexed by $\mathcal{O}$ instead of only $\mathbb{Z}$. We extend this definition to ideals $\mathfrak{a}$ of $\mathcal{O}$ by setting

$$B_{\mathfrak{a}} = \sum_{\alpha\in\mathfrak{a}} B_{\alpha},$$

the ideal generated by the ideals B_α for $\alpha \in \mathfrak{a}$. We will prove that this indeed extends the definition (in the sense that $B_{\alpha\mathcal{O}} = B_\alpha$), and that the resulting ideal-indexed sequence satisfies the strong divisibility property $B_{\mathfrak{a}} + B_{\mathfrak{b}} = B_{\mathfrak{a}+\mathfrak{b}}$. By the *elliptic divisibility sequence associated to P*, we will mean this sequence, indexed by ideals of $\mathcal{O}$.

By a *primitive divisor* of the term $B_{\mathfrak{a}}$, we now mean a prime $\mathfrak{p} \mid B_{\mathfrak{a}}$ which does not divide any term $B_{\mathfrak{b}}$ with $\mathfrak{a} \nmid \mathfrak{b}$. Our main theorem is a Zsigmondy-type theorem for elliptic curves with complex multiplication.

Main Theorem. *Let E, $\mathcal{O}$ and P be as above. Then for all but finitely many invertible $\mathcal{O}$-ideals $\mathfrak{a}$, the ideal $B_{\mathfrak{a}}$ has a primitive divisor.*

The Main Theorem applies both in the case $\mathcal{O} = \mathbb{Z}$ and in the *complex multiplication* case, that is, when $\mathcal{O}$ is a quadratic order, but is a new result only in the latter case.

The number of primitive divisors. If not all endomorphisms of E over $\bar{L}$ are defined over L, then our Main Theorem implies the following result on the number of primitive divisors in the $\mathbb{Z}$-indexed sequence $B_1, B_2, B_3, \cdots$. Let K' be the field of fractions of $\mathcal{O}' = \mathrm{End}_{\bar{L}}(E)$.

Corollary 1.2. *Define, for $n \in \mathbb{Z}$, the numbers*

$$r_n = \#\{p \in \mathbb{N} :\ p \mid n,\ p \textit{ is a prime ramifying in } \mathcal{O}'\mathbb{Z} \textit{ and } p \nmid n,\ p \nmid [\mathcal{O}_{K'} : \mathcal{O}']\},$$
$$s_n = \#\{p \in \mathbb{N} :\ p \mid n \textit{ and } p \textit{ is a prime splitting in } \mathcal{O}'/\mathbb{Z}\}.$$

Then for almost all n, the term B_n has at least $r_n + s_n + 1$ primitive divisors, of which at least s_n split in $K'L/L$.

In particular, this shows the existence of lots of split primitive divisors in elliptic divisibility sequences coming from elliptic curves over $\mathbb{Q}$ that have complex multiplication. It seems that there are also many inert primitive divisors, but we cannot prove this. There are conjectures by Cornelissen and Zahidi [2007] about the existence of inert primitive divisors that imply results related to Hilbert's Tenth Problem over $\mathbb{Q}$.

The size of the primitive part. For any integer n, we define the *primitive part* $D_n^{\mathbb{Z}}$ of B_n to be the L-ideal dividing B_n such that every prime divisor of $D_n^{\mathbb{Z}}$ is a primitive divisor of B_n and no divisor of $B_n/D_n^{\mathbb{Z}}$ is a primitive divisor of B_n. Our methods also yield estimates on the size of the primitive part of $\mathbb{Z}$-indexed elliptic divisibility sequences that are sharper than what can be gotten with Silverman's original proof. We use the notation $\|D_n^{\mathbb{Z}}\| := N_{L/\mathbb{Q}}(D_n^{\mathbb{Z}})^{1/[L:\mathbb{Q}]}$ for the "size" of the ideal $D_n^{\mathbb{Z}}$ and we denote the canonical height of the point P by $\widehat{h}(P)$.

Silverman's proof can be optimized to give an estimate

$$\log \|D_n^{\mathbb{Z}}\| \geq \widehat{h}(P)\Big(1 - \sum_{p\,|\,n} \frac{1}{p^2} - o(1)\Big)\, n^2,$$

where $0.5477 < 1 - \sum_p p^{-2} < 0.5478$ for the sum over *all* primes. If we apply our methods, we get the following sharper estimate.

Proposition 1.3. *For all* $\epsilon > 0$,

$$\log \|D_n^{\mathbb{Z}}\| = \widehat{h}(P)\, s_n\, n^2 + O(n^{\epsilon}) \qquad (\textit{as } n \to \infty),$$

where

$$s_n = \sum_{m\,|\,n} \mu(m) m^{-2} = \prod_{p\,|\,n} (1 - p^{-2})$$

is between $\zeta(2)^{-1} > 0.6079$ *and* 1.

In fact, the proof gives $O(d(n)(\log n)(\log\log n)^4)$ instead of $O(n^{\epsilon})$, where $d(n)$ is the number of divisors of n.

Division polynomials. An alternative approach to defining elliptic divisibility sequences is by using division polynomials. If E/L is an elliptic curve, given by a Weierstrass model, then for any integer $n \in \mathbb{Z}$, the *n-th division polynomial of E* is the polynomial $\psi_n = \psi_{E,n} \in L[x, y] \subset L(E)$, as given for short Weierstrass models in [Silverman 1986] and [Washington 2003] and in general in [Ayad 1992]. If $P \in E(L)$ is a fixed L-valued point on E, then we call the sequence $(\psi_n(P))_{n\in\mathbb{Z}}$ an *elliptic divisibility sequence of division polynomial type*.

Along with the division polynomials ψ_n, one usually also defines polynomials $\phi_n = \phi_{E,n} \in L[x]$ for which we have

$$[n]^* x = \frac{\phi_n}{\psi_n^2}. \tag{1.4}$$

This explains the similarity between B_n and $\psi_n(P)$: both represent the square root of the denominator of $x(nP)$, but they can differ because $\psi_n(P)$ and $\phi_n(P)$ may not be integers, and because there may be cancellation of factors in (1.4). However, B_n and $\psi_n(P)$ differ only in finitely many valuations. For a more precise statement, see [Ayad 1992].

The division polynomials satisfy the recurrence relation

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2 \quad \text{for } m, n \in \mathbb{Z}. \tag{1.5}$$

Ward [1948] extensively studied sequences of integers that satisfy both this recurrence and the divisibility property; he called them *elliptic divisibility sequences*. Later, his terminology was adopted for the sequences $(\psi_n(P))_n$ and $(B_n)_n$. In fact, every sequence of integers $(\psi_n)_n$ that satisfies (1.5) and the initial conditions $\psi_0 = 0$, $\psi_1 = 1$, $\psi_2\psi_3 \neq 0$, $\psi_2 \mid \psi_4$, excepting some degenerate cases, is of the form $\psi_n = \psi_{E,n}(P)$ for some elliptic curve $E/\mathbb{C}$ and some point $P \in E(\mathbb{C})$ [Ward 1948, Theorem 12.1].

Chudnovsky and Chudnovsky [1986] suggested letting sequences of division polynomial type be indexed by the endomorphism ring of the elliptic curve, using division polynomials ψ_α for arbitrary endomorphisms α. The special cases where the curve has complex multiplication by $\sqrt{-1}$ or a primitive third root of unity were studied by Ward [1950] and Durst [1952] respectively. The CM division polynomials ψ_α and their computational aspects have recently been studied in more detail by Satoh [2004].

2. Formal groups

Let L_v be the completion of the number field L with respect to a normalized discrete valuation v. Denote the ring of v-integers of L_v by R_v and let E be an elliptic curve, given by a Weierstrass equation

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with coefficients in R_v. For $n \geq 1$, define subsets $E_n(L_v)$ of $E(L_v)$ by

$$E_n(L_v) = \{P \in E(L_v) : v(x(P)) \leq -2n\} \cup \{O\}.$$

We want to study these sets because for $n \geq 1$, we have that

$$v(B_\alpha) \geq n \iff \alpha P \in E_n(L_v). \tag{2.2}$$

The formal group of E gives a means of studying $E_n(L_v)$.

We have two main goals in this section. First we will generalize part of the theory of formal groups as in [Silverman 1986] to arbitrary isogenies instead of only multiplication by integers in $\mathbb{Z}$. This will result in the identity

$$v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$$

which holds if $v(B_\alpha)$ is sufficiently large (see Proposition 2.8 and Lemma 3.4). This is very useful, because it bounds the part of the growth of B_α that is caused by the occurrence of higher powers of nonprimitive divisors.

At the end of this section, we will prove that the sets $E_n(L_v)$ are modules over the endomorphism ring $\mathbb{O}$ (see Corollary 2.10). By (2.2), this implies the divisibility property

$$B_\alpha \mid B_{\alpha\beta} \quad \alpha, \beta \in \mathcal{O}.$$

Formal groups and isogenies. We start by associating homomorphisms of formal groups to arbitrary isogenies of elliptic curves.

Let $z = -x/y$ and $w = -1/y$. Then the Weierstrass equation of the elliptic curve E becomes

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3. \tag{2.3}$$

Let $w(T) \in L_v[[T]]$ be the unique power series such that (2.3) is satisfied with $z = T$. Then $(T, w(T))$ is a "formal point" on the curve (2.3).

We define a homomorphism of rings $\mathcal{P} : L_v(E) \to L_v((T))$ from the function field of E to the field of Laurent series over L_v by $z \mapsto T$, $w \mapsto w(T)$. One could think of $\mathcal{P}$ as the map which "evaluates" elliptic functions in the formal point $(T, w(T))$.

As z is a uniformizer at the point at infinity O of E, we see that $\mathcal{P}$ maps functions that are regular at O to power series in $L_v[[T]]$.

Suppose that E' is another elliptic curve, also given by a Weierstrass equation with coefficients in R_v. We use $'$ in the notation to specify functions and so on related to E'. To any isogeny $\phi : E \to E'$ that is defined over L_v, we associate a power series

$$F_\phi(T) = \mathcal{P}(\phi^* z') \in L_v[[T]]. \tag{2.4}$$

This power series is a homomorphism of formal groups. We will not check this, since it will follow trivially from Lemma 2.6 below. Notice that $F_\phi(T)$ has no constant term, so we get a map $F_\phi^* : L_v((T)) \to L_v((T))$, $f(T) \mapsto f(F_\phi(T))$. We now have a commutative diagram

$$\begin{tikzcd}
L_v(E) \arrow[r, "\mathcal{P}", "\substack{z\mapsto T\\ w\mapsto w(T)}"'] & L_v((T)) \\
L_v(E') \arrow[u, "\phi^*"] \arrow[r, "\mathcal{P}'", "\substack{z'\mapsto T\\ w'\mapsto w'(T)}"'] & L_v((T)). \arrow[u, "F_\phi^*"']
\end{tikzcd} \tag{2.5}$$

We only need to check the commutativity of the diagram for the generators z' and w' of $L_v(E')$. For z', it holds by definition. For w', it follows from the fact that its image on the top right satisfies the Weierstrass equation for E' with $z' = T$.

As z is a uniformizer at O, the space of differentials that are regular at O is $\Omega_{E,O} = L_{v,O}(E)\,dz$ and we get a map

$$L_{v,O}(E)\,dz \to L_v[[T]]\,dT, \quad g dz \mapsto \mathcal{P}(g)\,dT,$$

which we also denote by $\mathcal{P}$.

Let $\omega \in \Omega_{E,O}$ denote the *invariant differential*

$$\omega = \frac{dx}{2y + a_1 x + a_3},$$

and write $\widehat{\omega}(T)$ for $\mathcal{P}(\omega)$. As ω is an invariant differential of the curve E, we see that $\widehat{\omega}(T)$ is an invariant differential of the formal group $\widehat{E}$ of E. In fact, the dz-coefficient of $\widehat{\omega}$ is 1, so it is the (unique) normalized invariant differential of the formal group $\widehat{E}$ of E.

The integral $\log(T)$ of $\widehat{\omega}$ is an isomorphism of formal groups from $\widehat{E}$ to the additive formal group $\mathbb{G}_a$. Denote the inverse by $\exp(T)$.

Lemma 2.6. *For any isogeny $\phi : E \to E'$ over L_v, we have*

$$F_\phi(T) = \exp_{\widehat{E}'}(c \log_{\widehat{E}}(T)),$$

where $c \in L_v$ is such that $\phi^*\omega' = c\omega$.

Proof. If we apply $\mathcal{P}$ to the identity $\phi^*\omega' = c\omega$, then we get $\widehat{\omega}'(F_\phi(T)) = c\widehat{\omega}(T)$. The result is obtained by integration, followed by application of $\exp_{\widehat{E}'}$. □

Recall that R_v is the ring of v-integers of L_v. Let $\mathfrak{M}$ be the maximal ideal of R_v and $l = R_v/\mathfrak{M}$ the residue field. Reduction of the Weierstrass equation gives a cubic curve $\widetilde{E}$ over l. We denote the group of nonsingular points by $\widetilde{E}^{\mathrm{ns}}(l) \subset \widetilde{E}(l)$.

Let $E_0(L_v)$ be the group of L_v-valued points that reduce to points in $\widetilde{E}_{\mathrm{ns}}(l)$ modulo v. Reduction modulo v then is a group homomorphism $E_0(L_v) \to \widetilde{E}_{\mathrm{ns}}(l)$ with kernel $E_1(L_v)$. By [Silverman 1986, VII.2.2], we have an isomorphism of groups

$$\begin{aligned} E_1(L_v) &\to \widehat{E}(\mathfrak{M}), \\ P &\mapsto z(P), \end{aligned} \tag{2.7}$$

where the inverse sends $u \in \mathfrak{M}$ to the point $P \in E(L_v)$ with coordinates $z(P) = u$, $w(P) = w(u)$. For any point $P \in E_1(L_v)$, the fact that $(x(P), y(P))$ satisfies the Weierstrass equation implies that $2v(y(P)) = 3v(x(P))$, and hence $v(z(P)) = -\frac{1}{2}v(x(P))$. In particular, the sets $E_n(L_v)$ are subgroups of $E(L_v)$ and correspond to the groups $\widehat{E}(\mathfrak{M}^n)$ through the isomorphism (2.7).

Now let $\phi : E \to E'$ be an isogeny defined over L_v, where we assume that both E and E' are given by Weierstrass equations with coefficients in R. Furthermore, let c be the unique element of L_v such that $\phi^*\omega' = c\omega$.

Proposition 2.8. *If both $v(x(P))$ and $v(x(P)) - 2v(c)$ are strictly smaller than $-2v(p)/(p-1)$, then*

$$v\big(x'(\phi(P))\big) = v\big(x(P)\big) - 2v(c).$$

Proof. By the isomorphism $E_1(L_v) \cong \widehat{E}(\mathfrak{M})$ above and Lemma 2.6, we have

$$z'(\phi(P)) = F_\phi(z(P)) = \exp_{\widehat{E}'}\bigl(c \log_{\widehat{E}}(z(P))\bigr).$$

By [Silverman 1986, IV.6.4], both $\log_{\widehat{E}}(u)$ and $\exp_{\widehat{E}'}(u)$ converge for $u \in \mathfrak{M}$ with $v(u) > v(p)/(p-1)$ and both preserve the valuation. Therefore, we find that $v\bigl(x'(\phi(P))\bigr) = -2v\bigl(z'(\phi(P))\bigr) = -2v\bigl(z(P)\bigr) - 2v(c) = v\bigl(x(P)\bigr) - 2v(c)$. □

Formal groups and Complex Multiplication. The main theorem of this section is the following.

Theorem 2.9. *For any $\alpha \in \mathbb{O} = \operatorname{End}_{L_v}(E)$, the power series $F_\alpha(T) \in L_v[[T]]$ has v-integral coefficients. In other words, the homomorphism of formal groups $F_\alpha(T)$ is defined over R_v.*

Corollary 2.10. *For any $n \geq 1$, the group $E_n(L_v)$ is an $\mathbb{O}$-submodule of $E(L_v)$. Moreover, we have an isomorphism of $\mathbb{O}$-modules*

$$E_n(L_v)/E_{n+1}(L_v) \cong l,$$

where l is the residue field of L_v.

Proof of the corollary. First of all, the theorem shows that $\widehat{E}(\mathfrak{M}^n)$ is an $\mathbb{O}$-module with the action of α given by $z \mapsto F_\alpha(z)$. Now for any $P \in E_n(L_v)$, convergence of $F_\alpha(z(P))$ implies convergence of $w\bigl(F_\alpha(z(P))\bigr)$. But by (2.5), $F_\alpha(z(P))$ and $w\bigl(F_\alpha(z(P))\bigr)$ can only converge to $z(\alpha P)$ and $w(\alpha P)$ respectively. In particular, the isomorphism of groups $E_n(L_v) \cong \widehat{E}(\mathfrak{M}^n)$ is an isomorphism of $\mathbb{O}$-modules.

The second statement follows from the obvious isomorphism

$$\widehat{E}(\mathfrak{M}^n)/\widehat{E}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1}. \qquad \square$$

As we will see, Theorem 2.9 follows easily from the theory of Néron models. However, we will also give a more elementary proof. The elementary proof actually consists of proofs for two special cases that together cover every case. One proof uses continuity of the coefficients of $F_\alpha(T)$ as functions of α and works only if p splits in the field of fractions of $\mathbb{O}$. The other uses explicit equations for isogenies, but fails in the exceptional case where $p = 2$ and 2 splits in $\mathbb{O}$.

For both the Néron model proof and the elementary proof, we will need to deal with changes of coordinates in the Weierstrass equations, so we will use the following lemma.

Lemma 2.11. *Every isomorphism $\psi : E \to E'$ over L_v of elliptic curves given by Weierstrass equations is of the form*

$$\psi(x, y) = (u^2 x + r, u^3 y + u^2 s x + t)$$

with $u \in L_v^*$ and $r, s, t \in L_v$. Such an isomorphism satisfies $\psi^*\omega' = u^{-1}\omega$. Moreover, if $v(u) \geq 0$ and both E and E' have v-integral coefficients, then r, s and t are v-integral.

Proof. This is exactly what is proven in the proof of [Silverman 1986, VII.1.3(d)]. □

Corollary 2.12. *Let ψ and u be as above. If $v(u) = 0$, then the power series $F_\psi(T)$ associated to ψ as in* (2.4) *has v-integral coefficients.*

Proof. From the equations above, we compute

$$\phi^* z' = \frac{u^{-1}z + ru^{-3}w}{1 - su^{-1}z - tu^{-3}w}.$$

As $u^{-1}, r, s, t \in R_v$, we find that $F_\psi(T)$ has coefficients in R_v. □

Proof using Néron models. Suppose that the elliptic curves E_1 and E_2 are given by Weierstrass equations with coefficients in R_v and let $\phi : E_1 \to E_2$ be an isogeny, defined over L_v.

Lemma 2.13. *If the Weierstrass equation for E_2 is minimal, that is, $v(\Delta)$ is minimal among all Weierstrass models of E_2 with coefficients in R_v, then $F_\phi(T)$ has v-integral coefficients.*

Proof. Let $\mathscr{E}_1$, $\mathscr{E}_2$ be the closed subschemes of $\mathbb{P}^2_{R_v}$ given by the Weierstrass equations of E_1, E_2 and denote the smooth parts by $\mathscr{E}_1^0$, $\mathscr{E}_2^0$. We will prove, using the Néron model, that the map $\phi : E_1 \to E_2$ can be extended to a morphism of schemes $\phi : \mathscr{E}_1^0 \to \mathscr{E}_2^0$ over R_v.

We then localize this morphism at the closed point s of the zero section of $\mathscr{E}_2^0$. Let $z_2 = -x_2/y_2$, $w_2 = -1/y_2$ be the coordinate functions of E_2. The completion of the local ring

$$\mathbb{O}_{\mathscr{E}_2^0, s} = R_v[z_2, w_2]_{(z_2)}$$

with respect to the ideal (z_2) is exactly the ring $R_v[[z_2]]$ of power series in z_2, where we identify w_2 with the power series $w_2(z_2)$ that was defined below (2.3). As ϕ maps the zero section to the zero section, it induces a morphism $R_v[[z_2]] \to R_v[[z_1]]$. The image of z_2 under this morphism is exactly $F_\phi(z_1)$, so $F_\phi(T)$ has coefficients in R_v.

It remains to prove that the extension of ϕ exists. Let $\mathscr{N}$ denote the Néron model of E_2 over R_v as in [Bosch, Lütkebohmert and Raynaud 1990, 1.2.1 and 1.3.2] or [Silverman 1994, § IV.5 and IV.6.1]. Then $\mathscr{N}$ is a smooth R_v-scheme with generic fibre $\mathscr{N}_{L_v} = E_2$ which satisfies the following universal property: for any smooth R_v-scheme X and any morphism of L_v-schemes $f : X_{L_v} \to E_2$, there exists a unique morphism of R_v-schemes $g : X \to \mathscr{N}$ extending f in the sense that $g_{L_v} = f$.

The special fibre $\mathcal{N}_l$ of $\mathcal{N}$ may consist of multiple components. One of them contains the special fibre of the identity section. Let $\mathcal{N}^0$ denote $\mathcal{N}$ with all other components of $\mathcal{N}_l$ removed. Then by [Bosch, Lütkebohmert and Raynaud 1990, 1.5.5] or [Silverman 1994, IV.9.1], we have $\mathscr{E}_2^0 = \mathcal{N}^0$. Moreover, by the universal property of the Néron model, ϕ extends to a unique morphism of R_v-schemes $\phi : \mathscr{E}_1^0 \to \mathcal{N}$ and since the special fibre of $\mathscr{E}_1^0$ has only one component, the image lies inside $\mathcal{N}^0 = \mathscr{E}_2^0$. □

Proof of Theorem 2.9. If the Weierstrass model of E is minimal, then Lemma 2.13 proves Theorem 2.9. Otherwise, let E'' be a minimal model. By a change of coordinates $z' = u^{-1}z''$, $w' = u^{-3}w''$ with $v(u) \geq 0$, we obtain a model E' from the minimal model E'' such that $v(\Delta(E')) = v(\Delta(E))$. Write F_α, F'_α and F''_α for the power series associated to α with respect to the different models. We know that F''_α has v-integral coefficients, so $F'_\alpha(T) = u^{-1}F''_\alpha(uT)$ also has v-integral coefficients. As $v(\Delta(E)) = v(\Delta(E'))$, it follows from Corollary 2.12 that $F_\alpha(T)$ has v-integral coefficients. □

Elementary proof. Let K be the field of fractions of $\mathbb{O}$.

Proof of Theorem 2.9 assuming that p splits in $K/\mathbb{Q}$. For any nonnegative integer n, consider the map $\Phi_n : K_v \to L_v$, mapping $\alpha \in K_v$ to the n-th coefficient of the power series $\exp_{\widehat{E}'}(\alpha \log_{\widehat{E}}(T)) \in L_v[[T]]$. The goal is to prove that $\Phi_n(\mathbb{O}) \subset R_v$ for every n. As p splits in $K/\mathbb{Q}$, we have $\mathbb{Q}_p = K_v$, so $\mathbb{O} \subset \mathbb{Z}_p$. The map Φ_n is continuous, because it is a polynomial map. Moreover, as $\widehat{E}$ is defined over R, we have $\Phi_n(\mathbb{Z}) \subset R$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we are done. □

The ring $\mathbb{O} = \mathrm{End}_{L_v}(E)$ is an order in the imaginary quadratic field K; hence it is generated as a ring over $\mathbb{Z}$ by a single element α. We have a homomorphism of rings $\mathbb{O} \to \mathrm{End}_{L_v}(\widehat{E})$ and we wish to show that the image is contained in the subring $\mathrm{End}_{R_v}(\widehat{E})$. It therefore suffices to prove that the generator α of $\mathbb{O}$ maps to an element of $\mathrm{End}_{R_v}(\widehat{E})$. We will use the formulas of Vélu [1971] that describe an isogeny explicitly in terms of its kernel. Therefore, we want to pick α in such a way that $v(N(\alpha)) = 0$ so that we know that the α-torsion is v-integral.

We make such a choice as follows: let $p > 0$ be the rational prime such that $v(p) > 0$ and let α_0 be any generator of $\mathbb{O}$. Write $\alpha = \alpha_0 + n$ with $n \in \mathbb{Z}$. Then $N(\alpha) = N(\alpha_0) + n\mathrm{Tr}(\alpha_0) + n^2$ is a quadratic polynomial in n, and hence has at most two zeroes modulo p. The only case in which we cannot pick an integer n with $p \nmid N(\alpha)$ is when $p = 2$ and the polynomial has two distinct roots modulo 2, that is, $p = 2$ splits in $\mathbb{O}$.

Lemma 2.14. *Let E/L_v be an elliptic curve, given by a Weierstrass equation with coefficients $a_1, \ldots, a_6 \in R_v$ and let Γ be a finite subgroup of $E(L_v)$. Then there is an elliptic curve E', together with an isogeny $\sigma : E \to E'$ with kernel Γ such that* *the coefficients of $F_\sigma(T)$ and the coefficients of the Weierstrass equation for E' are in the ring $B = \mathbb{Z}[a_1, \dots, a_6, x(Q), y(Q) : Q \in \Gamma]$ and moreover $\sigma^*\omega' = \omega$.*

Proof. Vélu's article [1971] gives a Weierstrass equation for an elliptic curve E' and an isogeny $\sigma : E \to E'$ with kernel Γ. The coefficients of the Weierstrass equation are computed explicitly as elements of B. Moreover, the isogeny σ is given as follows. Let S be a complete set of representatives of $\Gamma/\{\pm 1\}$. Then

$$\sigma^*x' = x + \sum_{Q\in S}\Big(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\Big),$$
$$\sigma^*y' = y + \sum_{Q\in S}\Big(u_Q\frac{2y + a_1x + a_3}{(x - x_Q)^3} + \frac{t_Q(a_1(x - x_Q) + (y - y_Q)) + v_Q}{(x - x_Q)^2}\Big),$$

where for each $Q \in S$, Vélu gives t_Q, u_Q and v_Q explicitly as elements of B.

The power series $w(T) = \mathcal{P}(-\frac{1}{y})$ has coefficients in $\mathbb{Z}[a_1, \dots, a_6]$ and starts with T^3. Therefore, $\mathcal{P}(x) = T/w(T)$ and $\mathcal{P}(y) = -1/w(T)$ have coefficients in $\mathbb{Z}[a_1, \dots, a_6]$ and start with T^{-2} and $-T^{-3}$ respectively. The formula above now shows that $\mathcal{P}(\sigma^*x')$ and $\mathcal{P}(\sigma^*y')$ have coefficients in B and the lowest degree terms are respectively T^{-2} and $-T^{-3}$. As a consequence, $F_\sigma(T) = -\mathcal{P}(\sigma^*y)$ is a power series over B with lowest degree term T. □

Proof of Theorem 2.9 if $v(2) = 0$ or 2 does not split in $\mathbb{O}/\mathbb{Z}$. As we have noted before, we can pick α such that $\mathbb{O} = \mathbb{Z}[\alpha]$ and $v(N(\alpha)) = 0$ and it suffices to prove the theorem for such an α.

Without loss of generality, we may assume that L_v contains the coordinates of all points in the kernel $E[\alpha]$ of α.

Apply Lemma 2.14 with $\Gamma = E[\alpha]$ to get an isogeny σ with kernel $E[\alpha]$. Then by [Silverman 1986, III.4.11], there is an isomorphism $\psi : E' \to E$ such that $\alpha = \psi \circ \sigma$.

Notice that every point in $E[\alpha]$ is $N(\alpha)$-torsion, so its coordinates are v-integral by [Silverman 1986, VII.3.4]. Therefore, both $F_\sigma(T)$ and E' have v-integral coefficients. The power series $F_\psi(T)$ also has v-integral coefficients because of Corollary 2.12 and $v(u) = -v(\alpha) = 0$. As $F_\alpha(T) = F_{\psi\circ\sigma}(T) = F_\psi(F_\sigma(T))$, this finishes the proof. □

Integrality of torsion points. We finish our discussion of formal groups with a result on integrality of $\mathbb{O}$-torsion points.

Let $\mathcal{F}$ be any formal group over R_v and suppose that $\mathrm{End}_{R_v}(\mathcal{F})$ contains a subring $\mathbb{O}$ isomorphic to an order in a number field. Identify $f(T) \in \mathbb{O}$ with $f'(0) \in R_v$ and let $\mathfrak{p} = \mathbb{O} \cap \mathfrak{M}$.

Lemma 2.15. *View $\mathcal{F}(\mathfrak{M})$ as an $\mathcal{O}$-module. Then for any torsion element $z \in \mathcal{F}(\mathfrak{M})$, the annihilator of z is $\mathfrak{p}$-primary, that is, not divisible by a prime different from $\mathfrak{p}$.*

Proof. For any $\alpha \in \mathcal{O} \subset R$, denote the corresponding element of $\operatorname{End}_{R_v}(\mathcal{F})$ by $[\alpha]$. Suppose that z has annihilator $\mathfrak{a}$. Write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, where $\mathfrak{c}$ is $\mathfrak{p}$-primary and $\mathfrak{b}$ is coprime to $\mathfrak{p}$. We need to prove $\mathfrak{b} = \mathcal{O}$. So suppose that $\mathfrak{b} \neq \mathcal{O}$. Take any pair of elements $\alpha \in \mathfrak{c} \setminus \mathfrak{a}$ and $\beta \in \mathfrak{b} \setminus \mathfrak{p}$, so $\alpha\beta \in \mathfrak{a}$. Now $[\alpha]z$ is a nonzero element of $\mathcal{F}(\mathfrak{M})$ that is in the kernel of $[\beta]$. But $[\beta](T) = \beta T + \cdots$ is an isomorphism, because $v(\beta) = 0$. Contradiction. □

Now suppose again that E/L_v is an elliptic curve, given by a Weierstrass equation with coefficients in R_v. Let $\mathcal{O} = \operatorname{End}_{L_v}(E)$ and $\mathfrak{p} = \mathfrak{M} \cap \mathcal{O}$.

Corollary 2.16. *Suppose that $Q \in E(L_v)$ is a torsion point. If the annihilator of Q is not $\mathfrak{p}$-primary, then $x(Q)$ is v-integral.* □

3. Elliptic divisibility sequences with complex multiplication

Let E/L be an elliptic curve, given by a Weierstrass equation with coefficients in the ring of integers of the number field L. Let $\mathcal{O} = \operatorname{End}_L(E)$ and let K be the field of fractions of $\mathcal{O}$. There is a natural choice of an embedding of K into L mapping an endomorphism to the element of L by which it multiplies invariant differentials of E.

Fix a point $P \in E(L)$ and let $(B_\alpha)_{\alpha\in\mathcal{O}}$ be defined by $x(\alpha P)\,\mathcal{O}_L = A_\alpha B_\alpha^{-2}$ (with A_α and B_α coprime). For an example, see Table 1.

In the previous section, we have defined $\mathcal{O}$-submodules $E_n(L_v)$ of $E(L_v)$ for which

$$v(B_\alpha) \geq n \iff \alpha P \in E_n(L_v). \tag{3.1}$$

As a consequence, we get the following result.

Lemma 3.2. *For all $\alpha, \beta \in \mathcal{O}$, if $\alpha \mid \beta$, then $B_\alpha \mid B_\beta$.* □

The *elliptic divisibility sequence* associated to P is the sequence $(B_\mathfrak{a})_\mathfrak{a}$, indexed by ideals $\mathfrak{a}$ of $\mathcal{O}$ and given by

$$B_\mathfrak{a} = \sum_{\alpha\in\mathfrak{a}} B_\alpha.$$

In other words, for every discrete valuation v of L, we have

$$v(B_\mathfrak{a}) = \min_{\alpha\in\mathfrak{a}} v(B_\alpha).$$

By Lemma 3.2, we have $B_{\alpha\mathcal{O}} = B_\alpha$ for every $\alpha \in \mathcal{O}$. Moreover, by definition we have the weak divisibility property: if $\mathfrak{a} \mid \mathfrak{b}$, then $B_\mathfrak{a} \mid B_\mathfrak{b}$. Actually, we even have the following *strong divisibility property*.

α	B_α	
1	1	$= 1$
$1+i$	$1+i$	
2	$(1+i)^2$	$= 2$
$2+i$	$2-i$	
$2+2i$	$(3)(\underline{1+i})^3$	
3	$(3+2i)(3-2i)$	$= 13$
$3+i$	$(\underline{1+i})(\underline{2+i})(4-i)$	
$3+2i$	$(5+4i)(6-i)$	
$3+3i$	$(\underline{1+i})(\underline{3+2i})(\underline{3-2i})$	
4	$(\underline{1+i})^4(\underline{3})(7)$	$= \underline{2}^2 \cdot 3 \cdot 7$
$4+i$	$(5-2i)(14-i)$	
$4+2i$	$(\underline{1+i})^2(\underline{4+i})(\underline{2-i})(16+9i)$	
$4+3i$	$(\underline{2+i})(14-9i)(32+23i)$	
$4+4i$	$(\underline{1+i})^5(\underline{3})(\underline{7})(8+7i)(8-7i)$	
5	$(\underline{2+i})^2(\underline{2-i})^2(6+5i)(6-5i)$	$= 5^2 \cdot 61$
$5+i$	$(\underline{1+i})(\underline{6+i})(\underline{5-4i})(31-20i)$	
$5+2i$	$(11+4i)(2+7i)(40+17i)$	
$5+3i$	$(\underline{1+i})(\underline{14+i})(\underline{5+2i})(159-40i)$	
$5+4i$	$(17-10i)(27-2i)(173+172i)$	
$\vdots$		$\vdots$
6	$(\underline{1+i})^2(\underline{3+2i})(\underline{3-2i})(239)$	$= \underline{2} \cdot \underline{13} \cdot 239$
7	$(1469+84i)(1469-84i)$	$= 2165017$
8	$(\underline{1+i})^6(\underline{3})(\underline{7})(31)(\underline{8+7i})(\underline{8-7i})(16+i)(16-i)$	$= \underline{2}^3 \cdot \underline{3} \cdot \underline{7} \cdot 31 \cdot 113$ $\cdot 257$

Table 1. The curve $E : y^2 = x^3 - 2x$ has CM by $\mathbb{Z}[i]$ via $i(x, y) = (-x, iy)$. This table gives the sequence defined by $P = (-1, 1)$. The nonprimitive divisors are underlined in both the $\mathbb{Z}[i]$-indexed sequence on the left and the $\mathbb{Z}$-indexed sequence on the right. Some primitive divisors on the right are not primitive on the left.

Lemma 3.3. *For any pair of* $\mathbb{O}$*-ideals* $\mathfrak{a}$, $\mathfrak{b}$, *we have*

$$B_{\mathfrak{a}+\mathfrak{b}} = B_{\mathfrak{a}} + B_{\mathfrak{b}}.$$

Proof. The divisibility property implies that the left hand side divides the right. Now let v be a discrete valuation of L and let n be the valuation of the right hand side. Then $v(B_{\mathfrak{a}}), v(B_{\mathfrak{b}}) \geq n$, so αP and βP are in the group $E_n(L_v)$ for all $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}$. As every element of $\mathfrak{a} + \mathfrak{b}$ is of the form $\alpha + \beta$ and we have that

$(\alpha+\beta)P = \alpha P + \beta P$, it follows that $\gamma P \in E_n(L_v)$ for every $\gamma \in \mathfrak{a}+\mathfrak{b}$, so the valuation of the right hand side is at least n. □

Notice that any interpolation of the $\mathbb{O}$-indexed sequence to an ideal-indexed sequence is completely determined by the strong divisibility property.

We call a prime $\mathfrak{q}$ of L a *primitive divisor* of $B_{\mathfrak{a}}$ if it divides $B_{\mathfrak{a}}$, but does not divide any $B_{\mathfrak{b}}$ with $\mathfrak{a} \nmid \mathfrak{b}$. Given $\mathfrak{q}$, there is a unique ideal $\mathfrak{r}_{\mathfrak{q}}$ of $\mathbb{O}$ such that $\mathfrak{q}$ is a primitive divisor of $B_{\mathfrak{r}_{\mathfrak{q}}}$. We call $\mathfrak{r}_{\mathfrak{q}}$ the *rank of apparition* of $\mathfrak{q}$. Notice that $\mathfrak{r}_{\mathfrak{q}}$ is the annihilator of P in the $\mathbb{O}$-module $E(L_{\mathfrak{q}})/E_1(L_{\mathfrak{q}})$, which is the reduction of E modulo $\mathfrak{q}$ if E is nonsingular modulo $\mathfrak{q}$. For any ideal $\mathfrak{a}$ of $\mathbb{O}$, we have

$$\mathfrak{q} \mid B_{\mathfrak{a}} \iff \mathfrak{r}_{\mathfrak{q}} \mid \mathfrak{a}.$$

For any $\mathfrak{a}$, we can factor the ideal $B_{\mathfrak{a}}$ as a product of an ideal $D_{\mathfrak{a}}$ and an ideal $B_{\mathfrak{a}}/D_{\mathfrak{a}}$ in such a way that all primes dividing $D_{\mathfrak{a}}$ are primitive divisors of $B_{\mathfrak{a}}$ and all primes dividing $B_{\mathfrak{a}}/D_{\mathfrak{a}}$ are not. We call $D_{\mathfrak{a}}$ the *primitive part of* $B_{\mathfrak{a}}$. In the same way, we can define the primitive part of the classical $\mathbb{Z}$-indexed sequence and denote it by $D_n^{\mathbb{Z}}$. The Main Theorem is equivalent to the statement that $D_{\mathfrak{a}} = \mathbb{O}_L$ for only finitely many $\mathfrak{a}$ coprime to the conductor.

Valuations. For any discrete valuation v of L, let p be the characteristic of the residue field. For any ideal $\mathfrak{a}$ of $\mathbb{O}$, set $v(\mathfrak{a}) = \min_{\alpha\in\mathfrak{a}} v(\alpha)$, or equivalently $v(\mathfrak{a}) = v(\mathfrak{a}\,\mathbb{O}_L)$. From the theory of formal groups, we get the following important property of elliptic divisibility sequences.

Lemma 3.4. *For every pair of nonzero integral $\mathbb{O}$-ideals $\mathfrak{a}$, $\mathfrak{b}$, if $v(B_{\mathfrak{a}}) > \frac{v(p)}{p-1}$, then*

$$v(B_{\mathfrak{a}\mathfrak{b}}) = v(B_{\mathfrak{a}}) + v(\mathfrak{b}).$$

Proof. Assume first that $\mathfrak{a}$ and $\mathfrak{b}$ are principal, say $\mathfrak{a} = \alpha\mathbb{O}$ and $\mathfrak{b} = \beta\mathbb{O}$. Then the statement follows immediately from Proposition 2.8 applied to the map β and the point αP.

Now let $\mathfrak{a}$ and $\mathfrak{b}$ be arbitrary. We claim

$$v(B_{\mathfrak{a}\mathfrak{b}}) = \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}).$$

Proof of the claim: If $\alpha\in\mathfrak{a}$, $\beta\in\mathfrak{b}$, then $\alpha\beta\in\mathfrak{a}\mathfrak{b}$, so "$\leq$" follows from the divisibility property. On the other hand, let $\gamma \in \mathfrak{a}\mathfrak{b}$ be such that $v(B_\gamma)$ is minimal. Then $v(B_{\mathfrak{a}\mathfrak{b}}) = v(B_\gamma)$. We can write γ in the form $\gamma = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$, so by (3.1), we have

$$v(B_\gamma) \geq \min_{1\leq i\leq n} v(B_{\alpha_i\beta_i}) \geq \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}),$$

which proves the claim.

Notice that by the divisibility property, $v(B_\alpha) \geq v(B_\mathfrak{a}) > \frac{v(p)}{p-1}$ for all $\alpha \in \mathfrak{a}$, so the claim implies

$$v(B_{\mathfrak{ab}}) = \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}}(v(B_\alpha) + v(\beta)) = \min_{\alpha\in\mathfrak{a}} v(B_\alpha) + \min_{\beta\in\mathfrak{b}} v(\beta) = v(B_\mathfrak{a}) + v(\mathfrak{b}). \qquad \square$$

Lemma 3.4 for $\mathbb{Z}$-indexed sequences is also given by Silverman [1988] for $L = \mathbb{Q}$ and Cheon and Hahn [1998; 1999] for L an arbitrary number field. The versions in [Silverman 1988] and [Cheon and Hahn 1999] are correct, but, unfortunately, [Cheon and Hahn 1998] omits the condition $v(B_m) > v(p)/(p-1)$ and mentions only the weaker condition $v(B_m) > 0$, which is too weak, as we can see from the following example.

Example 3.5. Let $E/\mathbb{Q}$ be given by the Weierstrass equation $y^2+xy = x^3+x^2-2x$ and let $P = (-\frac{1}{4}, \frac{7}{8}) \in E(\mathbb{Q})$. Then P is a nontorsion point and $2P = (\frac{121}{64}, \frac{913}{512})$, so $B_1 = 2$, $B_2 = 8$, so that $\mathrm{ord}_2(B_2) \neq \mathrm{ord}_2(B_1) + \mathrm{ord}_2(2)$, contradicting Lemma 1 of [Cheon and Hahn 1998].

Suppose that v is normalized, that is, $v(L^*) = \mathbb{Z}$. If $v(p) < p-1$, then the conditions $v(B_\mathfrak{a}) > 0$ and $v(B_\mathfrak{a}) > v(p)/(p-1)$ are equivalent. Notice that we can only have $v(p) \geq p-1$ if v is ramified or $p = 2$, so there are only finitely many valuations for which we cannot use the weaker condition $v(B_\mathfrak{a}) > 0$.

In fact, if $L = \mathbb{Q}$ and 2 divides the coefficient a_1 of the Weierstrass equation (2.1), then the duplication formula [Silverman 1986, III.2.3(d)] tells us that even in the case $v(2) > 0$ we may use the condition $v(B_m) > 0$.

For the finitely many remaining valuations, we will use an asymptotic version. The first step is the following lemma.

Lemma 3.6. *For any pair of elements $\alpha, \beta \in \mathbb{Z}$, if $v(B_\alpha) > 0$, then*

$$v(B_{\alpha\beta}) \geq v(B_\alpha),$$

where we have equality if and only if $v(\beta) = 0$.

Proof. Let $n = v(B_\alpha)$. By Corollary 2.10, the $\mathbb{O}$-module $E_n(L_v)/E_{n+1}(L_v)$ is isomorphic to the residue field l of L_v. If $v(\beta) = 0$, then β induces an automorphism of l, and hence we have equality. Otherwise, β acts as multiplication by 0 on l and we have $v(B_{\alpha\beta}) > n$. $\square$

For any valuation v, let r be the positive generator of $\mathfrak{r}_v \cap \mathbb{Z}$, where $\mathfrak{r}_v$ is the rank of apparition of v.

Lemma 3.7. *There is a bound $F_v \in \mathbb{Z}$ such that for all integers $m \in r\mathbb{Z}$, we have $|v(B_m) - v(m)| \leq F_v$.*

Proof. Let $r > 0$ be a generator of $\mathfrak{r}_v \cap \mathbb{Z}$, let k be the smallest integer greater than $v(p)/(p-1)$ and let p^l be the largest power of p dividing m/r. Then Lemma 3.6

gives $v(B_m) = v(B_{rp^l})$, so we may assume $m = rp^l$. If $l \geq k$, then Lemma 3.4 with $\mathfrak{b} = (p^{l-k})$, $\mathfrak{a} = (rp^k)$ gives $v(B_m) - v(m) = v(B_{rp^k}) - v(rp^k)$, which is constant and there are only finitely many remaining possibilities for l. □

Corollary 3.8. *For all pairs* $(m, n) \in (r\mathbb{Z} \times \mathbb{Z})$, *we have* $|v(B_{mn}) - v(B_m) - v(n)| \leq 2F_v$. □

For every ideal $\mathfrak{a}$ of $\mathbb{O}$, set $N(\mathfrak{a}) = [\mathbb{O} : \mathfrak{a}]$.

Corollary 3.9. *For every ideal* $\mathfrak{a}$ *of* $\mathbb{O}$, *we have* $v(B_\mathfrak{a}) \leq F_v + v(N(\mathfrak{a}))$.

Proof. By the divisibility property, we have $v(B_\mathfrak{a}) \leq v(B_{N(\mathfrak{a})}) \leq v(N(\mathfrak{a})) + F_v$. □

Silverman's proof. In [1988], Silverman proved that for $\mathbb{O} = \mathbb{Z}$, all but finitely many terms have a primitive divisor. His proof generalizes to arbitrary number fields L, but not to sequences indexed by quadratic imaginary orders. We will now look at Silverman's proof and see what goes wrong if we try to apply it to sequences indexed by (ideals of) the endomorphism ring.

Let V^∞ be the set of archimedean valuations of L that restrict to the standard absolute value on $\mathbb{Q}$. Let V^0 be the set of nonarchimedean valuations of L that are normalized in the sense that each satisfies $|\frac{1}{p}|_v = p$ for some prime number $p \in \mathbb{Z}$. For every $v \in V = V^\infty \cup V^0$, let $n_v = [L_v : \mathbb{Q}_v]$. For fractional ideals I of L, set $\|I\| = \left|N_{L/\mathbb{Q}}(I)\right|^{1/[L:\mathbb{Q}]}$. Let h_x be the height on E relative to x, defined by $h_x(P) = h(x(P))$, where h is the logarithmic height on $\overline{\mathbb{Q}}$ as given in [Silverman 1986, § VIII.6]. Then by definition

$$\begin{aligned} h_x(\alpha P) &= \sum_{v \in V} \frac{n_v}{[L : \mathbb{Q}]} \log \max\{|x(\alpha P)|_v, 1\} \\ &= \log \|B_\alpha^2\| + \sum_{v \in V^\infty} \frac{n_v}{[L : \mathbb{Q}]} \log \max\{|x(\alpha P)|_v, 1\}. \end{aligned} \tag{3.10}$$

A theorem of Siegel [Silverman 1986, IX.3.1] says that the (finitely many) terms in the final sum are $o(1)\, h_x(\alpha P)$ as $\|\alpha\|$ tends to infinity, where $o(1)$ denotes something which tends to 0. At the same time, those terms are clearly nonnegative, so

$$(1 - o(1))\, h_x(\alpha P) \leq \log \|B_\alpha^2\| \leq h_x(\alpha P) \qquad \text{as } \|\alpha\| \to \infty.$$

We express this in terms of the canonical height function $\widehat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$, as defined in [Silverman 1986, § VIII.9]. That function satisfies

$$\widehat{h}(P) = (\deg(f))^{-1} h(f(P)) + O(1)$$

for every function $f \in L(E)$ and hence $\widehat{h}(\phi(P)) = \deg(\phi)\, \widehat{h}(P)$ for every isogeny of elliptic curves ϕ. As the degree of multiplication by α is $\|\alpha\|^2$ and the degree of the function x is 2, we get

$$(1-o(1))\,\|\alpha\|^2\,\widehat{h}(P) \le \frac{1}{2}\log\|B_\alpha^2\| \le \|\alpha\|^2\,\widehat{h}(P) + O(1) \qquad \text{as } \|\alpha\| \to \infty.$$

The classical proof of the existence of primitive divisors is based on these estimates, combined with the following result. Let $D_n^{\mathbb{Z}}$ be the primitive part of B_n in the $\mathbb{Z}$-indexed sequence, so $B_n/D_n^{\mathbb{Z}}$ is the greatest $\mathbb{O}_L$-ideal dividing B_n that is not divisible by any primitive divisors of B_n.

Lemma 3.11. *There is a positive integer N such that for all $n \in \mathbb{Z}$,*

$$\frac{B_n}{D_n^{\mathbb{Z}}} \;\Big|\; N\prod_p p\, B_{n/p},$$

where the product ranges over the primes dividing n.

Proof. Let v be a discrete valuation of L, normalized by $v(L^*) = \mathbb{Z}$ and let $\mathfrak{q} \subset \mathbb{O}_L$ be the prime ideal corresponding to v.

Suppose that the valuation of the left hand side is positive. Then $\mathfrak{q}$ is not a primitive divisor of B_n, so there is a prime $p \mid n$ for which $v(B_{n/p}) > 0$.

Let $r > 0$ be such that $r\mathbb{Z} = \mathfrak{r}_v \cap \mathbb{Z}$ and let $q > 0$ be the rational prime such that $v(q) > 0$. If $v(q) < q-1$, then apply Lemma 3.4 with $\mathfrak{a} = (n/p)$ and $\mathfrak{b} = (p)$. This yields $v(B_n) = v(B_{n/p}) + v(p)$, which is at most equal to the valuation of the right hand side.

For the finitely many valuations with $v(q) \ge q-1$, we apply Corollary 3.8 and find that $v(B_n) \le v(B_{n/p}) + v(p) + 2F_v$. Hence the assertion follows if we take N such that $v(N) \ge 2F_v$ for those finitely many valuations. □

The lemma and the estimates together imply

$$\begin{aligned}\log\|D_n^{\mathbb{Z}}\| &\ge \log\|B_n\| - \log\|n\| - \sum_{p\mid n}\log\|B_{n/p}\| - \log\|N\| \\ &\ge \Big(1 - o(1) - \sum_{p\mid n} p^{-2}\Big)\, n^2\,\widehat{h}(P) \qquad (n\to\infty),\end{aligned}$$

where $1 - \sum_{p\mid n} p^{-2} \ge 0.547$. From some point on, $\|D_n^{\mathbb{Z}}\|$ has to be greater than 1, which proves the following theorem.

Theorem 3.12 ([Silverman 1988]). *For all but finitely many $n \in \mathbb{N}$, B_n has a primitive divisor in the $\mathbb{Z}$-indexed sequence.*
□

Unfortunately, this proof does not work for elliptic divisibility sequences with complex multiplication, since there are too many primes of small norm: if we repeat the argument for example with $\mathbb{O} = \mathbb{Z}[i]$, then the estimate becomes

$$\log \|D_\alpha\| \geq \Big(1 - o(1) - \sum_{\mathfrak{p} \mid \alpha} |\mathfrak{p}|^{-2}\Big) |\alpha|^2 \widehat{h}(P).$$

If $30 \mid \alpha$, then $1+i, 2+i, 2-i$ and 3 are prime divisors of α and $\sum_{\mathfrak{p} \mid \alpha} |\mathfrak{p}|^{-2} \geq \frac{1}{2} + \frac{1}{9} + \frac{1}{5} + \frac{1}{5} > 1$, which makes the estimate useless.

The proof of Theorem 3.12 that we have seen is an inclusion-exclusion argument with a single inclusion and one exclusion for every prime, which is insufficient in the general case as we have just shown. Therefore, we will go all the way with the inclusion-exclusion principle.

Notice that every inclusion gives an $o(1)$, so if we have a growing number of inclusions, then we need to know more about the $o(1)$ functions involved. Furthermore, inclusion-exclusion works best with unique factorization, so we really need the ideal-indexed sequence and our estimates will need to hold for the ideal-indexed sequence as well.

We start with the estimates for the element-indexed sequence.

David's Theorem. The more explicit version of Siegel's theorem that we will use is David's theorem. It estimates linear forms in elliptic logarithms and the result is similar to Baker's result for ordinary logarithms.

Let $L \subset \mathbb{C}$ be a number field, k an integer and E/L an elliptic curve, together with a lattice Λ and a complex analytic isomorphism $f : \mathbb{C}/\Lambda \to E(\mathbb{C})$. For $1 \leq i \leq k$, fix an L-valued point $P_i \in E(L)$ and an elliptic logarithm u_i of P_i, that is, a complex number u_i such that $f(u_i) = P_i$.

Theorem 3.13 (David). *Let $\mathscr{L}$ be the linear form $X_1 u_1 + \cdots + X_k u_k$ in the variables $X_1, \ldots, X_k$. There exists a constant F, depending on E, L, f and the P_i, such that for all $b = (b_1, \ldots, b_k) \in L^n$, if $B = \max_i \{H(b_i)\}$ is sufficiently large and $\mathscr{L}(b) \neq 0$, then*

$$\log |\mathscr{L}(b)| > -F \log(B) (\log\log(B))^{k+1}.$$

Proof. This is a special case of [David 1995, Théorème 2.1]. □

Corollary 3.14. *Let E be an elliptic curve, given by a general Weierstrass equation with coefficients in a number field L and let $P \in E(L)$ be a point of infinite order. For any archimedean valuation v of L, there is a constant G such that for all $\alpha \in \mathbb{O}$ with $\|\alpha\|$ large enough,*

$$\log |x(\alpha P)|_v < G \log \|\alpha\| (\log\log \|\alpha\|)^4.$$

Proof. Completion with respect to v gives an embedding of L into $\mathbb{C}$. Now let $u_1, u_2 \in \mathbb{C}$ be generators of the period lattice Λ of E, define $\mathscr{F} = ([-\frac{1}{2}, \frac{1}{2}]u_1 + [-\frac{1}{2}, \frac{1}{2}]u_2)$ and let $u_3 \in \mathbb{C}$ be an elliptic logarithm of P. Take $b_3 = \alpha$ and let

$b_1, b_2 \in \mathbb{Z}$ be such that $\mathscr{L} = b_1 u_1 + b_2 u_2 + b_3 u_3$ is in $\mathscr{F}$. Then $f(\mathscr{L}) = \alpha P$ and on the compact set $\mathscr{F}$, we have $x(f(z)) = z^{-2} g(z)$ for a holomorphic, hence bounded, function g. Therefore, there is a constant C such that

$$\begin{aligned}\log|x(\alpha P)| &\leq -2\log|\mathscr{L}| + C\\ &< 2F\log(B)(\log\log(B))^4 + C\end{aligned}$$

if $B = \max_i |b_i|$ is large enough.

As $-b_1 u_1$ is the integer multiple of u_1 that is nearest to the intersection of the line $u_1\mathbb{R}$ with the line $\alpha u_3 + u_2\mathbb{R}$, we see that $|b_1|$ is bounded by a linear function in $|\alpha|$. In the same way, $|b_2|$ is also bounded by a linear function in $|\alpha|$. □

If we apply this to (3.10), then we get

$$\log\|B_\alpha\| = \|\alpha\|^2\,\widehat{h}(P) \;+\; O(\log\|\alpha\|\,(\log\log\|\alpha\|)^4) \quad (\|\alpha\| \to \infty).$$

Attaching points to the ideal-indexed sequence. David's theorem uses points on elliptic curves, but we need the estimates also for the ideal-indexed sequence. Therefore, for every ideal $\mathfrak{a}$ of $\mathbb{O}$, we will define a point $\mathfrak{a}P$. These points will not all lie on E, but they will lie on a finite set of isogenous curves.

For any $\alpha \in \mathbb{O}$, let $E[\alpha]$ be the kernel of $[\alpha]$. Then for any ideal $\mathfrak{a}$, we define

$$E[\mathfrak{a}] = \bigcap_{\alpha\in\mathfrak{a}} E[\alpha]$$

and we get a quotient isogeny

$$\mathfrak{a} : E \to E/E[\mathfrak{a}] =: E_{\mathfrak{a}}$$

which is defined over L [Silverman 1986, III.4.13.2]. Let $\mathscr{C}$ be the set of integral $\mathbb{O}$-ideals modulo equivalence, where we call $\mathfrak{a}$ and $\mathfrak{b}$ equivalent if there exists an element $x \in K^*$ such that $\mathfrak{a} = x\mathfrak{b}$. By [Cox 1989, Proposition 7.4], the set $\mathscr{C}$ is the union of the class groups of the orders $\mathbb{O}' \subset \mathbb{O}_K$ that contain $\mathbb{O}$, hence it is finite. If $\mathfrak{a}$ and $\mathfrak{b}$ are in the same class in $\mathscr{C}$, then the curves $E_{\mathfrak{a}}$ and $E_{\mathfrak{b}}$ are isomorphic over L. For each class $[\mathfrak{a}] \neq [\mathbb{O}]$ in $\mathscr{C}$, we fix an elliptic curve $E_{[\mathfrak{a}]}$, together with a Weierstrass equation with coefficients in $\mathbb{O}_L$, such that $E_{[\mathfrak{a}]}$ is isomorphic to $E_{\mathfrak{a}}$. For the trivial class, we take $E_{[\mathbb{O}]} = E$. Then we have an isogeny $\mathfrak{a} : E \to E_{[\mathfrak{a}]}$ which is defined up to automorphism of $E_{[\mathfrak{a}]}$.

For any pair of ideals $\mathfrak{a}$, $\mathfrak{b}$ such that $\mathfrak{a} \mid \mathfrak{b}$, there exists a unique quotient isogeny $\lambda = \lambda_{\mathfrak{a},\mathfrak{b}}$ such that $\mathfrak{b} = \lambda \circ \mathfrak{a}$ [Silverman 1986, III.4.11]. As both $\mathfrak{a}$ and $\mathfrak{b}$ are defined over L, so is λ.

For every ideal $\mathfrak{a}$, the point $\mathfrak{a}P \in E_{[\mathfrak{a}]}(L)$ is defined up to automorphism of $E_{[\mathfrak{a}]}$. We now define $\widetilde{A}_{\mathfrak{a}}$ and $\widetilde{B}_{\mathfrak{a}}$ to be the coprime $\mathbb{O}_L$-ideals such that

$$x(\mathfrak{a}P)\,\mathbb{O}_L = \widetilde{A}_{\mathfrak{a}}\widetilde{B}_{\mathfrak{a}}^{-2}.$$

It follows from Corollary 2.10 that $\widetilde{B}_{\mathfrak{a}}$ depends only on the ideal $\mathfrak{a}$ and the choice of Weierstrass equation, but not on the automorphism. Moreover, $\alpha P = (\alpha\mathbb{O})P$ (up to automorphism), so if $\mathfrak{a}$ is principal, then $\widetilde{B}_{\mathfrak{a}} = B_{\mathfrak{a}}$.

For every ideal class $[\mathfrak{a}]$, define the invariant differential

$$\omega_{[\mathfrak{a}]} = \omega_{E_{[\mathfrak{a}]}} = \frac{dx_{E_{[\mathfrak{a}]}}}{y_{E_{[\mathfrak{a}]}}}$$

and the fractional $\mathbb{O}_L$-ideal

$$C_{[\mathfrak{a}]} = \frac{\mathfrak{a}^*\omega_{[\mathfrak{a}]}}{\omega_E}\,(\mathfrak{a}\mathbb{O}_L)^{-1}.$$

Note that the ideal $C_{[\mathfrak{a}]}$ does not depend on the choice of a representative $\mathfrak{a}$ and that $C_{[\mathbb{O}]}$ equals $\mathbb{O}_L$.

Let V be the set of normalized discrete valuations of L. For any v in V, let $p = p_v$ be the prime number such that $v(p) > 0$ and let t_v be the least integer greater than $v(p)/(p-1) + C_{[\mathfrak{a}]} - C_{[\mathfrak{b}]}$ for all $[\mathfrak{a}]$, $[\mathfrak{b}]$. It exists, because the set of ideal classes is finite.

Lemma 3.15. *Let $\mathfrak{a} \mid \mathfrak{b}$ be $\mathbb{O}$-ideals and $v \in V$ a normalized discrete valuation. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then*

$$v(\widetilde{B}_{\mathfrak{b}}) = v(\widetilde{B}_{\mathfrak{a}}) + v(\mathfrak{b}) - v(\mathfrak{a}) + v(C_{[\mathfrak{b}]}) - v(C_{[\mathfrak{a}]}).$$

Proof. This result follows if we apply Proposition 2.8 to the isogeny $\lambda = \lambda_{\mathfrak{a},\mathfrak{b}}$, which satisfies $v(\lambda^*\omega_{[\mathfrak{b}]}/\omega_{[\mathfrak{a}]}) = v(\mathfrak{b}) - v(\mathfrak{a}) + v(C_{[\mathfrak{b}]}) - v(C_{[\mathfrak{a}]})$. □

Corollary 3.16. *Let v, $\mathfrak{a}$ be as above. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then $v(B_{\mathfrak{a}}) = v(\widetilde{B}_{\mathfrak{a}}) - v(C_{[\mathfrak{a}]})$.*

Proof. For any $\alpha \in \mathfrak{a}$, we have

$$v(B_\alpha) = v(\widetilde{B}_\alpha) = v(\widetilde{B}_{\mathfrak{a}}) + v(\alpha) - v(\mathfrak{a}) - v(C_{[\mathfrak{a}]}) \geq v(\widetilde{B}_{\mathfrak{a}}) - v(C_{[\mathfrak{a}]}),$$

where the inequality is an equality if $v(\alpha) = v(\mathfrak{a})$. As $v(B_{\mathfrak{a}}) = \min\{v(B_\alpha) : \alpha \in \mathfrak{a}\}$, the result follows. □

From now on we restrict to invertible ideals $\mathfrak{a}$. For the general case, see Section 4. Let S be the subset of valuations $v \in V$ such that $t_v = 1$.

Lemma 3.17. *For every $v \in S$ and every invertible $\mathbb{O}$-ideal $\mathfrak{a}$, we have $v(\widetilde{B}_{\mathfrak{a}}) = v(B_{\mathfrak{a}})$.*

Proof. Notice first of all that $v \in S$ implies $v(C_{[\mathfrak{a}]}) = 0$ for all $\mathfrak{a}$. By Corollary 3.16, the only thing we need to prove is that if $v(B_{\mathfrak{a}}) > 0$, then $v(\widetilde{B}_{\mathfrak{a}}) > 0$.

Let $\mathfrak{a} = \alpha\mathbb{O} + \beta\mathbb{O}$. Then $\alpha\mathfrak{a}^{-1}$ and $\beta\mathfrak{a}^{-1}$ are coprime $\mathbb{O}$-ideals, so we can take $a \in \alpha\mathfrak{a}^{-1}$ and $b \in \beta\mathfrak{a}^{-1}$ such that $a + b = 1$. Then $0 > v(x(\alpha P)) \geq v(x(a\mathfrak{a}P))$ and $0 > v(x(\beta P)) \geq v(x(b\mathfrak{a}P))$. As $E_{[\mathfrak{a}],1}(L_v)$ is a group, we find $v(x(\mathfrak{a}P)) < 0$, so we are done. □

For the finitely many valuations that are not in S, we will be satisfied with the following asymptotic version.

Lemma 3.18. *For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ and any $v \in V$, we have*

$$v(B_{\mathfrak{a}}) = v(\widetilde{B}_{\mathfrak{a}}) + O\big(v(N(\mathfrak{a}))\big) \qquad (N(\mathfrak{a}) \to \infty).$$

Proof. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then the assertion follows from Corollary 3.16. Otherwise, it is equivalent to Corollary 3.9. □

If we apply Lemma 3.17 to the valuations in S and Lemma 3.18 to the rest, then we find

$$\log N(B_{\mathfrak{a}}) = \log N(\widetilde{B}_{\mathfrak{a}}) + O(\log N(\mathfrak{a})) \qquad (N(\mathfrak{a}) \to \infty). \tag{3.19}$$

Next, we apply David's Theorem, so let v be any *archimedean* valuation of L.

Proposition 3.20. *There is a constant G such that for all but finitely many invertible $\mathcal{O}$-ideals $\mathfrak{a}$,*

$$\log |x(\mathfrak{a}P)|_v < G \log \|\mathfrak{a}\| \, (\log\log \|\mathfrak{a}\|)^4.$$

Proof. First of all, notice that it suffices to prove this for every ideal class separately. So fix $[\mathfrak{a}] \in \mathscr{C}$ and a representative $\widetilde{\mathfrak{a}}$ of $[\mathfrak{a}]$.

Let $\Lambda = u_1\mathbb{Z} + u_2\mathbb{Z}$ be a lattice such that $E_{[\mathfrak{a}],L_v}(\mathbb{C}) \cong \mathbb{C}/\Lambda$ and let $u_3 \in \mathbb{C}$ be such that $u_3 (\mathrm{mod}\ \Lambda)$ corresponds to $[\widetilde{\mathfrak{a}}]P$.

For any $\mathfrak{a} \in [\mathfrak{a}]$, let $b_3 = \alpha/\beta$ be a generator of $\mathfrak{a}/\widetilde{\mathfrak{a}}$. Then the point $\mathfrak{a}P$ corresponds to $b_3 u_3$ (mod Λ).

Let $b_1, b_2 \in \mathbb{Z}$ be such that $\mathscr{L} = b_1u_1 + b_2u_2 + b_3u_3$ is in a fixed fundamental parallelogram for Λ. Then by David's theorem,

$$\log |x(\mathfrak{a}P)| < 2F \log(B)\, (\log\log(B))^4$$

if $B = \max_i H(b_i)$ is large enough. Notice that the denominator of b_3 divides $\widetilde{\mathfrak{a}}$, so $\log H(b_3) = \log \|b_3\| + O(1) = \log \|\mathfrak{a}\| + O(1)$. At the same time, b_1 and b_2 are bounded by a linear function in $\|b_3\|$, so we find the desired result. □

Theorem 3.21. *For all invertible $\mathcal{O}$-ideals $\mathfrak{a}$, we have*

$$\log \|B_{\mathfrak{a}}\| = \|\mathfrak{a}\|^2\, \widehat{h}(P) \;+\; O(\log \|\mathfrak{a}\| \, (\log\log \|\mathfrak{a}\|)^4) \quad (\|\mathfrak{a}\| \to \infty),$$

where $\|\mathfrak{a}\| = [\mathcal{O} : \mathfrak{a}]^{1/[K:\mathbb{Q}]}$.

Proof. If we apply Proposition 3.20 to (3.10), then we get

$$\log \|\widetilde{B}_{\mathfrak{a}}\| = \widehat{h}(\mathfrak{a}P) \;+\; O(\log \|\mathfrak{a}\| (\log\log \|\mathfrak{a}\|)^4).$$

The left hand side is $\log \|B_{\mathfrak{a}}\| + O(\log \|\mathfrak{a}\|)$ by (3.19). If $\mathcal{O} = \mathcal{O}_K$, then [Silverman 1994, II.1.5] says that $\mathfrak{a}$ has degree $\|\mathfrak{a}\|^2$. In general, it is [Shimura 1998, Proposition II.10]. □

Corollary 3.22. *For any pair of nonzero invertible $\mathbb{O}$-ideals $\mathfrak{a}$, $\mathfrak{b}$ such that $\|\mathfrak{a}\|$ is suitably large,*

$$B_{\mathfrak{a}} \,|\, B_{\mathfrak{b}} \iff \mathfrak{a} \,|\, \mathfrak{b}.$$

In particular, for any pair of nonzero elements α, β such that $\|\alpha\|$ is suitably large,

$$B_{\alpha} \,|\, B_{\beta} \iff \alpha \,|\, \beta.$$

Proof. Suppose that $B_{\mathfrak{a}} \,|\, B_{\mathfrak{b}}$. If $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$, then $B_{\mathfrak{d}} = (B_{\mathfrak{a}}, B_{\mathfrak{b}}) = B_{\mathfrak{a}}$ and $\mathfrak{d} \,|\, \mathfrak{a}$. If $\mathfrak{d}$ strictly contains $\mathfrak{a}$, then this contradicts the bounds of Theorem 3.21. □

Proof of the Main Theorem. We will now use the estimates and an inclusion-exclusion argument to prove the existence of primitive divisors.

We have seen in Lemma 3.4 that only a small part of the growth of $B_{\mathfrak{a}}$ comes from higher powers of nonprimitive divisors. We "neglect" this by introducing $B'_{\mathfrak{a}} = \prod_{\mathfrak{b} \,|\, \mathfrak{a}} D_{\mathfrak{b}}$, in which these higher powers are eliminated.

Lemma 3.23. *For all $\mathfrak{a}$ and almost every discrete valuation v, we have*

$$v(B'_{\mathfrak{a}}) \le v(B_{\mathfrak{a}}) \le v(B'_{\mathfrak{a}}) + v(\mathfrak{a}).$$

With an added $F_v + \log N(\mathfrak{a})$ on the right hand side, the inequality holds for all v.

In particular,

$$\bigl|\log \|B_{\mathfrak{a}}\| - \log \|B'_{\mathfrak{a}}\|\bigr| \le \log \|\mathfrak{a}\| + C.$$

Proof. Let v be any discrete valuation of L. The first inequality is true by definition. Now suppose that $v(B_{\mathfrak{a}}) > 0$ and let $\mathfrak{r}$ be the rank of apparition of v. If $v(p) < p-1$, then Lemma 3.4 implies $v(B_{\mathfrak{a}}) \le v(B_{\mathfrak{a}\mathfrak{r}}) = v(B_{\mathfrak{r}}) + v(\mathfrak{a}) = v(B'_{\mathfrak{a}}) + v(\mathfrak{a})$. For the finitely many valuations with $v(p) \ge p-1$, Corollary 3.9 shows that the same holds with an added $F_v + \log N(\mathfrak{a})$.

The final statement follows if one sums over all v. □

We will now prove the Main Theorem for ideals coprime to the index $f = [\mathbb{O}_K : \mathbb{O}]$. For the general case, see Section 4.

Proof. Let μ be the Möbius function for the set of ideals of $\mathbb{O}$ coprime to f, so

$$\mu(\mathfrak{b}) = \begin{cases} 0 & \text{if a square of an ideal divides } \mathfrak{b}, \\ (-1)^n & \text{if } \mathfrak{b} \text{ is a product of } n \text{ distinct primes.} \end{cases}$$

The inclusion-exclusion principle yields

$$\begin{aligned} \log \|D_{\mathfrak{a}}\| &= \sum_{\mathfrak{b} \,|\, \mathfrak{a}} \mu(\mathfrak{b}) \log \|B'_{\mathfrak{a}/\mathfrak{b}}\| \\ &= \sum_{\mathfrak{b} \,|\, \mathfrak{a}} \mu(\mathfrak{b}) \log \|B_{\mathfrak{a}/\mathfrak{b}}\| \; O(\log \|\mathfrak{a}\|), \end{aligned}$$

to which we can apply Theorem 3.21 and get

$$\begin{aligned}\log \|D_{\mathfrak{a}}\| &= \widehat{h}(P) \sum_{\mathfrak{b} \mid \mathfrak{a}} \mu(\mathfrak{b})\, \|\mathfrak{a}/\mathfrak{b}\|^2 \;+\; \sum_{\mathfrak{b} \mid \mathfrak{a}} O(\log \|\mathfrak{a}\|\, (\log\log \|\mathfrak{a}\|)^4) \\ &= \|\mathfrak{a}\|^2 \widehat{h}(P) \prod_{\mathfrak{p} \mid \mathfrak{a}} (1 - \|\mathfrak{p}\|^{-2}) \;+\; O(\|\mathfrak{a}\|^{\epsilon}).\end{aligned}$$

The product is at least

$$\prod_{p \le \|\mathfrak{a}\|} (1 - p^{-1})^2,$$

and Mertens' Theorem [Hardy and Wright 1938, 22.9 Theorem 430] states that

$$\prod_{p \le X} (1 - p^{-1}) \sim \frac{e^{-\gamma}}{\log X} \quad (X \to \infty),$$

where $\gamma \approx 0.5772$ is the Euler constant. If we pick $\epsilon < 2$, then this finishes the proof of the Main Theorem for ideals coprime to the index f. In the general case, inclusion-exclusion is harder and we will show how to do it in Section 4.

For $\mathbb{Z}$-indexed sequences, regardless of whether the curve has complex multiplication, (3.24) is exactly Proposition 1.3. □

We will now prove the corollary about splitting behavior of primitive divisors in $\mathbb{Z}$-indexed sequences over CM curves. Let K' be the field of fractions of $\mathbb{O}' = \operatorname{End}_{\overline{L}}(E)$.

Corollary 3.24. *Suppose that not all endomorphisms of E over $\overline{L}$ are defined over L. Define for $n \in \mathbb{Z}$, the numbers*

$$\begin{aligned} r_n &= \#\{p \in \mathbb{N} :\ p \mid n,\ p \text{ is a prime ramifying in } \mathbb{O}'/\mathbb{Z} \text{ and } p \nmid [\mathbb{O}_{K'} : \mathbb{O}']\}, \\ s_n &= \#\{p \in \mathbb{N} :\ p \mid n \text{ and } p \text{ is a prime splitting in } \mathbb{O}'/\mathbb{Z}\}. \end{aligned}$$

Then for almost all n, the term B_n has at least $r_n + s_n + 1$ primitive divisors, of which at least s_n split in $K'L/L$.

Proof. Let σ denote the unique nontrivial automorphism of KL/L. Notice that $B_{\sigma(\mathfrak{a})} = \sigma(B_{\mathfrak{a}})$ for every $\mathbb{O}$-ideal $\mathfrak{a}$.

Suppose that n is large enough such that $B_{\mathfrak{a}}$ has a primitive divisor (in the $\mathbb{O}$-ideal-indexed sequence) for all $\mathfrak{a}$ with $\|\mathfrak{a}\| \ge \sqrt{n}$.

For any prime number $p \mid n$ that splits in $K/\mathbb{Q}$, write $(p) = \mathfrak{p}\sigma(\mathfrak{p})$. Then $B_{n/\mathfrak{p}}$ has a primitive divisor $\mathfrak{q} \subset \mathbb{O}_L$. If $\mathfrak{q}$ is ramified or inert in KL/L, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, so $\mathfrak{q}$ is also a divisor of $B_{n/\sigma(\mathfrak{p})}$, contradicting the assumption that $\mathfrak{q}$ is primitive at $B_{n/\mathfrak{p}}$. Therefore, $\mathfrak{q}$ is a prime of L that splits in KL/L and is a primitive of B_n in the $\mathbb{N}$-indexed sequence.

There are at least $r_n + 1$ more primitive divisors, because B_n itself also has a primitive divisor as well as each $B_{n/\mathfrak{p}}$ where $p = \mathfrak{p}^2$ is a ramifying prime divisor of n. □

4. The general case

We will now show how to give a proof of the Main Theorem even for ideals that may not be coprime to the index $[\mathbb{O}_K : \mathbb{O}]$. The set of all ideals does not have unique factorization, so the Möbius functions become more tricky. Moreover, when we do inclusion-exclusion with invertible ideals that are not coprime to $[\mathbb{O}_K : \mathbb{O}]$, we will encounter ideals that are not invertible. The first thing we need to do is therefore to generalize Theorem 3.21 to ideals that may not be invertible.

The only part of the proof of Theorem 3.21 that uses invertibility of the ideal $\mathfrak{a}$ is the part of the proof of Lemma 3.17 that states that if $v(B_\mathfrak{a}) > 0$, then $v(\widetilde{B}_\mathfrak{a}) > 0$. We prove this in the general case for a smaller set of valuations S'. Recall that S was the set of all normalized discrete valuations v of L for which $v(p) < p - 1$ and $v(C_{[\mathfrak{a}]}) = 0$ for all $[\mathfrak{a}]$. We let S' be the set of valuations in S for which also $v([\mathbb{O}_K : \mathbb{O}]) = 0$ and the Weierstrass equation of $E_{[\mathfrak{a}]}$ is nonsingular for every $[\mathfrak{a}] \in \mathscr{C}$. Notice that S' still contains all but finitely many valuations of V.

Lemma 4.1. *For every $v \in S'$ and every $\mathbb{O}$-ideal $\mathfrak{a}$, we have that $v(\widetilde{B}_\mathfrak{a}) = v(B_\mathfrak{a})$.*

Proof. The only thing left to prove is that if $v(B_\mathfrak{a}) > 0$, then $v(\widetilde{B}_\mathfrak{a}) > 0$. We already know this for invertible ideals $\mathfrak{a}$. Write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, where $\mathfrak{b}$ is coprime to the index $f = [\mathbb{O}_K : \mathbb{O}]$ and $\mathfrak{c}$ divides f^n for some integer n. Without loss of generality, we may assume that all points in $E_{[\mathfrak{c}]}[f^n]$ are defined over L_v and that $v(L_v) = \mathbb{Z}$. We claim that the reduction morphism

$$E_{[\mathfrak{b}]}(L_v)[f^n] \to (E_{[\mathfrak{b}]}(L_v)/E_{[\mathfrak{b}],1}(L_v))[f^n] \tag{4.2}$$

is an isomorphism of $\mathbb{O}$-modules. This morphism of $\mathbb{O}$-modules is injective by [Silverman 1986, VII.3.4] or Lemma 2.15 and since $E_{[\mathfrak{b}]}$ has good reduction modulo v and $v(f) = 0$, both sides have the same cardinality f^{2n} [Silverman 1986, III.6.4(b)], which proves the claim.

Now consider the point $\mathfrak{b}P \in E_{[\mathfrak{b}]}(L_v)$. Since the lemma is already proved for invertible ideals, we know that $(\mathfrak{b}P + E_{[\mathfrak{b}],1}(L_v))$ is γ-torsion for every $\gamma \in \mathfrak{c}$. As (4.2) is an isomorphism of $\mathbb{O}$-modules, this implies that there is a point $Q \in E_{[\mathfrak{b}]}(L_v)[\mathfrak{c}]$ such that $\mathfrak{b}P \equiv Q$ modulo $E_{[\mathfrak{b}],1}(L_v)$. In particular, by Lemma 2.13 (or also Proposition 2.8 if we remove some more valuations from S), $\mathfrak{c}\mathfrak{b}P \equiv \mathfrak{c}Q$ modulo $E_{[\mathfrak{b}\mathfrak{c}],1}(L_v)$ and $\mathfrak{c}Q = O$ on $E_{[\mathfrak{b}\mathfrak{c}]}$. □

It follows that Theorem 3.21 holds for all ideals $\mathfrak{a}$ of $\mathbb{O}$.

Next, we do inclusion-exclusion in general. Let $\mu(\mathfrak{a},\mathfrak{b})$ be defined recursively for $\mathfrak{b}\mid\mathfrak{a}$ by

$$\mu(\mathfrak{a},\mathfrak{a})=1 \quad\text{and}\quad \sum_{\mathfrak{c}\mid\mathfrak{b}\mid\mathfrak{a}}\mu(\mathfrak{a},\mathfrak{b})=0 \quad(\text{for all } \mathfrak{c}\mid\mathfrak{a} \text{ with } \mathfrak{c}\neq\mathfrak{a}).$$

Previously, $\mu(\mathfrak{a},\mathfrak{b})$ depended only on $\mathfrak{a}/\mathfrak{b}$ and we denoted it by $\mu(\mathfrak{a}/\mathfrak{b})$.

The inclusion-exclusion principle, Lemma 3.23 and Theorem 3.21 give

$$\log\|D_{\mathfrak{a}}\| = \widehat{h}(P)\sum_{\mathfrak{b}\mid\mathfrak{a}}\mu(\mathfrak{a},\mathfrak{b})\,\|\mathfrak{b}\|^2 + \sum_{\mathfrak{b}\mid\mathfrak{a}}O(\log\|\mathfrak{a}\|\,(\log\log\|\mathfrak{a}\|)^4).$$

The set of ideals of $\mathcal{O}$ is the direct sum of the sets of ideals of the localizations of $\mathcal{O}$ at its primes. Therefore, the Möbius function of the ideals of $\mathcal{O}$ is the product of the Möbius functions of the localizations at the primes of $\mathcal{O}$.

Lemma 4.3. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ and $I\subset\mathcal{O}_{\mathfrak{p}}$ a nontrivial invertible ideal of the localization. Then there is a unique ideal $J_0\mid I$ (which is not necessarily invertible) such that $J_0\neq I$ and such that for every ideal $J\mid I$ with $J\neq I$, we have $J\mid J_0$. Moreover, the norm of this ideal is $N(I)/N(\mathfrak{p})$.*

Note that in terms of the Möbius functions, we have $\mu(I,J_0)=-1$ and $\mu(I,J)=0$ for all $J\neq I, J_0$.

Proof. It is clear that any two ideals as in the lemma are equal, so we only need to prove the existence. If $\mathfrak{p}$ is invertible, then the statement holds with $J_0=I/\mathfrak{p}$.

So suppose that $\mathfrak{p}$ is singular and let p be the rational prime with $\mathfrak{p}\mid p$. Let n be such that $\mathcal{O}=\mathbb{Z}+n\mathcal{O}_K$ and set $\mathcal{O}'=\mathbb{Z}+(n/p)\,\mathcal{O}_K$. Let R and R' be the localizations of $\mathcal{O}$ and $\mathcal{O}'$ at the $\mathcal{O}$-ideal $\mathfrak{p}$. As I is invertible, it is principal, say $I=\alpha R$. Let $J_0=\alpha R'$. We need to show that every R-ideal J that strictly contains I contains J_0.

If we allow fractional ideals, then without loss of generality, we may assume $\alpha=1$, so $I=R$ and $J_0=R'$. Let $\omega\in R'$ be such that $R'=\mathbb{Z}_{(p)}+\omega\mathbb{Z}_{(p)}$ and let $T, N\in\mathbb{Z}_{(p)}$ be such that $\omega^2-T\omega+N=0$. We need to prove $\omega\in J$. Take any element γ of $J\setminus R$. We have $\gamma=a+b\omega$ with $a,b\in\mathbb{Q}$. After multiplication by a power of p, we may assume $\gamma\in(1/p)R\setminus R$, so pa and b are both in $\mathbb{Z}_{(p)}$, but not both in $p\mathbb{Z}_{(p)}$. If $a\in\mathbb{Z}_{(p)}$, then $b\notin p\mathbb{Z}_{(p)}$, hence $\omega=b^{-1}(\gamma-a)\in J$. Otherwise, $\gamma p\omega=ap\omega+bp(T\omega-N)$ is in J and so is $p\omega$, hence $ap\omega$ is in J and $ap\in R^*$.

Finally, from the construction, we get $N(I)/N(J_0)=[R':R]=p=[R:pR']=N(\mathfrak{p})$. □

We conclude that if $\mathfrak{a}$ is invertible, then

$$\log\|D_{\mathfrak{a}}\| = \|\mathfrak{a}\|^2\,\widehat{h}(P)\prod_{\mathfrak{p}\mid\mathfrak{a}}(1-\|\mathfrak{p}\|^{-2}) + O(\|\mathfrak{a}\|^{\epsilon}), \tag{4.4}$$

which proves the Main Theorem.

The following example shows why we restrict to invertible ideals in our main result. Suppose that the index $[\mathbb{O}_K : \mathbb{O}]$ is a prime number p and that p is inert in $\mathbb{O}_K$. For any $\mathbb{O}$-ideal $\mathfrak{a}$, we have $\mathfrak{a}\mathbb{O}_K \supset \mathfrak{a} \supset p\mathfrak{a}\mathbb{O}_K$. If $\mathfrak{a}$ is $\mathfrak{p}$-primary, then $\mathfrak{a}\mathbb{O}_K = p^n\mathbb{O}_K$ for some n. On the other hand, any group $\mathfrak{a}$ which is strictly between $p^n\mathbb{O}_K$ and $p^{n+1}\mathbb{O}_K$, is an $\mathbb{O}$-module and there are $p+1$ such groups. We find

$$\mu(p^n\mathbb{O}_K, \mathfrak{a}) = \begin{cases} 1 & \text{if } \mathfrak{a} = p^n\mathbb{O}_K, \\ -1 & \text{if } \mathfrak{a} \text{ is strictly between } p^{n-1}\mathbb{O}_K \text{ and } p^n\mathbb{O}_K, \\ p & \text{if } \mathfrak{a} = p^{n-1}\mathbb{O}_K, \\ 0 & \text{otherwise.} \end{cases}$$

The inclusion-exclusion principle now gives

$$\begin{aligned} \log \|D_{p^{n-1}\mathbb{O}_K}\| &= \widehat{h}(P)(p^{2n-1} - (p+1)p^{2n-2} + pp^{2n-3}) + O(n\log(n)^4) \\ &= O(n\log(n)^4). \end{aligned}$$

Only the error term remains, so we cannot conclude from this that there exists a primitive divisor. On the other hand, the size of the error term does leave some space for primitive divisors, so other methods are needed to give a result on primitive divisors of $B_{\mathfrak{a}}$ for noninvertible ideals $\mathfrak{a}$.

Acknowledgments

The research for this paper was done as a Master's thesis at Universiteit Utrecht under supervision of Gunther Cornelissen, to whom the author expresses his gratitude. Thanks also to Peter Stevenhagen and the anonymous referees for many useful comments.

References

[Ayad 1992] M. Ayad, "Points S-entiers des courbes elliptiques", *Manuscripta Math.* **76**:3-4 (1992), 305–324. MR 93i:11064 Zbl 0773.14014

[Bang 1886] A. S. Bang, "Taltheoretiske undersøgelser", *Zeuthen Tidskr.* (5) **4** (1886), 70–80, 130–137. JFM 19.0168.02

[Bosch, Lütkebohmert and Raynaud 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Cheon and Hahn 1998] J. Cheon and S. Hahn, "Explicit valuations of division polynomials of an elliptic curve", *Manuscripta Math.* **97**:3 (1998), 319–328. MR 99i:11039 Zbl 0922.11048

[Cheon and Hahn 1999] J. Cheon and S. Hahn, "The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve", *Acta Arith.* **88**:3 (1999), 219–222. MR 2000i:11084 Zbl 0933.11029

[Chudnovsky and Chudnovsky 1986] D. V. Chudnovsky and G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization tests", *Adv. in Appl. Math.* **7**:4 (1986), 385–434. MR 88h:11094 Zbl 0614.10004

[Cornelissen and Zahidi 2007] G. Cornelissen and K. Zahidi, "Elliptic divisibility sequences and undecidable problems about rational points", *J. Reine Angew. Math.* **613** (2007), 1–33.

[Cox 1989] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, Wiley, New York, 1989. MR 90m:11016 Zbl 0701.11001

[David 1995] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) **62**, Soc. math. de France, Paris, 1995. MR 98f:11078 Zbl 0859.11048

[Durst 1952] L. K. Durst, "The apparition problem for equianharmonic divisibility sequences", *Proc. Nat. Acad. Sci. U. S. A.* **38** (1952), 330–333. MR 14,139b Zbl 0046.28905

[Hardy and Wright 1938] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1938. MR 0067125 Zbl 0020.29201 JFM 64.0093.03

[Satoh 2004] T. Satoh, "Generalized division polynomials", *Math. Scand.* **94**:2 (2004), 161–184. MR 2005b:11078 Zbl 1064.11044

[Shimura 1998] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series **46**, Princeton University Press, Princeton, NJ, 1998. MR 99e:11076 Zbl 0908.11023

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1988] J. H. Silverman, "Wieferich's criterion and the *abc*-conjecture", *J. Number Theory* **30**:2 (1988), 226–237. MR 89m:11027 Zbl 0654.10019

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Vélu 1971] J. Vélu, "Isogénies entre courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A* **273** (1971), 238–241. MR 45 #3414 Zbl 0225.14014

[Ward 1948] M. Ward, "Memoir on elliptic divisibility sequences", *Amer. J. Math.* **70** (1948), 31–74. MR 9,332j Zbl 0035.03702

[Ward 1950] M. Ward, "Arithmetical properties of polynomials associated with the lemniscate elliptic functions", *Proc. Nat. Acad. Sci. U. S. A.* **36** (1950), 359–362. MR 12,159h Zbl 0041.36804

[Washington 2003] L. C. Washington, *Elliptic curves: number theory and cryptography*, Chapman & Hall/CRC, Boca Raton, FL, 2003. MR 2004e:11061 Zbl 1034.11037

[Zsigmondy 1892] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR 1546236 JFM 24.0176.02

Communicated by Bjorn Poonen
Received 2007-07-30 Revised 2007-11-12 Accepted 2007-12-25

streng@math.leidenuniv.nl
Mathematisch Instituut, Universiteit Leiden, Postbus 9512,
2300 RA Leiden, The Netherlands
http://www.math.leidenuniv.nl/~streng