now published as:

Marco Streng - Divsibility sequences for elliptic curves with complex multiplication, Algebra & Number Theory Vol. 2 (2008), No. 2, 183-208

http://dx.doi.org/10.2140/ant.2008.2.183

Elliptic Divisibility Sequences with Complex Multiplication

Marco Streng

Master's thesis, Universiteit Utrecht,
written under supervision of Gunther Cornelissen

June 3, 2006

Contents

Chapter I

Introduction

1 Elliptic divisibility sequences

Elliptic divisibility sequences are sequences of integers that appear as denominators of multiples of a point on an elliptic curve. More precisely, by an *elliptic divisibility sequence* we will mean a sequence as defined in the next paragraph.

We assume the reader is familiar with the basic theory of elliptic curves, as in [Sil86]. Let E/L be an elliptic curve, defined over a number field L and given by a general Weierstrass equation

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

with coefficients in the ring of integers $\mathcal{O}_L$. Fix a rational point P of infinite order in $E(L)$. Then define the sequence of integral L-ideals $B_1, B_2, B_3, \ldots$ by the equation

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right),$$

where the fractions are in lowest terms. Examples are in Table 3 on page 36 and Table 4 on page 37.

In the literature, the term elliptic divisibility sequence is used both for sequences of this form and for a related type of sequence which was studied extensively by Morgan Ward (for example [War48]). We will consider only the type of sequence that we have just defined.

If the elliptic curve has *complex multiplication*, then we may multiply points with elements of the CM-ring and it is natural to also look at the denominators of points αP, where α runs through that ring. This allows us to interpolate elliptic divisibility sequences to sequences indexed by the CM-ring. Such an interpolation for the sequences that were studied by Ward was mentioned for example by Chudnovsky and Chudnovsky in [CC86]. The special case of elliptic curves with complex multiplication by $\sqrt{-1}$ (lemniscate elliptic curves) was studied by Ward ([War50]) and the case of elliptic curves with complex multiplication by a third root of unity (equianharmonic elliptic curves) was studied by Durst ([Dur52]).

Our main goal is to generalize standard results for elliptic divisibility sequences to CM-indexed sequences. In order to do this, we will first transfer

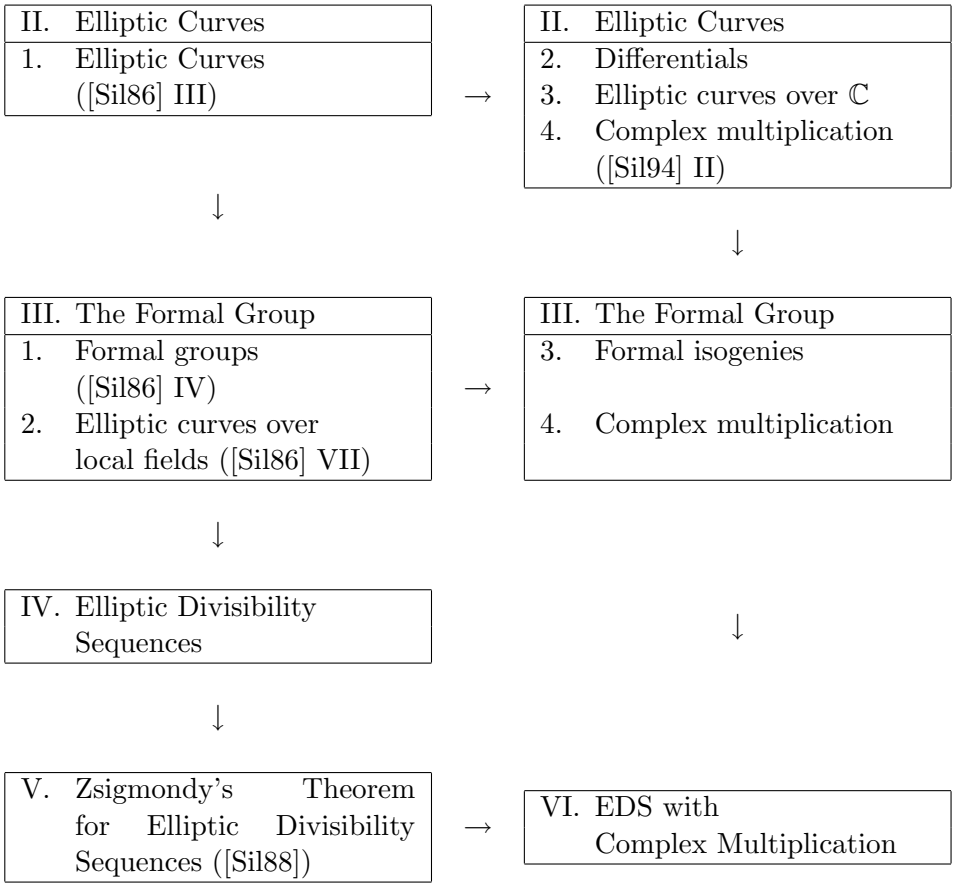


Table 1: The dependence between the chapters

classical divisibility results to more general morphisms of formal groups.

The result that we are most interested in is the result that almost every term in an elliptic divisibility sequence has a *primitive divisor* (i.e. a prime divisor that does not occur earlier in the sequence). The proof of this result for $(B_n)_{n\in\mathbb{N}}$ in [Sil88] fails for CM-indexed sequences and we will have to use the inclusion-exclusion principle and an estimate involving elliptic logarithms to fix this.

We also need to interpolate the indexing set further to the set of ideals of the CM-ring. The values of the sequence will then correspond to denominators of points on the conjugates of E over the Hilbert class field of the CM-ring.

Our method will also result in asymptotic bounds for the primitive part of $\mathbb{N}$-indexed elliptic divisibility sequences that are sharper than the bounds in the original proof.

2 Overview of the text

In Chapter II, we start with the definition of elliptic curves. Then we give a short analytic introduction to complex multiplication.

A very useful tool that we will use is the formal group of an elliptic curve,

which we study in Chapter III. The first two sections of that chapter contain only results that are also in Chapters IV and VII of [Sil86]. However, we will use slightly different definitions, because we will work with the given Weierstrass equation, instead of one that is minimal for the concerning valuation.

Then in the third section of Chapter III, we will associate formal group homomorphisms to isogenies. The fourth section applies the theory of formal groups to complex multiplication. The results of these last two sections will not be needed until we make our generalization in Chapter VI.

Chapter IV contains the definition of elliptic divisibility sequences and some standard properties, such as the strong divisibility property $\gcd(B_n, B_m) = B_{\gcd(n,m)}$ and some formulas about the orders with which primes occur in the sequences. Then, in Chapter V, we present some results from Silverman's article [Sil88], including the proof that from a certain term on, every term has a primitive divisor.

Finally, in Chapter VI, we will show the definitions and results for elliptic divisibility sequences with complex multiplication which we will now summarize.

3 Preview of the definitions and results

Let $L \subset \mathbb{C}$ be a number field and E/L an elliptic curve, given by a general Weierstrass equation with coefficients in the ring of integers $\mathcal{O}_L$ of L. Suppose that E has complex multiplication by the ring of integers $\mathcal{O} = \mathcal{O}_K$ of $K \subset \mathbb{C}$ and let M be the composite $M = KL \subset \mathbb{C}$. If P is a non-torsion point in $E(L)$, then we define, for every $\alpha \in \mathcal{O} \setminus \{0\}$, the (coprime) integral M-ideals A_α, B_α by

$$x([\alpha]P) = \frac{A_\alpha}{B_\alpha^2}.$$

This defines an $\mathcal{O} \setminus \{0\}$-indexed sequence $(B_\alpha)_\alpha$, which we call an *elliptic divisibility sequence with complex multiplication*.

We will see that it is natural to interpolate this sequence to the set of non-zero ideals of $\mathcal{O}$ by setting

$$B_{\mathfrak{a}} = \langle B_\alpha : \alpha \in \mathfrak{a} \rangle$$

and that this interpolation satisfies the strong divisibility property

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

We define a primitive divisor of $B_{\mathfrak{a}}$ to be a prime of M that divides $B_{\mathfrak{a}}$, but does not divide $B_{\mathfrak{b}}$ for any $\mathfrak{b}|\mathfrak{a}$ different from $\mathfrak{a}$.

The rest of Chapter VI is devoted to the proof of the following four main results:

Lemma (2.2)**.** *For any valuation v of M and all non-zero integral $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$, if $v(B_{\mathfrak{a}}) > \frac{v(p)}{p-1}$, then*

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

For any M-ideal I, let $||I|| = (N_{M/\mathbb{Q}}(I))^{1/[M:\mathbb{Q}]}$. For example, if $I = (x)$, where $x \in K$, then $||x||$ is simply the unique archimedean absolute value on K. Then

Proposition (5.14)**.**

$$\log ||B_{\mathfrak{a}}|| = ||\mathfrak{a}||^2 \, \widehat{h}(P) \; + \; O\left(\log ||\mathfrak{a}|| (\log\log ||\mathfrak{a}||)^4\right).$$

Theorem (6.5)**.** *For all but finitely many $\mathcal{O}$-ideals $\mathfrak{a}$, the ideal $B_{\mathfrak{a}}$ has a primitive divisor.*

Corollary (6.6)**.** *For any pair of non-zero $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ such that $||\mathfrak{a}||$ is sufficiently large,*

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

In particular, for any pair of non-zero elements α, β such that $||\alpha||$ is sufficiently large,

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

As a nice bonus, we get the following result on the splitting behavior of primes that divide terms of $\mathbb{N}$-indexed elliptic divisibility sequences for curves with complex multiplication.

Corollary (6.7)**.** *Given a number field L, an elliptic curve E/L with integral coefficients and a non-torsion point $P \in E(L)$.*

Suppose that E has complex multiplication by the ring of integers $\mathcal{O}$ of a quadratic imaginary field K and that $[KL : L] = 2$. However, look only at the $\mathbb{N}$-indexed sequence $B_1, B_2, B_3, \ldots$.

Then for all but finitely many $n \in \mathbb{N}$, the following holds:
If

$$\begin{aligned} r &= \#\{p | n \text{ prime of } \mathbb{N} : p \text{ ramifies in } K/\mathbb{Q}\}, \\ s &= \#\{p | n \text{ prime of } \mathbb{N} : p \text{ splits in } K/\mathbb{Q}\}, \end{aligned}$$

then B_n has at least $r + s + 1$ primitive divisors of which at least s split in KL/L.

In particular, this shows the existence of lots of split primitive divisors in elliptic divisibility sequences over curves that have complex multiplication. It seems that there are also many inert primitive divisors, but we cannot prove this. In fact, there are conjectures by Cornelissen and Zahidi ([CZ05]) about the existence of inert primitive divisors that imply results that are related to Hilbert's Tenth Problem over $\mathbb{Q}$.

On the other hand, we also get sharper estimates for the primitive part of ($\mathbb{N}$-indexed) elliptic divisibility sequences. If we denote by D_n the primitive part of the elliptic divisibility sequence $B_1, B_2, B_3, \ldots$, then Silverman's method gives an estimate

$$\frac{\log N(D_n)}{[L : \mathbb{Q}]} \geq (2 - \zeta(2) - o(1)) \, \widehat{h}(P) \, n^2,$$

where $2 - \zeta(2) \approx 0.355$ and by $o(1)$, we mean something which converges to 0 if $n \to \infty$. If we apply the same methods that we needed in the CM-case, then we get the sharper estimate

Proposition (6.8)**.** *For all* $\epsilon > 0$*,*

$$\frac{\log N(D_n)}{[L:\mathbb{Q}]} = \widehat{h}(P)s_n n^2 + O(n^\epsilon),$$

where

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

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

Here by $O(f(n))$ we mean "something which, in absolute value, grows at most as fast as $f(n)$." More precisely,

- $a(n) \leq b(n) + O(f(n))$ if there is a constant C such that for large enough n, $a(n) - b(n) \leq Cf(n)$;
- $a(n) \geq b(n) + O(f(n))$ if there is a constant C such that for large enough n, $b(n) - a(n) \leq Cf(n)$;
- $a(n) = b(n) + O(f(n))$ if both of the above hold, i.e. if there is a constant C such that for large enough n, $|a(n) - b(n)| \leq Cf(n)$.

4 Acknowledgements

I would like to thank Gunther Cornelissen for his help, and for suggesting that I could generalize results for elliptic divisibility sequences as a way to understand how the proofs work, which eventually became the goal of this entire text.

Thanks also to the people at the University of East Anglia for their hospitality during an inspiring visit, especially Graham Everest.

Also thanks to Jan Stienstra for the idea to use integer valued polynomials for proving integrality of formal homomorphisms, which later turned out to work in exactly the case for which the other proof fails.

Finally, thank you Marina for not complaining when I gave mathematics more attention than you.

Chapter II

Elliptic Curves

1 Elliptic curves

Definition. An *elliptic curve* E over a field L is a smooth algebraic curve of genus 1, together with a base point $O \in E(L)$.

We summarize the most basic facts about elliptic curves here. For more information we refer to [Sil86]. Every elliptic curve E/L is isomorphic to a projective curve, given by a general Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where O corresponds to the point at infinity $(0 : 1 : 0)$ and all the coefficients $a_1, \ldots, a_6$ are in L. On the other hand, any smooth curve that is given by a general Weierstrass equation is an elliptic curve.

We will focus on elliptic curve that are defined over a number field $L \subset \mathbb{C}$. By making a linear change of coordinates $x' = u^2x$, $y' = u^3y$, we can make sure that the coefficients $a_1, \ldots, a_6$ are in the ring of integers $\mathcal{O}_L$ of L. All the elliptic curves in this text will come with a given Weierstrass equation with coefficients that are algebraic integers.

Definition. Let E and E' be elliptic curves. An *isogeny* $\phi : E \to E'$ is a homomorphism of curves that sends the base point of E to the base point of E'.

This defines the category of elliptic curves, where the maps are the isogenies. In particular, an isomorphism is an isogeny which has a two-sided inverse isogeny and an endomorphism of an elliptic curve E is an isogeny from E to E.

Elliptic curves are commutative algebraic groups with identity element O and every isogeny is automatically a homomorphism of groups ([Sil86] III.4.8). For any elliptic curve E, the set of endomorphisms of E forms a ring $\mathrm{End}(E)$ with pointwise addition and multiplication given by composition.

2 Invariant differentials

Let E be an elliptic curve. The space of *differentials on* E is the $\overline{K}(E)$-vector space Ω_E, generated by the symbols dx for $x \in \overline{K}(E)$ and subject to the

relations

$$\begin{array}{rrcll} i. & d(x+y) & = & dx+dy & \text{for all } x,y \in \overline{K}(E), \\ ii. & d(xy) & = & xdy+ydy & \text{for all } x,y \in \overline{K}(E), \\ iii. & d(a) & = & 0 & \text{for all } a \in \overline{K}. \end{array}$$

In other words, it is the universal $\overline{K}$-derivation of $\overline{K}(E)$ (see [Har77] II §8).

Proposition/Definition 2.1. *The space of differentials on E that are invariant under translation is exactly the vector space of holomorphic differentials. It is one-dimensional and generated by*

$$\omega = \frac{1}{2y + a_1 x + a_3} dx.$$

We call this space the space of invariant differentials and we call ω the invariant differential for the given Weierstrass equation.

Proof. The space of holomorphic differentials has dimension equal to the genus $g = 1$ by the Riemann-Roch theorem ([Sil86] II.5.5a) and it contains ω by [Sil86] III.1.5.

Clearly any translation-invariant differential is holomorphic. Conversely, [Sil86] III.5.1 shows that ω, and hence every holomorphic differential, is invariant under translation. □

Corollary 2.2. *Suppose that E and E' are elliptic curves with fixed Weierstrass equations. Let ω and ω' be their invariant differentials. For every isogeny $\phi : E \to E'$ there is a constant $a_\phi \in \overline{K}$ such that $\phi^*\omega' = a_\phi \omega$.*

Proof. The differential $\phi^*\omega'$ is invariant under translation. To see this, notice that if τ_Q is the translation-by-Q-map, then $\tau_Q^* \phi^* \omega' = \phi^* \tau_{\phi(Q)}^* \omega' = \phi^* \omega'$ and $\tau_{\phi(Q)}^* \omega' = \omega'$. The previous proposition shows that the space of translation invariant differentials is one-dimensional, so $\phi^*\omega'$ is a multiple of ω. □

3 Elliptic curves over $\mathbb{C}$

With a suitable linear change of coordinates, any elliptic curve over $\mathbb{C}$ may be described by a classical Weierstrass equation of the form

$$E : y^2 = 4x^3 - g_2 x - g_3. \tag{1}$$

Recall that for any complete lattice $\Lambda \subset \mathbb{C}$, the Weierstrass $\wp$-function, given by

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is a meromorphic function on $\mathbb{C}$. It is periodic with period Λ and has a double pole with residue 0 at each lattice point and no other poles. Let the *Eisenstein series of weight* $2k$ be given by

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}$$

and let $g_2 = 60G_4$ and $g_3 = 140G_6$. Then $(\wp(z), \wp'(z))$ satisfies equation (1), which defines an elliptic curve E_Λ.

On the other hand, for any elliptic curve E given by a classical Weierstrass equation, path integration of the invariant differential yields a lattice Λ such that $E = E_\Lambda$, together with an inverse of the map $z \mapsto (\wp(z), \wp'(z))$.

If the elliptic curve E corresponds to the lattice Λ, then the above constructions give an isomorphism of complex analytic groups

$$\begin{array}{rcl} \mathbb{C}/\Lambda & \cong & E \\ z & \mapsto & (\wp(z), \wp'(z)) \\ \displaystyle\int_O^P \omega & \mapsto & P. \end{array}$$

If Λ_i corresponds to E_i, then isogenies $E_1 \to E_2$ correspond to holomorphic group homomorphisms $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ that can only be of the form $z \mapsto \alpha z$ with $\alpha\Lambda_1 \subset \Lambda_2$. ([Sil86] VI.5.3). This correspondence gives an isomorphism of rings

$$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\},$$

from which we can deduce ([Sil86] VI.5.5) that either

1. $\mathrm{End}(E) = \mathbb{Z}$ or
2. $\mathrm{End}(E)$ is isomorphic to an order in a quadratic imaginary extension K of $\mathbb{Q}$.

In the last case, we say that E has *complex multiplication*.

4 Complex multiplication

We know that $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic extension of $\mathbb{Q}$. So let $\mathcal{O} \subset \mathbb{C}$ be such that $\mathrm{End}(E) \cong \mathcal{O}$ and let $K \subset \mathbb{C}$ be the field of fractions of $\mathcal{O}$. Throughout this text, we will restrict to the case where $\mathcal{O}$ is the ring of integers $\mathcal{O}_K$ of K, in other words, $\mathcal{O}$ is the *maximal* order in K. This makes the theory much simpler, especially when we do inclusion-exclusion in the final chapter.

Notice that if K is a quadratic extension, then there are two isomorphisms $\mathrm{End}(E) \cong \mathcal{O}$. We pick the one that comes from the correspondence of the previous section:

Proposition 4.1. *There is a unique isomorphism*

$$[\,\cdot\,] : \mathcal{O} \to \mathrm{End}(E),$$

with the property that for any invariant differential ω,

$$[\alpha]^*\omega = \alpha\omega.$$

It may be constructed using the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z\mapsto\alpha z} & \mathbb{C}/\Lambda \\ {\scriptstyle\sim}\downarrow{\scriptstyle f} & & {\scriptstyle f}\downarrow{\scriptstyle\sim} \\ E & \xrightarrow[[\alpha]]{} & E \end{array}$$

Proof. There are at most two alternatives for the isomorphism, because the only automorphisms of $\mathcal{O}$ are the identity and complex conjugation. So let $[\,\cdot\,]$ be defined by the diagram.

Recall that the space of invariant differentials on an elliptic curve is one-dimensional (see for example Corollary 2.2), so any two invariant differentials are scalar multiples of each other.

So let ω be any invariant differential, then $f^*\omega$ is a multiple of the invariant differential dz on $\mathbb{C}/\Lambda$. Say $f^*\omega = c dz$. Then

$$[\alpha]^*\omega = ((f^{-1})^* \circ \alpha^* \circ f^*)\omega = (f^{-1})^*(\alpha c dz) = \alpha\omega.$$

If $\mathcal{O}$ is quadratic imaginary, then the other alternative comes from complex conjugation on $\mathcal{O}$, so it will satisfy $[\alpha]^*\omega = \overline{\alpha}\omega \neq \alpha\omega$. □

Lemma 4.2 ([Sil94] II.2.2a.)**.** *For all $\alpha \in \mathcal{O}$ and all $\sigma \in \mathrm{Aut}(\mathbb{C})$,*

$$[\alpha]_E^\sigma = [\sigma(\alpha)]_{E^\sigma}$$

Corollary 4.3. *If E is defined over a number field L, then every endomorphism of E is defined over the composite KL.*

Proof. For any σ that fixes KL, Lemma 4.2 says that $[\alpha]^\sigma = [\alpha]$. □

Example 4.4. For any non-zero $a \in \mathbb{C}$, let E be the elliptic curve given by $y^2 = x^3 + ax$. This curve has discriminant $-64a^3$ and j-invariant 1728. Then E has complex multiplication by $\mathbb{Z}[i]$ via $[i](x, y) = (-x, iy)$.

Example 4.5. For $a_3, a_6 \in \mathbb{C}$ with $a_3^2+4a_6 \neq 0$, let E be the elliptic curve given by $y^2+a_3y = x^3+a_6$. This curve has discriminant $-27(a_3^2+4a_6)^2$ and j-invariant 0. Let $\zeta_3 = e^{2\pi i/3}$, then E has complex multiplication by $\mathbb{Z}[\zeta_3] \subset \mathbb{Q}[i\sqrt{3}]$ via $[\zeta_3](x, y) = (\zeta_3 x, y)$.

Example 4.6. For non-zero $a \in \mathbb{C}$, let E be the elliptic curve given by $y^2 = x^3 + 4ax^2 + 2a^2x$. This curve has discriminant 2^8a^6 and j-invariant 8000. Let $\alpha = i\sqrt{2}$, then E has complex multiplication by $\mathbb{Z}[\alpha]$ via

$$[\alpha](x, y) = \left(\frac{y^2}{\alpha^2x^2}, \frac{y(x^2 - 2a^2)}{\alpha^3x^2}\right).$$

Chapter III

The Formal Group

In this chapter, we will discuss the theory of formal groups of elliptic curves and elliptic curves over local fields. The first two sections are a summary of facts from [Sil86] Chapter IV and Paragraph VII.2. We will deviate from that source by defining everything in terms of a given Weierstrass equation, whereas [Sil86] states everything in terms of a minimal Weierstrass equation for the concerning local field.

This has as a consequence that we have slightly different definitions of the reduced curve $\widetilde{E}$, the groups $\widetilde{E}_{\mathrm{ns}}$ and $E_n(K)$ and of a point being singular modulo a prime. In particular, each of these notions will depend on the given Weierstrass equation, whereas in [Sil86] they depend only on the K-isomorphism class of the curve. The reason for our choice is that it makes all the tools from the theory of formal groups more directly applicable.

In the third section, we will resume studying formal groups and we will associate formal group homomorphisms to isogenies.

Formal groups become useful if we look at them in relation to local fields. Whenever we speak about a local field K, we will mean a local field of characteristic 0, where "local field" means complete with respect to a discrete valuation and with a finite residue field. The local fields of characteristic 0 are exactly the finite extensions of $\mathbb{Q}_p$ for primes $p \in \mathbb{Z}$. ([Neu92], II.5.2). We will always use the following notation when dealing with a local field K.

v	the discrete valuation on K. We assume that v is normalized, i.e. $v(K) = \mathbb{Z}$.
R	$= \{x \in K : v(x) \geq 0\}$, the ring of integers of K.
$\mathfrak{M}$	$= \{x \in K : v(x) > 0\}$, the maximal ideal of R.
k	$= R/\mathfrak{M}$, the residue field of R. This is a finite field.
p	the characteristic of k. In other words, the unique prime in $\mathbb{Z}$ with $v(p) > 0$.

The prime p is the unique integer such that K extends $\mathbb{Q}_p$. The ramification index of this extension is $v(p)$.

1 Formal groups

We will now discuss formal groups. This section is basically a summary of facts from [Sil86], Chapter IV. It may function as a quick introduction into formal groups or as a reminder or a reference source. We will refer to Silverman's book for most of the proofs.

1.1 Formal groups

Let A be a commutative ring.

Definition. A *(commutative) formal group $\mathcal{F}$ defined over A* is a formal power series $F(X,Y) \in A[[X,Y]]$ satisfying:

i. $F(X,Y) = X + Y +$ (terms of total degree at least 2). We will abbreviate this as $F(X,Y) = X + Y +$h.o.t.

ii. $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (associativity),

iii. $F(X,Y) = F(Y,X)$ (commutativity),

iv. $F(X,0) = X$ and $F(0,Y) = Y$ (unit),

v. There is a unique power series $i(T) \in A[[T]]$ such that $F(T,i(T)) = 0$ (inverse).

Remark 1.1. In fact, i. and ii. imply iv. and v. ([Sil86], exercise 4.1). If A has no (additive) torsion elements which are (multiplicative) nilpotents, then i. and ii. also imply iii. ([Sil86], exercise 4.2).

Definition. Let $(\mathcal{F},F)$ and $(\mathcal{G},G)$ be formal groups defined over a ring A. A *homomorphism from $\mathcal{F}$ to $\mathcal{G}$* is a power series (with no constant term) $f(T) \in A[[T]]$ satisfying

$$f(F(X,Y)) = G(f(X),g(Y)).$$

This defines the category of formal groups over A.

1.2 The formal group of an elliptic curve

The formal groups that we are interested in are those that arise from elliptic curves. So suppose that E is an elliptic curve, given by a general Weierstrass equation

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

If we look at the change of coordinates

$$z = -\frac{x}{y}\,, \quad w = -\frac{1}{y}\,, \quad \left(x = \frac{z}{w}\,, \quad y = -\frac{1}{w}\right),$$

then O becomes the point $(z,w) = (0,0)$ and z is a uniformizer at that point. Moreover, the Weierstrass equation becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 \quad (= f(z,w)). \tag{2}$$

If we substitute this equation into itself recursively, then we find:

Proposition 1.2. *There is a unique power series $w(T) \in \mathbb{Z}[a_1, \ldots, a_6][[T]]$ such that $(T, w(T))$ satisfies equation (2). It is of the form $w(T) = T^3 +$ (higher order).*

Moreover, if K is a local field with maximal ideal $\mathfrak{M}$ and $z \in \mathfrak{M}$, then $w(z) \in \mathfrak{M}^3$ is the unique element of $\mathfrak{M}$ such that $(z, w(z))$ satisfies equation (2).

Proof. Both statements follow from the following general version of Hensel's Lemma. We will apply the lemma with $F(w) = f(T, w) - w$, $a = 0$, $\alpha = -1$ and $n = 3$.

Lemma 1.3 (Hensel's Lemma, [Sil86] IV.1.2)**.** *Let B be a ring which is complete with respect to some ideal $I \subset B$, and let $F(w) \in B[w]$ be a polynomial. Suppose that $a \in B$ satisfies (for some integer $n \geq 1$)*

$$F(a) \in I^n \quad \textit{and} \quad F'(a) \in B^*.$$

Then for any $\alpha \in B$ satisfying $\alpha \equiv F'(a) \pmod{I}$, the sequence

$$w_0 = a \quad w_{m+1} = w_m - F(w_m)/\alpha$$

converges to an element $b \in B$ satisfying

$$F(b) = 0 \quad \textit{and} \quad b \equiv a \pmod{I^n}.$$

If B is an integral domain, then these conditions determine b uniquely.

If we apply Hensel's lemma with $B = \mathbb{Z}[a_1, \ldots, a_6][[T]]$, $I = (T)$, then we get existence and uniqueness of $w(T)$. The fact that $w(T) = T^3 + \text{h.o.t.}$ follows directly from equation (2). If we apply Hensel's lemma with $B = R$ (the local ring of K) and $I = \mathfrak{M}$, then we find that there is a unique $w \in \mathfrak{M}$ such that (z, w) satisfies (2), but $w(z)$ converges so $(z, w(z))$ also satisfies (2). □

[Sil86] IV §1 computes that substitution of formal points $P = (\frac{X}{w(X)}, -\frac{1}{w(X)})$ and $Q = (\frac{Y}{w(Y)}, -\frac{1}{w(Y)})$ in the addition formula yields power series $F_{\widehat{E}}(X, Y)$ for $z(P + Q)$ and $i_{\widehat{E}}(X)$ for $z(-P)$. They are of the form

$$\begin{aligned} F_{\widehat{E}}(X, Y) &= X + Y + \text{h.o.t.} \in \mathbb{Z}[a_1, \ldots, a_6][[X, Y]] \quad \text{and} \\ i_{\widehat{E}}(X) &= -X + \text{h.o.t.} \in \mathbb{Z}[a_1, \ldots, a_6][[X, Y]]. \end{aligned}$$

Lemma 1.4. *The power series $F_{\widehat{E}}(X, Y)$ truly represents addition on E in the following sense: If $Z = F_{\widehat{E}}(X, Y)$, then*

$$\left(\frac{Z}{w(Z)}, -\frac{1}{w(Z)}\right) = \left(\frac{X}{w(X)}, -\frac{1}{w(X)}\right) + \left(\frac{Y}{w(Y)}, -\frac{1}{w(Y)}\right),$$

as an identity of formal power series in X and Y, where "+" means addition using the group law on the elliptic curve.

Proof. In the z-coordinate, this is true by definition of $F_{\widehat{E}}$. Also, both sides of the equation satisfy the Weierstrass equation for E, so if we make the appropriate change of coordinates, then both sides satisfy equation (2). But then they are equal by Hensel's Lemma 1.3 applied to the ideal $I = (X, Y)$ of the ring $B = \mathbb{Z}[a_1, \ldots, a_n][[X, Y]]$. □

Corollary 1.5. *The power series $F_{\widehat{E}}$ defines a formal group $\widehat{E}/\mathbb{Z}[a_1, \ldots, a_6]$ for which the inverse is given by $i_{\widehat{E}}(T)$.*

Proof. The above lemma shows that the formal group axioms can be deduced from the corresponding properties for E. □

1.3 Groups associated to formal groups

Let K be a local field and let $\mathcal{F}$ be a formal group over the local ring R of K. As K is complete, every power series converges on the maximal ideal $\mathfrak{M}$, so we can view the formal group law $F(X, Y)$ as an actual group law as follows.

Definition. The *group associated to $\mathcal{F}/R$*, denoted $\mathcal{F}(\mathfrak{M})$, is the set $\mathfrak{M}$ with the group operations given by

$$x \oplus_{\mathcal{F}} y = F(x, y) \quad \text{and} \quad \ominus_{\mathcal{F}} x = i(x).$$

For integers $n \geq 1$, we also define the subgroups $\mathcal{F}(\mathfrak{M}^n)$ consisting of the sets $\mathfrak{M}^n$.

The group laws are well-defined and the formal group axioms imply that $\mathcal{F}(\mathfrak{M})$ is a group and $\mathcal{F}(\mathfrak{M}^n)$ is a subgroup. Also, every formal group homomorphism becomes an actual group homomorphism.

We will see in the next section that for a local field K, the change of coordinates $z = -x/y, w = -1/y$ yields an isomorphism between $\widehat{E}(\mathfrak{M})$ and a subgroup of $E(K)$.

It is not hard to see that

Lemma 1.6. *For every $n \geq 1$, the identity map of sets*

$$\mathcal{F}(\mathfrak{M}^n)/\mathcal{F}(\mathfrak{M}^{n+1}) \to \mathfrak{M}^n/\mathfrak{M}^{n+1}$$

is an isomorphism of groups.

Proof. Given $x, y \in \mathfrak{M}^n$, $x \oplus_{\mathcal{F}} y = x + y + \text{h.o.t.} \equiv x + y \mod \mathfrak{M}^{2n}$, so the identity map is a bijective group homomorphism. □

We can say the following about torsion:

Lemma 1.7. *Every torsion element of $\mathcal{F}(\mathfrak{M})$ has order a power of p.*

Proof. Suppose that there is an element whose order is not a power of p. If we multiply by a power of p, then we find an element x whose order m is coprime to p.

The power series which represents formal multiplication by m (obtained by substituting $F(X, Y)$ in itself recursively) has coefficients in R and leading coefficient $m \in R^*$, so by [Sil86] IV.2.4 it has an inverse power series with coefficients in R. Therefore, it is injective, which contradicts the existence of the m-torsion element. □

1.4 Differentials and formal logarithms

Let $A((T))$ be the ring of formal Laurent series over A and $A[[T]]$ the ring of formal power series over A.

Definition. The space of *differentials on* $A((T))$ is the free $A((T))$-module generated by the symbol dT together with the map $d : A((T)) \to A((T))dT$, given by $df(T) = f'(T)dT$. In the same way, we define the space of *differentials on* $A[[T]]$.

One immediately checks the rules

$$\begin{array}{rrcll} i. & d(x+y) & = & dx+dy & \text{for all } x,y \in A((T)), \\ ii. & d(xy) & = & xdy+ydy & \text{for all } x,y \in A((T)), \\ iii. & d(a) & = & 0 & \text{for all } a \in A. \end{array}$$

Moreover, we have the chain rule for power series:

Lemma 1.8. *Given* $f(T), g(T) \in A[[T]]dT$ *with* $g(0) = 0$*, we have*

$$d(f(g(T))) = f'(g(T))dg(T).$$

Proof. We need to prove $\frac{d}{dT}f(g(T)) = f'(g(T))g'(T)$. For $f(T) = T^n$ with $n \geq 0$, this is easy to see from the Leibniz rule $(ii.)$. By linearity $(i.)$, it holds for all polynomials $f(T)$. Now suppose that $f(T)$ is a power series. Let $h(T)$ be a polynomial that is congruent to $f(T)$ modulo T^{n+1}. Then $h'(T)$ is $f'(T)$ modulo T^n, so $\frac{d}{dT}f(g(T)) = f'(g(T))g'(T)$ holds modulo T^n. As n is arbitrary, we now have the desired result. □

Let $(\mathcal{F}, F)$ be a formal group over A.

Definition. We say that a differential $\omega = P(T)dT \in A[[T]]$ is *invariant* for $\mathcal{F}$ if

$$\omega(F(T,S)) = \omega(T),$$

where $\omega(F(T,S)) = P(F(T,S))dF(T,S) = P(F(T,S))\frac{\partial F}{\partial X}(T,S)dT$. We say that ω is *normalized* if furthermore, $P(0) = 1$.

Lemma 1.9. *For every formal group* $\mathcal{F}/A$*, there is a unique normalized invariant differential* $\omega_{\mathcal{F}}$ *in* $A[[T]]dT$*.*

Proof. [Sil86] IV.4.2. □

Definition. The *formal logarithm* $\log_{\mathcal{F}}(T)$ is the unique primitive of the invariant differential such that $\log_{\mathcal{F}}(0) = 0$.

In other words, if $\omega_{\mathcal{F}}(T) = P(T)dT$, then $\log'_{\mathcal{F}}(T) = P(T)$ and $\log_{\widehat{E}}(0) = 0$.

Definition. The *formal exponentiation* homomorphism $\exp_{\mathcal{F}}(T)$ is the unique inverse of $\log_{\mathcal{F}}(T)$ (in the sense that $\exp(\log(T)) = \log(\exp(T)) = T$, existence and uniqueness: [Sil86] IV.2.4).

Let K be a local field of characteristic 0.

Theorem 1.10. *The formal logarithm converges on $\mathfrak{M}$ to an element of K. Moreover, if $r > v(p)/(p-1)$ is an integer, then the formal exponentiation converges on $\mathfrak{M}^r$ and we have an isomorphism*

$$\begin{aligned} \mathcal{F}(\mathfrak{M}^r) &\cong \mathfrak{M}^r \\ z &\mapsto \log_{\mathcal{F}}(z) \\ \exp_{\mathcal{F}}(u) &\leftarrow\!\shortmid u. \end{aligned}$$

Proof. Everything is clear except convergence, which is proven in [Sil86] IV.6.4. □

Corollary 1.11. *The isomorphisms in the above theorem preserve the valuation.*

Proof. This is clear from the theorem, because the map also induces an isomorphism for all integers $r' > r$. □

2 Elliptic curves over local fields

In this section, we repeat [Sil86] VII §2 with the difference that we work with any Weierstrass equation with integral coefficients, not just a minimal one. We also solve exercises 7.4 and 7.6 of the same chapter.

Throughout the section, K will be a local field and $v, R, \mathfrak{M}, k$ and p are as on page 11. Furthermore, E will be an elliptic curve, defined over K, given by a (not necessarily minimal) Weierstrass equation with coefficients in R.

2.1 Reduction modulo $\mathfrak{M}$

If we reduce the coefficients of a Weierstrass equation modulo $\mathfrak{M}$, then we get a Weierstrass equation for a curve $\widetilde{E}$ over k.

We can write every point $P \in \mathbb{P}^n(K)$ as $(x_0 : \cdots : x_n)$ with $x_i \in R$ for all i and $x_i \in R^*$ for at least one i. If we then reduce the coordinates modulo $\mathfrak{M}$, we get a (well-defined) point $\widetilde{P} \in \mathbb{P}^n(k)$. In particular, if $P \in E(K)$, then $\widetilde{P}$ will be in $\widetilde{E}(k)$.

Let $\widetilde{E}_{\mathrm{ns}}(k)$ be the group of nonsingular points of $\widetilde{E}(k)$. Reduction sends straight lines to straight lines, so it preserves the chord-and-tangent addition. Hence the set $E_0(K)$ of points in $E(K)$ that are non-singular modulo v is a subgroup of $E(K)$ and the reduction map is a homomorphism $E_0(K) \to E_{\mathrm{ns}}(k)$. Denote the kernel of the reduction homomorphism by $E_1(K)$, i.e.

$$E_1(K) = \{P \in E(K) : \widetilde{P} = \widetilde{O}\}.$$

2.2 The formal group

Let us first show why the formal group is useful when studying elliptic curves. Let x, y be the coordinate functions of E. Let $z = -x/y \in K(E)$, then

Lemma 2.1. *The map*

$$\begin{array}{rcl} E_1(K) & \longrightarrow & \widehat{E}(\mathfrak{M}) \\ P & \mapsto & z(P) \end{array}$$

is an isomorphism of groups which satisfies $v(z) = -\frac{1}{2}v(x)$. *Its inverse is given by* $z \mapsto (\frac{z}{w(z)}, -\frac{1}{w(z)})$

Proof. First we look at the promised inverse. Proposition 1.2 shows that $w(z) \in K$, so we have a well-defined map $\phi : \widehat{E}(\mathfrak{M}) \to \mathbb{P}^2(K)$, given by $\phi : z \mapsto (z : -1 : w(z))$. Its image lies in $E(K)$, because $(z, w(z))$ satisfies (2). Also, as $w(z) \in \mathfrak{M}$, $\phi(z)$ is congruent to the point at infinity modulo $\mathfrak{M}$, so the image of ϕ lies inside $E_1(K)$.

Now we need to show that it is a homomorphism. So let $z_1, z_2 \in \widetilde{E}(\mathfrak{M})$. Then by definition of the group law on $\widehat{E}$, we have $z_1 \oplus z_2 = -\frac{x}{y}(\phi(z_1)+\phi(z_2))$, so $(z_1 \oplus z_2, -\frac{1}{y}(\phi(z_1) + \phi(z_2)))$ satisfies equation (2). Hence by uniqueness in Proposition 1.2, we also have $w(z_1 \oplus z_2) = -\frac{1}{y}(\phi(z_1) + \phi(z_2))$. In other words, we have $\phi(z_1 \oplus z_2) = \phi(z_1) + \phi(z_2)$, so ϕ is a group homomorphism. Its kernel is clearly 0 by definition.

Next, we show surjectivity, so let $(x, y) \in E_1(K)$ be any element. If one of $v(x), v(y)$ is ≥ 0, then the fact that they satisfy $y^2 + \cdots = x^3 + \cdots$ implies that both are ≥ 0, so $(x : y : 1)$ reduces to a point in the affine plane, contradicting $(x, y) \in E_1(K)$. Therefore, $v(x) < 0$ and $v(y) < 0$. Now the fact that they satisfy $y^2 + \cdots = x^3 + \cdots$ tells us that $3v(x) = 2v(y)$, so $v(z) = v(x) - v(y) = -\frac{1}{2}v(x) < 0$. In particular, $z \in \mathfrak{M}$. Now $(z, -1/y)$ satisfies equation (2) and $v(-1/y) = -v(y) > 0$, so again by uniqueness of $w(z)$, we find $w(z) = -1/y$, so $\phi(z) = (x, y)$, which proves surjectivity of ϕ. □

Corollary 2.2. *If* $P \in E_1(K)$ *is a torsion point, then the order of* P *is a power of* p.

Proof. Lemma 1.7 says that every torsion element of $\widehat{E}(\mathfrak{M})$ has order a power of p. □

2.3 The groups $E_n(K)$

For $n \geq 1$, define subsets $E_n(K) \subset E(K)$ by

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

For $n = 1$, this definition coincides with the other definition of $E_1(K)$. Indeed, if (x, y) is congruent to O, then we have seen in the proof of the above lemma that $3v(x) = 2v(y) < 0$, so $v(x) \leq -2$. If, on the other hand, $v(x) \leq -2$, then (x, y) is congruent to a, hence the, point at infinity.

Lemma 2.3 ([Sil86], exercise 7.4)**.** *The sets* $E_n(K)$ *are subgroups of* $E(K)$ *and for* $n \geq 1$,

$$E_n(K)/E_{n+1}(K) \cong k^+,$$

where k^+ *is the additive group of the residue field* k.

Proof. First of all, via the isomorphism of Lemma 2.1, the set $E_n(K)$ corresponds to the subgroup $\widehat{E}(\mathfrak{M}^n)$ of $\widehat{E}(\mathfrak{M})$, so it is a subgroup of $E(K)$. Then Lemma 1.6 says that

$$\widehat{E}(\mathfrak{M}^n)/\widehat{E}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1} \cong k^+,$$

where the second isomorphism is a basic fact about discrete valuations ([Neu92] II.3.9). □

2.4 The v-adic topology on a variety

We will now define the v-adic topology on the set of K-valued points of E in order to prove finiteness of the index $[E(K) : E_0(K)]$. We will only use this to remark that every prime divides some term of the elliptic divisibility sequence.

Let K be a field, together with a valuation $|\cdot| = |\cdot|_v$ (archimedean or non-archimedean). By the *v-adic topology* on $\mathbb{A}^n(K)$, we mean the product topology on K^n of the v-adic topology on K. It is easy to see that this is exactly the topology induced by the v-adic maximum norm on the vector space K^n. Denote this norm by $||\cdot||$.

Lemma 2.4. *Let $\mathbb{A}^n(K)$ and $\mathbb{A}^m(K)$ have the v-adic topology. Then every rational function f in n variables is a continuous map from D to $\mathbb{A}^m(K)$, where $D \subset \mathbb{A}^n(K)$ is the set of points where f does not have a pole. Furthermore, the set D is open.*

Proof. We prove this for $m = 1$. Then it holds for all m, because $\mathbb{A}^m(K)$ has the product topology.

The assertion clearly holds for linear maps. Suppose that f and g are continuous at $x \in \mathbb{A}^n(K)$. For any $\epsilon > 0$, if $||x' - x||$ is small enough such that $|f(x') - f(x)|, |g(x') - g(x)| < \epsilon$, then

$$\begin{aligned} |(f \cdot g)(x') - (f \cdot g)(x)| &= |f(x')g(x') - f(x')g(x) + f(x')g(x) - f(x)g(x)| \\ &\leq |f(x')||g(x') - g(x)| + |g(x)||f(x') - f(x)| \\ &< (|f(x')| + |g(x)|)\epsilon \\ &< (|f(x)| + |g(x)| + \epsilon)\epsilon. \end{aligned}$$

Hence $f \cdot g$ is continuous. Therefore, all polynomials are continuous. In particular the domain D of any rational function is open.

Now all we need to show is that $1/f$ is continuous outside the zeros of f. For any $\epsilon > 0$, if $||x' - x||$ is small enough such that $|f(x') - f(x)| < \min\{\epsilon, \frac{1}{2}|f(x)|\}$, then

$$\begin{aligned} |1/f(x') - 1/f(x)| &= \left|\frac{f(x) - f(x')}{f(x')f(x)}\right| \\ &< \frac{1}{|f(x)|}\frac{1}{|f(x')|}\epsilon \\ &< \frac{1}{|f(x)|^2}2\epsilon. \end{aligned}$$

Hence $1/f$ is continuous at x. □

By the *v-adic topology on* $\mathbb{P}^n(K)$, we mean the quotient topology from $\mathbb{A}^{n+1}(K) \setminus \{0\}$ for the equivalence relation defining $\mathbb{P}^n$, where $\mathbb{A}^{n+1}(K)$ has the v-adic topology. The following lemma shows that this is also the topology that one obtains when $\mathbb{P}^n(K)$ is constructed by glueing $\mathbb{A}^n(K)$'s.

Lemma 2.5. *Let $\mathbb{P}^n(K)$ have the v-adic topology. Every algebraic affine subset $\mathbb{A}^n(K)$ of $\mathbb{P}^n(K)$ is open and the subspace topology on $\mathbb{A}^n(K)$ is equal to the v-adic topology.*

Proof. Choose the coordinates in such a way that $\mathbb{A}^n(K) = \{(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K) : x_0 \neq 0\}$. This is allowed because the previous lemma says that birational maps are homeomorphisms. Let $\pi : \mathbb{A}^{n+1}(K) \setminus \{0\} \to \mathbb{P}^n$ denote the quotient map. Then $\pi^{-1}(\mathbb{A}^n(K)) = x_0^{-1}(K \setminus \{0\})$ is open in $\mathbb{A}^{n+1}(K) \setminus \{0\}$, so $\mathbb{A}^n(K)$ is open in $\mathbb{P}^n(K)$.

Next, suppose that $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ and $\epsilon > 0$. Then

$$\pi^{-1}(B(x, \epsilon)) = \{(y_0, y_1, \ldots, y_n) : \forall_{i \neq 0} |\frac{y_i}{y_0} - x_i| < \epsilon\}.$$

The rational maps $\frac{y_i}{y_0} - x_i$ are continuous and the set $\{z : |z| < \epsilon\}$ is open, so $B(x, \epsilon)$ is open in the topology on $\mathbb{P}^n(K)$.

Finally, suppose that $U \subset \mathbb{A}^{n+1}$ is open in the topology on $\mathbb{P}^n(K)$. Then $\pi^{-1}(U)$ is open, so for any $y = (y_0, y_1, \ldots, y_n) \in \mathbb{A}^{n+1}(K) \setminus \{0\}$ with $(y_0 : y_1 : \cdots : y_n) \in U$, there is an $\epsilon > 0$ such that $B(y, \epsilon) \subset \pi^{-1}(U)$, hence $\pi(B(y, \epsilon)) \subset U$. But then the ball $B((\frac{y_1}{y_0}, \ldots, \frac{y_n}{y_0}), \frac{\epsilon}{y_0})$ in $\mathbb{A}^n(K)$ is a subset of $\pi(B(y, \epsilon)) \subset U$. □

Lemma 2.6. *Let $\mathbb{P}^n(K)$ and $\mathbb{P}^m(K)$ have the v-adic topology. Then every rational function $f : \mathbb{P}^n(K) \to \mathbb{P}^m(K)$ is a continuous map.*

Proof. Given $x \in \mathbb{P}^n(K)$, let $\mathbb{A}^n(K) \ni x$ and $\mathbb{A}^m(K) \ni f(x)$ be affine algebraic subsets of $\mathbb{P}^n(K)$ and $\mathbb{P}^m(K)$. The previous two lemmas now show that f is continuous at x. □

Lemma 2.7. *Suppose that $K = \mathbb{R}, K = \mathbb{C}$ or K is a local field. Then $\mathbb{A}^n(K)$ is complete and every closed bounded subset C of $\mathbb{A}^n(K)$ is compact.*

Proof. It is clear that $\mathbb{A}^n(K)$ is complete. Now C is a closed subset of a complete space, hence complete. To show that a metric space is compact, it suffices to show that every sequence has a convergent subsequence, so by completeness of C, it suffices to show that every sequence has a Cauchy subsequence.

A way to do this is by using total boundedness: We claim that C is totally bounded, i.e. that for every $\epsilon > 0$ there is finite cover of C by ϵ-balls. We select the subsequence as follows. For $n = 1, 2, 3, \ldots$, cover C by finitely many balls of radius $1/n$. By the pigeon-hole principle, there is a $1/n$-ball which contains infinitely many elements of the sequence. Keep only the first n terms of the sequence and those in the selected $1/n$-ball. This results in a Cauchy sequence, because any pair of terms after the n-th will have distance $< 2/n$.

Proof of the claim: Let $\epsilon > 0$ be arbitrary. If $K = \mathbb{R}$ or $K = \mathbb{C}$, then we can cover $\{z \in K : |z| < M\}$ by at most $(2M/\epsilon)^2$ ϵ-balls. Hence (with

the maximum-norm) we need at most $(2M/\epsilon)^{2n}$ balls to cover C. If K is a local field, let m be the smallest positive integer such that $p^{-m} \leq \epsilon$. Let $R = \{x \in K : |x| \leq 1\}, \mathfrak{M} = \{x \in K : |x| < 1\}$. Then $B(x, \epsilon) = x + \mathfrak{M}^m$ and $R/\mathfrak{M}^m$ is finite, so R has a finite cover by ϵ-balls. Again, we get a finite cover of C by ϵ-balls. □

Lemma 2.8. *Suppose that $K = \mathbb{R}, K = \mathbb{C}$ or K is a local field. Then $\mathbb{P}^n(K)$ is compact.*

Proof. For $j = 0, \ldots, n$, let

$$C_j = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(K) : x_j = 1 \text{ and for all } i \neq j,\ x_i \leq 1\}.$$

Then C_j is compact by the previous lemma. Also, every point in $\mathbb{P}^n(K)$ is in some C_j, so $\mathbb{P}^n(K)$ is the union of finitely many compact sets. □

From now on, assume that K is a local field. Let the finite set $\mathbb{P}^n(k)$ have the discrete topology. Let the *reduction map* $\widetilde{\cdot} : \mathbb{P}^n(K) \to \mathbb{P}^n(k)$ be given by $(x_0 : \cdots : x_n) \mapsto (x_0 (\mathrm{mod}\ \mathfrak{M}) : \cdots : x_n (\mathrm{mod}\ \mathfrak{M}))$ if all $x_i \in R$ and at least one $x_i \in R^*$.

Lemma 2.9. *The reduction map $\mathbb{P}^n(K) \to \mathbb{P}^n(k)$ is continuous.*

Proof. Let $\widetilde{x} \in \mathbb{P}^n(k)$ be any point. We will show that the pre-image of $\{\widetilde{x}\}$ is open. So let $x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$ be any point which gets mapped to $\widetilde{x}$. If we multiply the coordinates by a suitable element of K^*, then $x_j \in R$ for all j and $x_i \in R^*$ for some i. If we divide by x_i, then we find $x_i = 1$. Hence we may assume (by symmetry) that $x_0 = 1$. Let $\mathbb{A}^n(K)$ be an affine neighborhood of x. Then every element of $B(x, 1) \subset \mathbb{A}^n(K)$ is of the form $x + y$, where $y = (y_1, \ldots, y_n)$ satisfies $y_i \in \mathfrak{M}$ for all i. Therefore, the open neighborhood $B(x, 1)$ of x gets mapped inside $\{\widetilde{x}\}$ by the reduction map. □

2.5 $E_n(K)$ has finite index

As an application of the v-adic topology, we prove

Lemma 2.10. *$E_0(K)$ has finite index in $E(K)$.*

Proof. We follow [Sil86], exercise 7.6. Let $\mathbb{P}^N(K)$ have the v-adic topology. Then $\mathbb{P}^N(K)$ is compact and rational functions are continuous. In particular, $E(K)$ is the zero set of a rational function, so it is a closed subset of a compact space, hence compact as well.

The reduction map is continuous and $E_0(K)$ is the pre-image of an open set, so it is open.

Every coset of $E_0(K)$ is the image of $E_0(K)$ under a translation map τ_Q and such a map is birational, hence a homeomorphism, so every coset of $E_0(K)$ is open. Now the cosets of $E_0(K)$ form an open cover of $E(K)$ with no strict subcover, so there can only be finitely many. □

Corollary 2.11. *For every integer $n \geq 1$, $E_n(K)$ has finite index in $E(K)$.*

Proof. The above lemma shows that the index of $E_0(K)$ in $E(K)$ is finite.

To see that the index of $E_1(K)$ in $E_0(K)$ is finite, notice that $E_1(K)$ was defined as the kernel of the reduction map $E_0(K) \to \widetilde{E}_{\mathrm{ns}}(k)$, so $[E_0(K) : E_1(K)] = \#\widetilde{E}_{\mathrm{ns}}(k)$, which is finite, because k is.

Finally, Lemma 2.3 shows that $\#E_n(K)/E_{n+1}(K) = \#k$ for $n \geq 1$. □

3 Formal groups and isogenies

3.1 Substitution

Let's get back to formal groups. It is convenient to work with the coordinates $z = -x/y, w = -1/y$, where x, y are the given Weierstrass coordinates. By the point (a, b), we will therefore mean the point with $z = a, w = b$, which is $(a/b, -1/b)$ in the usual Weierstrass coordinates.

Let E be an elliptic curve, defined over any field K. Formal substitution of $(T, w(T))$ for (z, w) is a well-defined ring homomorphism from the field of rational functions $\overline{K}(E)$ on E, to the field of formal Laurent series $\overline{K}((T))$ over $\overline{K}$.

If a function $f \in \overline{K}(E)$ is regular at the point O ($z = w = 0$), then the Laurent series $f(T, w(T))$ is a power series. Therefore, substitution induces a map $K_O(E) \to K[[T]]$, where $\overline{K}_O(E)$ is the local ring of functions that are regular at O and $\overline{K}[[T]]$ is the ring of formal power series over $\overline{K}$. In particular,

Definition. If $\phi : E \to E'$ is an isogeny, then we define the *formal homomorphism associated to* ϕ by

$$F_\phi(T) = (z' \circ \phi)(T, w(T)),$$

where $z' = -x'/y'$ is the coordinate function for E' and by $(T, w(T))$ we mean the point with $z = -x/y = T$, $w = -1/y = w(T)$.

Example 3.1. Trivial examples are $F_{[0]} = 0$, $F_{[1]} = T$ and if $a_1 = a_3 = 0$, then $F_{[-1]} = -T$. But we can also calculate the following examples directly from the addition formula.

$$\begin{aligned}
F_{[2]} &= 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)\,T^4 + \left(2a_2^2 - 6a_1a_3 - 12a_4\right)T^5 \\
&\quad + \left(-7a_3a_1^2 - a_2^2a_1 - 6a_4a_1 - 2a_2a_3\right)T^6 + O\left(T^7\right), \\
F_{[3]} &= 3T - 3a_1T^2 + \left(a_1^2 - 8a_2\right)T^3 + (12a_1a_2 - 39a_3)\,T^4 \\
&\quad + \left(-6a_2a_1^2 - 9a_3a_1 + 24a_2^2 - 96a_4\right)T^5 + O\left(T^6\right), \\
F_{[-1]} &= -T - a_1T^2 - a_1^2T^3 + \left(-a_1^3 - a_3\right)T^4 + \left(-a_1^4 - 3a_3a_1\right)T^5 \\
&\quad + \left(-a_1^5 - 6a_3a_1^2 - a_2a_3\right)T^6 + O\left(T^7\right).
\end{aligned}$$

Example 3.2. Let E be an elliptic curve with a rational two-torsion point. We may move the two-torsion point to $(0, 0)$. Then E can be given by $y^2 = x^3 + ax^2 + bx$ and there is an isogeny of degree 2 given by

$$\phi : E \to E' : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right),$$

where $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Then $z(\phi(z/w, -1/w)) = w/(z^2 - bw^2)$, so

$$\begin{aligned} F_\phi(T) &= T + aT^3 + \left(a^2 + 2b\right) T^5 + \left(a^3 + 6ba\right) T^7 \\ &\quad + \left(a^4 + 12ba^2 + 6b^2\right) T^9 + \left(a^5 + 20ba^3 + 30b^2a\right) T^{11} + O\left(T^{12}\right). \end{aligned}$$

Lemma 3.3. *Let $w(T)$ (resp. $w'(T)$) be the power series from Proposition 1.2 for the curve E (resp. E'). Then*

a. $F_\phi(T)$ truly represents ϕ in the sense that

$$\phi(T, w(T)) = (F_\phi(T), w'(F_\phi(T))). \tag{3}$$

b. F_ϕ is a homomorphism of formal groups. In other words, $F_\phi(F_{\widehat{E}}(T, S)) = F_{\widehat{E}'}(F_\phi(T), F_\phi(S))$.

c. $F_{\phi\circ\psi}(T) = F_\phi(F_\psi(T))$. In categorical language, we may say that formal substitution is a functor from the category of elliptic curves over K to the category of formal groups over K.

d. If $\phi, \psi : E \to E'$, then $F_{\phi+\psi}(T) = F_{\widehat{E}}(F_\phi(T), F_\psi(T))$.

Proof. a. By definition, the identity is true on the z-coordinate, so we only need to show that the w-coordinates of both sides are equal. Notice that the left hand side of (3) satisfies the defining equation for E', because $(T, w(T))$ satisfies the defining equation for E and ϕ is a rational map from E to E'. The right hand side of (3) also satisfies the defining equation for E', because $(T, w'(T))$ does and we have simply substituted $F_\phi(T)$ for T.

We now know that $w_1(T) = w(F_\phi(T))$ and $w_2(T) = w(\phi(P(T)))$ are power series such that $(F_\phi(T), w_i(T))$ satisfies (2). This fixes the coefficients of $w_i(T)$, as we can see by induction. Therefore, $w_1(T) = w_2(T)$.

b. By Lemma 1.4,

$$\begin{aligned} F_{\widehat{E}'}(F_\phi(T), F_\phi(S)) &= z\left((F_\phi(T), w'(F_\phi(T))) + (F_\phi(S), w'(F_\phi(S))) \right) \\ &= z\left(\phi(T, w(T)) + \phi(S, w(S)) \right) \qquad \text{(from } a.\text{)} \\ &= (z \circ \phi)\left((T, w(T)) + (S, w(S)) \right) \qquad (\phi \text{ is a hom.}) \\ &= (z \circ \phi)\left(F_{\widehat{E}}(T, S), w(F_{\widehat{E}}(T, S)) \right) \qquad \text{(Lemma 1.4)} \\ &= F_\phi(F_{\widehat{E}}(T, S)), \end{aligned}$$

so F_ϕ is a homomorphism of formal groups.

We can verify *c.* directly from *a.*

d. Let $P = (T, w(T))$, then

$$\begin{aligned} F_{\phi+\psi}(T) &= z((\phi + \psi)P) \\ &= z(\phi(P) + \psi(P)) \\ &= z(P(F_\phi(T)) + P(F_\psi(T))) \quad \text{(by } a.\text{)} \end{aligned}$$

By definition of $F_{\widehat{E}}(X, Y)$, this is equal to $F_{\widehat{E}}(F_\phi(T), F_\psi(T))$. □

Example 3.4. If we substitute $(T, w(T))$ in the equations $[m+n](P) = [m]P + [n]P$, and $[-m](P) = -[m]P$, then we find

$$\begin{aligned} F_{[m+n]}(T) &= F_{\widehat{E}}(F_{[m]}(T), F_{[n]}(T)), \\ F_{[-m]}(T) &= i_{\widehat{E}}(F_{[m]}(T)). \end{aligned}$$

Recall that $F_{[1]}(T) = T$ and that $F_{\widehat{E}}$ and $i_{\widehat{E}}$ have coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$, this shows that $F_{[m]}(T)$ has coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$ for all $m \in \mathbb{Z}$ and that the leading coefficient is m.

3.2 Differentials

The rules that define the space of differentials Ω_E (page 8) still hold after substitution of $(T, w(T))$ for (z, w), so substitution gives a map $\Omega_E \to K((T))dT$. A differential form $\omega \in \Omega_E$ is called regular at O if it is of the form gdz with $g \in \overline{K}_O(E)$ (see [Sil86] II.4.3). Therefore substitution also gives a map $\Omega_{E,O} \to K[[T]]dT$, where $\Omega_{E,O}$ denotes the space of differentials that are regular at O.

By Lemma 1.9 (also [Sil86] IV.4.2) there is a unique normalized invariant differential for $\widehat{E}$ and it is in $\mathbb{Z}[a_1, \ldots, a_6][[T]]dT$. We denote it by $\widehat{\omega}(T)$. The following lemma gives the relation between invariant differentials on E and invariant differentials for $\widehat{E}$.

Lemma 3.5. *Suppose that $\omega \in \Omega_E$ is an invariant differential on E. Then $\omega(T, w(T))$ is a differential in $\overline{K}[[T]]dT$ that is invariant for the formal group $\widehat{E}$.*

If $\omega = \frac{dx}{2y+a_1x+a_3}$ is the invariant differential of E, then $\omega(T)$ is equal to the normalized invariant differential $\widehat{\omega}(T) \in \mathbb{Z}[a_1, \ldots, a_6][[T]]dT$ of $\widehat{E}$.

Proof. First of all, ω is everywhere regular. In particular at O, so $\omega(T, w(T)) \in K[[T]]dT$.

Next, [Sil86] III.5.1 shows

$$\tau_Q^* \omega = \omega,$$

where τ_Q is the translation-by-Q map. This is done by writing out $\tau_Q^*\omega(P) = \omega(P + Q)$ to $a(P, Q)\omega(P)$ using the rules *i.*, *ii.* and *iii.* and then showing $a(P, Q) = 1$. These rules stay valid if we substitute $(T, w(T))$ for P and $(S, w(S))$ for Q, so

$$\begin{aligned} \omega(F_{\widehat{E}}(T, S), w(F_{\widehat{E}}(T, S))) &= \omega(P + Q) = \omega(P) \\ &= \omega(T, w(T)), \end{aligned}$$

so $\omega(T, w(T))$ is an invariant differential for $\widehat{E}/K$.

Next, suppose that $\omega = 1/(2y + a_1x + a_3)dx$. Let $P(T) \in \overline{K}[[T]]$ be such that $\omega(T, w(T)) = P(T)dT$, then we can easily see that $P(0) = 1$ by writing out the definition (for example in Table 2 on page 25 or in [Sil86] page 113), so $\omega(T, w(T))$ must be equal to the unique normalized invariant differential for $\widehat{E}$. □

3.3 Explicit formal homomorphisms

We can now prove

Lemma 3.6. *For any isogeny $\phi : E_1 \to E_2$,*

$$F_\phi(T) = \exp_{\widehat{E_2}}(a_\phi \log_{\widehat{E_1}}(T)),$$

where a_ϕ is such that $\phi^*\omega_2 = a_\phi\omega_1$ (see Corollary 2.2 of Chapter II).

Proof. If we substitute $(T, w(T))$, then $\phi^*\omega_2 = a_\phi\omega_1$ turns into

$$\widehat{\omega}_2(F_\phi(T)) = a_\phi\widehat{\omega}_1(T). \tag{4}$$

If we integrate this, then we get (using the chain rule 1.8 and the definition $\widehat{\omega}(f(T)) = P(f(T))df(T) = P(f(T))f'(T)dT$),

$$\log_{\widehat{E}_2}(F_\phi(T)) = a_\phi \log_{\widehat{E}_1}(T) + C$$

with $C \in \overline{K}$, because the map $d : \overline{K}[[T]] \to \overline{K}[[T]]dT$ has kernel $\overline{K}$.

Putting $T = 0$ shows $C = 0$, so if we apply $\exp_{\widehat{E}_2}$, then we get the desired equation. □

We can use this result to write out the first few terms of the sequence F_ϕ. See for example Table 2 on page 25.

Remark 3.7. Using only formal group theory, one can in fact derive for any formal homomorphism $F : \mathcal{F} \to \mathcal{G}$ the expression

$$F(T) = \exp_{\mathcal{G}}(F'(0)\log_{\mathcal{F}}(T)).$$

For example, this follows if we integrate [Sil86] IV.4.3.

3.4 Consequences for local fields

Let K be a local field of characteristic 0 and let E, E' be elliptic curves over K, given by Weierstrass equations with v-integral coefficients.

Proposition 3.8. *Suppose that $\phi : E \to E'$ is an isogeny which is defined over K and let a_ϕ be such that $\phi^*\omega' = a_\phi\omega$. If both*

$$-\frac{1}{2}v(x(P)) > \frac{v(p)}{p-1} \quad \text{and} \quad -\frac{1}{2}v(x(P)) + v(a_\phi) > \frac{v(p)}{p-1},$$

then

$$v(x'(\phi(P))) \;=\; v(x(P)) - 2v(a_\phi).$$

Proof. The condition $-\frac{1}{2}v(x(P)) > v(p)/(p-1)$ implies in particular $P \in E_1(K)$. Let $z = z(P)$. Then $v(z) = -\frac{1}{2}v(x(P))$ so $v(z), v(z) + v(a_\phi) > v(p)/(p-1)$. Therefore Corollary 1.11 shows that $\log_{\widehat{E}}(z)$ converges and satisfies $v(\log_{\widehat{E}}(z)) = v(z)$. Next, $v(\log_{\widehat{E}}(z)) + v(a_\phi) > v(p)/(p-1)$, so we can apply Corollary 1.11 again to find that $\exp_{\widehat{E}'}(a_\phi \log_{\widehat{E}}(z))$ converges to an element t with $v(t) = v(\log_{\widehat{E}}(z)) + v(a_\phi) = v(z) + v(a_\phi)$. But if $F_\phi(z)$ converges, then it converges to $z(\phi(z, w(z))) = z(\phi(P))$, so we are done. □

$$
\begin{aligned}
w(T) &= T^3 + a_1T^4 + \left(a_1^2 + a_2\right)T^5 + \left(a_1^3 + 2a_2a_1 + a_3\right)T^6 \\
&+ \left(a_1^4 + 3a_2a_1^2 + 3a_3a_1 + a_2^2 + a_4\right)T^7 + O\left(T^8\right) \\
x(T) &= \frac{T}{w(T)} = \frac{1}{T^2} - \frac{a_1}{T} - a_2 - a_3T + \left(-a_1a_3 - a_4\right)T^2 + O\left(T^3\right) \\
y(T) &= \frac{-1}{w(T)} = -\frac{1}{T^3} + \frac{a_1}{T^2} + \frac{a_2}{T} + a_3 + \left(a_1a_3 + a_4\right)T + O\left(T^2\right) \\
\widehat{\omega}(T) &= \frac{1}{2y(T) + a_1x(T) + a_3}x'(T)dT \\
&= \Big(1 + a_1T + \left(a_1^2 + a_2\right)T^2 + \left(a_1^3 + 2a_2a_1 + 2a_3\right)T^3 \\
&+ \left(a_1^4 + 3a_2a_1^2 + 6a_3a_1 + a_2^2 + 2a_4\right)T^4 + O\left(T^5\right)\Big)dT \\
\log_{\widehat{E}}(T) &= T + \frac{a_1T^2}{2} + \frac{1}{3}\left(a_1^2 + a_2\right)T^3 + \frac{1}{4}\left(a_1^3 + 2a_2a_1 + 2a_3\right)T^4 \\
&+ \frac{1}{5}\left(a_1^4 + 3a_2a_1^2 + 6a_3a_1 + a_2^2 + 2a_4\right)T^5 + O\left(T^6\right) \\
\exp_{\widehat{E}}(T) &= T - \frac{a_1T^2}{2} + \frac{1}{6}\left(a_1^2 - 2a_2\right)T^3 + \frac{1}{24}\left(-a_1^3 + 8a_2a_1 - 12a_3\right)T^4 \\
&+ \frac{1}{120}\left(a_1^4 - 22a_2a_1^2 + 36a_3a_1 + 16a_2^2 - 48a_4\right)T^5 + O\left(T^6\right) \\
F_{[\alpha]}(T) &= \alpha T - \frac{1}{2}\left((\alpha - 1)\alpha a_1\right)T^2 \\
&+ \frac{1}{6}(\alpha - 1)\alpha\left((\alpha - 2)a_1^2 - 2(\alpha + 1)a_2\right)T^3 \\
&- \frac{1}{24}\Big((\alpha - 1)\alpha\Big((\alpha^2 - 5\alpha + 6)a_1^3 + 4(-2\alpha^2 + \alpha + 3)a_2a_1 \\
&\qquad + 12(\alpha^2 + \alpha + 1)a_3\Big)\Big)T^4 \\
&+ O\left(T^5\right)
\end{aligned}
$$

Table 2: The power series written out explicitly. Lemma 3.6 was used for calculating $F_{[\alpha]}(T)$.

4 Formal groups and complex multiplication

In the fourth and last section of this chapter we will apply the theory of formal groups to elliptic curves with complex multiplication.

The only result of this section that will be used for elliptic divisibility sequences is the fact that the groups $E_n(M_v)$ are $\mathcal{O}$-submodules of $E(M_v)$. In order to prove this, we will need to show that the power series that are involved have integral coefficients. First, let us define formal modules.

4.1 Formal modules

We will now study complex multiplication using formal modules. Formal modules are not standard: a more standard approach is to use the endomorphism ring of the formal group.

Let A and B be commutative rings.

Definition. A *formal B-module $\mathcal{F}$ defined over A* is a formal group $\mathcal{F}/A$ with group law $F(X,Y)$, together with, for every $\alpha \in B$, a formal homomorphism $[\alpha] : \mathcal{F} \to \mathcal{F}$, such that for all $\alpha, \beta \in B$:

i. $[\alpha+\beta](T) = F([\alpha](T), [\beta](T))$,

ii. $[\alpha\beta](T) = [\alpha]([\beta](T))$ and

iii. $[1](T) = T$.

We say that it is *proper* if furthermore A contains B and $[\alpha](T) = \alpha T + \text{h.o.t.}$

Example 4.1. Given a number field $L \subset \mathbb{C}$ and an elliptic curve E/L with complex multiplication by the ring of integers $\mathcal{O}$ of the field $K \subset \mathbb{C}$. Let $M = KL \subset \mathbb{C}$ be the composite.

Then every endomorphism of E is defined over M, so we can set $[\alpha](T) = F_{[\alpha]}(T) \in M[[T]]$. Lemma 3.3 shows that the formal module axioms are satisfied, so this makes the formal group $\widehat{E}$ into a formal $\mathcal{O}$-module, defined over M. Lemma 3.6 shows that it is in fact a proper formal $\mathcal{O}$-module.

Modules associated to formal modules

Let M_v be a local field and $\mathcal{F}$ a formal B-module *defined over the ring of integers R of M_v*. Then the groups $\mathcal{F}(\mathfrak{M}^r)$ become B-modules if we set $\beta \cdot x = [\beta](x)$.

If $B \subset R$ and the formal B-module $\mathcal{F}$ is proper, then the identity map of sets

$$\mathcal{F}(\mathfrak{M}^n)/\mathcal{F}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1} \tag{5}$$

is not only an isomorphism of groups (Lemma 1.6), but also an isomorphism of B-modules. Moreover, Remark 3.7 shows that if $\mathcal{F}$ is proper, then the valuation preserving isomorphisms

$$\begin{array}{rcll} \mathcal{F}(\mathfrak{M}^r) & \cong & \mathfrak{M}^r & (r > \frac{v(p)}{p-1}) \\ z & \mapsto & \log_{\mathcal{F}}(z) & \end{array}$$

of Theorem 1.10 are isomorphisms of B-modules.

In order to be able to use this for elliptic curves with complex multiplication, we need to prove

Theorem 4.2. *The formal $\mathcal{O}$-module of Example 4.1 is defined over $\mathcal{O}_M$. In other words, for any $\alpha \in \mathcal{O}$, the power series $F_{[\alpha]}(T)$ has coefficients in $\mathcal{O}_M$.*

Let v be any discrete valuation of M and let $p \in \mathbb{N}$ be the prime such that $v(p) > 0$. What we need to prove is that the coefficients of $F_{[\alpha]}(T)$ are v-integral for every $\alpha \in \mathcal{O}$. We give two proofs of this. The first uses only properties of formal groups and power series, but works only if p is split in $K/\mathbb{Q}$. The second uses explicit equations for isogenies, but fails if 2 splits in $K/\mathbb{Q}$ and $p = 2$. Together they cover every case, so they prove Theorem 4.2.

4.2 Formal modules and integrality

Lemma 4.3. *The set of polynomials in $\mathbb{Q}[x]$ that have only integral values on $\mathbb{Z}$ is a free abelian group, generated by the binomial coefficients*

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \qquad (n \in \mathbb{Z}, n \geq 0).$$

Proof. Notice that the binomial coefficients form a $\mathbb{Q}$-basis for $\mathbb{Q}[x]$. Given $f(x) = \sum_n c_n \binom{x}{n}$, we have to show that $f(x)$ has integer values on $\mathbb{Z}$ if and only if all the coefficients c_n are in $\mathbb{Z}$.

The "if" part is a basic fact about binomial coefficients (in fact, it is a special case of Lemma 4.4 below). We prove the "only if" part with induction on n. Suppose that $f(x)$ has integer values on $\mathbb{Z}$ and that $c_0, \ldots, c_{n-1} \in \mathbb{Z}$. Then $f(n)$ is an integer and $f(n) = \sum_k c_k \binom{n}{k}$. If $k > n$, then $\binom{n}{k} = 0$, and if $k < n$, then $c_k \in \mathbb{Z}$ by the induction hypothesis. Therefore, the remaining term $c_k \binom{n}{n} = c_k$ is an integer. □

Lemma 4.4. *Let $\mathcal{O}$ be the ring of integers of any number field K. Given a prime $\mathfrak{p}$ of $\mathcal{O}$, let $p \in \mathbb{N}$ be the prime such that $\mathfrak{p}|p$ and let v be the normalized discrete valuation of K at $\mathfrak{p}$.*

Suppose that p is totally split in K. Then for any non-negative integer n, the binomial coefficient

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

is a polynomial in x which assumes only v-integral values on $\mathcal{O}$.

Proof. Of the assumption that p splits completely in K we only use that $N(\mathfrak{p}) = p$ and $v(p) = v(\mathfrak{p})$. Given any pair $\beta \in \mathcal{O}$, $n \in \mathbb{N}$, we need to show that

$$\frac{\beta(\beta-1)\cdots(\beta-n+1)}{n!}$$

is v-integral. The valuation of the denominator is

$$v(n!) = \mathrm{ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

We will show that the valuation of the numerator is at least as large by showing that, for any k, at least $\lfloor \frac{n}{p^k} \rfloor$ elements of $B = \{\beta, \beta-1, \ldots, \beta-n+1\}$ are divisible by $\mathfrak{p}^k$.

Notice that for any k and any $\alpha \in \mathcal{O}$, the residue classes modulo $\mathfrak{p}^k$ of $\alpha, \alpha-1, \ldots, \alpha-p^k+1$ are all different. To see this, notice that if two of them are equal modulo $\mathfrak{p}^k$, then their difference is in $\mathfrak{p}^k \cap \mathbb{Z} = p^k\mathbb{Z}$, while it is also less than p^k. Therefore, their difference is 0, so we see that $\alpha, \alpha-1, \ldots, \alpha-p^k+1$ are pairwise distinct modulo $\mathfrak{p}^k$.

But there are only $N(\mathfrak{p}^k) = p^k$ residue classes modulo $\mathfrak{p}^k$, which means that one of $\alpha, \alpha-1, \ldots, \alpha-p^k+1$ is divisible by $\mathfrak{p}^k$. This holds for every set of p^k subsequent elements of B.

We can partition the set B into $\lfloor \frac{n}{p^k} \rfloor$ sets of at least p^k subsequent elements, which proves that for any k, at least $\lfloor \frac{n}{p^k} \rfloor$ elements of B are divisible by $\mathfrak{p}^k$. □

Example 4.5. The lemma does not hold for inert or ramifying primes. For example if $K = \mathbb{Q}(i)$, then 2 ramifies as $(1+i)^2$ and 3 is inert and we see

$$\binom{i}{3} = \frac{i(i-1)(i-2)}{6} = \frac{i(2+i)(2-i)}{3(1+i)}.$$

We can now prove

Proposition 4.6. *Let v be any valuation of M such that $v_{|K}$ is split in $K/\mathbb{Q}$. Then for any $\alpha \in \mathcal{O}$, the power series $F_{[\alpha]}(T)$ has v-integral coefficients.*

Proof. The proof will be completely formal. The fact that E has actual complex multiplication by $\mathcal{O}$ will not even be used, just the fact that we can make $\widehat{E}$ into a formal $\mathcal{O}$-module by setting $[\alpha](T) := \exp_{\mathcal{F}}(\alpha \log_{\mathcal{F}}(T))$, which we can do for any formal group. In the case of an elliptic curve with complex multiplication, this gives the same power series $[\alpha]T = F_{[\alpha]}(T)$ by Lemma 3.6.

View $a_1, \ldots, a_6$ as formal variables and $\widehat{E}/\mathbb{Z}[a_1, \ldots, a_6]$ as a formal group over a polynomial ring. If we look at the expression

$$[X](T) = \exp_{\mathcal{F}}(X \log_{\mathcal{F}}(T)) \in \mathbb{Z}[a_1, \ldots, a_6][X][[T]]$$

as a power series in T, then every coefficient is a polynomial

$$c_n(X) = \sum_e f_{n,e}(X) a_1^{e_1} \cdots a_6^{e_6} \in \mathbb{Z}[X][a_1, \ldots, a_6].$$

Using repeatedly the fact that the power series $F_{\widehat{E}}(T,S)$ and $i_{\widehat{E}}(T)$ have coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$, we find that $F_{[\alpha]}(T)$ has coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$ for every $\alpha \in \mathbb{Z}$. In other words, $c_n(\alpha) \in \mathbb{Z}[a_1, \ldots, a_6]$ for every $\alpha \in \mathbb{Z}$.

This is equivalent to saying that every coefficient $f_{n,e}(X)$ is an integer-valued polynomial, hence a $\mathbb{Z}$-linear combination of binomial coefficients. In particular, $f_{n,e}$ takes v-integral values on $\mathcal{O}$ by Lemma 4.4. As the elliptic curves which we consider all have integral coefficients, we find that $c_n(\alpha)$ is v-integral for every $\alpha \in \mathcal{O}$. □

Example 4.7. In Table 2 on page 25, we see that the T^3-coefficient of $F_{[\alpha]}(T)$ is equal to

$$\binom{\alpha}{3}a_1^2 - 2\left(\binom{\alpha}{2} + \binom{\alpha}{3}\right)a_2.$$

We can now see from Example 4.5 that we cannot prove integrality for any elliptic curve E and any quadratic imaginary field K. We will really need the fact that there is actual complex multiplication of E by $\mathcal{O}$.

4.3 Explicit equations for isogenies

In this section, we will use explicit formulas for the elliptic curve endomorphisms $[\alpha]$ to show that the power series $F_{[\alpha]}(T)$ has v-integral coefficients for almost every valuation v of M. We start with equations for isomorphisms. Then we write down Vélu's formula, which gives equations for all isogenies up to isomorphism.

Proposition 4.8. *Suppose that E' and E are elliptic curves, given by Weierstrass equations over a number field M. Any M-isomorphism $\phi : E' \to E$ is of the form*

$$\phi(x', y') = (u^2x' + r, u^3y' + u^2sx' + t) \tag{6}$$

with $u, r, s, t \in K, u \neq 0$.

With this notation, we have

a. $F_\phi(T) \in \mathbb{Z}[r, s, t, u^{-1}][[T]]$ and $F_\phi(uT) \in \mathbb{Z}[r, s, t, u][[T]]$.

b. Let ω' resp. ω denote invariant differentials for E' resp. E. Then $\phi^*\omega = u^{-1}\omega'$.

c. If $E = E'$, then $u \in \mathcal{O}^*$.

d. If v is a discrete valuation of K such that $v(u) \geq 0$ and each of the coefficients of E and E' is v-integral. Then r, s and t are also v-integral.

e. In particular, if $v(u) = 0$ and each of the coefficients of E and E' is v-integral, then the coefficients of $F_\phi(T)$ are v-integral.

Proof. Every isomorphism is of this form by [Sil86] III.3.1b. Table III.1.2 of [Sil86] gives relations between u, r, s, t and the coefficients of E and E'. That table also shows part *b.*.

We compute

$$z(\phi(\frac{z}{w}, -\frac{1}{w})) = \frac{u^{-1}z + ru^{-3}w}{1 - su^{-1}z - tu^{-3}w},$$

which proves part *a.*.

To see part *c.*, notice that if $E = E'$, then $\phi = [w]$ for some $w \in \mathcal{O}^*$ and $[w]^*\omega = w\omega'$, so $u = w^{-1}$ by *b.*.

Notice that part *e.* follows directly if we combine *a.* and *d.*, so now we only have to show *d.*. Suppose that u and the coefficients of E and E' are v-integral for some valuation v. Then the table mentioned above gives the following information: If $v(2) = 0$, then the identity for b_6' shows $v(r) \geq 0$ and

if $v(3) = 0$, then we get the same result from the identity for b_8'. Next, the identity for a_2' shows $v(s) \geq 0$ and the identity for a_6' shows $v(t) \geq 0$. □

Formula 4.9 (Vélu)**.** *Suppose that E is an elliptic curve, given by a general Weierstrass equation and suppose that F is a subgroup of finite order. Let F_2 be the set of points of order 2 in F. Let R be such that $R, -R$ forms a partition of $F \setminus \{O\} \setminus F_2$ and let $S = F_2 \cup R$.*

Then there is an elliptic curve E' and an isogeny $\sigma : E \to E' : (x, y) \mapsto (X, Y)$ with kernel F, given by

$$X = x + \sum_{Q \in S} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$Y = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + t_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1 u_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \right),$$

where

$$\begin{aligned}
Q &= (x_Q,\ y_Q), \\
g_Q^x &= 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q, \\
g_Q^y &= -2y_Q - a_1 x_Q - a_3, \\
t_Q &= \begin{cases} g_Q^x & \text{if } Q \in F_2, \\ 6x_Q^2 + b_2 x_Q + b_4 & \text{if } Q \notin F_2, \end{cases} \\
u_Q &= 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6, \\
b_2 &= a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1 a_3, \\
b_6 &= a_3^2 + 4a_6.
\end{aligned}$$

The image curve E' is given by

$$E \ : \ Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6,$$

where

$$\begin{aligned}
A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \\
A_4 = a_4 - 5t, \quad A_6 = a_6 - b_2 t - 7w, \\
t = \sum_{Q \in S} t_Q, \quad w = \sum_{Q \in S} (u_Q + x_Q t_Q).
\end{aligned}$$

Furthermore, $\sigma^* \omega_E = \omega_{E'}$.

Proof. The equations for E' and σ and the identity $\sigma^* \omega_E = \omega_{E'}$ are given in [Vél71]. □

Lemma 4.10. *Let σ be as in Vélu's formula. If the coefficients of E are v-integral, as well as all the points in F, then $F_\sigma(T)$ has v-integral coefficients.*

Proof. Set

$$\left.\begin{array}{rcccl} x(T) & = & \frac{T}{w(T)} & = & T^{-2} - a_1 T^{-1} - a_2 - \cdots \\ y(T) & = & -\frac{1}{w(T)} & = & -T^{-3} + a_1 T^{-2} + \cdots \end{array}\right\} \in \mathbb{Z}[a_1, \ldots, a_6]((T)).$$

Then for any $Q \in E[\alpha]$,

$$\frac{1}{x(T) - x_Q} = \frac{T^2}{T^2 x(T) - x_Q T^2}$$

is a Laurent series with v-integral coefficients and a zero of order 2.

Substituting $x(T)$ and $y(T)$ in Vélu's formula, we find that X is a Laurent series with v-integral coefficients and lowest degree term T^{-2}, while Y is a Laurent series with v-integral coefficients and lowest degree term $-T^{-3}$. Therefore, $F_\sigma(T) = -X/Y$ is a power series with v-integral coefficients. □

Proposition 4.11. *Any isogeny $\phi : E_1 \to E_2$ may be written as a composition $\psi \circ \sigma$, where σ is an isogeny of the form in Vélu's Formula 4.9 and ψ is an isomorphism of the form in Proposition 4.8.*

If $\phi^* \omega_2 = a_\phi \omega_1$, where ω_1, resp. ω_2 are the invariant differentials for E_1 resp. E_2, then the isomorphism satisfies $u = a_\phi^{-1}$.

Proof. Let $\sigma : E_1 \to E'$ be the isogeny from Vélu's formula with the same kernel as ϕ. Then by [Sil86] III.4.11, there is an isomorphism $\psi : E' \to E_2$ such that $\phi = \psi \circ \sigma$. Furthermore, by Proposition 4.8*b.* and the last remark in Formula 4.9, $u = a_\psi^{-1} = a_\phi^{-1}$. □

Corollary 4.12. *Given a discrete valuation v of M and an elliptic curve E, given by a general Weierstrass equation with v-integral coefficients. For any $\alpha \in \mathcal{O}$, if $v(N(\alpha)) = 0$, then $F_{[\alpha]}(T)$ has v-integral coefficients.*

Proof. It suffices to prove this for any extension of (M, v), so we may assume without loss of generality that M contains the coordinates of all points in the kernel $E[\alpha]$ of $[\alpha]$.

Let $\phi = \psi \circ \sigma$ be the factorization in the above proposition. Notice that every point in $E[\alpha]$ is $N(\alpha)$-torsion, so its coordinates are v-integral by Corollary 2.2 (also [Sil86] VII.3.4).

Therefore, by Lemma 4.10, $F_\sigma(T)$ has v-integral coefficients. On the other hand, we see in Vélu's formula that the image curve of σ has v-integral coordinates, so by *e.* of Proposition 4.8, $F_\psi(T)$ has v-integral coefficients. Now *c.* of Lemma 3.3 shows that $F_\phi(T) = F_\psi(F_\sigma(T))$ has v-integral coefficients. □

Proposition 4.13. *Let v be any valuation of M and let $p \in \mathbb{N}$ be the prime such that $v(p) > 0$. Suppose that $p \neq 2$ or that p does not split in $K/\mathbb{Q}$. Then for any $\alpha \in \mathcal{O}$, $F_{[\alpha]}(T)$ has v-integral coefficients.*

Proof. Let $\mathfrak{p}$ be the prime of K such that $v(\mathfrak{p}) > 0$ and pick β such that $\mathcal{O} = \mathbb{Z} + \beta\mathbb{Z}$. We claim that there is an $n \in \mathbb{Z}$ such that $N(n + \beta)$ is coprime to $\mathfrak{p}$.

Assuming the claim for now, Corollary 4.12 shows that $F_{[n+\beta]}(T)$ has v-integral coefficients for the n of the claim. Using repeatedly the fact that $F_{\widehat{E}}$ and $i_{\widehat{E}}$ have v-integral coefficients and that $F_{[x+y]}(T) = F_{\widehat{E}}(F_{[x]}(T), F_{[y]}(T))$ for all $x, y \in \mathcal{O}$ (Lemma 3.3), we find that $F_{[\alpha]}(T)$ has v-integral coefficients for every $\alpha \in \mathcal{O}$.

Proof of the claim: If both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ do not divide β, then it is trivial. So suppose that $\mathfrak{p}|\beta$. Then $\{n \in \mathbb{Z} : \mathfrak{p}|(\beta + n)\} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. If $p \neq 2$, then $\beta + 1$ and $\beta + 2$ are both not divisible by $\mathfrak{p}$, but they cannot both be divisible by $\overline{\mathfrak{p}}$, which proves the claim if $p \neq 2$. If $p = 2$, then by assumption, p does not split, so $\mathfrak{p} = \overline{\mathfrak{p}}$. Hence in that case $\beta + 1$ is not divisible by $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. □

The exception in this proposition is more than covered by Proposition 4.6, so we have now proved Theorem 4.2. □

4.4 The $\mathcal{O}$-modules $E_n(M_v)$

Lemma 4.14. *The sets $E_n(M_v)$ are $\mathcal{O}$-submodules of $E(M_v)$. We have an isomorphism of $\mathcal{O}$-modules*

$$E_n(M_v)/E_{n+1}(M_v) \cong k, \tag{7}$$

where the residue field k is seen as an $\mathcal{O}$-module.

Proof. We know that $\widehat{E}$ is a proper formal $\mathcal{O}$-module over the ring of integers of M, so in particular over the ring of integers R of M_v.

For any $n \geq 1$ and any $P \in E_n(M_v)$, $F_{[\alpha]}(z(P))$ converges, so Lemma 3.3*a.* shows that $[\alpha]P$ corresponds to $F_{[\alpha]}(z(P))$ through the isomorphism of groups

$$\begin{array}{rcl} E_n(M_v) & \cong & \widehat{E}(\mathfrak{M}^n) \quad \text{(Lemma 2.1)} \\ P & \mapsto & z(P). \end{array}$$

This shows that $E_n(M_v)$ is an $\mathcal{O}$-submodule of $E(M_v)$ and that the isomorphism of Lemma 2.1 is an isomorphism of $\mathcal{O}$-modules.

Together with the isomorphism of $\mathcal{O}$-modules

$$\widehat{E}(\mathfrak{M}^n)/\widehat{E}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1} \cong k, \quad \text{(see (5))}$$

this proves the assertion. □

4.5 Torsion in formal modules

We finish the chapter with a result on integrality of $\mathcal{O}$-torsion. This will not be used later in the text.

Definition. Given an $\mathcal{O}$-module F and an element z, the *order* of z is the kernel of the map $\mathcal{O} \to B : \alpha \mapsto [\alpha]z$.

Lemma 4.15. *Suppose that $\mathcal{O}$ the ring of integers of a number field K and let M be a number field containing K. Let M_v be the localization of M at a discrete valuation v. Suppose that $\mathcal{F}$ is a formal $\mathcal{O}$-module, defined over the ring of integers R of M_v. Let $\mathfrak{p}$ be the prime of $\mathcal{O}$ such that $v(\mathfrak{p}) > 0$.*

Then for any torsion element $z \in \mathcal{F}(\mathfrak{M})$,

1. *The order of z is a power of $\mathfrak{p}$.*

2. *If z has order $\mathfrak{p}^n$, then*
$$v(z) \leq \frac{v(\mathfrak{p})}{p^n - p^{n-1}}.$$

Proof. 1. Suppose that z has order $\mathfrak{a}$, which is not a power of $\mathfrak{p}$. Let $\mathfrak{b}$ be coprime to $\mathfrak{p}$ and such that $\mathfrak{a} = \mathfrak{b}\mathfrak{p}^n$. Take an element β of $\mathfrak{b}$ such that $v(\beta) = v(\mathfrak{b}) = 0$ and an element α of $\mathfrak{p}^n$ which is not in $\mathfrak{a}$. Notice that α exists, because otherwise $\mathfrak{a} = \mathfrak{p}^n$ is a power of $\mathfrak{a}$. Then $[\alpha]z \neq 0$ and $[\alpha\beta]z = 0$, so we can replace z by $[\alpha]z$ and find an element of order dividing β.

Now $0 = [\beta]z = \beta z + \text{h.o.t.} \neq 0$. Contradiction.

2. Let α be an element of $\mathfrak{p}$ with minimal valuation. We follow the proof of [Sil86] IV.6.1.

We start by proving that there are power series $f(T), g(T) \in R[[T]]$ such that $g(0) = 0$, $f(T) = 1 + \text{h.o.t.}$ and
$$[\alpha](T) = \alpha f(T) + g(T^p).$$
Let $\omega(T) = P(T)dT$ be the normalized invariant differential of the formal group $\mathcal{F}$. Then [Sil86] IV.4.3 states (alternatively (4) of this text if we are speaking about the formal group of an elliptic curve with complex multiplication)
$$\alpha\omega(T) = \omega([\alpha](T)).$$
Because $P(T) = 1 + \text{h.o.t.} \in R$, we can read this as
$$\alpha(1 + \cdots)dT = (1 + \cdots)[\alpha]'(T)dT,$$
so $[\alpha]'(T) \in \alpha R[[T]]$. Hence every term aT^n such that n is not divisible by p has to satisfy $v(a) \geq v(\alpha)$. In other words, $a \in \alpha R$.

We prove *2.* by induction on n. So suppose $z \neq 0$ and $[\alpha](z) = 0$. Then
$$0 = \alpha f(z) + g(z^p)$$
and the only way to eliminate the leading term αz is by having $v(z^p) \leq v(\alpha z) = v(\mathfrak{p}) + v(z)$. Hence
$$v(\mathfrak{p}) \geq (p-1)v(z),$$
which proves *2.* for $n = 1$. Now assume that *2.* is true for n and let $z \in \widehat{E}(\mathfrak{M})$ have order $\mathfrak{p}^{n+1}$. Then
$$\begin{aligned} v([\alpha](z)) &= v(\alpha f(z)) + g(x^p) \\ &\geq \min\{v(\alpha z), v(x^p)\}. \end{aligned}$$
By the induction hypothesis,
$$v(\alpha)/(p^n - p^{n-1}) \geq v([\alpha](z)).$$
Therefore,
$$v(\alpha)/(p^n - p^{n-1}) \geq \min\{v(\alpha z), v(z^p)\}.$$

Notice that as $n \geq 1$, we have $v(\alpha z) > v(\alpha) \geq v(\alpha)/(p^n - p^{n-1})$, so the previous inequality implies

$$v(\alpha)/(p^n - p^{n-1}) \geq v(z^p) = pv(z),$$

which is exactly the desired result. □

Corollary 4.16. *Let $P \in E(M)$ be any M-valued torsion point.*

1. *If the order of P is not a prime power, then $x(P) \in \mathcal{O}_M$.*
2. *For any prime $\mathfrak{p}$ of $\mathcal{O}$, if P has order $\mathfrak{p}^n$, then for every discrete valuation v of M,*

$$v(x(P)) \geq -2\frac{v(\mathfrak{p})}{p^n - p^{n-1}},$$

where $p \in \mathbb{N}$ is the prime such that $\mathfrak{p}|p$. □

Chapter IV

Elliptic Divisibility Sequences

1 Denominators of rational points

Let L be a number field and E/L an elliptic curve, given by a general Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{8}$$

with coefficients $a_1, \ldots, a_6$ in the ring of integers $\mathcal{O}_L$ of L. Then every L-valued point has the following property.

Lemma 1.1. *For every point $P \in E(L)$, different from O, there are unique integral L-ideals A, B, C with A and B coprime such that*

$$x(P) = \frac{A}{B^2}, \quad y(P) = \frac{C}{B^3}.$$

Furthermore, B and C are coprime.

Proof. For any discrete valuation v of L, the Weierstrass equation shows that $v(x) < 0$ if and only if $v(y) < 0$ and if this is the case, then $3v(x) = 2v(y)$.

Notice that even if $x = 0$ (resp. $y = 0$), then y (resp. x) is integral, so $A = x, B = 1, C = y$ is the unique solution and 0 is coprime only to 1. □

This brings us to our main object of study for this chapter. Let P be a rational non-torsion point on an elliptic curve E/L, which is given by a Weierstrass equation with integral coefficients. Then for every $n \in \mathbb{N}$, we can write

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right). \tag{9}$$

with unique integral ideals A_n, B_n, C_n with $(A_n, B_n) = 1$. This defines a sequence of ideals $B_1, B_2, B_3, \ldots$. We call such a sequence an *elliptic divisibility sequence* or an *elliptic denominator sequence*. Tables 3 and 4 contain examples that are factored into primes and primes are underlined at the place where they occur for the first time in the sequence.

$$
\begin{aligned}
B_1 &= 1\\
B_2 &= \underline{2}\\
B_3 &= \underline{13}\\
B_4 &= 2^2 \cdot \underline{3} \cdot \underline{7}\\
B_5 &= \underline{5}^2 \cdot \underline{61}\\
B_6 &= 2 \cdot 13 \cdot \underline{239}\\
B_7 &= \underline{2165017}\\
B_8 &= 2^3 \cdot 3 \cdot 7 \cdot \underline{31} \cdot \underline{113} \cdot \underline{257}\\
B_9 &= 13 \cdot \underline{16921} \cdot \underline{192853}\\
B_{10} &= 2 \cdot 5^2 \cdot \underline{17} \cdot 61 \cdot \underline{79} \cdot \underline{337} \cdot \underline{8161}\\
B_{11} &= \underline{2377} \cdot \underline{3221811719677}\\
B_{12} &= 2^2 \cdot 3^2 \cdot 7 \cdot \underline{11} \cdot 13 \cdot \underline{23} \cdot \underline{47} \cdot 239 \cdot \underline{359} \cdot \underline{577} \cdot \underline{1201}\\
B_{13} &= 37 \cdot \underline{41} \cdot \underline{198953} \cdot \underline{51396663946057}\\
B_{14} &= 2 \cdot \underline{1009} \cdot \underline{2351} \cdot 2165017 \cdot \underline{3503833734241}\\
B_{15} &= 5^2 \cdot 13 \cdot 61 \cdot \underline{11329} \cdot \underline{14401} \cdot \underline{57601} \cdot \underline{1475701} \cdot \underline{1644061}\\
B_{16} &= 2^4 \cdot 3 \cdot 7 \cdot 31 \cdot 113 \cdot 257 \cdot \underline{2113} \cdot \underline{2593} \cdot \underline{46271} \cdot \underline{101281} \cdot \underline{623013889}\\
B_{17} &= \underline{29} \cdot \underline{197} \cdot \underline{36721} \cdot \underline{46916533} \cdot \underline{12833635727822694321517}\\
B_{18} &= 2 \cdot 13 \cdot \underline{239} \cdot \underline{719} \cdot \underline{1151} \cdot 16921 \cdot \underline{187631} \cdot 192853 \cdot \underline{68531759} \cdot \underline{9788425919}\\
B_{19} &= \underline{39370035996866731492397} \cdot \underline{935840962959734589514 8113}\\
B_{20} &= 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 17 \cdot \underline{19} \cdot 61 \cdot \underline{73} \cdot 79 \cdot \underline{89} \cdot 337 \cdot \underline{353} \cdot \underline{593} \cdot \underline{1459} \cdot \underline{1601} \cdot \underline{2833} \cdot \underline{5879} \cdot\\
&\quad \underline{8081} \cdot 8161 \cdot \underline{26041} \cdot \underline{264599}\\
B_{21} &= 13 \cdot 2165017 \cdot \underline{102651529} \cdot \underline{5448808889775508858979152713339758685352249}\\
B_{22} &= 2 \cdot \underline{1231} \cdot \underline{1759} \cdot 2377 \cdot \underline{69697} \cdot \underline{831599} \cdot \underline{1306447} \cdot \underline{81865377793} \cdot\\
&\quad 3221811719677 \cdot \underline{32427388266593}\\
B_{23} &= \underline{6827230790591535045377341363921193050113334582920057672010412638560073}\\
B_{24} &= 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31 \cdot 47 \cdot 113 \cdot 239 \cdot 257 \cdot 359 \cdot \underline{383} \cdot 577 \cdot 1201 \cdot \underline{15647} \cdot\\
&\quad \underline{203039} \cdot \underline{268993} \cdot \underline{391009} \cdot \underline{39237409} \cdot \underline{2402076769} \cdot \underline{111000722593}\\
B_{25} &= 5^3 \cdot 61 \cdot \underline{277 \cdot 521 \cdot 1553 \cdot 1025621 \cdot 89094101 \cdot 94290401 \cdot 86610864881} \cdot\\
&\quad \underline{22765620047223591706572670760486476301}
\end{aligned}
$$

Table 3: Some terms of the EDS given by $E : y^2 = x^3 - 2x$, $P = (-1, 1)$.

$$
\begin{aligned}
B_1 &= 1 \\
B_2 &= 1 \\
B_3 &= \underline{2} \\
B_4 &= 1 \\
B_5 &= \underline{5} \\
B_6 &= 2^3 \\
B_7 &= \underline{37} \\
B_8 &= \underline{3} \cdot \underline{19} \\
B_9 &= 2 \cdot \underline{137} \\
B_{10} &= 5 \cdot \underline{7} \cdot \underline{13} \\
B_{11} &= \underline{61} \cdot \underline{101} \\
B_{12} &= 2^4 \cdot \underline{11} \cdot \underline{127} \\
B_{13} &= \underline{165713} \\
B_{14} &= 37 \cdot \underline{1291} \\
B_{15} &= 2 \cdot 5 \cdot \underline{943429} \\
B_{16} &= 3 \cdot 19 \cdot \underline{83} \cdot \underline{14741} \\
B_{17} &= \underline{29} \cdot \underline{3041} \cdot \underline{11497} \\
B_{18} &= 2^3 \cdot \underline{17} \cdot \underline{23} \cdot 137 \cdot \underline{7901} \\
B_{19} &= \underline{1237} \cdot \underline{10193} \cdot \underline{11329} \\
B_{20} &= 5 \cdot 7 \cdot 13 \cdot \underline{1217} \cdot \underline{3156697} \\
B_{21} &= 2 \cdot 37 \cdot \underline{84977} \cdot \underline{9185453} \\
B_{22} &= \underline{47} \cdot 61 \cdot 101 \cdot \underline{2729} \cdot \underline{799817} \\
B_{23} &= \underline{89} \cdot \underline{28429} \cdot \underline{9291839693} \\
B_{24} &= 2^5 \cdot 3^2 \cdot 11 \cdot 19 \cdot \underline{43} \cdot \underline{59} \cdot 127 \cdot \underline{16490213} \\
B_{25} &= 5^2 \cdot \underline{761713} \cdot \underline{1556313465913} \\
B_{26} &= \underline{41} \cdot \underline{149} \cdot \underline{239} \cdot \underline{4271} \cdot 165713 \cdot \underline{753611} \\
B_{27} &= 2 \cdot 137 \cdot \underline{63275741} \cdot \underline{2476652547037} \\
B_{28} &= 37 \cdot \underline{53} \cdot \underline{113} \cdot \underline{1291} \cdot \underline{11057} \cdot \underline{58963203163} \\
B_{29} &= \underline{853} \cdot \underline{9921337} \cdot \underline{16439698126501721} \\
B_{30} &= 2^3 \cdot 5 \cdot 7 \cdot 13 \cdot \underline{281} \cdot \underline{1361} \cdot \underline{4519} \cdot 943429 \cdot \underline{1277496791}
\end{aligned}
$$

Table 4: Some terms of the EDS given by $E : y^2 + xy = x^3 + x^2 - 2x$, $P = (-1, -1)$.

2 Valuations (1)

Let B be an elliptic divisibility sequence.

Lemma 2.1. *For any pair of integers $m, n \in \mathbb{N}$ and any valuation v, if $v(B_n) > 0$, then*

$$v(B_{mn}) \geq v(B_n).$$

We have equality if and only if $v(m) = 0$.

Proof. Let $r = v(B_n) = -\frac{1}{2}x([n]P)$ and let L_v be the localization of L at v. First of all, the fact that $E_r(L_v)$ is a group (Lemma 2.3 of Chapter III) shows $v(B_{nm}) = -\frac{1}{2}v(x([nm]P)) \geq r$. Second, the isomorphism $E_r(K)/E_{r+1}(K) \cong k^+$ (Lemma 1.6 of Chapter III) shows that $v(x([nm]P)) \in E_{r+1}(K)$ if and only if $p|m$. □

Corollary 2.2. *With the same hypothesis as the above lemma, if $p \in \mathbb{N}$ is the prime such that $v(p) > 0$ and if $p^k|m$, then*

$$v(B_{mn}) \geq v(B_n) + k$$

Proof. The previous lemma tells us that $v(B_{mn}) \geq v(B_{np^k})$ and that for all l, $v(B_{np^{l+1}}) \geq v(B_{np^l}) + 1$. If we apply induction, then we get the result. □

We will see in Lemma 4.1 that in many cases, we can actually make the stronger statement $v(B_{nm}) = v(B_n) + v(m)$. First we will show that elliptic divisibility sequences are divisibility sequences.

3 Divisibility sequences

Definition. Let $u = (u_n)_{n\in\mathbb{N}}$ be a sequence integral ideals in some number field. We call u *divisible*, or a *divisibility sequence* if for all $m, n \in \mathbb{N}$,

$$m|n \Rightarrow u_m|u_n.$$

If u satisfies the stronger condition

$$u_{(m,n)} = (u_m, u_n),$$

then we call the sequence *strongly divisible*, or a *strong divisibility sequence.*

Lemma 3.1. *Every elliptic divisibility sequence is a* strong divisibility sequence*. In particular, it is a divisibility sequence.*

Proof. First we show that the sequence is divisible. Then we have in particular $B_{(m,n)}|(B_m, B_n)$.

So suppose that $m|n$. For any discrete valuation v of L, $v(B_n) \geq v(B_m)$. Indeed if $v(B_m) = 0$, then it is trivial and if $v(B_m) > 0$, then it is Lemma 2.1. As v was arbitrary, we have $B_m|B_n$.

Now we only have to show $(B_m, B_n)|B_{(m,n)}$. So suppose again that v is any discrete valuation of L. Let $r = v((B_m, B_n))$. Let $d = (m, n)$ and let $x, y \in \mathbb{Z}$ be such that $xm + yn = d$. Then $v(B_{xm}) \geq v(B_m) \geq r$ and similarly $v(B_{yn}) \geq r$. As $E_r(L_v)$ is a group, we find $dP = xmP + ynP \in E_r(L_v)$, so $v(B_d) \geq r$. As v was arbitrary, we conclude $(B_m, B_n)|B_{(m,n)}$. □

We will now give the promised stronger lemma about valuations of B_n.

4 Valuations (2)

Let B be an elliptic divisibility sequence over a number field L.

Lemma 4.1. *For any pair $m, n \in \mathbb{N}$, if $v(B_n) > \frac{v(p)}{p-1}$, then*

$$v(B_{mn}) = v(B_n) + v(m).$$

We give the same proof twice. The first time applying the formal isogenies from Section III.3; the second time, for those who have not read that section, written out explicitly using the theory as it is in [Sil86] Chapter IV. This second proof is also in [Sil88] and [CH98], although the conclusion of [CH98] is too strong, as we can see in Example 4.2.

First proof. Apply Proposition 3.8 of Chapter III to $\phi = [m]$ and use the fact that $[m]^*\omega = m\ \omega$ for every invariant differential ω. That fact can be found in Example 3.4 of Chapter III or in [Sil86] III.5.3. □

Second proof. We use the isomorphism $E_1(K) \cong \widehat{E}(\mathfrak{M})$ from Lemma 2.1 of Chapter III, but instead of the isomorphism $\widehat{E}(\mathfrak{M}^n)/\widehat{E}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1}$, we now we use the formal logarithm.

We know from Theorem 1.10 of Chapter III (also [Sil86] IV.6.4b) that the formal logarithm defines an isomorphism

$$\log_{\widehat{E}} : \widehat{E}(\mathfrak{M}^r) \to \mathfrak{M}^r$$

for every $r > \frac{v(p)}{p-1}$. In particular for $r = v(z) = -\frac{1}{2}v(x)$. The fact that we also have an isomorphism for every integer $r' > r$ shows that it preserves the valuation. Therefore,

$$\begin{aligned} v(z(mP)) &= v(\log_{\widehat{E}}(z(mP))) \\ &= v(m \log_{\widehat{E}}(z(P))) \\ &= v(m) + v(\log_{\widehat{E}}(z(P)) \\ &= v(m) + v(z(P)), \end{aligned}$$

which is the desired result. □

Example 4.2. In Lemma 1 of [CH98], the condition $v(B_n) > \frac{v(p)}{p-1}$ is replaced by the weaker $v(B_n) > 0$. Unfortunately, this condition is too weak, as we can see from the following example, which is also visible in B_3 and B_6 of Table 4 on page 37.

Let $K = \mathbb{Q}_2$ be the field of 2-adic integers, and let the elliptic curve E be given by the Weierstrass equation $x^2 + xy = x^3 + x^2 - 2x$. Let $P = (-\frac{1}{4}, \frac{7}{8})$, then P is a non-torsion point in $E_1(K)$ and $2P = (\frac{121}{64}, \frac{913}{512})$, so $v(x(2P)) = -6$, but $v(x(P)) - 2v(2) = -2 - 2 = -4$.

Notice that if $v(p) < p-1$, then the conditions $v(B_n) > 0$ and $v(B_n) > v(p)/(p-1)$ are equivalent. The only prime ideals $\mathfrak{p}$ of L for which $v_{\mathfrak{p}}(p) \geq p-1$ are the primes that are ramified (i.e. $v(p) > 1$) and the primes that lie above 2 (i.e. $\mathfrak{p}|2$). There are only finitely many of each of these types.

For these finitely many problematic primes, we will be satisfied with the following asymptotic result.

Lemma 4.3. *For every pair $m, n \in \mathbb{N}$, if $v(B_n) > 0$, then*

$$v(B_{mn}) = v(B_n) + v(m) + O(1),$$

where the $O(1)$ constants do not depend on m and n.

Proof. Let n_0 be the smallest positive integer such that $v(B_{n_0}) > 0$. Notice that for every natural number n, $v(B_n) > 0 \iff n_0|n$. Indeed, if $n_0|n$, then $B_{n_0}|B_n$. On the other hand, if $v(B_n) > 0$, then $v(B_d) > 0$, where $d = (n, n_0)$, which contradicts minimality of n_0 unless n_0 divides n.

We will prove that for every n such that $n_0|n$,

$$v(B_n) = v(n) + O(1). \tag{10}$$

From this, we get that if n, m are positive integers and $v(B_n) > 0$, then $v(B_{mn}) = v(n) + v(m) + O(1) = v(B_n) + v(m) + O(1)$.

So let's prove (10). First of all, we may restrict to the case where n/n_0 is a power of p, because both sides of the equation do not change if we multiply n by an integer that is coprime to p. (For the left hand side, this is Lemma 2.1.)

Let k be the smallest integer greater than $\frac{v(p)}{p-1}$. Then by Corollary 2.2, $v(B_{n_0p^k}) \geq v(B_{n_0}) + k > 1 + v(p)/(p-1)$.

Now suppose that $n/n_0 \geq p^k$ is a power of p. Then by Lemma 4.1,

$$v(B_n) = v(B_{n_0p^k}) + v\left(\frac{n}{n_0p^k}\right) = v(B_{n_0p^k}) + v(n) - v(n_0p^k) = v(n) + O(1).$$

Now only the (finitely many) cases $n/n_0 = 1, p, p^2, \ldots, p^{l-1}$ remain, so we adjust the $O(1)$ constants for each of these cases. □

Finally, we give a result which puts some restrictions on the Weierstrass equation, but can be used in the case $p = 2$ for all points with $v(x) < 0$. This is not relevant for the rest of the text.

Lemma 4.4. *Let L be a field and v a discrete valuation on L such that $v(2) > 0$. Suppose that the coefficients of the Weierstrass equation satisfy $2|a_1$ and $v(a_3) > v(2) - 2$ (for example if the Weierstrass equation in short form). Then for all $m, n \in \mathbb{N}$, if $v(B_n) > 0$, then*

$$v(B_{mn}) = v(B_n) + v(m).$$

Proof. The duplication formula ([Sil86], III 2.3d) reads

$$x_2 = x\frac{1 - b_4x^{-2} - 2b_6x^{-3} - b_8x^{-4}}{4 + b_2x^{-1} + 2b_4x^{-2} + b_6x^{-3}}$$

with the notation

$$\begin{array}{rclcrcl} b_2 & = & a_1^2 + 4a_2, & & b_4 & = & 2a_4 + a_1a_3, \\ b_6 & = & a_3^2 + 4a_6, & & b_8 & = & a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{array}$$

Notice that the valuation of the numerator is 0. We will show that the valuation of the denominator is determined only by the term "4", which proves the lemma for $m = 2$.

By assumption, $2|a_1$, so $4|a_1^2 + 4a_2 = b_2$ and $2|2a_4 + a_1a_3 = b_4$, so the second and third terms of the denominator have valuation at least $v(4x^{-1}) > v(4)$.

The valuation of the last term is at least $v(b_6) + 6$, because $v(x) \leq -2$. We have $b_6 = a_3^2 + 4a_6$, so if $v(a_3) \geq v(2)$, then $v(b_6) \geq v(4)$ and we are done. If $v(a_3) < v(2)$, then $v(b_6) + 6 = 2v(a_3) + 6 > 2v(2)$ by hypothesis.

We have now proved the lemma for $m = 2$ and with induction for all powers of 2. If $m = 2^l m'$ with $2 \nmid m'$, then we get $v(B_{nm}) = v(B_{n2^l}) = v(B_n) + lv(2) = v(B_n) + v(m)$, where the first equality follows from Lemma 2.1. □

Corollary 4.5. *Suppose that $E/\mathbb{Q}$ is given by a Weierstrass equation with coefficients in $\mathbb{Z}$ such that $2|a_1$. If B is an elliptic divisibility sequence defined over the curve E, then for every discrete valuation v and all $n, m \in \mathbb{N}$, if $v(B_n) > 0$, then*

$$v(B_{mn}) = v(B_n) + v(m).$$

□

Chapter V

Zsigmondy's Theorem for Elliptic Divisibility Sequences

1 Theorems of primitive divisors

In Table 3 on page 36 and Table 4 on page 37, primes are underlined at the place where they occur for the first time. Almost every term in each of the sequences seems to have a prime divisor which does not occur any earlier in the sequence. We call such a new prime factor a *primitive divisor*. This chapter is dedicated to Silverman's proof in [Sil88] that for any elliptic divisibility sequence, from some point on, every term indeed has a primitive divisor.

Such a statement was proven by Bang (1886, [Ban86]) for the sequence $a^n - 1$ and later a more general version was independently proven by Zsigmondy ([Zsi92], 1892). Even though Bang was earlier, a theorem of primitive divisors is usually called a "Zsigmondy theorem" and the following theorem is usually called Zsigmondy's theorem.

Theorem 1.1 (Bang, Zsigmondy)**.** *Given coprime integers $a > b > 0$, let $l(n) = a^n - b^n$. Then $l(n)$ has a primitive divisor unless*

i. $a = 2, b = 1$ and $n = 6$, or

ii. $a + b = 2^k$ for some integer k and $n = 2$. □

Another example of a Zsigmondy theorem is the result of Bilu, Hanrot and Voutier in 2001 for the Lucas and Lehmer sequences that are defined as follows.

Definition. A *Lehmer pair* (α, β) is a pair of algebraic integers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. A *Lucas pair* is a Lehmer pair such that $\alpha + \beta$ is already a rational integer.

For any Lucas pair (α, β), define the *Lucas sequence* by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n = 0, 1, 2, \ldots).$$

Similarly, for any Lehmer pair (α, β), define the *Lehmer sequence* by

$$v_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd;} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

Theorem 1.2 (Bilu, Hanrot, Voutier ([BHV01]))**.** *For every Lucas or Lehmer sequence, the n-th term has a primitive divisor for all $n > 30$.* □

We call an integer Z a *Zsigmondy bound* for a sequence A if for every $n > Z$, A_n has a primitive divisor. Both of the above theorems have a very strong form in the sense that they give a *uniform* Zsigmondy bound, independent of the parameters. Our results for elliptic divisibility sequences are not uniform: We will only show that for any given sequence, there is a Zsigmondy bound.

It is expected however, that there does exist a uniform Zsigmondy bound for all elliptic divisibility sequences where the Weierstrass model is in global minimal form ([EMW06]). For some special families of elliptic curves that satisfy Lang's conjecture (below), uniform bounds do indeed exist:

Theorem 1.3 (Everest, McLaren, Ward ([EMW06]))**.** *Let $\mathcal{F}$ denote a family of elliptic curves $E/\mathbb{Q}$, given by Weierstrass models in global minimal form, and rational points $P, Q \in E(\mathbb{Q})$, with P a non-torsion point and Q a 2-torsion point such that either*

1. *P does not lie in the real connected component of the identity, or*
2. *$x(P) - x(Q)$ is a square.*

Suppose furthermore that Lang's Conjecture holds for the family; in other words, there is a uniform constant $c = c(\mathcal{F}) > 0$ such that for every triple $(E, P, Q) \in \mathcal{F}$, the inequality $\widehat{h}(P) \geq c \log \Delta(E)$ holds.

Then there is a uniform Zsigmondy bound for all sequences arising from the family. □

In the same article, some examples of families as in the above theorem are given. A different example of a family of elliptic divisibility sequences with a uniform Zsigmondy bound is the following, where the Zsigmondy bound is given explicitly.

Theorem 1.4 (Everest, McLaren, Ward ([EMW06]))**.** *Suppose that the curve E is given by a Weierstrass equation*

$$E : y^2 = x^3 - T^2 x,$$

with $T > 0$ a square-free rational integer, and suppose that E has a non-torsion point P in $E(\mathbb{Q})$. Let $B_1, B_2, \ldots$ be the elliptic divisibility sequence for P. Then B_n has a primitive divisor for

1. *every even $n > 10$,*
2. *every odd $n > 3$ if $x(P) < 0$ and*
3. *every odd $n > 21$ if $x(P)$ is a square.* □

2 Primitive divisors and the primitive part

Suppose that $B = (B_n)_{n\in\mathbb{N}}$ is any sequence of integral ideals of some number field. For any $n \in \mathbb{N}$, a *primitive divisor* of B_n is a prime (ideal of L) that divides B_n, but does not divide B_m for any $m < n$. The *primitive part* D_n of B_n is the unique ideal $D_n|B_n$ such that D_n is a product of primitive divisors of B_n, while B_n/D_n is a product of only non-primitive divisors.

In order to prove the Zsigmondy theorem for elliptic divisibility sequences, we will give asymptotic lower bounds for the primitive part and show that it goes to infinity. In particular, the primitive part has to be greater than 1 from some point on. In fact, the lower bounds are quite large, and we will see that the logarithm of the primitive part will grow asymptotically faster than $0.355\widehat{h}(P)n^2$, where $\widehat{h}(P)$ is the canonical height of P, which we will introduce later. Actually, this is not optimal, and we will eventually prove in Proposition 6.8 of Chapter VI that the logarithm of the primitive part is $s_n\widehat{h}(P)n^2 + O(n^\epsilon)$, where $s_n = \prod_{p|n}(1-p^{-2})$ is between $1/\zeta(2) \approx 0.6$ and 1.

To show that D_n goes to infinity, we will first give bounds for B_n. Then the lemmas about valuations of elliptic divisibility sequences will show that the non-primitive part of B_n is unable to keep up with B_n, so there has to be a non-trivial primitive part. For the bounds on B_n, we will use approximations involving the *height* of a point.

3 The height of a point

The *height* $h_x(P)$ of a point P is a measure for the arithmetic complexity of the point. In order to define the height on an elliptic curve, we should first define the height on a number field (or, more accurately, on the projective line $L \cup \{\infty\}$ over a number field L).

On $\mathbb{Q}$, the height will simply be given by $h(a/b) = \log\max\{|a|, |b|\}$ if a/b is a fraction in lowest terms. The simplest way to define such a height on $E(\mathbb{Q})$ is by letting $h(P) = h(x(P))$ if $P \neq O$ and $h(O) = 0$.

More generally, we can define a height function on $E(L)$ as follows. Let M_L be the set of standard absolute values as in [Sil86] VIII §5. This is a full set of representatives for the places of L and it is chosen as follows. The set $M_\mathbb{Q}$ contains

a. the standard absolute value, given by $|x|_\infty = \max\{x, -x\}$ and

b. for every prime $p \in \mathbb{Z}$, a p-adic valuation, given by $|p^n a/b|_p = p^{-n}$ if $p \nmid ab$.

For a general number field L, let M_L contain all valuations whose restriction to $\mathbb{Q}$ is a valuation in $M_\mathbb{Q}$.

Let M_L^0 denote the set of non-archimedean standard absolute values and M_L^∞ the set of archimedean standard absolute values.

Given a point $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(L)$, the *height of P relative to L* is defined by

$$H_L(P) = \prod_{v\in M_L} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v},$$

where $n_v = [L_v : \mathbb{Q}_v]$. This is independent of the choice of homogeneous coordinates for P, because of the product formula (see [Sil86] VIII.5.4a). We now define the *absolute height* function on $\mathbb{P}^n(\overline{\mathbb{Q}})$ by

$$H(P) = H_L(P)^{1/[L:\mathbb{Q}]},$$

where L is a number field such that P is L-valued. It is independent on the choice of L (see [Sil86] VIII.5.4c).

Let h be the logarithm of this height function. If we restrict $h : \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{R}$ to $\mathbb{Q}$, then $h(a/b) = \prod_{v \in M_L} \max\{|a|_v, |b|_v\}^{n_v} = \max\{|a|_\infty, |b|_\infty\}$, so this gives us the same height on $\mathbb{Q}$ that we mentioned at the beginning of this section.

We now define the height on an elliptic curve as follows.

Definition. Given an elliptic curve E/L and a function $f \in \overline{L}(E)$. The *height on E relative to f* is the function $h_f : E(\overline{L}) \to \mathbb{R}$, given by

$$h_f(P) = h(f(P)).$$

If $f = x$ and $L = \mathbb{Q}$, then this gives the same height function on $E(\mathbb{Q})$ that was mentioned above.

It is sometimes more useful to use the *canonical height*, which is defined by

$$\widehat{h}(P) = \frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f(2^N P),$$

where $f \in L(E)$ is any non-constant even function. This is independent of the choice of f ([Sil86] VIII.9.1).

The basic properties of height functions ([Sil86] VIII.9.3) then say

$$\begin{aligned} (\deg f)\widehat{h} &= h_f + O(1), \\ \widehat{h}(mP) &= m^2 \widehat{h}(P), \\ \widehat{h}(P) &\geq 0 \qquad \text{(equal iff } P \text{ is a torsion point).} \end{aligned}$$

If we put these equations together and use $\deg x = 2$, then we get

$$h_x(mP) = 2m^2 \widehat{h}(P) + O(1), \tag{11}$$

where the $O(1)$ constants depend on E, but not on m or P.

4 Siegel's theorem

The aim of this section is to show that the denominator B_n^2 of $x(nP)$ grows about just as fast as the height of nP. In fact, the denominator of any non-constant even function grows about just as fast as the height.

The idea is as follows. Suppose that $x(P) \in \mathbb{Q}$ is written in lowest terms as $x = \frac{A}{B^2}$. Then $h_x(P) = \max\{\log|A|, \log B^2\}$. If $B^2 \geq |A|$, then $2\log B = h_x(P)$ and if $B^2 \leq |A|$, then $\log B^2 = \log|A| - \log|x(P)| = h_x(P) - \log|x(P)|$. Therefore, $2\log B = h_x(P) - \max\{\log|x(P)|, 0\}$, so the size of $x(P)$ gives an indication of the amount by which B_n can differ from $\widehat{h}(nP) = n^2\widehat{h}(P)$.

To show that $x(P)$ cannot grow too fast, we will use the following approximation result by Siegel, for which we first introduce a definition:

Definition. The *v-adic distance from P to Q* is given by

$$d_v(P,Q) = \min\{|t_Q(P)|_v^{1/e}, 1\},$$

for a function $t_Q \in L_v(C)$ with a zero of order $e \geq 1$ at Q.

This definition depends on the choice of t_Q, but the limit in the following theorem does not.

Theorem 4.1 (Siegel)**.** *Let E/L be an elliptic curve with $\#E(L) = \infty$, $f \in L(E)$ a non-constant even function, $v \in M_L$, and $Q \in E(\overline{L})$. Then*

$$\lim_{\substack{P \in E(L) \\ h_f(P) \to \infty}} \frac{\log d_v(P,Q)}{h_f(P)} = 0.$$

Proof. [Sil86] IX.3.1 □

Notice that $S := \liminf \frac{\log d_v(P,Q)}{h_f(P)} \leq 0$ by definition of d_v, so the statement of Siegel's theorem is $S \geq 0$, meaning that the accuracy with which you approximate Q with a point P will not keep up with the height of the point P. The point that we will approximate will be O, because approximating O is the same as having an x-coordinate which goes to infinity.

For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_L$, define the *numerator* $\mathrm{num}(\mathfrak{a})$ and the *denominator* $\mathrm{den}(\mathfrak{a})$ to be the coprime integral ideals of L for which $a = \mathrm{num}(\mathfrak{a})/\mathrm{den}(\mathfrak{a})$. Let $N_{L/\mathbb{Q}}$ be the norm function. Then we have,

Lemma 4.2. *For any $x \in L$,*

$$\log N(\mathrm{den}(x)) \quad = \quad [L:\mathbb{Q}]\ h(x) - \sum_{v \in M_L^\infty} n_v \log \max\{|x|_v, 1\}.$$

Proof. The norm is multiplicative and for any prime ideal $\mathfrak{p}$, we have $N(\mathfrak{p}) = \#\mathcal{O}_L/\mathfrak{p} = p^{n_v} = |\mathfrak{p}|_{v_\mathfrak{p}}^{-n_v}$, so

$$\begin{aligned}
\log N(\mathrm{den}(x)) &= \sum_{v \in M_L^0} n_v \log(|\mathrm{den}(x)|_v^{-1}) \\
&= \sum_{v \in M_L^0} n_v \log \max\{|x|_v, 1\} \\
&= \sum_{v \in M_L} n_v \log \max\{|x|_v, 1\} - \sum_{v \in M_L^\infty} n_v \log \max\{|x|_v, 1\} \\
&= [L:\mathbb{Q}]h(x) - \sum_{v \in M_L^\infty} n_v \log \max\{|x|_v, 1\}.
\end{aligned}$$

□

In other words, the norm of the denominator of x is the height of a minus some terms coming from the (finitely many) archimedean absolute values of a.

We will use the non-standard notation $||\mathfrak{a}|| := N(\mathfrak{a})^{1/[L:\mathbb{Q}]}$. If L is $\mathbb{Q}$ or a quadratic imaginary extension, then this is just the unique archimedean valuation. In all other cases, the function $||\cdot||$ is *not* a valuation, but only a multiplicative function on the ideals. With this notation, the previous equation becomes

$$\frac{\log||\mathrm{den}(x)||}{h(x)} = 1 + \frac{1}{[L:\mathbb{Q}]}\sum_{v\in M_L^\infty} n_v \frac{\log\min\{|1/x|_v, 1\}}{h(x)}.$$

And on an elliptic curve, for any non-constant even function t and any point $P \in E(L)$, this is

$$\frac{\log||\mathrm{den}(t(P))||}{h_t(P)} = 1 + \frac{1}{[L:\mathbb{Q}]}\sum_{v\in M_L^\infty} n_v e \frac{d_v(P,Q)}{h_t(P)},$$

for any point Q where t has a pole of order e. Siegel's theorem says that the finitely many terms in the sum on the right go to zero as the height of P goes to infinity, so we are left with

$$\lim_{\substack{P\in E(L)\\ h_f(P)\to\infty}} \frac{\log||\mathrm{den}(t(P))||}{h_t(P))} = 1.$$

In other words, the denominator of any non-constant even function grows just like the height. Using equation (11) to write this in terms of the canonical height, we get

$$\frac{\log||\mathrm{den}(t(nP))||}{\deg t} = (1-o(1))\ n^2\ \widehat{h}(P),$$

where $o(1)$ means a function which goes to zero if n goes to infinity.

In particular, for $t = x$, we have $B_n^2 = \mathrm{den}(t(nP))$ and $\deg x = 2$, so

Lemma 4.3. *With the notation $||\mathfrak{a}|| := N(\mathfrak{a})^{1/[L:\mathbb{Q}]}$, we have*

$$(1-o(1))n^2\widehat{h}(P) \le \log||B_n|| \le n^2\widehat{h}(P) + O(1),$$

Proof. We have just proved the lower bound. The stronger upper bound follows directly from the definitions as follows. The last term (the sum) in Lemma 4.2 is at most 0, so $\log||B_n^2|| \le h_x(nP) = 2n^2\widehat{h}(P) + O(1)$. □

5 Lower bounds for the primitive part

The following lemma bounds the non-primitive part of B_n by an expression in earlier terms of the sequence. One should think of the factors M and q as "small", because we have seen that B_n grows much faster.

Lemma 5.1. *There is an integer $M > 0$ such that for all $n \in \mathbb{N}$,*

$$\frac{B_n}{D_n} \ \Big|\ M \prod_{\substack{q|n\\ prime}} qB_{n/q}.$$

Proof. Suppose that $\mathfrak{p}$ is a non-primitive prime divisor of B_n. Then $\mathfrak{p}$ divides some B_m with $m < n$. But then $\mathfrak{p}|(B_n, B_m) = B_{(m,n)}$, so we may assume $m|n$, which implies $m|n/q$ for some q. Hence $\mathfrak{p}|B_{n/q}$.

So unless $e(\mathfrak{p}/p) \geq p-1$, we have (Lemma 4.1 of Chapter IV)

$$v_{\mathfrak{p}}(B_n) = v(B_{n/q}) + v(q) \leq v\left(\prod qB_{n/q}\right).$$

For the finitely many primes $\mathfrak{p}$ for which $e(\mathfrak{p}/p) \geq p-1$, the above inequality holds up to an $O(1)$ constant (Lemma 4.3 of Chapter IV), which we absorb into the factor M. □

In particular, we have the inequality

$$\log||D_n|| \geq \log||B_n|| - \sum_{q|n} \log||B_{n/q}|| - \log n - \log||M||,$$

which we could regard as the result of an inclusion-exclusion argument with only a single inclusion: The "new" divisors in D_n are all the divisors in B_n except those that are in $B_{n/q}$ for some q. This is a very crude estimate, but it will suffice for now. We will do sharper estimates when we need them in Chapter VI. For now,

$$\begin{array}{rcrcl}
\log||D_n|| & \geq & \log||B_n|| - \sum_{q|n}\log||B_{n/q}|| & - & O(\log n) \\
& \geq & \left((1-o(1))n^2 - \sum_{p|n}(n/p)^2\right)\widehat{h}(P) & & \text{(by 4.3)} \\
& = & \left(1 - o(1) - \sum_{p|n} p^{-2}\right) n^2\widehat{h}(P) & & \\
& \geq & (2 - \zeta(2) - o(1))\, n^2\widehat{h}(P) & & \\
& \geq & (0.355 - o(1))\, n^2\widehat{h}(P) & . &
\end{array}$$

So we see that $||D_n||$ goes to infinity. In particular, from some point on, $||D_n||$ has to be greater than 1, so B_n has a primitive divisor. In other words,

Theorem 5.2 ([Sil88])**.** *For all but finitely many $n \in \mathbb{N}$, B_n has a primitive divisor. Moreover, the primitive part D_n satisfies*

$$\log||D_n|| \geq (0.355 - o(1))\; n^2\;\widehat{h}(P).$$

□

We now have more than enough information to prove

Corollary 5.3. *If we replace P by a large enough multiple, then for all positive integers m, n.*

$$B_m|B_n \quad \Longleftrightarrow \quad m|n$$

Proof. Let d be such that every term of the sequence beyond the d-th has a primitive divisor and replace P by dP. We have already seen the implication to the left. So suppose that $B_m|B_n$. Then $B_{(m,n)} = (B_m, B_n) = B_m$. As B_m has a primitive divisor, it cannot be equal to $B_{(m,n)}$ unless $(m,n) = m$. But then $m|n$. □

Chapter VI

Elliptic Divisibility Sequences with Complex Multiplication

In this chapter, we let elliptic divisibility sequences be indexed by the full endomorphism ring, instead of only $\mathbb{N}$.

In the first section, we introduce elliptic divisibility sequences with complex multiplication and present some results that follow directly from the theory of formal groups. Then in Section 2, we discuss what it means for a sequence to be (strongly) divisible if it is indexed by a number ring. This results in our choice to have the sequence indexed by the ideals of the CM-ring.

Then in the third section, we will see that Siegel's theorem is not good enough anymore, so Section 4 will be devoted to a much more explicit result: David's theorem.

In the section after that, we will do some extra work that is needed only if the endomorphism ring has class number greater than one: We attach points to the terms $B_{\mathfrak{a}}$ where $\mathfrak{a}$ is non-principal. These points will lie on a set of elliptic curves that is indexed by the class group of K. Then finally, in Section 6, we will prove Zsigmondy's theorem for elliptic divisibility sequences with complex multiplication.

Note that we assume throughout this text that the endomorphism ring is the full ring of integers of its field of fractions.

1 Elliptic divisibility sequences with complex multiplication

Suppose that $L \subset \mathbb{C}$ is a number field and that E/L is an elliptic curve, given by a Weierstrass equation with coefficients in the ring of integers $\mathcal{O}_L$ of L. Suppose furthermore that E has complex multiplication by the *ring of integers* $\mathcal{O}$ of $K \subset \mathbb{C}$ and let M be the composite $M = KL \subset \mathbb{C}$.

Recall from Section 4 of Chapter II that we can make a natural choice for the isomorphism $[\cdot] : \mathcal{O} \cong \mathrm{End}(E)$ such that $[\alpha]^*\omega = \alpha\omega$ and that every endomorphism of E is defined over M.

If P is a non-torsion point in $E(L)$, then we may define the (coprime)

integral M-ideals A_α, B_α by

$$x([\alpha]P) = \frac{A_\alpha}{B_\alpha^2}$$

for $\alpha \in \mathcal{O} \setminus \{0\}$. This defines an $\mathcal{O} \setminus \{0\}$-indexed set $(B_\alpha)_\alpha$, which we call an *elliptic divisibility sequence with complex multiplication.*

Example 1.1. For any non-zero $a \in \mathbb{C}$, let E be the elliptic curve given by $y^2 = x^3 + ax$ as in Example 4.4 of Chapter II. Then E has complex multiplication by $\mathbb{Z}[i]$ via $[i](x, y) = (-x, iy)$. Table 5 on page 53 gives an example of a sequence defined by a curve of this form.

If L does not contain K, then there is a non-trivial automorphism of KL/L. The following lemma shows how elliptic sequences behave with respect to such an automorphism.

Lemma 1.2. *For every non-zero $\alpha \in \mathcal{O}$ and every automorphism σ of KL/L,*

$$B_{\sigma(\alpha)} = \sigma(B_\alpha)$$

Proof. Both E and P are defined over L, hence fixed by σ, so the statement is a special case of Lemma 4.2 of Chapter II. □

The theory of formal groups in Chapter III gives us the following two important results.

Lemma 1.3. *For all $\alpha, \beta \in \mathcal{O}$, if $\alpha|\beta$, then $B_\alpha|B_\beta$.*

Proof. Let v be any discrete valuation of M. and let $n = v(B_\alpha)$. Then $[\alpha]P \in E_n(M_v)$, which is an $\mathcal{O}$-module by Lemma 4.14 of Chapter III.

If $\alpha|\beta$, then $[\beta]P$ is also in that $\mathcal{O}$-module, which proves that $v(B_\beta) \geq n$. □

Lemma 1.4. *For any discrete valuation v of M, let $p \in \mathbb{N}$ be the prime with $\mathfrak{p}|p$. Then for all non-zero $\alpha, \beta \in \mathcal{O}$, if $v(B_\alpha) > v(p)/(p-1)$, then*

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

Proof. This is Proposition 3.8 of Chapter III, together with the fact that $[\beta]^*\omega = \beta\omega$ (Proposition 4.1 of Chapter II). □

For the problematic primes with $e(\mathfrak{p}/p) \geq p - 1$, we will give an asymptotic version later (Lemma 2.5).

2 Divisible sequences indexed by rings of integers

In this section, we look at sequences that are indexed by the ring of integers of a number field and satisfy the divisibility property $\alpha|\beta \Rightarrow B_\alpha|B_\beta$. It turns out that it is natural to have them indexed by ideals. We will define what it means for an ideal-indexed sequence to be strongly divisible and we will define primitive divisors of such a sequence.

In the case of elliptic divisibility sequences, for any ideal $\mathfrak{a}$, we will later define actual points $[\mathfrak{a}]P$ so that we can give the estimates involving heights that are needed for the Zsigmondy theorem. We will do this in Section 5.

α	B_α	D_α^{CM}	$D_\alpha^{\mathbb{N}}$
1	1	1	1
$1+i$	$1+i$	$1+i$	
2	$2=(1+i)^2$	1	2
$2+i$	$2-i$	$2-i$	
$2+2i$	$3(1+i)^3$	3	
3	$13=(3+2i)(3-2i)$	$(3+2i)(3-2i)$	13
$3+i$	$(1+i)(2+i)(4-i)$	$4-i$	
$3+2i$	$(5+4i)(6-i)$	$(5+4i)(6-i)$	
$3-3i$	$(1+i)(3+2i)(3-2i)$	1	
4	$84=(1+i)^4\cdot 3\cdot 7$	7	21
$4+i$	$(5-2i)(14-i)$	$(5-2i)(14-i)$	
$4+2i$	$(1+i)^2(4+i)(2-i)(16+9i)$	$16+9i$	
$4+3i$	$(2+i)(14-9i)(32+23i)$	$(14-9i)(32+23i)$	
$4-4i$	$(1+i)^5\cdot 3\cdot 7(8+7i)(8-7i)$	$(8+7i)(8-7i)$	
5	$(2+i)^2(2-i)^2(6+5i)(6-5i)$	$(6+5i)(6-5i)$	1525
$5+i$	$(1+i)(6+i)(5-4i)(31-20i)$	$31-20i$	
$5+2i$	$(11+4i)(2+7i)(40+17i)$	$(11+4i)(2+7i)(40+17i)$	
$5+3i$	$(1+i)(14+i)(5+2i)(159-40i)$	$159-40i$	
$5+4i$	$(17-10i)(27-2i)(173+172i)$	$(17-10i)(27-2i)(173+172i)$	
$5-5i$	$\begin{pmatrix}(1+i)(2+i)(2-i)(4+i)\\(4-i)(6+5i)(6-5i)\cdot 79\end{pmatrix}$	79	

α	$\log\lvert B_\alpha\rvert$	$\log\lvert D_\alpha^{\mathrm{CM}}\rvert$	$\log\lvert D_\alpha\rvert$
6	8.7345601	5.4764636	5.4764636
7	14.587939	14.587939	14.587939
8	18.834415	8.9830633	13.710451
9	24.470944	21.905994	21.905994
10	30.052763	9.0071220	22.029866
11	36.574559	36.574559	36.574559
12	42.286454	19.959874	28.715612
13	51.095908	43.771418	51.095908
14	58.845276	28.884879	43.564190
15	68.283492	38.092377	58.388793
16	77.562001	38.648214	58.034439
17	87.731841	79.081341	87.731841
18	97.456309	43.811288	66.815755
19	109.52561	109.52561	109.52561
20	120.70842	37.540767	86.917990
21	134.00371	116.85082	116.85082
22	146.96000	73.412035	109.69229
23	160.79929	160.79929	160.79929
24	174.41374	78.638952	117.72369
25	189.87781	122.68541	180.93862
26	204.38755	86.491875	152.59850
27	221.63325	197.16230	197.16230
28	238.24699	115.22917	173.71813
29	255.77504	239.34097	255.77504
30	273.21161	78.612647	176.72864

Table 5: This is the same example from Table 3 on page 36: $E: y^2 = x^3 - 2x$, $P = (-1, 1)$. The curve E has CM by $\mathbb{Z}[i]$ via $[i](x, y) = (-x, iy)$. D_α^{CM} is the part of B_α that is coprime to all B_β with $\beta|\alpha$, $(\beta) \neq (\alpha)$, while $D_m^{\mathbb{N}}$ is the primitive part of the sequence $B_1, B_2, B_3, \ldots \in \mathbb{Z}$. It is clear in this example that $B_{u\alpha} = B_\alpha$ for $u \in \{\pm 1, \pm i\}$ and Lemma 1.2 says that $B_{\overline{\alpha}} = \overline{B_\alpha}$.

2.1 Divisibility

Let K, M be any pair of number fields. Let $\mathcal{O}_K$ be the ring of integers of K and let $I(K)$ be the set of non-zero ideals of $\mathcal{O}_K$.

Definition. If $\mathcal{I}$ is either $I(K)$ or $\mathcal{O}_K$, then we say that an $\mathcal{I}$-indexed sequence $B = \{B_i\}_{i\in\mathcal{I}}$ of M-ideals is *divisible* if for all $i, j \in \mathcal{I}$,

$$i|j \quad \Longrightarrow \quad B_i|B_j.$$

If an $\mathcal{O}_K$-indexed sequence B is divisible, then it makes sense to make it into an $I(K)$-indexed sequence as follows:

Definition. Suppose that B is a divisible $\mathcal{O}_K$-indexed sequence. Let the *induced $I(K)$-indexed sequence*, also denoted B, be defined by

$$B_{\mathfrak{a}} = \langle B_x : x \in \mathfrak{a} \rangle .$$

Notice that for any discrete valuation v and any ideal J of any number field, we have $v(J) = \min_{y\in J} v(y)$, so the above definition of $B_{\mathfrak{a}}$ is equivalent to

$$v(B_{\mathfrak{a}}) = \min_{x\in\mathfrak{a}} v(B_x) \quad \text{for all } v.$$

The induced sequence is divisible by definition. Also, because the old B was divisible, we have $B_{(x)} = B_x$ for all $x \in \mathcal{O}_K$.

Definition. We say that an $I(K)$-indexed sequence B is *strongly divisible* if for every pair $\mathfrak{a}, \mathfrak{b}$, we have

$$B_{(\mathfrak{a},\mathfrak{b})} = (B_{\mathfrak{a}}, B_{\mathfrak{b}}). \tag{12}$$

Clearly every strongly divisible sequence is divisible.

Lemma 2.1. *Let B be a divisible $\mathcal{O}_K$-indexed sequence of M-ideals. If for every discrete valuation v of M and all $x, y \in \mathcal{O}_K$, we have*

$$v(B_{x+y}) \geq \min\{v(B_x), v(B_y)\}, \tag{13}$$

then the induced ideal-indexed sequence is strongly divisible. In that case, it is the unique interpolation of B to a strongly divisible $I(K)$-indexed sequence.

In particular this is true for elliptic divisibility sequences with complex multiplication.

Proof. Let $\mathfrak{a}, \mathfrak{b} \in I(K)$ be any pair of ideals. Then $B_{(\mathfrak{a},\mathfrak{b})}|(B_{\mathfrak{a}}, B_{\mathfrak{b}})$ by the divisibility property. On the other hand, for any discrete valuation v,

$$v(B_{(\mathfrak{a},\mathfrak{b})}) = \min_{z\in(\mathfrak{a},\mathfrak{b})} v(B_z)$$

and any $z \in (\mathfrak{a}, \mathfrak{b})$ is of the form $z = x + y$ with $x \in \mathfrak{a}, y \in \mathfrak{b}$. But then by assumption,

$$\begin{aligned} v(B_z) &\geq \min\{v(B_x), v(B_y)\} \\ &\geq \min\{v(B_{\mathfrak{a}}), v(B_{\mathfrak{b}})\} = v((B_{\mathfrak{a}}, B_{\mathfrak{b}})). \end{aligned}$$

Therefore, for any v, we have $v(B_{(\mathfrak{a},\mathfrak{b})}) \geq v((B_\mathfrak{a}, B_\mathfrak{b}))$.

As every ideal is generated by two elements, any strongly divisible $I(K)$-indexed sequence that interpolates B is completely determined by (12).

Notice that (13) holds for elliptic divisibility sequences, because $E_r(M_v) = \{P \in E(M_v) : v(x(P)) \leq -2r\}$ is a group for all $r \geq 1$ (see Lemma 2.3 of Chapter III). □

Because of this lemma, we may think of elliptic divisibility sequences with complex multiplication as sequences that are indexed by the non-zero ideals of $\mathcal{O}$.

2.2 Results for the ideal-indexed sequence

In this section, we generalize Lemma 1.4 about orders of primes in elliptic divisibility sequences to the ideal-indexed sequence and we give an asymptotic version for problematic primes.

Lemma 2.2. *For any discrete valuation v of M, let $p \in \mathbb{N}$ be the prime such that $v(p) > 0$. Then for all non-zero $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}$, if $v(B_\mathfrak{a}) > \frac{v(p)}{p-1}$, then*

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

Proof. We claim

$$v(B_{\mathfrak{ab}}) \quad = \quad \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}). \tag{14}$$

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

$$\begin{aligned} v(B_{\mathfrak{ab}}) &= \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} (v(B_\alpha) + v(\beta)) \\ &= \min_{\alpha\in\mathfrak{a}} v(B_\alpha) + \min_{\beta\in\mathfrak{b}} v(\beta) \\ &= v(B_\mathfrak{a}) + v(\mathfrak{b}). \end{aligned}$$

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

$$v(B_x) \geq \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}),$$

which proves "$\geq$". □

For the "problematic" valuations with $v(p) \geq p - 1$, we give some lemmas that show that this result "almost" holds with the weaker condition $v(B_\mathfrak{a}) > 0$.

Lemma 2.3. *For all non-zero $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$, if $v(B_\mathfrak{a}) > 0$, then*

$$v(B_{\mathfrak{ab}}) \geq v(B_\mathfrak{a}).$$

Furthermore, we have equality if and only if $v(\mathfrak{b}) = 0$.

Proof. The inequality $\geq$ is the divisibility property, which we already know to be true. Let $n = v(B_{\mathfrak{a}})$ and let $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ such that $v(\mathfrak{p}) > 0$.

First, suppose that $v(\mathfrak{b}) > 0$. Let $\gamma = \alpha_1\beta_1 + \cdots + \alpha_r\beta_r$ be any element of $\mathfrak{ab}$, where $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$. We need to show that $[\gamma]P \in E_{n+1}(M_v)$, so it suffices to show that this holds for $\gamma = \alpha_i\beta_i$. Notice that $v(\beta_i) > 0$, so β_i becomes zero in the residue field k of the local field M_v. But Lemma 4.14 of Chapter III states that $E_n(M_v)/E_{n+1}(M_v) \cong k$ as $\mathcal{O}$-modules, so $[\beta_i][\alpha_i]P \in E_{n+1}(M_v)$, which is what we needed to show.

Now there remains the case where $v(\mathfrak{b}) = 0$. In that case, $\mathfrak{p} \nmid \mathfrak{b}$ and $\mathfrak{p}$ is prime, so $\mathfrak{p}$ and $\mathfrak{b}$ are coprime. Therefore, there are $x, y \in \mathcal{O}$, $\beta \in \mathfrak{b}, \delta \in \mathfrak{p}$ such that $x\beta + y\delta = 1$. Let $\alpha \in \mathfrak{a}$ be such that $v(B_\alpha) = v(B_{\mathfrak{a}}) = n$. Then $[\alpha]P$ is not in $E_{n+1}(M_v)$, so

$$O \not\equiv [\alpha]P = [(x\beta + y\delta)][\alpha]P \equiv [x\beta][\alpha]P \mod E_{n+1}(M_v),$$

so $[\alpha\beta]P$ is not in $E_{n+1}(M_v)$, which proves that $v(B_{\mathfrak{ab}}) \leq n$. □

We now have all the ingredients that we need in order to proceed as in the proof of Lemma 4.3 of Chapter IV:

Lemma 2.4. *For every non-zero $\mathcal{O}$-ideal $\mathfrak{a}$, if $v(B_{\mathfrak{a}}) > 0$, then*

$$v(B_{\mathfrak{a}}) = v(\mathfrak{a}) + O(1). \tag{15}$$

Proof. Let $\mathfrak{r}$ be the ideal consisting of all $\alpha \in \mathcal{O}$ such that $v(B_\alpha) > 0$. Then the assumption $v(B_{\mathfrak{a}}) > 0$ is equivalent to $\mathfrak{r}|\mathfrak{a}$.

Let $\mathfrak{p}$ be the unique prime of $\mathcal{O}$ such that $v(\mathfrak{p}) > 0$. By the equality in Lemma 2.3, both sides of (15) do not change if we multiply $\mathfrak{a}$ by something which is coprime to $\mathfrak{p}$. Therefore, we may assume that $\mathfrak{a}$ is of the form $\mathfrak{r}\mathfrak{p}^l$ for some non-negative integer l.

Let $k > v(p)/(p-1)$ be an integer. Then by repeated use of the inequality in Lemma 2.3, we find that $v(B_{\mathfrak{r}\mathfrak{p}^k}) > v(p)/(p-1)$. Therefore, by Lemma 2.2, if $l \geq k$, then

$$v(B_{\mathfrak{r}\mathfrak{p}^l}) = v(B_{\mathfrak{r}\mathfrak{p}^k}) + v(\mathfrak{p}^{l-k}) = v(\mathfrak{r}\mathfrak{p}^l) + O(1),$$

and only the finitely many cases where $l < k$ remain. □

In particular, Lemma 2.2 with the weaker condition $v(B_{\mathfrak{a}}) > 0$ holds up to $O(1)$. In other words,

Lemma 2.5. *For all non-zero $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$, if $v(B_{\mathfrak{a}}) > 0$, then*

$$v(B_{\mathfrak{ab}}) = v(B_{\mathfrak{a}}) + v(\mathfrak{b}) + O(1).$$

□

2.3 The primitive part

Let B be a strongly divisible $I(K)$-indexed sequence of M-ideals. We call a prime $\mathfrak{p}$ of M a *primitive divisor of* $B_\mathfrak{a}$ if it divides $B_\mathfrak{a}$, but does not divide $B_\mathfrak{b}$ for any $\mathfrak{b}|\mathfrak{a}$ with $\mathfrak{b} \neq \mathfrak{a}$. By the *primitive part of* $B_\mathfrak{a}$, we mean the ideal $D_\mathfrak{a}|B_\mathfrak{a}$ such that $D_\mathfrak{a}$ is a product of only primitive divisors of $B_\mathfrak{a}$, while $B_\mathfrak{a}/D_\mathfrak{a}$ is not divisible by any primitive divisors of $B_\mathfrak{a}$.

Notice that the primitive part of an $I(K)$-indexed sequence may differ from the primitive part of the underlying $\mathbb{N}$-indexed sequence, because a prime may be primitive at n for the $\mathbb{N}$-indexed sequence, but divide some B_α with $\alpha|n$ and $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. If we denote the primitive part of the $I(K)$-indexed sequence by D_α^{CM} and the primitive part of the $\mathbb{N}$-indexed sequence by $D_\alpha^{\mathbb{N}}$, then $D_\alpha^{CM}|D_\alpha^{\mathbb{N}}$. See Table 5 on page 53 for an example.

Notice that $\mathfrak{p}$ is primitive for at most one ideal $\mathfrak{a}$, because if $\mathfrak{p}|B_\mathfrak{a}$ and $\mathfrak{p}|B_\mathfrak{b}$, then the strong divisibility property implies $\mathfrak{p}|B_{(\mathfrak{a},\mathfrak{b})}$. By the *rank of apparition* of $\mathfrak{p}$, we will mean the unique ideal $\mathfrak{r}_\mathfrak{p}$ such that $\mathfrak{p}$ is a primitive divisor of $B_{\mathfrak{r}_\mathfrak{p}}$. Then

$$\begin{aligned} \mathfrak{p}|B_\mathfrak{a} &\iff \mathfrak{r}_\mathfrak{p}|\mathfrak{a} \\ \mathfrak{p}|D_\mathfrak{a} &\iff \mathfrak{r}_\mathfrak{p} = \mathfrak{a} \qquad \text{and} \end{aligned}$$

$$v(D_\mathfrak{a}) = \begin{cases} v_\mathfrak{p}(B_\mathfrak{a}) & \text{if } \mathfrak{a} = \mathfrak{r}_\mathfrak{p} \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

Notice that in the case of an elliptic divisibility sequence, every prime divides some $B_\mathfrak{a}$. (See Lemma 2.10 of Chapter III).

3 Generalization of parts of the classical Zsigmondy proof

We will now try to imitate the classical proof of Zsigmondy's theorem for elliptic divisibility sequences when the sequence is indexed by $\mathcal{O} \cong \mathrm{End}(E)$.

We will run into some difficulties, but still get some results that we can use in the successful proof in Section 6.

The height

We will use the following generalization of $\widehat{h}([m]P) = m^2\widehat{h}(P)$:

Lemma 3.1. *Given an isogeny $\phi : E \to E'$. For any point $P \in E(\overline{\mathbb{Q}})$,*

$$\widehat{h}(\phi(P)) = \deg(\phi)\widehat{h}(P).$$

Corollary 3.2. *For every $\alpha \in \mathcal{O}$,*

$$\widehat{h}([\alpha]P) = |\alpha|^2\ \widehat{h}(P).$$

Proof of the lemma. Recall that the canonical height is defined by

$$\widehat{h}(P) = \frac{1}{\deg f} \lim_{N\to\infty} 4^{-N} h_f(2^N P),$$

where $f \in M(E)$ is any non-constant even function. The coordinate function x is an even function and isogenies are group homomorphisms, so $x \circ \phi \circ [-1] = x \circ [-1] \circ \phi = x \circ \phi$, so $x \circ \phi$ is also an even function. Therefore,

$$\begin{aligned}
\widehat{h}(\phi(P)) &= \frac{1}{\deg x} \lim_{N\to\infty} 4^{-N} h_x([2^N]\phi(P))) \\
&= \frac{1}{\deg x} \lim_{N\to\infty} 4^{-N} h_{x\circ\phi}([2^N]P) \\
&= \frac{\deg(x\circ\phi)}{\deg x} \widehat{h}(P) \\
&= \deg\phi \ \ \widehat{h}(P).
\end{aligned}$$

□

Proof of the corollary. $[\deg[\alpha]] = [\alpha]\widehat{[\alpha]} = [\alpha\overline{\alpha}] = [|\alpha|^2]$. □

The bounds

The asymptotic bounds for $h_x([\alpha]P)$ thus become,

$$h_x([\alpha]P) = 2|\alpha|^2 \ \widehat{h}(P) + O(1), \tag{17}$$

so Lemma 4.3 of Chapter V turns into

$$(1 - o(1))|\alpha|^2\widehat{h}(P) \le \log|B_\alpha| \le |\alpha|^2 \ \widehat{h}(P) + O(1). \tag{18}$$

This already allows us to prove the following, of which we will give a stronger version later.

Lemma 3.3. *Suppose that $\mathcal{O}$ is a PID. If we replace P by a large enough multiple, then for all $\alpha, \beta \in \mathcal{O} \setminus \{0\}$,*

$$B_\alpha | B_\beta \quad \Longleftrightarrow \quad \alpha|\beta$$

Proof. By (18), there is an M such that for all α with $|\alpha| > M$,

$$(3/4)|\alpha|^2\widehat{h}(P) \le \log|B_\alpha| \le (5/4)|\alpha|^2\widehat{h}(P).$$

Replace P by MP. Then $\widehat{h}(P)$ gets replaced by $\widehat{h}(MP) = M^2\widehat{h}(P)$, so we have for every α, $(3/4)|\alpha|^2\widehat{h}(P) \le \log|B_\alpha| \le (5/4)|\alpha|^2\widehat{h}(P)$.

So let's prove the assertion when P is replaced by MP. We have already seen the implication to the left. So suppose that $B_\alpha | B_\beta$ and let $\delta = (\alpha, \beta)$. By the strong divisibility property, $B_\delta = (B_\alpha, B_\beta) = B_\alpha$. If $\delta \neq \alpha$, then $|\delta|^2 \le |\alpha|^2/2$, so $\log|B_\delta| \le (5/4)|\delta|^2\widehat{h}(P) \le 5/8|\alpha|^2\widehat{h}(P) < \log|B_\alpha|$, which contradicts $B_\alpha = B_\delta$. Hence α is equal to δ, which divides β. □

If we assume that $\mathcal{O}$ is a PID and we would use the same estimates as in the non-CM case, then we would get

$$\log|D_\alpha| \geq \Big(1 - o(1) - \sum_{\mathfrak{p}|\alpha} |\mathfrak{p}|^{-2}\Big)|\alpha|^2\widehat{h}(P). \tag{19}$$

Now this is the place where the proof of Chapter V breaks down: As primes can be split in K, there are too many primes with small norm. For example, if $K = \mathbb{Q}(i)$ and $30|\alpha$, then $1+i, 2+i, 2-i$ and 3 are prime divisors of α, so $\sum_{\mathfrak{p}|\alpha} |\mathfrak{p}|^{-2} \geq \frac{1}{2} + \frac{1}{9} + \frac{1}{5} + \frac{1}{5} > 1$, which makes the estimates useless. Therefore, a single inclusion is insufficient and we will need to go all the way with the inclusion-exclusion principle.

Heuristics

Let μ be the Möbius function for the set of integral ideals of $\mathcal{O}$:

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

Let's see what we can get from the inclusion-exclusion principle in a simplified situation. Assume that $\mathcal{O}$ is a PID and ignore the $o(1)$'s and $O(1)$'s, as well as the fact that non-primitive divisors sometimes have a higher order in later terms than in earlier terms. Then we get the estimate

$$B_\alpha \sim \prod_{(\beta)|\alpha} D_\beta.$$

Using the inclusion-exclusion principle, this yields

$$\begin{aligned} \log|D_\alpha| &\sim \sum_{(\beta)|\alpha} \mu(\alpha/\beta)\log|B_\beta| \\ &\sim \sum_{(\beta)|\alpha} \mu(\alpha/\beta)|\beta|^2\widehat{h}(P) \\ &\sim (\sum_{(\beta)|\alpha} \mu(\beta)|\beta|^{-2})|\alpha|^2\widehat{h}(P) \end{aligned}$$

and we will show in Lemmas 6.3 and 6.4 that this grows very fast.

In order to make this proof work, we will need some more explicit $o(1)$ functions in (18), because the inclusion-exclusion principle gives an extra $o(1)$ for every inclusion. We will use a theorem of David to get more explicit bounds in the next section.

Also, an inclusion-exclusion argument is tricky if there is no unique factorization. This is another reason why it is convenient to have the sequence indexed by ideals. In order to be able to use the ideal-indexed sequence, we will need estimates for them as well. We will get them in Section 5.

4 David's Theorem

We want to have explicit $o(1)$-functions in our estimate (18), but unfortunately they do not follow from the classical proof of Siegel's theorem. Therefore, we will use David's theorem instead, which is the elliptic curve analogue of Baker's theorem ([Bak66]–[Bak68]).

Baker's theorem gives explicit lower bounds for linear forms in logarithms of algebraic numbers. The logarithmic map is the inverse of the exponential map and in the same way, we call the inverse of the isomorphism $\mathbb{C}/\Lambda \to E(\mathbb{C})$ the *elliptic logarithm*. David's theorem gives explicit lower bounds for linear forms in *elliptic* logarithms of algebraic points on elliptic curves.

4.1 Archimedean v-adic distance and the distance on the torus

By a linear change of coordinates, we can give a model for our elliptic curve of the form

$$E : Y^2 = 4X^3 - g_2X - g_3. \tag{20}$$

An archimedean valuation v corresponds to an embedding of M in $\mathbb{C}$ by Ostrowski's Theorem [Neu92] II.4.2. Using this embedding, we find a lattice Λ and a Weierstrass function $\wp$ as in Section 3 of Chapter II. Let $\mathcal{P}$ be a fundamental parallelogram of Λ with 0 as an interior point and let z_0 be the point in $\mathcal{P}$ corresponding to $P \in E(M)$. Notice that X corresponds to the elliptic function $\wp(z)$ on $\mathbb{C}/\Lambda$, so

$$X([\alpha]P) = \wp(\alpha z + \omega) \quad \text{for all } \alpha \in \mathcal{O}, \omega \in \Lambda.$$

The function $\wp$ has a pole of order 2 at 0 and no other poles on the closure of $\mathcal{P}$, so $z^2\wp(z)$ is a holomorphic function on $\mathcal{P}$, hence bounded. Therefore,

$$\log|\wp(z)|_v = -2\log|z+\omega| + O(1) \tag{21}$$

for all $z \in \mathbb{C}$ and $\omega \in \Lambda$ such that $z + \omega \in \mathcal{P}$. This relates the v-adic distance from P to O on E to the distance from z to Λ in $\mathbb{C}$.

4.2 David's Theorem

The notation for David's theorem is as follows. Let $E/\mathbb{C}$ be an elliptic curve, given by the equation

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_2 \in \overline{\mathbb{Q}}.$$

Let Λ be the associated period lattice and $\wp$ the associated Weierstrass function. Let $M \subset \mathbb{C}$ be a number field, containing g_2 and g_3.

Let the height functions H and $h = \log H$ on $\mathbb{P}^N(\overline{\mathbb{Q}})$ and $\overline{\mathbb{Q}} \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ be defined as in Section 3 of Chapter V.

Let k be a positive integer and for $i = 1, 2, \ldots, k$, let $u_i \in \mathbb{C}$ be an elliptic logarithm of an M-valued point P_i (i.e. u_i is a complex number such that $P_i = (\wp(u_i), \wp'(u_i)) \in E(M)$).

Theorem 4.1 (David)**.** *With the above notation, let $L = \beta_1 u_1 + \cdots + \beta_k u_k$ with $\beta_j \in M$. Then there is a constant F such that for all $\beta_1, \ldots, \beta_k \in M$, if $B = \max_i\{H(\beta_i)\}$ is large enough and $L \neq 0$, then*

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

Proof. This is a special case of [Dav95] Théorème 2.1. □

Remark 4.2. David's theorem actually gives explicit bounds:

Let ω_1, ω_2 be a pair of generators for Λ, such that $\tau = \frac{\omega_2}{\omega_1}$ is in the usual fundamental domain

$$\mathcal{F} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0, -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1\}$$

for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane.

Let the height $h(E)$ of the curve E be defined by

$$h(E) = \max\{1, h(1 : g_2 : g_3), h(j(E))\}.$$

Let the canonical height function $\widehat{h}$ on $E(M)$ be defined as in section Section 3 of Chapter V and let

$$\begin{aligned} D &= [M : \mathbb{Q}], \\ \log(V) &= \max\left\{\widehat{h}(P_i), h(E), \frac{3\pi|u_i|^2}{|\omega_1|^2 \mathrm{Im}(\tau) D}\right\}, \\ C &= 2.9 \cdot 10^6 \cdot 10^{6k} \cdot 4^{2k^2} \cdot (k+1)^{2k^2+9k+12.3} \quad \text{and} \\ F &= C\ D^{2k+2}\ (\log V)^k (1+\epsilon)^{k+2}. \end{aligned}$$

Then F suffices and B is large enough if

$$\begin{aligned} B &\geq \max\{V^{1/D}, \exp(eh(E))\} \quad \text{and} \\ \log\log B &\geq \frac{1}{\epsilon}(h(E) + \log D). \end{aligned}$$

Now let M be any number field and E/M an elliptic curve with complex multiplication by a subring $\mathcal{O}$ of M.

Proposition 4.3. *Let v be any archimedean valuation of M and $P \in E(M)$ any M-valued non-torsion point. Then there is a constant G such that for all $\alpha \in \mathcal{O}$ with $|\alpha|$ large enough,*

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

Proof. It suffices to prove this after a linear transformation, so assume that E is given by a classical Weierstrass equation (20). Embed M into $\mathbb{C}$ in such a way that the absolute value on $\mathbb{C}$ corresponds to $|\cdot|_v$. Then it suffices to prove the result for the absolute value on $\mathbb{C}$.

Let $\{u_1, u_2\}$ be a basis for the lattice Λ that corresponds to E and let $u_3 \in \mathbb{C}$ be an elliptic logarithm of P, i.e. an element of $\mathbb{C}$ such that $(\wp(u_3), \wp'(u_3)) = P$. Let $\mathcal{P}$ be the fundamental parallelogram $\{t_1u_1 + t_2u_2 : -\frac{1}{2} \leq t_i < \frac{1}{2}\}$.

For any $\alpha \in \mathcal{O}$, let $b_3 = \alpha$ and let $b_1, b_2 \in \mathbb{Z}$ be such that $L = b_1u_1 + b_2u_2 + \alpha u_3 \in \mathcal{P}$. Then $x([\alpha]P) = \wp(L)$, so by (21), $\log|x([\alpha]P)| = \log|\wp(L)| \leq -2\log|L| + C_1$, for some constant C_1. Therefore,

$$\begin{aligned}\log|x([\alpha]P)| &\leq -2\log|L| + C_1 \\ &< 2F\log(B)(\log\log(B))^4 + C_1\end{aligned}$$

if B is large enough.

We know that the field of fractions K of the endomorphism ring $\mathcal{O}$ has a unique archimedean valuation. Therefore, for $b = b_i$, we have $H(b)^{[K:\mathbb{Q}]} = \prod_{v\in M_K}\max\{|b|_v, 1\} = \prod_{v\in M_K^\infty}|b|_v^{e_v} = |b|^{[K:\mathbb{Q}]}$, hence $B = \max\{|b_1|, |b_2|, |\alpha|\}$. Also, b_1u_1 is the integer multiple of u_1 that is nearest to αu_3 projected on $u_1\mathbb{R}$, so $|b_1|$ is bounded by a linear function of $|\alpha|$ and the same holds for $|b_2|$. □

This gives us the following estimates for $\log||B_\alpha||$:

Corollary 4.4.

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

Proof. Recall Lemma 4.2 of Chapter V:

$$\log||\mathrm{den}(x)|| = \; h(x) - \sum_{v\in M_L^\infty}\frac{n_v}{[L:\mathbb{Q}]}\log\max\{|x|_v, 1\}.$$

If we apply the above proposition to each of the finitely many terms in the sum, then we get the desired result. □

Remark 4.5. The exponent 4 in Proposition 4.3 is not always optimal. In the following two cases, we may replace it by 3. For the sake of generality, and because it makes little difference, we will not use this later.

1. The embedding $M \subset \mathbb{C}$ is real and $\alpha = n \in \mathbb{Z}$,
2. E has complex multiplication by an order in $K \neq \mathbb{Q}$.

Proof. In the proof of Proposition 4.3, do the following:
1. Pick u_1 to be the fundamental real period and omit u_2. Let $E_0(\mathbb{R})$ be the connected component of $E(\mathbb{R})$ that contains the point at infinity. Then u_1 is obtained by integrating the invariant differential along $E_0(\mathbb{R})$.

The set $E_0(\mathbb{R})$ corresponds to the set $\mathbb{R}/u_1\mathbb{Z}$, because $\int_O^P\omega$ could be calculated by integrating along $E_0(\mathbb{R})$, which results in real numbers. Therefore, $E_0(\mathbb{R})$ is a subgroup of $E(\mathbb{R})$. Clearly x is bounded on the complement of $E_0(\mathbb{R})$, so if P has order m in $E(\mathbb{R})/E_0(\mathbb{R})$, then it suffices to prove the proposition with P replaced by mP.

So suppose that $P \in E_0(\mathbb{R})$. Then we can take $u_2 \in \mathbb{R}$ such that $P = (\wp(u_2), \wp'(u_2))$. Then for any $\alpha = n \in \mathbb{Z}$, let $b \in \mathbb{Z}$ be such that $L = bu_1 + nu_2 \in [-\frac{1}{2}u_2, \frac{1}{2}u_2]$. Then the estimates in the proof of Proposition 4.3 become

$$\log|x(nP)| < G\log(n)(\log\log(n))^3$$

for large enough n.
2. Let $a \in \mathbb{C}, \mathfrak{a} \subset \mathcal{O}$ be such that $\Lambda = a\mathfrak{a}$. Let $u_1 = a$, then $\Lambda \subset \mathcal{O}u_1$. Let $u_2 \in \mathbb{C}$ be such that $(\wp(u_2), \wp'(u_2)) = P$. This time, we allow b to range through $\mathfrak{a} \subset \mathcal{O}$. Then bu_1 ranges through Λ. Then we get

$$\log|x([\alpha]P)| < 2F(\log(B)(\log\log(B))^3 + C_1$$

for large enough B, where $B = \max\{|b|, |\alpha|\}$. And now the triangle inequality tells us that $|bu_1| \leq R + |\alpha u_2|$, where R is an upper bound for $|\cdot|$ on a fundamental domain for Λ. This gives us linear upper bounds for $|b|$ in terms of $|\alpha|$. □

David's theorem gives lower bounds for the logarithmic distance to the lattice, but it needs the fact that the points and curves are defined over number fields. This is crucial, because the following argument shows that on any elliptic curve $E/\mathbb{C}$, we can construct a point $P \in E(\mathbb{C})$ for which even Siegel's Theorem $\frac{\log|x(nP)|}{n^2} \to 0$ does not hold.

Lemma 4.6. *Let $g : \mathbb{N} \to \mathbb{R}$ be any function such that $g(n) > 0$ for all n. Then there is a real number $u \in \mathbb{R} \setminus \mathbb{Q}$ such that for infinitely many $m, n \in \mathbb{Z}$, $0 < |m + nu| < g(n)$.*

Corollary 4.7. *Let $f : \mathbb{N} \to \mathbb{R}$ be any function and let E be any elliptic curve, defined over $\mathbb{C}$. Then there is a non-torsion point $P \in E(\mathbb{C})$ such that for infinitely many $n \in \mathbb{Z}$, $|x(nP)| > f(n)$.*

Proof of Lemma 4.6. It suffices to prove the lemma for any smaller function g. So suppose that g is decreasing and $\lim_{n\to\infty} g(n) = 0$. Let $\widetilde{g}(n) = g(n)/n$. We construct a Cauchy sequence $\frac{m_j}{n_j}$ as follows. Let $m_1 = n_1 = 1$, and for any j let $n_{j+1} > 2^j/\widetilde{g}(n_j)$. Then there is an integer m_{j+1} such that $0 < |\frac{m_j}{n_j} - \frac{m_{j+1}}{n_{j+1}}| < 2^{-j}\widetilde{g}(n_j)$, so let m_{j+1} be such an integer. Then for any k, $|\frac{m_j}{n_j} - \frac{m_{j+k}}{n_{j+k}}| \leq |\frac{m_j}{n_j} - \frac{m_{j+1}}{n_{j+1}}| + \cdots + |\frac{m_{j+k-1}}{n_{j+k-1}} - \frac{m_{j+k}}{n_{j+k}}| < 2^{-j+1}\widetilde{g}(n_j)$, so the sequence is Cauchy. Let $-u$ be the limit. Then for all $j > 1$, $|m_j + n_j u| = n_j|\frac{m_j}{n_j} + u| = n_j \lim_{k\to\infty} |\frac{m_j}{n_j} - \frac{m_{j+k}}{n_{j+k}}| \leq n_j 2^{-j+1}\widetilde{g}(n_j) < g(n_j)$.

For any n, let m be such that $|m + nu|$ is minimal. If u is rational, then $|m + nu|$ is a periodic sequence in n, so it has a minimal non-zero value. This contradicts $g \to 0$, hence $u \in \mathbb{R} \setminus \mathbb{Q}$. □

Proof of the corollary. By changing f, we see that it suffices to prove the corollary with E given by a classical Weierstrass equation. Suppose that $\mathcal{P}$ is the fundamental domain given by $\{s\omega_1 + t\omega_2 : s, t \in [-\frac{1}{2}, \frac{1}{2}]\}$ for some pair of generators ω_1, ω_2 of Λ. Apply the lemma to $g(n) = \min\{\frac{1}{|\omega_1|}e^{-\frac{1}{2}(f(n)+C)}, \frac{1}{2}\}$, where C is larger than the $O(1)$ constants in (21). Pick $P = (\wp(u\omega_1), \wp'(u\omega_1))$.

There are infinitely many m, n such that $0 < |m + nu| < g(n)$ and for each n, there can only be one m, so there are infinitely many n. For each of them, the inequality $|m + nu| < g(n)$ implies $(m + nu)\omega_1 \in \mathcal{P}$, so equation (21) says that $\log x(nP) \geq -2\log|(m + nu)\omega_1| - C > -2\log(g(n)|\omega_1|) - C \geq f(n)$.

The point P is a torsion point if and only if u is rational, but $u \notin \mathbb{Q}$. □

5 Attaching points to the ideal-indexed sequence

The purpose of this section is to attach a point on an elliptic curve to $B_{\mathfrak{a}}$ in the case where $\mathfrak{a}$ is non-principal and to derive height estimates from this.

5.1 Elliptic curves over $\mathbb{C}$

Let $\Lambda \subset \mathbb{C}$ be a lattice such that $\mathbb{C}/\Lambda \cong E_{\mathbb{C}}$ and suppose that E has complex multiplication by the ring of integers $\mathcal{O}$ of $K \subset \mathbb{C}$.

Proposition 5.1. *Given two non-zero fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K,*

a. $\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$;

b. The elliptic curve $E_{\mathfrak{a}\Lambda}$ has complex multiplication by $\mathcal{O}$;

c. $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in the class group $\mathcal{C}l(K)$ of K.

Hence there is a well-defined action of the class group of K on the set of $\mathbb{C}$-isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$, determined by

$$\overline{\mathfrak{a}} * E_{\Lambda} \cong E_{\mathfrak{a}^{-1}\Lambda}.$$

Proof. [Sil94] II.1.2 □

For every ideal class $\overline{\mathfrak{a}}$, fix an elliptic curve $E_{\overline{\mathfrak{a}}}$ such that $E_{\overline{\mathfrak{a}}} \cong \overline{\mathfrak{a}} * E_{\Lambda}$. Let $E_{\overline{\mathcal{O}}} = E$. Notice that $\mathfrak{b}^{-1}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda$ for every pair of integral $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$, hence there is a natural map

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{b}^{-1}\Lambda & \to & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda \\ z & \mapsto & z, \end{array} \tag{22}$$

which induces an isogeny

$$E_{\mathfrak{b}^{-1}\Lambda} \to E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda}.$$

In turn, this induces an isogeny

$$[\mathfrak{a}] : E_{\overline{\mathfrak{b}}} \to E_{\overline{\mathfrak{a}\mathfrak{b}}}$$

up to the choices of isomorphisms $E_{\overline{\mathfrak{b}}} \cong E_{\mathfrak{b}^{-1}\Lambda}$ and $E_{\overline{\mathfrak{a}\mathfrak{b}}} \cong E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda}$. In other words, $[\mathfrak{a}]$ is defined up to composition with automorphisms of $E_{\overline{\mathfrak{b}}}$ and $E_{\overline{\mathfrak{a}\mathfrak{b}}}$. But automorphisms of an elliptic curve are of the form $[u]$, where $u \in \mathcal{O}^*$ and they 'commute' with isogenies in the following sense:

Proposition 5.2. *Let E_1, E_2 be elliptic curves with complex multiplication by $\mathcal{O}$ and let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi \quad \textit{for all } \alpha \in \mathcal{O}.$$

Proof. [Sil94] II.1.1.1 □

Therefore, the isogeny $[\mathfrak{a}] : E_{\overline{\mathfrak{b}}} \to E_{\overline{\mathfrak{ab}}}$ is defined up to composition with an automorphism of $E_{\overline{\mathfrak{ab}}}$.

Lemma 5.3. *If $\mathfrak{a} = (\alpha)$ is a principal ideal, then the new map $[\mathfrak{a}]$ is equal to $[\alpha]$ up to composition with an automorphism of $E_{\overline{\mathfrak{ab}}}$.*

Proof. The map $[\alpha]$ is defined by multiplication by α on $\mathbb{C}/\mathfrak{b}^{-1}\Lambda$. This is the same as (22) followed by multiplication by α as a map $\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda \longrightarrow \mathbb{C}/\mathfrak{b}^{-1}\Lambda$. □

Lemma 5.4. *We have multiplicativity in the sense that $[\mathfrak{a}\,] \circ [\mathfrak{b}] = [\mathfrak{ab}]$ up to automorphisms of the image curve.*

Proof. The trivial commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{c}^{-1}\Lambda & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{c}^{-1}\Lambda \\ & \searrow^{z\mapsto z} & \downarrow{\scriptstyle z\mapsto z} \\ & & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}^{-1}\Lambda \end{array}$$

induces a commutative diagram

$$\begin{array}{ccc} E_{\overline{\mathfrak{c}}} & \xrightarrow{[\mathfrak{b}]} & E_{\overline{\mathfrak{bc}}} \\ & \searrow^{[\mathfrak{ab}]} & \downarrow{\scriptstyle [\mathfrak{a}]} \\ & & E_{\overline{\mathfrak{abc}}} \end{array}$$

up to composition with automorphisms at any curve in the diagram. If we use Proposition 5.2, then we can move all the automorphisms to the lower right. □

5.2 Rationality

Let L be a number field such that each of the curves $E_{\overline{\mathfrak{a}}}$ is given by a Weierstrass equation with coefficients in the ring of integers $\mathcal{O}_L$ of L.

We can always choose $E_{\overline{\mathfrak{a}}}$ such that this is the case: If the endomorphism ring $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then the j-invariant of each of the curves $E_{\overline{\mathfrak{a}}}$, is algebraic over $\mathbb{Q}$ (see [Sil94] II.2.2.1) and $E_{\overline{\mathfrak{a}}}$ is defined over $\mathbb{Q}(j(E_{\overline{\mathfrak{a}}}))$ (see [Sil86] III.1.4c).

Remark 5.5. A more advanced part of the theory of complex multiplication tells us more about which field L we may take.

More precisely, [Sil94] II.4.3 shows that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$ (the class number of K) and the j-invariants of the elliptic curves $E_{\overline{\mathfrak{a}}}$ are exactly the $\mathrm{Gal}(\overline{K}/K)$ conjugates of the j-invariant of E.

Hence $\mathbb{Q}(j(E))/\mathbb{Q}$ has degree h_K, which is exactly the number of $\mathrm{Gal}(\overline{K}/K)$ conjugates of $j(E)$, so $L = \mathbb{Q}(j(E))$ contains all the j-invariants of the curves $E_{\overline{\mathfrak{a}}}$.

Next, [Sil94] II.2.2c says that for each pair of curves $E_{\overline{\mathfrak{a}}}$, $E_{\overline{\mathfrak{b}}}$ there is a finite extension L'/L such that every isogeny from $E_{\overline{\mathfrak{a}}}$ to $E_{\overline{\mathfrak{b}}}$ is defined over L'. Let M be a finite extension of L which contains each of the fields L' and the field K. For example, if K has class number 1, then there is only one curve, so we may take $M = KL$ by [Sil94] II.2.2b (also Corollary 4.3 of Chapter II).

Let $P \in E(L)$ be any non-torsion point. For every ideal $\mathfrak{a}$ of $\mathcal{O} = \mathcal{O}_K$, we find a point $[\mathfrak{a}]P \in E_{\overline{\mathfrak{a}}}(M)$ which is defined up to automorphism of $E_{\overline{\mathfrak{a}}}$. We can now define $\mathcal{A}'_{\mathfrak{a}}$ and $\mathcal{B}'_{\mathfrak{a}}$ to be the coprime $\mathcal{O}_M$-ideals such that

$$x([\mathfrak{a}]P) = \frac{\mathcal{A}'_{\mathfrak{a}}}{\mathcal{B}'^2_{\mathfrak{a}}}.$$

This equation defines $\mathcal{B}'_{\mathfrak{a}}$ independently of the choice of the automorphism of $E_{\overline{\mathfrak{a}}}$ as one can see from the explicit equations for automorphisms in *c.* and *d.* of Proposition 4.8 in Chapter III. Notice that $\mathcal{B}'_{\mathfrak{a}}$ *does* depend on the choice of the curve $E_{\overline{\mathfrak{a}}}$.

Notice that for all $\alpha \in \mathcal{O}$,

$$\mathcal{B}'_{(\alpha)} = B_\alpha.$$

5.3 Invariant differentials

As the space of invariant differentials is one-dimensional (see Corollary 2.2 of Chapter II), there are constants $a_{\mathfrak{a},\overline{\mathfrak{b}}}$ such that such that $[\mathfrak{a}]^*\omega_{\overline{\mathfrak{a}\mathfrak{b}}} = a_{\mathfrak{a},\overline{\mathfrak{b}}}\,\omega_{\overline{\mathfrak{a}}}$ for every ideal $\mathfrak{a}$ and every ideal class $\overline{\mathfrak{b}}$. We will now determine these constants.

First, we fix a representative $\widetilde{\mathfrak{d}}$ of each ideal class $\overline{\mathfrak{d}}$. Do this in such a way that the trivial class is represented by (1). Then we fix isomorphisms $E_{\overline{\mathfrak{d}}} \cong E_{\widetilde{\mathfrak{d}}^{-1}\Lambda}$ and denote by $f_{\overline{\mathfrak{d}}}$ the induced analytic isomorphism $\mathbb{C}/\widetilde{\mathfrak{d}}^{-1}\Lambda \to E_{\overline{\mathfrak{d}}}$. Notice that $f^*_{\overline{\mathfrak{d}}}$ sends the invariant differential on $E_{\overline{\mathfrak{d}}}$ to some multiple of the invariant differential dz on $\mathbb{C}/\mathfrak{d}^{-1}\Lambda$, say $c_{\overline{\mathfrak{d}}}dz$. Let $\mathfrak{c} = \mathfrak{a}\widetilde{\mathfrak{b}}$. Then the isogeny $[\mathfrak{a}]$ is defined (up to automorphism) by the commutative diagram

$$\begin{array}{ccccc}
\mathbb{C}/\widetilde{\mathfrak{b}}^{-1}\Lambda & \xrightarrow[z\mapsto z]{} & \mathbb{C}/\mathfrak{c}^{-1}\Lambda & \xrightarrow[z\mapsto(\mathfrak{c}/\widetilde{\mathfrak{c}})z]{\sim} & \mathbb{C}/\widetilde{\mathfrak{c}}^{-1}\Lambda \\
\downarrow{\scriptstyle f_{\overline{\mathfrak{b}}}} & & & & \downarrow{\scriptstyle f_{\overline{\mathfrak{c}}}} \\
E_{\overline{\mathfrak{b}}} & & \xrightarrow[[\mathfrak{a}]]{} & & E_{\overline{\mathfrak{c}}},
\end{array}$$

where $\mathfrak{c}/\widetilde{\mathfrak{c}}$ denotes a generator of the principal ideal $\mathfrak{c}/\widetilde{\mathfrak{c}}$. Therefore

$$[\mathfrak{a}]^*\omega_{\overline{\mathfrak{c}}} = c_{\overline{\mathfrak{b}}}^{-1} c_{\overline{\mathfrak{c}}} (\mathfrak{c}/\widetilde{\mathfrak{c}})\omega_{\overline{\mathfrak{b}}},$$

hence

$$a_{\mathfrak{a},\overline{\mathfrak{b}}} = c_{\overline{\mathfrak{b}}}^{-1} c_{\overline{\mathfrak{c}}} \widetilde{\mathfrak{b}}\widetilde{\mathfrak{c}}^{-1}\mathfrak{a}. \tag{23}$$

Notice that this implies that $c_{\overline{\mathfrak{b}}}^{-1} c_{\overline{\mathfrak{c}}}$ is an element of M.

For any ideal class $\overline{\mathfrak{d}}$, let the normalization constant $N_{\overline{\mathfrak{d}}}$ be the fractional M-ideal $N_{\overline{\mathfrak{d}}} = c_{\overline{\mathfrak{d}}}^{-1} c_1 \widetilde{\mathfrak{d}}$. Then

$$a_{\mathfrak{a},\overline{\mathfrak{b}}} = \frac{N_{\overline{\mathfrak{b}}}}{N_{\overline{\mathfrak{a}\mathfrak{b}}}}\mathfrak{a}. \tag{24}$$

Notice that $N_1 = 1$, so

$$a_{[\mathfrak{a}],1} = \frac{\mathfrak{a}}{N_{\overline{\mathfrak{a}}}}. \tag{25}$$

This suggests that we should put

$$\mathcal{B}_{\mathfrak{a}} := N_{\overline{\mathfrak{a}}}\mathcal{B}'_{\mathfrak{a}}.$$

Notice that $\mathcal{B}_{(\alpha)} = B_\alpha$.

Remark 5.6. One might wonder if it is possible to choose the curves $E_{\overline{\mathfrak{a}}}$ in such a way that the normalization constants $N_{\overline{\mathfrak{a}}}$ all become 1. We do not know the answer to this question.

A suggestion of a choice for which it seems fair that the constants are 1 is the following: Let σ run through the automorphisms of the extension $K(j(E))/K$. Then by [Sil94] II.4.3, the values of $\sigma(j(E))$ are exactly the j-invariants of the curves with CM by $\mathcal{O}$. Pick for each σ an extension to $\overline{L}$, then the curves E^σ form a full set of representatives for the isomorphism classes of elliptic curves with CM by $\mathcal{O}$.

We can prove that with a choice of curves such that $N_{\overline{\mathfrak{a}}} = 1$ for every $\overline{\mathfrak{a}}$ (if such a choice is possible), we would in fact have $B_{\mathfrak{a}} = \mathcal{B}_{\mathfrak{a}}$ for all $\mathfrak{a}$.

5.4 Results from the formal group

Next, the theory of formal groups tells us

Proposition 5.7. *Let $\mathfrak{p}|p$ be a prime of M and v the valuation at $\mathfrak{p}$. If*

$$v(\mathcal{B}_{\mathfrak{a}}) > \frac{v(p)}{p-1} + v(N_{\overline{\mathfrak{a}}}) \quad \textit{and} \quad v(\mathcal{B}_{\mathfrak{a}}) + v(\mathfrak{b}) > \frac{v(p)}{p-1} + v(N_{\overline{\mathfrak{a}\mathfrak{b}}}),$$

then

$$v(\mathcal{B}_{\mathfrak{a}\mathfrak{b}}) = v(\mathcal{B}_{\mathfrak{a}}) + v(\mathfrak{b}).$$

Proof. The assumptions are equivalent to $v(\mathcal{B}'_{\mathfrak{a}}) > \frac{v(p)}{p-1}$ and $v(\mathcal{B}'_{\mathfrak{a}}) + v(a_{[\mathfrak{b}],\overline{\mathfrak{a}}}) > \frac{v(p)}{p-1}$ by (24). Therefore, Proposition 3.8 of Chapter III says that

$$v(\mathcal{B}'_{\mathfrak{a}\mathfrak{b}}) = v(\mathcal{B}'_{\mathfrak{a}}) + v(a_{[\mathfrak{b}],\overline{\mathfrak{a}}}),$$

which is what we needed to prove by (24). □

For any discrete valuation v of M, let r_v be the smallest integer such that for all $\overline{\mathfrak{d}}$,

$$r_v > \frac{v(p)}{p-1} + v(N_{\overline{\mathfrak{d}}})$$

Notice that $r_v = 1$ for all but finitely many v, because the class group is finite and there are finitely many primes of M that are ramified or lying above 2.

The above proposition implies in particular,

Corollary 5.8. *If $v(\mathcal{B}_{\mathfrak{a}}) \geq r_v$, then*

$$v(\mathcal{B}_{\mathfrak{a}\mathfrak{b}}) = v(\mathcal{B}_{\mathfrak{a}}) + v(\mathfrak{b}).$$

Corollary 5.9. *If $v(\mathcal{B}_\mathfrak{a}) \geq r_v$, then*

$$v(B_\mathfrak{a}) = v(\mathcal{B}_\mathfrak{a}).$$

Proof. First of all, notice that by definition

$$\begin{aligned} v(B_\mathfrak{a}) &= \min_{\alpha \in \mathfrak{a}} v(B_\alpha) \\ &= \min_{\alpha \in \mathfrak{a}} v(\mathcal{B}_\alpha). \end{aligned}$$

On the other hand, Corollary 5.8 shows that for all $\alpha \in \mathfrak{a}$,

$$v(\mathcal{B}_\alpha) = v(\mathcal{B}_\mathfrak{a}) + v(\alpha/\mathfrak{a}).$$

This proves "$\geq$" and if we take α such that $v(\alpha) = v(\mathfrak{a})$, then it shows "$\leq$". □

Proposition 5.10. *If $r_v = 1$ and $v(N_{\bar{\mathfrak{a}}}) = 1$, then*

$$v(\mathcal{B}_\mathfrak{a}) = v(B_\mathfrak{a}).$$

Proof. By Corollary 5.9, it suffices to show that $v(B_\mathfrak{a}) > 0$ implies $v(\mathcal{B}_\mathfrak{a}) > 0$. If $\mathfrak{a}$ is principal, then this is trivial. Otherwise, fix an isogeny $[\mathfrak{a}]$ and let α, β be a pair of generators of $\mathfrak{a}$. Then $\alpha/\mathfrak{a}$ and $\beta/\mathfrak{a}$ are coprime, so there exist $a \in \alpha/\mathfrak{a}$, $b \in \beta/\mathfrak{a}$ such that $a + b = 1$.

As $\alpha \in \mathfrak{a}$, we have $v(\mathcal{B}_\alpha) = v(B_\alpha) > 0$. Notice that $\alpha | a\mathfrak{a}$ by definition of a, so Corollary 5.8 implies $v(\mathcal{B}_{a\mathfrak{a}}) > 0$. As $v(N_{\bar{\mathfrak{a}}}) = 0$, this is equivalent to $v(x([a][\mathfrak{a}]P)) < 0$ and in the same way, we find $v(x([b][\mathfrak{a}]P)) < 0$. Using the fact that $E_{\bar{\mathfrak{a}},1}(M_v)$ is a group, we find $v(x([\mathfrak{a}]P)) < 0$, because $a + b = 1$.

This proves $v(\mathcal{B}_\mathfrak{a}) = v(\mathcal{B}'_\mathfrak{a}) > 0$. □

For the finitely many valuations that remain, we will be satisfied with

Lemma 5.11.

$$v(\mathcal{B}_\mathfrak{a}) = v(B_\mathfrak{a}) + O(v(\mathfrak{a}))$$

Proof. If $v(\mathcal{B}_\mathfrak{a}) \geq r_v$, then it follows from Corollary 5.9 that $v(\mathcal{B}_\mathfrak{a}) = v(B_\mathfrak{a})$, so we may assume $v(\mathcal{B}_\mathfrak{a}) < r_v$. But in that case, what we need to prove is equivalent to

$$v(B_\mathfrak{a}) = O(v(\mathfrak{a})),$$

which is true by Lemma 2.4. □

We use this to get the following estimate, which allows us to use the point $[\mathfrak{a}]P$ to get estimates for $\log ||B_\mathfrak{a}||$.

Corollary 5.12.

$$\begin{aligned} \log ||\mathcal{B}'_\mathfrak{a}|| &= \log ||\mathcal{B}_\mathfrak{a}|| + O(1) \\ &= \log ||B_\mathfrak{a}|| + O(\log ||\mathfrak{a}||) \end{aligned}$$

Proof. The first identity holds by definition, so we only need to prove the second. Consider the expressions $\log ||\mathcal{B}_\mathfrak{a}|| = \sum_\mathfrak{p} \log ||\mathfrak{p}|| v_\mathfrak{p}(\mathcal{B}_\mathfrak{a})$ and $\log ||B_\mathfrak{a}|| = \sum_\mathfrak{p} \log |\mathfrak{p}| v_\mathfrak{p}(B_\mathfrak{a})$. For all but finitely many valuations they are equal by Proposition 5.10; for the rest, Lemma 5.11 states that they differ by $O(\log ||\mathfrak{a}||)$. □

5.5 The height

Recall that Lemma 3.1 said $\widehat{h}(\phi(P)) = \deg(\phi)\widehat{h}(P)$ and note that $[\mathfrak{a}]$ has degree $||\mathfrak{a}||^2$ by [Sil94] II.1.5. Therefore,

$$\widehat{h}([\mathfrak{a}]P) = ||\mathfrak{a}||^2 \, \widehat{h}(P). \tag{26}$$

5.6 David's theorem

Theorem 5.13. *There is a constant G such that for all $\mathfrak{a}$ with $||\mathfrak{a}||$ large enough and every archimedean valuation v of M,*

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

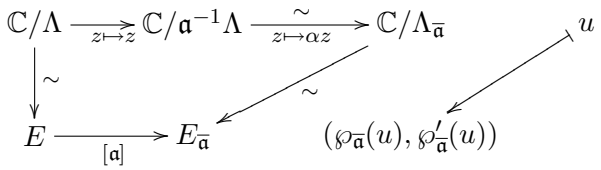
Proof. First of all, notice that it suffices to prove this for every ideal class separately, because the class group is finite. So let $\overline{\mathfrak{a}}$ be any ideal class. Next, notice that we can write $E_{\overline{\mathfrak{a}}}$ in the form

$$E_{\overline{\mathfrak{a}}} : Y^2 = 4X^3 - g_2X - g_3$$

and it suffices to prove the theorem for this equation.

Let $\Lambda_{\overline{\mathfrak{a}}}$ be the lattice for this curve and let $\wp_{\overline{\mathfrak{a}}}$ be the Weierstrass function associated to this lattice. Then $\Lambda = \widetilde{\mathfrak{a}}\Lambda_{\overline{\mathfrak{a}}}$ is a lattice such that E_Λ is isomorphic to E.

For any $\mathfrak{a} \in \overline{\mathfrak{a}}$, let α be a generator of $\mathfrak{a}/\widetilde{\mathfrak{a}}$. Then $[\mathfrak{a}]$ is defined by the commutative diagram



Let $u_1 \in \mathbb{C}$ be such that $u_1 (\mathrm{mod}\ \Lambda)$ corresponds to P. Then the diagram shows that for any $\mathfrak{a} \in \overline{\mathfrak{a}}$, the point $[\mathfrak{a}]P$ corresponds to $\alpha u_1 \ (\mathrm{mod}\ \Lambda_{\overline{\mathfrak{a}}})$. In particular, $(\wp_{\overline{\mathfrak{a}}}(u_1), \wp'_{\overline{\mathfrak{a}}}(u_1)) = [\widetilde{\mathfrak{a}}]P$ is an M-valued point on $E_{\overline{\mathfrak{a}}}$.

Let u_2, u_3 be generators for the lattice $\Lambda_{\overline{\mathfrak{a}}}$ and fix a fundamental domain $\mathcal{P}$ for $\Lambda_{\overline{\mathfrak{a}}}$ which contains 0 as an interior point. Then $\wp_{\overline{\mathfrak{a}}}$ has a pole of order 2 at 0 and no other poles on $\mathcal{P}$. For any $\mathfrak{a}$, let $b_1, b_2 \in \mathbb{Z}$ be such that $J := b_1u_1 + b_2u_2 + \alpha u_3 \in \mathcal{P}$. Then $x([\mathfrak{a}]P) = J^{-2}g(J)$, where g is holomorphic, hence bounded, on $\mathcal{P}$. Therefore $\log|x([\mathfrak{a}]P)| = -2\log|J| + O(1)$.

Now David's Theorem 4.1 says

$$\log|J| > -F\log(B)(\log\log(B))^4,$$

for large enough B, where $B = \max\{H(b_1), H(b_2), H(\alpha)\}$.

Now K has a unique archimedean valuation, so for $p, q \in \mathcal{O}$,

$$\begin{aligned} H(p/q)^{[K:\mathbb{Q}]} &= \prod_{v\in M_K} \max\{|p/q|_v, 1\} \\ &\le \max\{|p/q|^{[K:\mathbb{Q}]}, 1\} \prod_{v\in M_K^0} |1/q|_v^{e_v} \\ &= \max\{|p|, |q|\}^{[K:\mathbb{Q}]}. \end{aligned}$$

Notice also that $(\alpha) = \mathfrak{a}/\widetilde{\mathfrak{a}} = (\mathfrak{a}\overline{\widetilde{\mathfrak{a}}})/N(\widetilde{\mathfrak{a}})$, so $N(\widetilde{\mathfrak{a}})$ and $N(\widetilde{\mathfrak{a}})\alpha$ are both in $\mathcal{O}$. Therefore, $B \leq \max\{|b_1|, |b_2|, N(\widetilde{\mathfrak{a}}), N(\widetilde{\mathfrak{a}})|\alpha|\}$.

Also, b_1 is the integer multiple of u_1 that is nearest to αu_3 projected on $u_1\mathbb{R}$ so $|b_1|$ is bounded by a linear function of $|\alpha|$ and the same holds for $|b_2|$. At the same time, $|\alpha| = ||\alpha|| = ||\mathfrak{a}||/||\widetilde{\mathfrak{a}}||$, so $\log|\alpha| = \log||\mathfrak{a}|| + O(1)$. Hence we find

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

for some G if $||\mathfrak{a}||$ is large enough. □

This implies the following estimate for $\log||B_{\mathfrak{a}}||$:

Proposition 5.14.

$$\log||B_{\mathfrak{a}}|| = ||\mathfrak{a}||^2\,\widehat{h}(P) \;+\; O\left(\log||\mathfrak{a}||(\log\log||\mathfrak{a}||)^4\right).$$

Proof. Recall that Lemma 4.2 of Chapter V shows that

$$\log||\mathcal{B}'_{\mathfrak{a}}|| = \; h(x([\mathfrak{a}]P)) - \sum_{v\in M_M^\infty} \frac{n_v}{[M:\mathbb{Q}]}\log\max\{|x([\mathfrak{a}]P)|_v, 1\}.$$

If we apply the above theorem to each of the finitely many terms in the sum, then we get

$$\log||\mathcal{B}'_{\mathfrak{a}}|| \;\; = \;\; \widehat{h}([\mathfrak{a}]P) \;+\; O\left(\log||\mathfrak{a}||(\log\log||\mathfrak{a}||)^4\right).$$

The left hand side is $\log||B_{\mathfrak{a}}|| + O(\log||\mathfrak{a}||)$ by Corollary 5.12 and $\widehat{h}([\mathfrak{a}]P) = ||\mathfrak{a}||^2\widehat{h}(P)$ by (26). □

6 Zsigmondy's Theorem

We will now use the estimates and an inclusion-exclusion argument to prove the existence of primitive divisors. It is convenient to introduce a new symbol $B'_{\mathfrak{a}} = \prod_{\mathfrak{b}|\mathfrak{a}} D_{\mathfrak{b}}$, which is almost the same as $B_{\mathfrak{a}}$.

To be precise,

Lemma 6.1.

$$\log||B'_{\mathfrak{a}}|| = \log||B_{\mathfrak{a}}|| + O(\log||\mathfrak{a}||).$$

Proof. We show that for every discrete valuation v with $v(p) < p-1$, $v(B'_{\mathfrak{a}}) \leq v(B_{\mathfrak{a}}) \leq v(B'_{\mathfrak{a}}) + v(\mathfrak{a})$ and that the same holds with an extra $O(1)$ for the finitely many remaining valuations.

If $v(B_{\mathfrak{a}}) = 0$, then $v(B'_{\mathfrak{a}}) = 0 = v(B_{\mathfrak{a}})$. Otherwise, let $\mathfrak{r}$ be the rank of apparition of (the prime associated to) v. Then $\mathfrak{r}|\mathfrak{a}$ and we distinguish between two cases:

If $v(p) < p-1$, then Lemma 2.2 shows that

$$v(B_{\mathfrak{a}}) = v(B_{\mathfrak{r}}) + v(\mathfrak{a}/\mathfrak{r}) = v(B'_{\mathfrak{a}}) + v(\mathfrak{a}/\mathfrak{r}), \tag{27}$$

which is between $v(B'_{\mathfrak{a}})$ and $v(B'_{\mathfrak{a}}) + v(\mathfrak{a})$. For the finitely many valuations with $v(p) \geq p-1$, Lemma 2.5 states that (27) holds up to $O(1)$. □

For any $n \in \mathbb{N}$, let $d(n)$ be the number of positive integers that divide n. Notice that the number of ideals that divide $\mathfrak{a}$ is at most $d(N(\mathfrak{a}))$.

Lemma 6.2. *For every $\epsilon > 0$, $d(n) = O(n^\epsilon)$.*

Proof. If $(n, m) = 1$, then $d(nm) = d(n)d(m)$. Also, for all primes p and all integers $k \geq 0$, $d(p^k) = k + 1 \leq 2^k$.

For primes p with $2^{1/\epsilon} \leq p$, this implies $d(p^k) \leq p^{k\epsilon}$. There are only finitely many primes smaller than $2^{1/\epsilon}$. For these, let $c_p \in \mathbb{R}$ be large enough such that $k + 1 < c_p(p^\epsilon)^k$ for all $k \geq 1$ and let $c = \prod_p c_p$. Then for all n, $d(n) \leq c\, n^\epsilon$. □

Let μ be the Möbius function for the set of integral ideals of $\mathcal{O}$,

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

Then the inclusion-exclusion principle yields

$$\begin{aligned} \log ||D_\mathfrak{a}|| &= \sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{a}/\mathfrak{b}) \log ||B'_\mathfrak{b}|| \\ &= \sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{a}/\mathfrak{b}) \log ||B_\mathfrak{b}|| + \sum_{\mathfrak{b}|\mathfrak{a}} O(\log ||\mathfrak{b}||), \qquad \text{(Lemma 6.1)} \end{aligned}$$

to which we can apply Proposition 5.14 (alternatively Corollary 4.4 if $h_K = 1$) and get

$$\begin{aligned} \log ||D_\mathfrak{a}|| &= \widehat{h}(P) \sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{a}/\mathfrak{b}) ||\mathfrak{b}||^2 + \sum_{\mathfrak{b}|\mathfrak{a}} O\left(\log ||\mathfrak{b}|| (\log\log ||\mathfrak{b}||)^4\right) \\ &= \widehat{h}(P) ||\mathfrak{a}||^2 \Big(\sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{b}) ||\mathfrak{b}||^2 \Big) + O(d(N(\mathfrak{a}))(\log ||\mathfrak{a}||)^2) \\ &= \widehat{h}(P) ||\mathfrak{a}||^2 \Big(\sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{b}) ||\mathfrak{b}||^2 \Big) + O(||\mathfrak{a}||^\epsilon). \end{aligned} \tag{28}$$

We can bound this from below with some analytic number theory. If we look at a CM-indexed sequence, then we use

Lemma 6.3. *For any quadratic number field K (with arbitrary class number), there is a constant $C > 0$ such that for all ideals $\mathfrak{a}$ of $\mathcal{O}$,*

$$\sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{b}) N(\mathfrak{b})^{-1} \geq \frac{e^{-2\gamma}}{(\log N(\mathfrak{a}))^2} (1 - o(1)),$$

where $\gamma \approx 0.5772$ is the Euler constant.

Proof.

$$\begin{aligned} \sum_{\mathfrak{b}|\mathfrak{a}} \mu(\mathfrak{b}) N(\mathfrak{b})^{-1} &= 1 - \sum_{\mathfrak{p}_1|\mathfrak{a}} N(\mathfrak{p}_1)^{-1} + \sum_{\mathfrak{p}_1 \neq \mathfrak{p}_2|\mathfrak{a}} N(\mathfrak{p}_1\mathfrak{p}_2)^{-1} - \cdots \\ &= \prod_{\mathfrak{p}|\mathfrak{a}} (1 - N(\mathfrak{p})^{-1}) \geq \prod_{p \leq N(\mathfrak{a})} (1 - p^{-1})^2 \end{aligned}$$

For the last inequality: if $\mathfrak{p}|p$ is split or ramified, then $1 - N(\mathfrak{p})^{-1} = 1 - p^{-1}$ and there are at most 2 primes $\mathfrak{p}$ with $\mathfrak{p}|p$, so we get two factors $1 - p^{-1}$. If $\mathfrak{p} = p$ is inert, then $1 - N(\mathfrak{p})^{-1} = 1 - p^{-2} = (1 - p^{-1})(1 + p^{-1}) \geq (1 - p^{-1})^2$. Finally, Mertens' theorem ([HW38] 22.9 Theorem 430) states

$$\prod_{p \leq X} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log X},$$

where $a \sim b$ means that the quotient $\frac{a}{b}$ converges to 1 or, equivalently, that $a = b(1 + o(1))$. □

If we consider an $\mathbb{N}$-indexed sequence, then we may use

Lemma 6.4. *For any $n \in \mathbb{N}$,*

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

is between $\frac{1}{\zeta(2)} \approx 0.6079$ and 1. (See Figure 1 on page 73 for a plot.)

Proof.

$$\begin{aligned} s_n &= \sum_{m|n} \mu(m) m^{-2} \\ &= 1 - \sum_{p_1|n} p_1^{-2} + \sum_{p_1 \neq p_2 | n} (p_1 p_2)^{-2} - \cdots \\ &= \prod_{p|n} (1 - p^{-2}) \end{aligned}$$

and

$$\begin{aligned} \prod_{p} (1 - p^{-2})^{-1} &= \prod_{p} \sum_{k=0}^{\infty} p^{-2k} \\ &= \sum_{m \in \mathbb{N}} m^{-2} \\ &= \zeta(2). \end{aligned}$$

□

So if we pick $\epsilon < 2$ and use Lemma 6.3/6.4, we find

$$\log ||D_{\mathfrak{a}}|| \geq \widehat{h}(P) e^{-2\gamma} \frac{||\mathfrak{a}||^2}{(2 \log ||\mathfrak{a}||)^2} \big(1 - o(1)\big) - O(||\mathfrak{a}||^{\epsilon}) \to \infty$$

if $||\mathfrak{a}|| \to \infty$. In particular,

Theorem 6.5. *For all but finitely many $\mathcal{O}$-ideals $\mathfrak{a}$, the ideal $B_{\mathfrak{a}}$ has a primitive divisor.* □

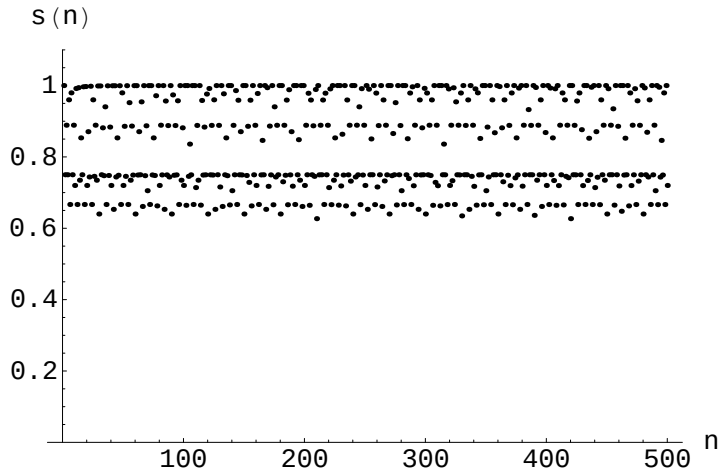


Figure 1: $s_n = \sum_{m|n} \mu(m) m^{-2} = \prod_{p|n}(1 - p^{-2})$

Corollary 6.6. *For any pair of non-zero $\mathcal{O}$-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 non-zero elements α, β such that $||\alpha||$ is suitably large,

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

Proof. We have already seen "$\Leftarrow$". On the other hand, 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 $\mathfrak{d} | \mathfrak{a}$. But $B_{\mathfrak{a}}$ has a primitive divisor, so this implies $\mathfrak{d} = \mathfrak{a}$. □

We get the following nice corollary about splitting behavior of primitive divisors of $\mathbb{N}$-indexed sequences:

Corollary 6.7. *Given a number field L, an elliptic curve E/L with integral coefficients and a non-torsion point $P \in E(L)$.*

Suppose that E has complex multiplication by the ring of integers $\mathcal{O}$ of a quadratic imaginary field K and that $[KL : L] = 2$. However, look only at the $\mathbb{N}$-indexed sequence $B_1, B_2, B_3, \ldots$.

Then for all but finitely many $n \in \mathbb{N}$, the following holds:

If

$$\begin{aligned} r &= \#\{p | n \text{ prime of } \mathbb{N} : p \text{ ramifies in } K/\mathbb{Q}\}, \\ s &= \#\{p | n \text{ prime of } \mathbb{N} : p \text{ splits in } K/\mathbb{Q}\}, \end{aligned}$$

then B_n has at least $r + s + 1$ primitive divisors of which at least s split in KL/L.

Proof. Let σ denote the unique non-trivial automorphism of KL/L. Suppose that n is large enough such that $B_{\mathfrak{a}}$ has a primitive divisor (in the $\mathcal{O}$-indexed sequence) for all $\mathfrak{a}$ with $N(\mathfrak{a}) \geq n$.

For any split $p|n$, write $p = \mathfrak{p}\sigma(\mathfrak{p})$. Then $B_{n/\mathfrak{p}}$ has a primitive divisor $\mathfrak{q}$ which cannot divide $B_{n/\mathfrak{p}'}$ for any $\mathfrak{p}' \neq \mathfrak{p}$. If $\mathfrak{q}$ is ramified or inert, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, so by Lemma 1.2, $\mathfrak{q}$ is also a divisor of $B_{n/\sigma(\mathfrak{p})}$.

But then $\mathfrak{q}|(B_{n/\mathfrak{p}}, B_{n/\sigma(\mathfrak{p})}) = B_{n/p}$, contradicting the fact that $\mathfrak{q}$ is a primitive divisor. Therefore, $q = \mathfrak{q}\sigma(\mathfrak{q})$ is a prime of L that splits in KL/L and is primitive for B_n in the $\mathbb{N}$-indexed sequence.

There are at least $r+1$ 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. □

This shows for example that in Table 3 on page 36, after a certain point, every second term has at least two primitive divisors, while every fifth term has at least two primitive divisors of which at least one is congruent to 1 mod 4.

We may also apply the inclusion-exclusion principle with $\mathbb{N}$ as an index set regardless of the CM-ring. Then we get the following estimate for the primitive part of the $\mathbb{N}$-indexed sequence:

Proposition 6.8. *For all $\epsilon > 0$,*

$$\log ||D_n|| = \widehat{h}(P) s_n n^2 + O(n^\epsilon),$$

where

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

is between $\zeta(2)^{-1} \approx 0.6079$ and 1. In particular, the ($\mathbb{N}$-indexed) sequence $B_1, B_2, B_3, \ldots$ has a primitive part that is larger than the non-primitive part from some point on. (See Figure 2 on page 75 for a plot.)

Proof. We can do all the estimates with $\mathbb{N}$ as index set instead of the set of ideals of $\mathcal{O}$. Then (28) becomes

$$\log ||D_n|| = \widehat{h}(P) s_n n^2 + O(n^\epsilon)$$

The (in)equalities for s_n are in Lemma 6.4. □

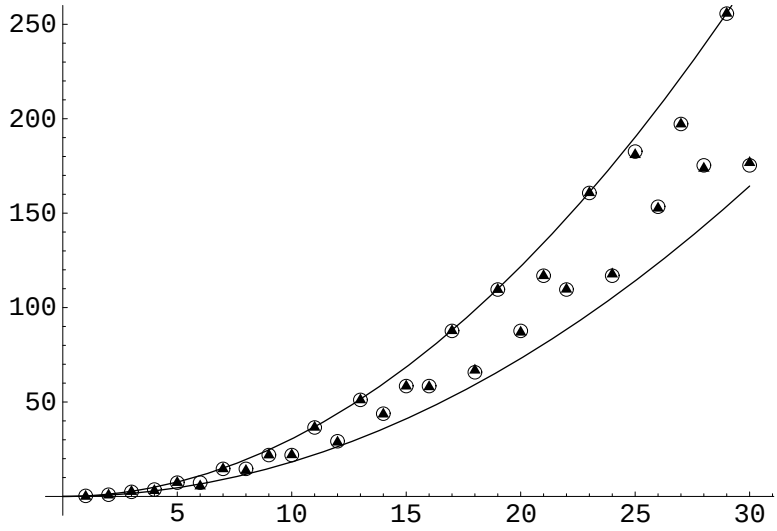


Figure 2: A plot of the logarithm of the primitive part of an elliptic divisibility sequence. The parabola at the top is $\widehat{h}(P)n^2$, which is up to a constant the absolute maximum of $\log ||B_n||$ itself. The circles are the values of $\widehat{h}(P)s_n n^2$ and the parabola at the bottom is a lower bound for that function. The triangles are the logarithms of the primitive part in the example of Table 5 on page 53.

Bibliography

[Aya92] Mohamed Ayad. Points S-entiers des courbes elliptiques. *manuscripta mathematica*, 76:305–324, 1992.

[Bak66] A. Baker. Linear forms in the logarithms of algebraic numbers, I. *Mathematika*, 13:204–216, 1966.

[Bak67a] A. Baker. Linear forms in the logarithms of algebraic numbers, II. *Mathematika*, 14:102–107, 1967.

[Bak67b] A. Baker. Linear forms in the logarithms of algebraic numbers, III. *Mathematika*, 14:220–228, 1967.

[Bak68] A. Baker. Linear forms in the logarithms of algebraic numbers, IV. *Mathematika*, 15:204–216, 1968.

[Bak90] A. Baker. *Transcendental number theory.* Cambridge University Press, 1990.

[Ban86] A.S. Bang. Taltheoretiske undersøgelser. *Zeuthen Tidskr.*, IV:70–80, 130–137, 1886.

[BHV01] Yuri Bilu, Guillaume Hanrot, and Paul Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001.

[CC86] D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7, 1986.

[CH98] J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *manuscripta mathematica*, 97(3):319–328, 1998.

[CZ05] Gunther Cornelissen and Karim Zahidi. Complexity of undecidable formulæ in the rationals and inertial Zsigmondy theorems for elliptic curves. 2005. arXiv:math.NT/0412473 v2.

[Dav95] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France*, 62, 1995.

[Dur52] L.K. Durst. The apparition problem for equianharmonic divisibility sequences. *Prod. Natl. Acad. Sci. U.S.A.*, 38:330–333, 1952.

[EK05] Graham Everest and Helen King. Prime powers in elliptic divisibility sequences. *Mathematics of computation*, 74(252):2061–2071, 2005.

[EMW06] Graham Everest, Gerard McLaren, and Tom Ward. Primitive divisors of elliptic divisibility sequences. *Journal of Number Theory*, 118(1):71–89, 2006. Preprint.

[EvdPSW03] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2003.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[HW38] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1938.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[Poo02] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers. In *Proceedings of the Algorithmic Number Theory Symposium V*, volume 2369 of *Springer Lecture Notes in Computer Science*, 2002.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[Sil88] Joseph H. Silverman. Wieferich's criterion and the abc-conjecture. *Journal of Number Theory*, 30:226–237, 1988.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[ST94] R.J. Stroeker and N. Tzanakis. Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arithmetica*, LXVII.2:177–196, 1994.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sc. Paris*, 273:238–241, 1971.

[War48] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 7:31–74, 1948.

[War50] Morgan Ward. Arithmetical properties of the elliptic polynomials associated with the lemniscate elliptic functions. *Proc. Natl. Acad. Sci. U.S.A.*, 36:359–362, 1950.

[Zsi92] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math.*, 3:265–284, 1892.

Index