MATH. SCAND. 94 (2004), 161–184

GENERALIZED DIVISION POLYNOMIALS

TAKAKAZU SATOH

Abstract

Let E be an elliptic curve with complex multiplication by the ring O_F of integers of an imaginary quadratic field F. We give an explicit condition on $\alpha \in O_F$ so that there exists a rational function ψ_α satisfying $\operatorname{div} \psi_\alpha = \sum_{P \in \operatorname{Ker}[\alpha]}[P] - N_{F/\mathbf{Q}}(\alpha)[\mathcal{O}]$ where $[\alpha]$ is the multiplication by α map. We give an algorithm to compute ψ_α based on recurrence formulas among these functions. We prove that the time complexity of this algorithm is $O(N_{F/\mathbf{Q}}(\alpha)^{2+\varepsilon})$ bit operations under an FFT based multiplication algorithm as $N_{F/\mathbf{Q}}(\alpha)$ tends to infinity for the fixed E.

1. Introduction

Let k be a perfect field. It is known that for an elliptic curve E/k and $n \in \mathbf{N}$ there exists a rational function ψ_n on E satisfying $\operatorname{div}(\psi_n) = \sum_{P \in E[n]}[P] - n^2[\mathcal{O}]$, where $\mathcal{O}$ is the point at infinity. See e.g. Silverman[10, Exercise 3.7] for $\operatorname{char}(k) \neq 2, 3$, Koblitz[7] for $\operatorname{char}(k) = 2$. If E is given by the Weierstrass model, such functions are polynomials of coordinate functions and they are called division polynomials.

Now let $E : Y^2 = X^3 + aX + b$ be an elliptic curve admitting complex multiplications by the ring O_F of integers of an imaginary quadratic field F where a and b are algebraic integers. Put $K := F(a, b)$. In this paper, we generalize division polynomials for some $\alpha \in O_F - \mathbf{Z}$. Our goal is to give a deterministic algorithm to compute generalized division polynomials and to estimate its bit complexities. More specifically, in Corollary 2.6, we prove that a rational function ψ_α on E satisfying $\operatorname{div}(\psi_\alpha) = \sum_{P \in \operatorname{Ker}[\alpha]}[P] - N_{F/\mathbf{Q}}(\alpha)[\mathcal{O}]$ exists if and only if either $N_{F/\mathbf{Q}}(\alpha)$ is an odd integer or $2|\alpha$ (in O_F). We call such an element of O_F *unbiased*. Then, with a suitable normalization, we derive the relation

$$\psi_\beta^2 \psi_{\alpha+\gamma} \psi_{\alpha-\gamma} - \psi_\alpha^2 \psi_{\beta+\gamma} \psi_{\beta-\gamma} = \psi_{\alpha+\beta} \psi_{\alpha-\beta} \psi_\gamma^2 \tag{1.1}$$

for $\alpha, \beta, \gamma \in O_F$ provided all indexes appearing in (1.1) are unbiased (Corollary 3.7). Choosing γ carefully, we obtain recurrence formulas which gives an efficient algorithm to compute generalized division polynomials. Since our

Received February 14, 2003.

generalized polynomials only exist for unbiased elements in O_F, it is important to construct recurrence formulas with unbiased elements. In Corollary 4.3, we prove that ψ_α is a polynomial of coordinate functions with coefficients in O_K, the ring of integers of K. Choose $\omega \in O_F$ satisfying $O_F = \mathbf{Z} + \omega\mathbf{Z}$. (Later in (2.2), we specify ω explicitly.) Define $\|n + m\omega\| := \max(|n|, |m|)$. Note $N_{F/\mathbf{Q}}(\alpha) = O(\|\alpha\|^2)$. Using integrality of ψ_α, we can estimate the growth rate of the coefficients of ψ_α to be $O(\|\alpha\|^2 \log \|\alpha\|)$ in Theorem 6.4. Combining these results, we obtain, as our main result, an estimate for the time complexity (measured by the number of bit operations) to compute ψ_α:

THEOREM. *Let μ be a constant such that the number of bit operations used for multiplication of two n bit integers is $O(n^\mu)$. Assume that $\alpha \in O_F$ is unbiased. Then, we can compute ψ_α with $O((\|\alpha\|^4 \log \|\alpha\|)^\mu)$ bit operations.*

In order to avoid technical difficulties, we limit ourselves to the case where $\mathrm{End}(E)$ is the maximal order of F. Under this restriction, $\mathrm{End}(E)$ is a Dedekind domain and, in particular, every non-zero ideal has a prime ideal decomposition.

Generalized division polynomials are closely related to the problem of finding the explicit form of complex multiplications. Stark[12] obtained the following algorithm to compute explicit complex multiplication. Let $\wp$ be the Weierstrass $\wp$-function associated to E. For a given $\alpha \in O_F$, his algorithm finds polynomials u, v with coefficients in K such that $\wp(\alpha z) = u(\wp(z))/v(\wp(z))$ by the continued fraction approximation. From v, it is possible (in theory) to obtain ψ_α. (For example, v is a constant multiple of ψ_α^2 if $N_{F/\mathbf{Q}}(\alpha)$ is odd.) Although the growth rate of the number of arithmetic operations in K to obtain v is of polynomial order w.r.t. $N_{F/\mathbf{Q}}(\alpha)$, the time complexity w.r.t. bit operations is not known. Straightforward implementation suggests that its space complexity grows exponentially as $N_{F/\mathbf{Q}}(\alpha)$ tends to the infinity. Hence, Stark's algorithm is infeasible in practice.

A better method is to perform Stark's algorithm once for ω. Assume that $\alpha := m + n\omega \in O_F$ is given. Since the m times map and the n times map are expressed in terms of ordinal division polynomials, we obtain an explicit formula for complex multiplication by α. This is what was done by Abel [1] for the case $O_F = \mathbf{Z}[\sqrt{-1}]$. (Of course, no computational complexity analysis is given in this 19th century paper.) This method performs several arithmetic operations over $K(X)$ whose time complexities w.r.t. bit operations are difficult to estimate because they involve greatest common divisor computations over $K[X]$.

Although our main interest is an efficient algorithm to compute generalized division polynomials, some topics related to (1.1) have independent interests. Durst [5] obtained (1.1) in the case where γ in (1.1) is restricted to be a unit

and where E is of the form $Y^2 = X^3 + b$. Chudnovsky and Chudnovsky [4] mentioned this relation in the context of elliptic curve primality and factorization tests, but no further relation than Durst [5] is given. As to integrality, in case that the class number of $F := \mathbf{Q}(\sqrt{-d})$ is one and that $d \geq 7$, Joux and Morain [6, §2] proved that $\frac{1}{d}\psi_{\sqrt{-d}}$ (H_d in their notation) is a polynomial of the X-coordinate function with coefficients in $\mathbf{Z}$. This is better than Corollary 4.3 by a factor of d. It is an open problem that for which F or α a similar property holds. As to the space complexity, we note that McKee [8] gave a slightly better estimate than ours for ordinal division polynomials.

The rest of this paper is organized as follows. After giving some notation, we introduce the notion of unbiasedness in Section 2 and prove some basic properties. In Section 3, generalized division polynomials are defined and we prove the recurrence formula (1.1). Section 4 is devoted to the proof of the integrality of generalized division polynomials. Section 5, which is of different nature from the preceding sections, considers the space complexity on arithmetic operations on O_K. Finally in Section 6, we prove our main result Theorem 6.6.

NOTATION. Let E be an elliptic curve given by

$$Y^2 = X^3 + aX + b \tag{1.2}$$

with algebraic integers a and b. The X-coordinate function and Y-coordinate function are denoted by ξ and η, respectively. The point at infinity of E is denoted by $\mathcal{O}$. We use $\tau := -\xi/\eta$ as a local parameter at $\mathcal{O}$ unless otherwise noted. Throughout this paper, we assume E admits complex multiplication by the ring O_F of integers of an imaginary quadratic field F. Put $K := F(a, b)$. For $\alpha \in O_F$, there is a unique endomorphism $[\alpha] \in \mathrm{End}(E)$ satisfying $\tau \circ [\alpha] = \alpha\tau + O(\tau^2)$. The map $[\cdot]$ is a ring isomorphism (see e.g. Silverman[11, Prop. II.1.1]). For an ideal $\mathfrak{a}$ of O_F, we put

$$E[\mathfrak{a}] := \{ P \in E : [\alpha]P = \mathcal{O} \text{ for all } \alpha \in \mathfrak{a} \}.$$

It is proven in Silverman[11, Prop. II.1.4] that $E[\mathfrak{a}]$ is a free $O_F/\mathfrak{a}$ module of rank 1. In particular, $\#E[\mathfrak{a}] = N(\mathfrak{a})$ where $N(\cdot)$ is the norm of an ideal. By a prime ideal, we mean a non-zero prime ideal. The principal ideal of O_F generated by $\alpha \in O_F$ is denoted by $\langle\alpha\rangle_F$. For simplicity, we write $E[\langle\alpha\rangle_F]$ as $E[\alpha]$. For $A \in E$ and $f \in K(E)$, we denote the order of zero of f at A by $\mathrm{ord}_A f$, whereas for a prime ideal $\mathfrak{p}$ of a Dedekind domain R and $\alpha \in R$, we understand $\mathrm{ord}_\mathfrak{p} a$ as an additive $\mathfrak{p}$-adic valuation of a. These two usages of ord are clearly distinguished by context.

ACKNOWLEDGEMENTS. Universitet i Tromsø (Norway), Aarhus universitet (Denmark), and Institut National de Recherche en Informatique et en Automatique (France) are gratefully thanked for their hospitality and for good research environments. The author would like to thank Professor François Morain at École Polytechnique for valuable discussion.

2. Unbiased Ideals

In this section, we introduce the notion of unbiased groups and unbiased ideals. Then we obtain some basic properties of unbiased ideals.

DEFINITION 2.1. A finite Abelian group G is said to be *unbiased* if $\sum_{g\in G} g = 0$.

Note that unbiasedness depends only on the isomorphism classes of Abelian groups.

LEMMA 2.2. *Let G be a finite Abelian group.*

(1) *Assume that $G = G_1 \oplus G_2$ where $\gcd(\#G_1, \#G_2) = 1$. Then G is unbiased if and only if both G_1 and G_2 are unbiased.*

(2) *The group G is unbiased if $\#G$ is odd.*

(3) *Assume that $\#G$ is even. Then G is unbiased if and only if G contains a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.*

PROOF. (1) Observe

$$\sum_{g\in G} g = \sum_{g_1\in G_1}\sum_{g_2\in G_2} (g_1, g_2) = \left(\#G_2 \sum_{g_1\in G_1} g_1, \#G_1 \sum_{g_2\in G_2} g_2\right).$$

Hence "if part" is obvious. To prove converse, note that $(\#G_2)a = 0$ for $a \in G_1$ implies $a = 0$ since $\#G_2$ is prime to $\#G_1$. Thus, G_1 is unbiased. Unbiasedness of G_2 follows from the same way.

(2) Since $\sum_{g\in G} g = \sum_{-g\in G} -g = -\sum_{g\in G} g$, we have

$$2\sum_{g\in G} g = 0. \tag{2.1}$$

Multiplying $\frac{\#G+1}{2} \in \mathbf{Z}$, we have the assertion.

(3) Due to (1) and (2), we may assume that G is isomorphic to $\mathbf{Z}/2^{n_1}\mathbf{Z}\oplus\cdots\oplus \mathbf{Z}/2^{n_r}\mathbf{Z}$ where $r \in \mathbf{N}$ and $n_1, \ldots, n_r \in \mathbf{N}$. By a straightforward computation, we see that the latter group is unbiased if and only if $r \geq 2$. Assume that G contains subgroup which is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Then G contains at least three elements of order two. Hence G cannot be cyclic, which means

$r \geq 2$. Therefore G is unbiased. On the other hand, in case of $r \geq 2$, the group $\mathbf{Z}/2^{n_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/2^{n_r}\mathbf{Z}$ contains a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. So does G.

DEFINITION 2.3. We say an ideal $\mathfrak{a}$ of O_F is *unbiased* if $\mathfrak{a}$ is the zero ideal or $E[\mathfrak{a}]$ is an unbiased subgroup of E. An element α of O_F is said to be *unbiased* if the principal ideal generated by α is unbiased.

LEMMA 2.4. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of O_F. The following properties hold:*

(1) $E[\mathfrak{a}+\mathfrak{b}] = E[\mathfrak{a}] \cap E[\mathfrak{b}]$.

(2) *If $\mathfrak{a}+\mathfrak{b} = O_F$, then $E[\mathfrak{a}] \oplus E[\mathfrak{b}]$ is isomorphic to $E[\mathfrak{a}\mathfrak{b}]$ under the map φ defined by $\varphi(P, Q) := P + Q$.*

PROOF. (1) Obviously, $E[\mathfrak{a}+\mathfrak{b}] \subset E[\mathfrak{a}]$ and $E[\mathfrak{a}+\mathfrak{b}] \subset E[\mathfrak{b}]$. Hence $E[\mathfrak{a}+\mathfrak{b}] \subset E[\mathfrak{a}] \cap E[\mathfrak{b}]$. Let $\gamma \in \mathfrak{a}+\mathfrak{b}$. Take $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ satisfying $\alpha+\beta = \gamma$. Then for any $P \in E[\mathfrak{a}] \cap E[\mathfrak{b}]$ it holds that $[\gamma]P = ([\alpha]+[\beta])P = \mathcal{O}$, which implies $P \in E[\mathfrak{a}+\mathfrak{b}]$.

(2) Let $P \in E[\mathfrak{a}]$ and $Q \in E[\mathfrak{b}]$. Since O_F is commutative, $P+Q \in E[\mathfrak{a}\mathfrak{b}]$. We prove φ is surjective. By the assumptions, there exist $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$. For any $A \in E[\mathfrak{a}\mathfrak{b}]$, we have $A = [\beta]A + [\alpha]A$ with $[\beta]A \in E[\mathfrak{a}]$ and $[\alpha]A \in E[\mathfrak{b}]$. Therefore, φ is surjective. Then φ must be injective because $\#E[\mathfrak{a}\mathfrak{b}] = N(\mathfrak{a}\mathfrak{b}) = \#E[\mathfrak{a}]\#E[\mathfrak{b}]$.

THEOREM 2.5. *Let $\mathfrak{a}$ be an ideal of O_F. Then $\mathfrak{a}$ is unbiased if and only if either $\langle 2\rangle_F | \mathfrak{a}$ (i.e. $\langle 2\rangle_F \supset \mathfrak{a}$) or $N(\mathfrak{a})$ is odd.*

PROOF. The assertion clearly holds for the zero ideal. In what follows, we assume that $\mathfrak{a}$ is not the zero ideal. The if part is a direct consequence of Lemma 2.2. To prove converse, we have to show that $\mathfrak{a}$ is a biased ideal if $2|N(\mathfrak{a})$ and $\langle 2\rangle_F \nmid \mathfrak{a}$. We consider the following three cases.

(i) In case that 2 remains prime in O_F: Any ideal of O_F with even norm is divisible by $\langle 2\rangle_F$, hence there is nothing to prove.

(ii) In case that 2 ramifies: Let $\langle 2\rangle_F = \mathfrak{p}^2$. Then, there exists a non-negative integer e and an ideal $\mathfrak{b}$ whose norm is odd such that $\mathfrak{a} = \mathfrak{p}^e\mathfrak{b}$. But if $e = 0$, then $N(\mathfrak{a})$ is odd and if $e \geq 2$, then $\langle 2\rangle_F | \mathfrak{a}$. Therefore $e = 1$ and hence $E[\mathfrak{a}] = E[\mathfrak{p}] \oplus E[\mathfrak{b}]$. Moreover, $\#E[\mathfrak{p}] = 2$ and $\#E[\mathfrak{b}]$ is odd. Since $E[\mathfrak{p}]$ is biased, $E[\mathfrak{a}]$ is also biased.

(iii) In case that 2 splits: By the similar observation as above, $\mathfrak{a}$ decomposes as $\mathfrak{a} = \mathfrak{p}^e\mathfrak{b}$ where $e \geq 1$, $\mathfrak{p}$ is one of prime ideals dividing $\langle 2\rangle_F$ and $\mathfrak{b}$ is an ideal of odd norm. Therefore, $E[\mathfrak{a}] = E[\mathfrak{p}^e] \oplus E[\mathfrak{b}]$. Since 2 splits, we have $E[\mathfrak{p}^e] \cong O_F/\mathfrak{p}^e \cong \mathbf{Z}/2^e\mathbf{Z}$. Hence $E[\mathfrak{p}^e]$ is biased and so is $E[\mathfrak{a}]$.

COROLLARY 2.6. *Let $\alpha \in O_F$. Then α is unbiased if and only if either $2|\alpha$ in O_F or $N_{F/\mathbf{Q}}(\alpha)$ is odd.*

COROLLARY 2.7. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be unbiased ideals. Then* $\mathfrak{ab}$ *is also unbiased.*

COROLLARY 2.8. *Let* d *be a square free positive integer such that* $F = \mathbf{Q}(\sqrt{-d})$. *Put*

$$\omega := \begin{cases} \sqrt{-d} & (-d \equiv 2, 3 \bmod 4), \\ \dfrac{-1+\sqrt{-d}}{2} & (-d \equiv 1 \bmod 4). \end{cases} \tag{2.2}$$

Let m *and* n *be integers.*

(1) *In case of* $d \equiv 1 \bmod 4$, $m + n\omega$ *is unbiased except for* $m \equiv n \equiv 1 \bmod 2$.

(2) *In case of* $d \equiv 2 \bmod 4$, $m + n\omega$ *is unbiased except for* $m \equiv 0 \bmod 2$ *and* $n \equiv 1 \bmod 2$.

(3) *In case of* $d \equiv 3 \bmod 8$, *any element of* O_F *is unbiased.*

(4) *In case of* $d \equiv 7 \bmod 8$, $m + n\omega$ *is unbiased if and only if* $n \equiv 0 \bmod 2$.

PROOF. This corollary follows from Theorem 2.5 and the fact that $N_{F/\mathbf{Q}}(m+n\omega) = m^2 + n^2 d$ for $d \equiv 1, 2 \bmod 4$ and $N_{F/\mathbf{Q}}(m+n\omega) = m^2 - mn + \frac{1+d}{4}n^2$ for $d \equiv 3 \bmod 4$. Note 2 ramifies in case of (1) and (2), remains prime in case of (3), and splits in case of (4).

REMARK 2.9. The condition $\langle 2 \rangle_F | \mathfrak{a}$ cannot be replaced by $4|N(\mathfrak{a})$. Indeed, let $d \equiv 7 \bmod 8$ and let $\mathfrak{p}$ be a prime ideal dividing $\langle 2 \rangle_F$. Then, the ideal $\mathfrak{p}^2$ is biased and its norms is 4.

3. Generalized Division Polynomials

First we introduce generalized division polynomials and prove recurrence formulas among them. Our definition is straightforward analogue of a definition of ordinal division polynomials (see e.g. Cassels [3, Formulary]). For simplicity, we write $N_{F/\mathbf{Q}}(\alpha)$ as $N(\alpha)$ for $\alpha \in O_F$. To begin with, we recall a condition on a divisor which comes from a rational function. Let $D := \sum_{i=1}^{n} a_i [P_i]$ be a divisor on an elliptic curve E. Then there exists a rational function f on E whose divisor is D if and only if $\sum_{i=1}^{n} a_i = 0$ and $\sum_{i=1}^{n} a_i P_i = \mathcal{O}$ (see e.g. Silverman [10, Cor. III.3.5]). Therefore, for a finite subgroup G of D, there exists a rational function f on E satisfying $\mathrm{div}(f) = \sum_{P \in G} [P] - \#G[\mathcal{O}]$ if and only if G is an unbiased group. Similarly, for $\alpha \in O_F - \{0\}$, there exists a rational function f on E satisfying

$$\mathrm{div}(f) = \sum_{P \in \mathrm{Ker}[\alpha]} [P] - N(\alpha)[\mathcal{O}] \tag{3.1}$$

if and only if α is an unbiased endomorphism. However, a divisor determined a rational function only up to constant multiple. We specify this constants as follows.

DEFINITION 3.1. Let $\alpha \in O_F$ be a non-zero unbiased element. Define the α-th division polynomial ψ_α by $\operatorname{div} \psi_\alpha = \sum_{P \in \operatorname{Ker}[\alpha]} [P] - N(\alpha)[\mathcal{O}]$ and the normalization condition

$$\psi_\alpha = (-1)^{N(\alpha)-1} \alpha \tau^{-N(\alpha)+1} + \cdots. \tag{3.2}$$

We also define an auxiliary function $\tilde{\psi}_\alpha$ for any $\alpha \in O_F$ by conditions $\operatorname{div} \tilde{\psi}_\alpha = \sum_{P \in \operatorname{Ker}[\alpha]} 2[P] - 2N(\alpha)[\mathcal{O}]$ and $\tilde{\psi}_\alpha = \alpha^2 \tau^{-2N(\alpha)+2} + \cdots$. Since (2.1) holds for any finite group, such function exists and it holds that $\tilde{\psi}_\alpha = \psi_\alpha^2$ for unbiased α. By convention, we put $\psi_0 := 0$ and $\tilde{\psi}_0 := 0$.

EXAMPLE 3.2. For the curve $Y^2 = X^3 + 5X$, we see $\psi_{2+\sqrt{-1}}$ is a constant multiple of $\xi^2 + 2 - \sqrt{-1}$ by straightforward computation (or Stark's algorithm). Since $\xi = \tau^{-2} - 5\tau^2 + O(\tau^6)$, we have

$$\begin{aligned} \psi_{2+\sqrt{-1}} &= (2+\sqrt{-1})\xi^2 + 5 \\ &= (2+\sqrt{-1})\tau^{-4} - 15 - 10\sqrt{-1} + O(\tau^4). \end{aligned}$$

REMARK 3.3. In case $\alpha \in \mathsf{N}$, our ψ_α coincides with the notation used in [10, Exercise 3.7]. For a unit ε of O_F, we see $\psi_\varepsilon = \varepsilon$ (a constant function).

LEMMA 3.4. *Let α be an unbiased element. In case that $N(\alpha)$ is odd, $\psi_\alpha \in K[\xi]$ and $\deg_\xi \psi_\alpha = (N(\alpha)-1)/2$. Otherwise, $\frac{1}{\eta}\psi_\alpha \in K[\xi]$ and $\deg_\xi \left(\frac{1}{\eta}\psi_\alpha\right) = (N(\alpha)-4)/2$.*

PROOF. Since $\operatorname{Ker}[\alpha]$ is defined over K (recall $K \supset F$), there is $f \in K(E)$ satisfying (3.1). Noting $\xi \in K((\tau))$ and $\eta \in K((\tau))$, we see that f is expanded as $a_{-N(\alpha)+1}\tau^{-N(\alpha)+1} + \cdots$ with $a_{-N(\alpha)+1} \in K$. Threfore, there exists a constant $c \in K^\times$ satisfying $\psi_\alpha = cf$, which implies $\psi_\alpha \in K(E)$. Since $[-1](\operatorname{Ker}[\alpha]) = \operatorname{Ker}[\alpha]$, there exists constant c satisfying $\psi_\alpha \circ [-1] = c\psi_\alpha$. Note $\tau \circ [-1] = -\tau$. Therefore $\psi_\alpha \circ [-1] = \psi_\alpha$ for odd $N(\alpha)$ and $\psi_\alpha \circ [-1] = -\psi_\alpha$ for even $N(\alpha)$. Since $[-1]$ is the unique non-trivial element of $\operatorname{Gal}(K(E)/K(\xi))$, we see $\psi_\alpha \in K(\xi)$ for odd $N(\alpha)$ and $\frac{1}{\eta}\psi_\alpha \in K(\xi)$ for even $N(\alpha)$. However they are regular outside of $\{\mathcal{O}\}$. Hence we see they are polynomials of ξ. The assertions on degree follows from $\operatorname{ord}_\mathcal{O} \xi = -2$.

LEMMA 3.5. *Let α and β be non-zero unbiased elements of O_F. Then*

$$\psi_{\alpha\beta} = (\psi_\alpha \circ [\beta]) \cdot \psi_\beta^{N(\alpha)}.$$

PROOF. Since $\mathrm{char}(K) = 0$, every endomorphism is separable, hence unramified (Silverman [10, III.4.10(c)]). By a straightforward computation, we see $\operatorname{div}\psi_{\alpha\beta} = \operatorname{div}\big((\psi_\alpha \circ [\beta]) \cdot \psi_\beta^{N(\alpha)}\big)$. Indeed,

$$\begin{aligned}
\operatorname{div}\psi_{\alpha\beta} &= \sum_{P \in \mathrm{Ker}[\alpha]\circ[\beta]} [P] - N(\alpha\beta)[\mathcal{O}] \\
&= [\beta]^*\left(\sum_{P \in \mathrm{Ker}[\alpha]} [P]\right) - N(\alpha\beta)[\mathcal{O}] \\
&= [\beta]^*(\operatorname{div}\psi_\alpha + N(\alpha)[\mathcal{O}]) - N(\alpha)N(\beta)[\mathcal{O}] \\
&= \operatorname{div}([\beta]^*\psi_\alpha) + N(\alpha)\left(\sum_{P \in \mathrm{Ker}[\beta]} [P]\right) - N(\alpha)N(\beta)[\mathcal{O}] \\
&= \operatorname{div}(\psi_\alpha \circ [\beta]) + N(\alpha)\operatorname{div}\psi_\beta.
\end{aligned}$$

Thus there exists a constant $c \in K^\times$ satisfying $\psi_{\alpha\beta} = c(\psi_\alpha \circ [\beta]) \cdot \psi_\beta^{N(\alpha)}$. By definition,

$$\psi_{\alpha\beta} = (-1)^{N(\alpha\beta)-1}\alpha\beta\tau^{-N(\alpha)+1} + \cdots$$

while

$$\begin{aligned}
\psi_\alpha &= (-1)^{N(\alpha)-1}\alpha\tau^{-N(\alpha)+1} + \cdots \\
\psi_\alpha \circ [\beta] &= (-1)^{N(\alpha)-1}\alpha(\beta\tau + \cdots)^{-N(\alpha)+1} \\
&= (-1)^{N(\alpha)-1}\alpha\beta^{-N(\alpha)+1}\tau^{-N(\alpha)+1} + \cdots \\
\psi_\beta^{N(\alpha)} &= ((-1)^{N(\beta)-1}\beta\tau^{-N(\beta)+1} + \cdots)^{N(\alpha)} \\
&= (-1)^{N(\alpha\beta)-N(\alpha)}\beta^{N(\alpha)}\tau^{-N(\alpha\beta)+N(\alpha)} + \cdots.
\end{aligned}$$

Hence $c = 1$.

The proof of the next proposition is more or less the same as the proof for the ordinal division polynomials and is already outlined in Cassels [3, Formulary]. However, in case that α and $\beta \in O_F$ satisfies $\langle\alpha + \beta\rangle_F + \langle\alpha - \beta\rangle_F \neq O_F$, the function $\psi_{\alpha+\beta}\psi_{\alpha-\beta}$ have a double pole. We need to handle (at least) this case separately, which is omitted in [3].

PROPOSITION 3.6. *Let α and β be non-zero elements of O_F such that $\alpha + \beta$ and $\alpha - \beta$ are unbiased. Then*

$$\xi \circ [\alpha] - \xi \circ [\beta] = -\frac{\psi_{\alpha+\beta}\psi_{\alpha-\beta}}{\tilde{\psi}_\alpha\tilde{\psi}_\beta}.$$

PROOF. The assertion is obvious in case of $\alpha = \pm\beta$. Assume $\alpha \neq \beta$ and $\alpha \neq -\beta$ and consider the function φ defined by

$$\varphi := (\xi \circ [\alpha] - \xi \circ [\beta]) \frac{\tilde{\psi}_\alpha \tilde{\psi}_\beta}{\psi_{\alpha+\beta}\psi_{\alpha-\beta}}.$$

We show that φ has no pole. It is expanded as

$$\frac{((\alpha^{-2} - \beta^{-2})\tau^{-2} + \cdots)(\alpha^2\tau^{-2N(\alpha)+2} + \cdots)(\beta^2\tau^{-2N(\beta)+2} + \cdots)}{((-1)^{N(\alpha+\beta)-1}(\alpha+\beta)\tau^{-N(\alpha+\beta)+1} + \cdots) \cdot ((-1)^{N(\alpha-\beta)-1}(\alpha-\beta)\tau^{-N(\alpha-\beta)+1} + \cdots)}$$

at the point at infinity. Noting

$$N(\alpha+\beta) + N(\alpha-\beta) = 2N(\alpha) + 2N(\beta), \tag{3.3}$$

we see that φ is expanded as

$$\varphi = -1 + O(\tau) \tag{3.4}$$

at $\mathcal{O}$. For $P \in E[\alpha] - E[\beta]$, we have $\operatorname{ord}_P(\xi \circ [\alpha] - \xi \circ [\beta]) = -2$, $\operatorname{ord}_P(\tilde{\psi}_\alpha) = 2$, $\operatorname{ord}_P(\tilde{\psi}_\beta) = 0$, $\operatorname{ord}_P(\psi_{\alpha+\beta}) = \operatorname{ord}_P(\psi_{\alpha-\beta}) = 0$. Thus $\operatorname{ord}_P \varphi = 0$. The similar argument applies for $P \in E[\beta] - E[\alpha]$. Let $P \in E[\alpha] \cap E[\beta] - \{\mathcal{O}\}$ and let V_P be the translation by P map (i.e. $V_P(A) = P + A$). Observe

$$\xi \circ [\alpha] \circ V_{-P} = \alpha^{-2}(\tau \circ V_{-P})^{-2} + \cdots.$$

But $\tau \circ V_{-P}$ is a local parameter at P and $[\alpha] \circ V_{-P} = [\alpha]$. The same formula holds for β. Using $\alpha \neq \pm\beta$, we see $\operatorname{ord}_P(\xi \circ [\alpha] - \xi \circ [\beta]) = -2$. On the other hand, $\operatorname{ord}_P(\tilde{\psi}_\alpha) = 2$, $\operatorname{ord}_P(\tilde{\psi}_\beta) = 2$, $\operatorname{ord}_P(\psi_{\alpha+\beta}) = 1$ and $\operatorname{ord}_P(\psi_{\alpha-\beta}) = 1$. Hence $\operatorname{ord}_P \varphi = 0$.

Now we consider a possible pole of φ outside of $E[\alpha] \cup E[\beta]$. It comes from $\psi_{\alpha+\beta}\psi_{\alpha-\beta}$, hence it lies in $E[\alpha+\beta] \cup E[\alpha-\beta] - \{\mathcal{O}\}$. We consider three sub-cases. In case $P \in E[\alpha+\beta] - E[\alpha-\beta]$, we have $[\alpha](P) = -[\beta](P)$, which implies $\xi([\alpha](P)) = \xi([\beta](P))$. By definition, $\operatorname{ord}_P \psi_{\alpha+\beta} = 1$ and $\operatorname{ord}_P \psi_{\alpha-\beta} = 0$. Hence $\operatorname{ord}_P \varphi \geq 0$. The same is true for $P \in E[\alpha-\beta] - E[\alpha+\beta]$. Finally, assume $P \in E[\alpha+\beta] \cap E[\alpha-\beta]$ and $P \neq \mathcal{O}$. By the former condition, $2[\alpha](P) = \mathcal{O}$ and $2[\beta](P) = \mathcal{O}$. However, we have assumed $[\alpha](P) \neq \mathcal{O}$ and $[\beta](P) \neq \mathcal{O}$. Thus $[\alpha](P)$ and $[\beta](P)$ are non-trivial 2-torsion points of E. Since

$$\begin{aligned}\xi([\alpha](A-P)) &= \xi(-[\alpha](A-P)) = \xi([\alpha](-A) + [\alpha](P)) \\ &= \xi([\alpha](-A) - [\alpha](P)) = \xi([\alpha](-A-P))\end{aligned}$$

for all $A \in E$, we see that $\xi \circ [\alpha] \circ V_{-P}$ is an even function and that the expansion of $\xi \circ [\alpha]$ at P with respect to the local parameter $\tau \circ V_{-P}$ consists of even degree terms. The same holds for $[\beta]$. Therefore, $\xi([\alpha](P)) = \xi([\beta](P))$ means $\operatorname{ord}_P(\xi \circ [\alpha] - \xi \circ [\beta]) \geq 2$. On the other hand, $\operatorname{ord}_P \psi_{\alpha+\beta} = \operatorname{ord}_P \psi_{\alpha-\beta} = 1$. Consequently, $\operatorname{ord}_P \varphi \geq 0$.

Since φ has no poll at all, it is a constant function and its value is -1 by (3.4). This completes the proof.

COROLLARY 3.7. *Let α, β, γ be elements of O_F such that $\alpha \pm \beta$, $\beta \pm \gamma$, $\gamma \pm \alpha$ are unbiased. Then*

$$\tilde{\psi}_\beta \psi_{\alpha+\gamma} \psi_{\alpha-\gamma} - \tilde{\psi}_\alpha \psi_{\beta+\gamma} \psi_{\beta-\gamma} = \psi_{\alpha+\beta} \psi_{\alpha-\beta} \tilde{\psi}_\gamma.$$

PROOF. Again, the assertion is trivial for $\alpha\beta\gamma = 0$. Otherwise, this follows from Proposition 3.6 and the identity $(\xi \circ [\alpha] - \xi \circ [\gamma]) - (\xi \circ [\beta] - \xi \circ [\gamma]) = \xi \circ [\alpha] - \xi \circ [\beta]$.

Let ω be as in (2.2). For $\alpha \in F$, we put

$$\|\alpha\| := \max(|s|, |t|) \tag{3.5}$$

where $s, t \in \mathbf{Q}$ are uniquely determined by $\alpha = s + t\omega$.

PROPOSITION 3.8. *Let $\alpha \in O_F$ be unbiased. Then, there exist seven unbiased elements $\beta_1, \ldots, \beta_6 \in O_F$, $\delta \in \{1, 2, \omega, 1+\omega, 1-\omega, 1+2\omega\}$ and $t \in \{0, 1, 3\}$ satisfying the following conditions:*

(1) $\psi_\alpha = (\psi_{\beta_1}^2 \psi_{\beta_2} \psi_{\beta_3} - \psi_{\beta_4}^2 \psi_{\beta_5} \psi_{\beta_6})/\psi_\delta^t$

(2) $\|\beta_i\| \leq \frac{1}{2}\|\alpha\| + 2$ *for all i*

Explicitly, the following formulas holds for $u \in O_F$: In case of $d \equiv 3 \bmod 4$,

$$\begin{aligned}
\psi_{2u} &= \psi_u(\psi_{u-1}^2 \psi_{u+2} - \psi_{u+1}^2 \psi_{u-2})/\psi_2, \\
\psi_{2u+1} &= \psi_u^3 \psi_{u+2} - \psi_{u+1}^3 \psi_{u-1}, \\
\psi_{2u+\omega} &= (\psi_u^3 \psi_{u+2\omega} - \psi_{u+\omega}^3 \psi_{u-\omega})/\psi_\omega^3, \\
\psi_{2u+1+\omega} &= (\psi_u^3 \psi_{u+2+2\omega} - \psi_{u+1+\omega}^3 \psi_{u-1-\omega})/\psi_{1+\omega}^3.
\end{aligned} \tag{3.6}$$

Let $u = m + n\omega$ with $m, n \in \mathbf{Z}$. In case of $d \equiv 7 \bmod 8$,

(3.7)

$$\begin{aligned}
\psi_{2u} &= \psi_u(\psi_{u-1}^2 \psi_{u+2} - \psi_{u+1}^2 \psi_{u-2})/\psi_2 \qquad (n : \text{even}), \\
\psi_{2u} &= (\psi_{u-\omega}^2 \psi_{u+1+\omega} \psi_{u-1+\omega} - \psi_{u+\omega}^2 \psi_{u+1-\omega} \psi_{u-1-\omega})/\psi_{2\omega} \qquad (n : \text{odd}), \\
\psi_{2u+1} &= \psi_u^3 \psi_{u+2} - \psi_{u+1}^3 \psi_{u-1} \qquad (n : \text{even}), \\
\psi_{2u+1} &= (\psi_{u-\omega}^2 \psi_{u+2+\omega} \psi_{u+\omega} - \psi_{u+1+\omega}^2 \psi_{u+1-\omega} \psi_{u-1-\omega})/\psi_{1+2\omega} \qquad (n : \text{odd}).
\end{aligned}$$

In case of $d \equiv 1 \bmod 4$, *in addition to (3.7), we have*

(3.8)

$$\psi_{2u+\omega} = (\psi_u^3 \psi_{u+2\omega} - \psi_{u+\omega}^3 \psi_{u-\omega})/\psi_\omega^3 \qquad (m : \text{even}),$$

$$\psi_{2u+\omega} = (\psi_{u-1}^2 \psi_{u+1+2\omega} \psi_{u+1} - \psi_{u+1+\omega}^2 \psi_{u-1+\omega} \psi_{u-1-\omega})/\psi_\omega^3 \qquad (m : \text{odd}).$$

Similarly, in case of $d \equiv 2 \bmod 4$, *we have (3.7) and*

(3.9)

$$\psi_{2u+1+\omega} = (\psi_u^3 \psi_{u+2+2\omega} - \psi_{u+1+\omega}^3 \psi_{u-1-\omega})/\psi_{1+\omega}^3 \qquad (m \equiv n \bmod 2),$$

$$\psi_{2u+1+\omega} = (\psi_{u+\omega}^3 \psi_{u+2-\omega} - \psi_{u+1}^3 \psi_{u-1+2\omega})/\psi_{1-\omega}^3 \qquad (m \not\equiv n \bmod 2).$$

PROOF. Recurrence formulas (3.6)–(3.9) are immediate consequence of Corollary 3.7, which implies the existence of $\beta_1, \ldots, \beta_6$, δ and t. Unbiasedness of $\beta_1, \ldots, \beta_6$ and δ follows from Corollary 2.8. Finally, the assertion (2) is a consequence of the inequality

$$\|x + y\| \le \frac{1}{2}\|2x + z\| + \left\|y - \frac{z}{2}\right\|$$

for any $x, y, z \in F$.

4. Integrality of Division Polynomials

Let T be an indeterminate. For an unbiased element $\alpha \in O_F$, define $\Psi_\alpha(T) \in K[T]$ by

$$\psi_\alpha = \Psi_\alpha(\xi) \qquad (N_{F/\mathbf{Q}}(\alpha) \text{ is odd}),$$

$$\frac{1}{\eta}\psi_\alpha = \Psi_\alpha(\xi) \qquad (N_{F/\mathbf{Q}}(\alpha) \text{ is even}).$$

In this section, we prove that $\Psi_\alpha \in O_K[T]$. For a nonzero ideal $\mathfrak{a}$ of O_F, we put

$$\Delta_\mathfrak{a}(T) := \prod_{P \in E[\mathfrak{a}] - \{\mathcal{O}\}} (T - \xi(P)).$$

As before, we write $\Delta_{\langle\alpha\rangle_F}$ as Δ_α for $\alpha \in O_F$. Note

$$\text{div}\, \Delta_\mathfrak{a}(\xi) = 2\left(\sum_{P \in E[\mathfrak{a}]} [P] - N(\mathfrak{a})[\mathcal{O}]\right) \tag{4.1}$$

and hence

$$\Delta_\alpha(T) = \begin{cases} \alpha^{-2}\Psi_\alpha(T)^2 & (N_{F/\mathbf{Q}}(\alpha) \text{ is odd}), \\ \alpha^{-2}C(T)\Psi_\alpha(T)^2 & (N_{F/\mathbf{Q}}(\alpha) \text{ is even}). \end{cases} \tag{4.2}$$

Here, $C(T) := T^3 + aT + b$ with a, b defined in (1.2). Let $\mathfrak{P}$ be a prime ideal of O_K lying above a prime ideal $\mathfrak{p}$ of O_F. Recall that $\mathfrak{P}$-adic valuation has the standard extension to $K(T)$ in the sense of Zariski and Samuel[13, §IV.13], namely,

$$\operatorname{ord}_{\mathfrak{P}}\left(\sum_{i=0}^{n} \alpha_i T^i\right) := \min_{0 \le i \le n} \operatorname{ord}_{\mathfrak{P}} \alpha_i$$

on $K[T]$. In order to prove $\Psi_\alpha(T) \in O_K[T]$, it is suffice to prove

$$\operatorname{ord}_{\mathfrak{P}} \Delta_\alpha(T) \ge -2 \operatorname{ord}_{\mathfrak{P}} \alpha$$

for any prime ideal $\mathfrak{P}$. The fact that $\#E[m] = m^2$ for $m \in \mathbf{N}$ cause a difficulty to the proof of the above formula. Let A be an torsion point of E of order p^m. Then, as is well known (see e.g. Silverman [10, Th. VII.3.4]),

$$\operatorname{ord}_{\mathfrak{P}} \xi(A) \ge -2\frac{\operatorname{ord}_{\mathfrak{P}} p}{p^m - p^{m-1}}. \tag{4.3}$$

This inequality implies, for example,

$$\operatorname{ord}_{\mathfrak{P}} \Delta_p(T) \ge -2\frac{p^2 - 1}{p - 1} \operatorname{ord}_{\mathfrak{P}} p$$

which is insufficient for our purpose. This problem might be solved by the sharper inequality obtained by Oshikawa [9, Th. 4] with fine arguments on hight of the formal group associated the reduction of E at $\mathfrak{P}$ (including bad reductions). Here we employ an another method. We utilize the fact that $\Psi_n(T) \in O_K[T]$ for $n \in \mathbf{N}$. (This is well known. See e.g. Silverman [10, Exercise 3.7]. Recall that in (1.2), we assumed that a and b are algebraic integers.)

For a prime ideal $\mathfrak{p}$ of the Dedekind domain R and a non-zero ideal $\mathfrak{a}$ of a subring of R, we denote by $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$ the largest integer e such that $\mathfrak{p}^e$ divides $R\mathfrak{a}$.

LEMMA 4.1. *Let $\mathfrak{p}$ be a prime ideal of O_F and $\mathfrak{P}$ a prime ideal of O_K lying above $\mathfrak{p}$. Let $\mathfrak{a}$ be an ideal of O_F and put $e := \operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$. Then,* $\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{a}}(T) = \operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T)$.

PROOF. There exists an ideal $\mathfrak{b}$ of O_F such that $\mathfrak{a} = \mathfrak{p}^e\mathfrak{b}$. Recall $E[\mathfrak{a}] = E[\mathfrak{p}^e] \oplus E[\mathfrak{b}]$ by Lemma 2.4. Thus

$$\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{a}}(T) = \sum_{\substack{P \in E[\mathfrak{p}^e],\ Q \in E[\mathfrak{b}] \\ P \ne \mathcal{O} \text{ or } Q \ne \mathcal{O}}} \operatorname{ord}_{\mathfrak{P}}(T - \xi(P + Q)) \tag{4.4}$$

We show $\operatorname{ord}_{\mathfrak{P}} \xi(P+Q) \geq 0$ for $Q \neq \mathcal{O}$. Let $u \in \mathfrak{b} - \mathfrak{p}$. Put $A := P + Q$ and assume $\operatorname{ord}_{\mathfrak{P}} \xi(A) < 0$. Hence, A belongs to the group of points of the formal group associated to E over the $\mathfrak{P}$-adic completion of K at $\mathfrak{P}$. Let $r \in \mathfrak{p}^e$ be arbitrary. Since $\operatorname{End}(E)$ is commutative, $[u][r]A = [u][r]P + [r][u]Q = \mathcal{O}$. However, u is a $\mathfrak{P}$-adic unit and thus $[r]A = \mathcal{O}$. This implies $A \in E[\mathfrak{p}^e]$. Hence, $Q = P - A \in E[\mathfrak{p}^e]$, which contradicts to $Q \neq \mathcal{O}$ by Lemma 2.4. Therefore, $\operatorname{ord}_{\mathfrak{P}}(T - \xi(P+Q)) = 0$ for $Q \neq \mathcal{O}$ and the right hand side of (4.4) is

$$\sum_{P \in E[\mathfrak{p}^e] - \{\mathcal{O}\}} \operatorname{ord}_{\mathfrak{P}}(T - \xi(P)) = \operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T).$$

PROPOSITION 4.2. *Let $\mathfrak{a}$ be a non-zero ideal of O_F. Then,* $\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{a}}(T) \geq -2 \operatorname{ord}_{\mathfrak{P}} \mathfrak{a}$ *for a prime ideal $\mathfrak{P}$ of O_K.*

PROOF. Put $\mathfrak{p} := O_F \cap \mathfrak{P}$ and $e := \operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$. Let p be the prime number belonging to $\mathfrak{p}$. By the preceding lemma, we have only to prove

$$\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T) \geq -2e \operatorname{ord}_{\mathfrak{P}} \mathfrak{p}. \tag{4.5}$$

We consider three cases:

In case that p splits: we have $\operatorname{ord}_{\mathfrak{P}} \mathfrak{p} = \operatorname{ord}_{\mathfrak{P}} p$ and $E[\mathfrak{p}^e] \cong \mathbf{Z}/p^e\mathbf{Z}$. For $1 \leq m \leq e$, there are exactly $p^m - p^{m-1}$ points in $E[\mathfrak{p}^e]$ whose order is p^m. By (4.3),

$$\begin{aligned} \operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T) &= \sum_{P \in E[\mathfrak{p}^e] - \{\mathcal{O}\}} \min(0, \operatorname{ord}_{\mathfrak{P}} \xi(P)) \\ &\geq \sum_{m=1}^{e} (p^m - p^{m-1}) \frac{-2 \operatorname{ord}_{\mathfrak{P}} p}{p^m - p^{m-1}} = -2e \operatorname{ord}_{\mathfrak{P}} \mathfrak{p}. \end{aligned}$$

In case that p remains prime: Noting (4.2) and $\Psi_{p^e}(T) \in O_K[T]$, we have

$$\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T) = -2 \operatorname{ord}_{\mathfrak{P}} p^e + 2 \operatorname{ord}_{\mathfrak{P}} \Psi_{p^e}(T) \geq -2e \operatorname{ord}_{\mathfrak{P}} \mathfrak{p}.$$

In case that p ramifies: Assume first that e is even. Then, $\mathfrak{p}^e = \langle p^{e/2} \rangle_F$ and assertion follows the same argument as above. Let e be odd. In case of $e = 1$, we have $E[\mathfrak{p}] \cong \mathbf{Z}/p\mathbf{Z}$ and (4.5) holds by the same reason as the split case. Now assume $e \geq 3$ and put $n := (e-1)/2$ and $q := p^n$. As is well known $\xi \circ [q] = \xi - \psi_{q+1}\psi_{q-1}/\psi_q^2$ (which can also be proved by Proposition 3.6). Then, by a similar proof to Lemma 3.5, we have

$$\Delta_{\mathfrak{p}^e}(\xi) = q^{2(p-1)} \Delta_{\mathfrak{p}}(\xi \circ [q]) \Delta_q(\xi)^p = q^{-2} \Delta_{\mathfrak{p}}(\xi \psi_q^2 - \psi_{q-1}\psi_{q+1})\psi_q^2.$$

Thus,

$$\Delta_{\mathfrak{p}^e}(T) = \begin{cases} q^{-2}\Delta_{\mathfrak{p}}(G_q(T))\Psi_q(T)^2 & (p \neq 2), \\ q^{-2}\Delta_{\mathfrak{p}}(G_q(T))C(T)\Psi_q(T)^2 & (p = 2), \end{cases}$$

where

$$G_q(T) := \begin{cases} T\Psi_q(T)^2 - C(T)\Psi_{q-1}(T)\Psi_{q+1}(T) & (p \neq 2), \\ TC(T)\Psi_q(T)^2 - \Psi_{q-1}(T)\Psi_{q+1}(T) & (p = 2). \end{cases}$$

Because $\Psi_i(T) \in O_K[T]$ for any $i \in \mathbf{N}$, the polynomial $G_q(T)$ also belongs to $O_K[T]$. Thus,

$$\operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}^e}(T) \geq -2 \operatorname{ord}_{\mathfrak{P}} q + \operatorname{ord}_{\mathfrak{P}} \Delta_{\mathfrak{p}}(T) = -2e \operatorname{ord}_{\mathfrak{P}} \mathfrak{p}.$$

COROLLARY 4.3. *Let $\alpha \in O_F$ be unbiased. Then $\Psi_\alpha(T) \in O_K[T]$ and $\psi_\alpha \in O_K[\xi, \eta]$.*

5. Space Complexity for Polynomial Arithmetic Operations

We estimate space complexities for arithmetic operations on $O_K[T]$ where T is an indeterminate. Estimates for additions, subtractions and multiplication are simple. However, divisions give rise to a difficulty. For an integer n and its divisor m, the bit size of the quotient n/m is not greater than that of n. Such a property does not holds for $O_K[T]$. In order to clarify an obstacle, let us consider the integer ring $\mathbf{Z}[\sqrt{2}]$ of the *real* quadratic field $\mathbf{Q}(\sqrt{2})$. Then, $\sqrt{2} - 1$ is a unit and $(\sqrt{2} - 1)^n$ divides 1 for any $n \in \mathbf{N}$. But bit size of $1/(\sqrt{2} - 1)^n$ is, in any sense, unbounded as n tends to infinity because finitely many bits can represent finitely many elements in $\mathbf{Z}[\sqrt{2}]$. This suggests that we need to utilize the fact that F is an imaginary quadratic field in order to bound the space complexity. Our method is based on the fact that the bit size of $\alpha \in O_K$ is not that different from $L_K(\alpha) := \max_i \log_2 N_{F/\mathbf{Q}}(a_i)$ where $\alpha = \sum_i a_i\theta^i$ with $K = F(\theta)$.

First we note a technical lemma whose proof is given in Appendix. Although it looks like an abstract nonsense, such an abstraction is necessary because it is used twice in subsequent proofs with different coefficient rings. Let R be an integral domain. For polynomials f and $g \in R[T]$ we denote by $\operatorname{quo}(f, g)$ (resp. $\operatorname{rem}(f, g)$) the quotient (resp. remainder) of the division f/g in $k[T]$ where k is the field of fractions of R.

LEMMA 5.1. *Let R be an integral domain. Let $L \in \operatorname{Map}(R, \mathbf{R} \cup \{-\infty\})$ be a map satisfying the following conditions.*

(5.1) $L(0) = -\infty$.

(5.2) *There exists a constant* $c_1 \geq 0$ *such that* $L(\alpha \pm \beta) \leq \max(L(\alpha), L(\beta)) + c_1$ *for all* $\alpha, \beta \in R$.

(5.3) *There exists a constant* $c_2 \geq 0$ *such that* $L(\alpha\beta) \leq L(\alpha) + L(\beta) + c_2$ *for all* $\alpha, \beta \in R$.

For such a map L, *we define* $\tilde{L} \in \mathrm{Map}(R[T], \mathbf{R} \cup \{-\infty\})$ *by*

$$\tilde{L}\left(\sum_{i=0}^{n} a_i T^i\right) := \max_{0 \leq i \leq n} L(a_i). \tag{5.4}$$

Then, for polynomials $f, g \in R[T]$, *the following inequalities hold.*

(a) $\tilde{L}(f \pm g) \leq \max(\tilde{L}(f), \tilde{L}(g)) + c_1$.

(b) $\tilde{L}(fg) \leq \tilde{L}(f) + \tilde{L}(g) + c_1 \min(\deg f, \deg g) + c_2$.

(c) *Assume* $g \neq 0$ *and*

$$L(\mathrm{lc}(g)\alpha) \geq L(\alpha) \tag{5.5}$$

for all $\alpha \in R$. *Assume also* $\mathrm{quo}(f, g) \in R[T]$. *Put* $c_3 := \max(\tilde{L}(g) + c_1 + c_2, 0)$ *and* $\delta := \max(\deg f - \deg g, -1)$. *Then, we have*

$$\tilde{L}(\mathrm{quo}(f, g)) \leq \tilde{L}(f) + \delta c_3 \tag{5.6}$$

and

$$\tilde{L}(\mathrm{rem}(f, g)) \leq \tilde{L}(f) + (\delta + 1)c_3. \tag{5.7}$$

We now consider the computational complexity of arithmetic operations on $O_K[T]$. Let ω be as in (2.2). Put $\nu := [K : F]$ and take $\theta \in K$ satisfying $K = F(\theta)$. Later, we require θ to be an element of O_K, but for now θ is not necessarily an algebraic integer. Let H be the monic minimal polynomial of θ over F. It is important to construct K as a simple extension over F, not that over $\mathbf{Q}$. Define $L_F \in \mathrm{Map}(F, \mathbf{R} \cup \{-\infty\})$ and $L_K \in \mathrm{Map}(K, \mathbf{R} \cup \{-\infty\})$ by

$$L_F(\alpha) := \begin{cases} \log_2 N_{F/\mathbf{Q}}(\alpha) & (\alpha \neq 0) \\ -\infty & (\alpha = 0) \end{cases}$$

and

$$L_K\left(\sum_{i=0}^{\nu-1} a_i \theta^i\right) := \max_{0 \leq i < \nu} L_F(a_i),$$

respectively. Let $\tilde{L}_F$ be the extension of L_F to $F[T]$ as was done in (5.4).

THEOREM 5.2. *For $\alpha, \beta \in K$ and $c \in F$, we have*

$$L_K(c\alpha) = L_F(c) + L_K(\alpha),$$

$$L_K(\alpha + \beta) \leq \max(L_K(\alpha), L_K(\beta)) + 2,$$

$$L_K(\alpha\beta) \leq L_K(\alpha) + L_K(\beta) + (\nu - 1)(\tilde{L}_F(H) + 4).$$

PROOF. Put $\mathscr{P} := \{f \in F[T] : \deg(f) < \nu\}$. Determine A and $B \in \mathscr{P}_F$ by $\alpha = A(\theta)$ and $\beta = B(\theta)$, respectively. By definition, $L_K(\alpha) = \tilde{L}_F(A)$ and $L_K(\beta) = \tilde{L}_F(B)$. Since T is mapped to θ by the map $F[T] \to F[T]/\langle H \rangle_{F[T]} \cong K$, we have $L_K(\alpha + \beta) = \tilde{L}_F(A + B)$, $L_K(\alpha\beta) = \tilde{L}_F(\mathrm{rem}(AB, H))$ and $L_K(c\alpha) = \tilde{L}_F(cA)$. On the other hand, it is obvious that L_F satisfies (5.1) and (5.3) with $c_2 = 0$. By (3.3), we have

$$L_F(\alpha + \beta) \leq \max(L_F(\alpha), L_F(\beta)) + 2$$

for $\alpha, \beta \in F$, which shows that L_F satisfies (5.2) with $c_1 = 2$. Hence Lemma 5.1 is applicable to L_F and the first two assertions are proved. Since H is monic, the condition (5.5) for $L = L_F$ and $g = H$ is clearly satisfied. Thus, the last assertion follows from Lemma 5.1.

COROLLARY 5.3. *Let $\tilde{L}_K \in \mathrm{Map}(K[T], \mathbf{R} \cup \{-\infty\})$ be the extension of L_K as in (5.4).*

(a) *There exists a constant $c_4 > 0$ such that $\tilde{L}_K(f + g) \leq \max(\tilde{L}_K(f), \tilde{L}_K(g)) + c_4$ for all $f, g \in K[T]$.*

(b) *There exists a constant $c_5 > 0$ such that $\tilde{L}_K(fg) \leq \tilde{L}_K(f) + \tilde{L}_K(g) + (\min(\deg f, \deg g) + 1)c_5$ for all $f, g \in K[T]$.*

(c) *Let $g \in K[T]$ and assume $\mathrm{lc}(g) \in O_F$. Then, there exist a constant $c_6 > 0$ (depending on g) such that $\tilde{L}_K(\mathrm{quo}(f, g)) \leq \tilde{L}_K(f) + \delta c_6$ and that $\tilde{L}_K(\mathrm{rem}(f, g)) \leq \tilde{L}_K(f) + (\delta + 1)c_6$ for all $f \in K[T]$ where $\delta := \max(\deg f - \deg g, -1)$.*

PROOF. The corollary is an immediate consequence of Lemma 5.1 and Theorem 5.2.

From now on, we assume $\theta \in O_K$ and put $D := [O_K : O_F[\theta]]$. We represent $\alpha \in O_K$ as a ν-tuple $(\alpha_0, \ldots, \alpha_{\nu-1}) \in O_F^\nu$ where $\alpha = \sum_{i=0}^{\nu-1} \alpha_i \theta^i / D$. Each $u \in O_F$ is represented as a pair of integers (m, n) determined by $u = m + n\omega$ where ω is defined as (2.2). On the other hand, we put $S_F(m + n\omega) := \log_2(\max(|m|, 1)) + \log_2(\max(|n|, 1)) + 6$ and $S_K(\alpha) := \sum_{i=0}^{\nu-1} S_F(\alpha_i)$. The value $S_F(u)$ is considered to be the bit size to store $u \in O_F$ (not including length of m and n) by the data structure described as above.

THEOREM 5.4. *There exist constants* $c_7 > 0$ *and* $c_8 > 0$ *satisfying*

$$\frac{1}{2}L_K(\alpha) - c_7 \leq S_K(\alpha) \leq \nu L_K(\alpha) + c_8$$

for all non-zero $\alpha \in O_K$.

PROOF. Let $u := m + n\omega$ with $m, n \in \mathbf{Z}$ and $\alpha := \sum_{i=0}^{\nu-1} \alpha_i \theta^i / D$ with $\alpha_i \in O_F$. Apparently, $N_{F/\mathbf{Q}}(u) \leq (d+3)\max(m^2, n^2)$. Hence, there is a constant c_9 such that $\log_2 N_{F/\mathbf{Q}}(u) \leq c_9 + 2S_F(u)$ for all $u \in O_F$. Thus,

$$L_K(D\alpha) = \max_{0 \leq i < \nu} L_F(\alpha_i) \leq c_9 + 2 \max_{0 \leq i < \nu} S_F(\alpha_i) \leq c_9 + 2S_K(\alpha).$$

The left hand side is not less than $L_K(\alpha)$ since $D \in \mathbf{N}$. Conversely, $m^2 \leq \frac{4}{3}N_{F/\mathbf{Q}}(u)$ and $n^2 \leq \frac{4}{3}N_{F/\mathbf{Q}}(u)$. These are obvious for $d \not\equiv 3 \bmod 4$ (recall $F = \mathbf{Q}(\sqrt{-d})$). In case of $d \equiv 3 \bmod 4$, they follow from

$$N_{F/\mathbf{Q}}(m + n\omega) = \left(m - \frac{n}{2}\right)^2 + \frac{d}{4}n^2 = \frac{d+1}{4}\left(n - \frac{2}{d+1}m\right)^2 + \frac{d}{d+1}m^2.$$

and $d \geq 3$. Hence, there exists a constant c_{10} such that $S_F(u) \leq L_F(u) + c_{10}$ for all $u \in O_F - \{0\}$. We have $L_F(\alpha_i) \leq L_K(\alpha) + \log_2 D$ for all $0 \leq i < \nu$. Thus,

$$\begin{aligned} S_K(\alpha) &\leq \sum_{\alpha_i \neq 0} (L_F(\alpha_i) + c_{10}) + 6\#\{i : \alpha_i = 0\} \\ &\leq \nu \left(L_K(\alpha) + \log_2 D + c_{10} + 6\right). \end{aligned}$$

This concludes the proof.

Using the above results, we have, for example, $S_K(\alpha\beta) \leq 2\nu(S_K(\alpha) + S_K(\beta)) + O(1)$ for $\alpha, \beta \in O_K - \{0\}$. However, this is insufficient for our purpose. In the next section, we work with L_K as much as possible and use Theorem 5.4 only once during the proof on a space complexity.

6. Complexity to Compute Generalized Division Polynomials

We give time and space complexities to compute $\Psi_\alpha(T)$ as $\|\alpha\|$ tends to infinity. Recall that E is a fixed elliptic curve $Y^2 = C(X)$ where $C(T) = T^3 + aT + b$ (cf. (1.2)). We keep notation in the previous sections. For $f(T) := \sum_{i=0}^{n} \alpha_i T^i \in O_K[T]$, we put $\sigma(f) := \max_{0 \leq i < n} S_K(\alpha_i)$. Throughout this section, let μ be a constant such that the number of bit operations to multiply two n bit integers is $O(n^\mu)$ and that the number of arithmetic operations of a coefficient ring to multiply two polynomials of degree less than n is $O(n^\mu)$. In

what follows, $c_{11}, c_{12}, \ldots$ stand for suitable positive constants depending only on E.

First, we convert recurrence formulas (3.6)–(3.9) in terms of Ψ_u's and C, i.e. polynomials of one variable. The result is as follows. Let $u = m + n\omega$ with $m, n \in \mathbf{Z}$. In case of $d \equiv 3 \bmod 4$,

$$\Psi_{2u} = \begin{cases} \Psi_u(\Psi_{u-1}^2\Psi_{u+2} - \Psi_{u+1}^2\Psi_{u-2})/2C & (n : \text{odd}), \\ \Psi_u(\Psi_{u-1}^2\Psi_{u+2} - \Psi_{u+1}^2\Psi_{u-2})/2 & (n : \text{even}), \end{cases} \tag{6.1}$$

$$\Psi_{2u+1} = \begin{cases} \Psi_u^3\Psi_{u+2} - \Psi_{u+1}^3\Psi_{u-1}, & (n : \text{odd}), \\ C^2\Psi_u^3\Psi_{u+2} - \Psi_{u+1}^3\Psi_{u-1}, & (m : \text{even}, n : \text{even}), \\ \Psi_u^3\Psi_{u+2} - C^2\Psi_{u+1}^3\Psi_{u-1}, & (m : \text{odd}, n : \text{even}), \end{cases} \tag{6.2}$$

$$\Psi_{2u+\omega} = \begin{cases} (\Psi_u^3\Psi_{u+2\omega} - \Psi_{u+\omega}^3\Psi_{u-\omega})/\Psi_\omega^3, & (m : \text{odd}), \\ (C^2\Psi_u^3\Psi_{u+2\omega} - \Psi_{u+\omega}^3\Psi_{u-\omega})/\Psi_\omega^3, & (m : \text{even}, n : \text{even}), \\ (\Psi_u^3\Psi_{u+2\omega} - C^2\Psi_{u+\omega}^3\Psi_{u-\omega})/\Psi_\omega^3, & (m : \text{even}, n : \text{odd}), \end{cases} \tag{6.3}$$

$$\Psi_{2u+1+\omega} = \begin{cases} \frac{\Psi_u^3\Psi_{u+2+2\omega} - \Psi_{u+1+\omega}^3\Psi_{u-1-\omega}}{\Psi_{1+\omega}^3} & (m \not\equiv n \bmod 2), \\ \frac{C^2\Psi_u^3\Psi_{u+2+2\omega} - \Psi_{u+1+\omega}^3\Psi_{u-1-\omega}}{\Psi_{1+\omega}^3} & (m \equiv n \equiv 0 \bmod 2), \\ \frac{\Psi_u^3\Psi_{u+2+2\omega} - C^2\Psi_{u+1+\omega}^3\Psi_{u-1-\omega}}{\Psi_{1+\omega}^3} & (m \equiv n \equiv 1 \bmod 2). \end{cases} \tag{6.4}$$

In case of $d \equiv 7 \bmod 8$, recurrence formulas are

$$\Psi_{2u} = \begin{cases} \frac{\Psi_u(\Psi_{u-1}^2\Psi_{u+2} - \Psi_{u+1}^2\Psi_{u-2})}{2} & (n : \text{even}), \\ \frac{\Psi_{u-\omega}^2\Psi_{u+1+\omega}\Psi_{u-1+\omega} - \Psi_{u+\omega}^2\Psi_{u+1-\omega}\Psi_{u-1-\omega}}{\Psi_{2\omega}} & (n : \text{odd}), \end{cases} \tag{6.5}$$

$$\Psi_{2u+1} = \begin{cases} C^2\Psi_u^3\Psi_{u+2} - \Psi_{u+1}^3\Psi_{u-1}, & (m : \text{even}, n : \text{even}), \\ \Psi_u^3\Psi_{u+2} - C^2\Psi_{u+1}^3\Psi_{u-1}, & (m : \text{odd}, n : \text{even}), \\ \frac{C^2\Psi_{u-\omega}^2\Psi_{u+2+\omega}\Psi_{u+\omega} - \Psi_{u+1+\omega}^2\Psi_{u+1-\omega}\Psi_{u-1-\omega}}{\Psi_{1+2\omega}} & (m : \text{even}, n : \text{odd}), \\ \frac{\Psi_{u-\omega}^2\Psi_{u+2+\omega}\Psi_{u+\omega} - C^2\Psi_{u+1+\omega}^2\Psi_{u+1-\omega}\Psi_{u-1-\omega}}{\Psi_{1+2\omega}} & (m : \text{odd}, n : \text{odd}). \end{cases} \tag{6.6}$$

In case of $d \equiv 1 \bmod 4$, in addition to (6.5) and (6.6), we use

$$\Psi_{2u+\omega} = \begin{cases} \frac{C^2\Psi_u^3\Psi_{u+2\omega}-\Psi_{u+\omega}^3\Psi_{u-\omega}}{\Psi_\omega^3} & (m : \text{even}, n : \text{even}), \\ \frac{\Psi_u^3\Psi_{u+2\omega}-C^2\Psi_{u+\omega}^3\Psi_{u-\omega}}{\Psi_\omega^3} & (m : \text{even}, n : \text{odd}), \\ \frac{C^2\Psi_{u-1}^2\Psi_{u+1+2\omega}\Psi_{u+1}-\Psi_{u+1+\omega}^2\Psi_{u-1+\omega}\Psi_{u-1-\omega}}{\Psi_\omega^3} & (m : \text{odd}, n : \text{even}), \\ \frac{\Psi_{u-1}^2\Psi_{u+1+2\omega}\Psi_{u+1}-C^2\Psi_{u+1+\omega}^2\Psi_{u-1+\omega}\Psi_{u-1-\omega}}{\Psi_\omega^3} & (m : \text{odd}, n : \text{odd}). \end{cases} \tag{6.7}$$

Similarly, in case of $d \equiv 2 \bmod 4$, we use (6.5) and (6.6) and

$$\Psi_{2u+1+\omega} = \begin{cases} \frac{C^2\Psi_u^3\Psi_{u+2+2\omega}-\Psi_{u+1+\omega}^3\Psi_{u-1-\omega}}{\Psi_{1+\omega}^3} & (m \equiv n \equiv 0 \bmod 2), \\ \frac{\Psi_u^3\Psi_{u+2+2\omega}-C^2\Psi_{u+1+\omega}^3\Psi_{u-1-\omega}}{\Psi_{1+\omega}^3} & (m \equiv n \equiv 1 \bmod 2), \\ \frac{C^2\Psi_{u+\omega}^3\Psi_{u+2-\omega}-\Psi_{u+1}^3\Psi_{u-1+2\omega}}{\Psi_{1-\omega}^3} & (m : \text{even}, n : \text{odd}), \\ \frac{\Psi_{u+\omega}^3\Psi_{u+2-\omega}-C^2\Psi_{u+1}^3\Psi_{u-1+2\omega}}{\Psi_{1-\omega}^3} & (m : \text{odd}, n : \text{even}). \end{cases} \tag{6.8}$$

For completeness, we present an algorithm to compute Ψ_u.

ALGORITHM 6.1.
Input: unbiased $\alpha \in O_F$, $a, b \in O_K$, square free $d \in \mathbf{N}$.
Output: Ψ_α
Procedure:
1: if ($\|\alpha\| \leq 4$) {
2: if (Ψ_α is not yet computed) {
3: compute Ψ_α by Stark's method (or its variant) and store it
4: }
5: return Ψ_α;
6: }
7: compute Ψ_α by one of suitable formulas (6.1)–(6.8) (recursive call)
8: return Ψ_α;

REMARK 6.2. Since $\Psi_{-\alpha} = -\Psi_\alpha$, without loss of generality, we can restrict α to have non-negative real part. In practice, we have better to use a recurrence formula to compute $\Psi_{4\pm4\omega}$ and $\Psi_{4\pm3\omega}$ (if $4 \pm 3\omega$ is unbiased).

In the rest of this section, we analyze computational complexities of Algorithm 6.1. Since we store Ψ_α only for $\|\alpha\| \leq 4$, the asymptotic space complexity is bounded by $O(N_{F/\mathbf{Q}}(\alpha)\sigma(\Psi_\alpha))$. Once its space complexity is known,

we can estimate time complexities for multiplications needed in evaluation of recurrence formulas. In order to evaluate whole complexity of Algorithm 6.1, we need a growth rate estimate concerning such an algorithm containing recursive call. This is a variant of Aho, Ullman, Hopcroft [2, Theorem 2.1]. The proof will be given in Appendix.

LEMMA 6.3. *Let $a > 0$, $b > 0$, $c \geq 0$, $d \geq 0$ be real numbers and let $k \geq 2$, $l \geq 0$ be integers. Let $\gamma \in \mathrm{Map}(\mathbf{N}, \mathbf{R}_{>0})$ is a monotone non decreasing function and assume γ satisfies*

$$\gamma(n) \leq a\gamma\left(\left[\frac{n}{k}\right] + l\right) + bn^c(\log n)^d \tag{6.9}$$

for all $n \geq M_1$ with a constant $M_1 \geq 1$. Then,

$$\gamma(n) = \begin{cases} O(n^{\log_k a}(\log n)^d) & (a > k^c), \\ O(n^c(\log n)^{d+1}) & (a = k^c), \\ O(n^c(\log n)^d) & (0 < a < k^c). \end{cases}$$

Now we can prove our main results.

THEOREM 6.4. *The following estimates hold as $\|\alpha\|$ tends to infinity: $\tilde{L}_K(\Psi_\alpha) = O(\|\alpha\|^2 \log \|\alpha\|)$ and $\sigma(\Psi_\alpha) = O(\|\alpha\|^2 \log \|\alpha\|)$.*

PROOF. For $n \in \mathbf{N}$, define

$$\lambda(n) := \max_{\|\alpha\| \leq n} \tilde{L}_K(\Psi_\alpha) \tag{6.10}$$

where $\|\cdot\|$ is defined in (3.5). A generic form of recurrence formulas is

$$\Psi_\alpha = (C^{2t_1}\Psi_{\beta_1}^2\Psi_{\beta_2}\Psi_{\beta_3} - C^{2t_2}\Psi_{\beta_4}^2\Psi_{\beta_5}\Psi_{\beta_6})/\Psi_\delta^t$$

where $t_1, t_2 \in \{0, 1\}$ and $\beta_1, \ldots, \beta_6, \delta, t$ are as in Proposition 3.8. Note there are finitely many (pricisely six) possibilities for δ. Since $\mathrm{lc}(\Psi_\delta) \in O_F$,

$$\begin{aligned} \tilde{L}_K(\Psi_\alpha) &\leq \tilde{L}_K(C^{2t_1}\Psi_{\beta_1}^2\Psi_{\beta_2}\Psi_{\beta_3} - C^{2t_2}\Psi_{\beta_4}^2\Psi_{\beta_5}\Psi_{\beta_6}) + (N_{F/\mathbf{Q}}(\alpha) + c_{11})c_{12} \\ &\leq \max(\tilde{L}_K(C^{2t_1}\Psi_{\beta_1}^2\Psi_{\beta_2}\Psi_{\beta_3}), \tilde{L}_K(C^{2t_2}\Psi_{\beta_4}^2\Psi_{\beta_5}\Psi_{\beta_6})) \\ &\qquad + c_{13}N_{F/\mathbf{Q}}(\alpha) + c_{14} \\ &\leq \max(2\tilde{L}_K(\Psi_{\beta_1}) + \tilde{L}_K(\Psi_{\beta_2}) + \tilde{L}_K(\beta_3), \\ &\qquad 2\tilde{L}_K(\Psi_{\beta_4}) + \tilde{L}_K(\Psi_{\beta_5}) + \tilde{L}_K(\Psi_{\beta_6})) + c_{15}N_{F/\mathbf{Q}}(\alpha) + c_{16}. \end{aligned}$$

Because of Proposition 3.8(2) and (6.10), we have $\tilde{L}_K(\Psi_{\beta_i}) \leq \lambda\left(\left[\frac{\|\alpha\|}{2}\right]+2\right)$ and hence

$$\tilde{L}_K(\Psi_\alpha) \leq 4\lambda\left(\left[\frac{\|\alpha\|}{2}\right]+2\right)+c_{15}N_{F/\mathbf{Q}}(\alpha)+c_{16}.$$

Apparently, $N_{F/\mathbf{Q}}(\alpha) \leq (3+d)\|\alpha\|^2$. Since λ is a monotone non-decreasing function,

$$\tilde{L}_K(\Psi_\alpha) \leq 4\lambda\left(\left[\frac{n}{2}\right]+2\right)+c_{17}n^2+c_{16}$$

for all $\|\alpha\| \leq n$. Taking maximum for $\|\alpha\| \leq n$, we obtain

$$\lambda(n) \leq 4\lambda\left(\left[\frac{n}{2}\right]+2\right)+c_{17}n^2+c_{16}.$$

Hence, $\lambda(n) = O(n^2 \log n)$ by Lemma 6.3. Now assertion on $\tilde{L}_K$ is obvious and that on σ follows from Theorem 5.4.

REMARK 6.5. As for ordinal division polynomials, McKee [8] proved $\sigma(\Psi_n) = O(n^2)$, which is better than our result by a factor of $\log n$. It is an open problem whether we can remove the $\log\|\alpha\|$ factor from our result.

THEOREM 6.6. *Let U_α be the number of bit operations to compute Ψ_α by Algorithm 6.1. Then, $U_\alpha = O((\|\alpha\|^4 \log\|\alpha\|)^\mu)$.*

PROOF. The proof is similar to the preceding theorem. Letting $\gamma(n) := \max_{\|\alpha\|\leq n} U_\alpha$, we obtain

$$\begin{aligned} U_\alpha &\leq 6\gamma\left(\left[\frac{\|\alpha\|}{2}\right]+2\right)+O((N_{F/\mathbf{Q}}(\alpha)\sigma(\Psi_\alpha))^\mu) \\ &= 6\gamma\left(\left[\frac{\|\alpha\|}{2}\right]+2\right)+O((\|\alpha\|\log\|\alpha\|)^\mu) \end{aligned}$$

by Theorem 6.4. Thus $\gamma(n) \leq 6\gamma([n/2]+2)+O((n^4\log n)^\mu)$. Since $\mu \geq 1$, we have $2^{4\mu} \geq 6$ regardless of a multiplication algorithm. Then Lemma 6.3 yields $\gamma(n) = O((n^4\log n)^\mu)$, which proves the theorem.

7. Appendix: proofs of technical lemmas

Here we present proofs of two technical lemmas for completeness. The proofs are not difficult but highly computational.

PROOF OF LEMMA 5.1. Put $n := \deg f$ and $m := \deg g$. Assume $f(T) = \sum_{i=0}^{n} f_i T^i$ and $g(T) = \sum_{i=0}^{m} g_i T^i$. For simplicity, we understand that $g_i = 0$ for $i < 0$ or $i > m$.

(a) This is obvious from (5.1) and (5.2).

(b) Note

$$L\left(\sum_{i=1}^{\nu} a_i\right) \leq \max_{1\leq i\leq \nu} L(a_i) + (\nu - 1)c_1$$

for $\nu \in \mathbf{N}$ and $a_1, \ldots, a_\nu \in R$. This follows from an induction on ν. Without loss of generality, we may assume $n \leq m$. Then,

$$\begin{aligned}\tilde{L}(fg) &= \max_{0\leq k\leq m+n} L\left(\sum_{0\leq i\leq n} f_i g_{k-i}\right)\\ &\leq \max_{0\leq k\leq m+n} \max_{0\leq i\leq n} (\tilde{L}(f_i) + \tilde{L}(g_{k-i}) + c_2) + nc_1,\end{aligned}$$

from which the assertion follows.

(c) Put $q := \mathrm{quo}(f, g)$ and $r := \mathrm{rem}(f, g)$ for simplicity. We use induction on δ. The assertion clearly holds for $\delta = -1$, i.e., $\deg f < \deg g$. In case of $\delta = 0$, the condition $q \in R[T]$ implies that f_n is a multiple of g_m and that q is a constant f_n/g_m. Hence $L(f_n) = L(g_m q) \geq L(q)$ by (5.5) and in particular (5.6) holds. Then

$$\begin{aligned}\tilde{L}(r) = \tilde{L}(f - qg) &= \max_{0\leq i\leq n-1} (L(f_i - qg_{i-n+m}))\\ &\leq \max_{0\leq i\leq n-1} (\max(L(f_i), L(f_n) + L(g_{i-n+m}) + c_2) + c_1)\\ &\leq \tilde{L}(f) + \tilde{L}(g) + c_1 + c_2 \leq \tilde{L}(f) + c_3.\end{aligned}$$

Assume (5.6) and (5.7) are true in case $\delta < k$ for $k \in \mathbf{N}$. Suppose $\delta = k$. Put $f' := \mathrm{quo}(f, T)$ and $q' := \mathrm{quo}(q, T)$. Then $T(f' - q'g) = q_0 g + r - f_0$ where q_0 is the constant term of q. Hence $q_0 g + r - f_0$ is divisible by T and we have $f' = q'g + r'$ with $r' := \mathrm{quo}(q_0 g + r - f_0, T)$. Hence $\deg r' < \deg g$, which implies $r' = \mathrm{rem}(f', g)$. Note $f', q', r' \in R[T]$. Since $\deg f' - \deg g = \delta - 1 < k$, we have

$$\tilde{L}(q') \leq \tilde{L}(f') + (\deg(q) - 1)c_3 \tag{7.1}$$

and

$$\tilde{L}(r') \leq \tilde{L}(f') + \deg(q)c_3 \tag{7.2}$$

by the induction hypothesis. On the other hand, $Tr' + f_0 = q_0 g + r$ implies

$$L(q_0) \leq \tilde{L}(Tr' + f_0) = \max(\tilde{L}(r'), L(f_0)) \tag{7.3}$$

and

$$\tilde{L}(r) \le \tilde{L}(Tr' + f_0) + c_3 \tag{7.4}$$

by the induction hypothesis for $\delta \le 0$. Now, (5.6) follows from (7.1)–(7.3). Similarly, we have

$$\begin{aligned}\tilde{L}(r) &\le \max(\tilde{L}(r'), L(f_0)) + c_3 \le \max(\tilde{L}(f') + \deg(q)c_3, L(f_0)) + c_3 \\ &\le \tilde{L}(f) + (\deg(q) + 1)c_3.\end{aligned}$$

Thus, all the assertions are proved.

PROOF OF LEMMA 6.3. Define $g \in \mathrm{Map}((1,\infty), \mathbf{R})$ by $g(t) := \gamma\left(\left[t + \frac{kl}{k-1}\right]\right)$ for $t \ge 1$. We observe

$$\left[\frac{1}{k}\left[t + \frac{kl}{k-1}\right]\right] + l \le \left[\frac{1}{k}\left(t + \frac{kl}{k-1}\right) + l\right] = \left[\frac{t}{k} + \frac{kl}{k-1}\right].$$

(Note that $\frac{kl}{k-1}$ is a solution x of the equation $x = \frac{x}{k} + l$.) Using non decreasing property of γ and (6.9) we see

$$\begin{aligned}g(t) &\le a\gamma\left(\left[\frac{1}{k}\left[t + \frac{kl}{k-1}\right]\right] + l\right) + b\left[t + \frac{kl}{k-1}\right]^c \left(\log\left[t + \frac{kl}{k-1}\right]\right)^d \\ &\le a\gamma\left(\left[\frac{t}{k} + \frac{kl}{k-1}\right]\right) + b\left(t + \frac{kl}{k-1}\right)^c \left(\log\left(t + \frac{kl}{k-1}\right)\right)^d\end{aligned}$$

for $t \ge M_1 - \frac{kl}{k-1}$. Hence, there exist positive constants M_2 and M_3 satisfying

$$g(t) \le ag\left(\frac{t}{k}\right) + M_2 t^c (\log t)^d$$

for all $t \ge M_3$. Assume $t \ge kM_3$ and define $M_4 \in \mathbf{N}$ by $M_3 \le tk^{-M_4} < kM_3$, or, explicitly $M_4 := \left[\log_k \frac{t}{M_3}\right]$. Then, for $0 \le i < M_4$, it holds that

$$a^i g\left(\frac{t}{k^i}\right) \le a^{i+1} g\left(\frac{t}{k^{i+1}}\right) + a^i M_2 \left(\frac{t}{k^i}\right)^c \left(\log\left(\frac{t}{k^i}\right)\right)^d.$$

Summing up this formula for $0 \le i < M_4$, we obtain

$$\begin{aligned}g(t) &\le a^{M_4} g\left(\frac{t}{k^{M_4}}\right) + t^c M_2 (\log t)^d \sum_{i=0}^{M_4-1} \left(\frac{a}{k^c}\right)^i \\ &\le \left(\frac{t}{M_3}\right)^{\log_k a} g(kM_3) + t^c M_2 (\log t)^d \sum_{i=0}^{M_4-1} \left(\frac{a}{k^c}\right)^i\end{aligned} \tag{7.5}$$

In case of $a > k^c$, we have

$$\sum_{i=0}^{M_4-1}\left(\frac{a}{k^c}\right)^i = \frac{k(ak^{-c})^{M_4}-1}{ak^{-c}-1} \le \frac{\frac{k(t/M_3)^{\log_k a}}{k^{c(\log_k(t/M_3)-1)}}-1}{ak^{-c}-1} = O(t^{\log_k a - c})$$

and hence $g(t) = O(t^{\log_k a}(\log t)^d)$. In case of $a = k^c$, the inequality (7.5) clearly shows $g(t) = O(t^c(\log t)^{d+1})$. In case of $0 < a < k^c$, the series $\sum_{i=0}^{\infty}\left(\frac{a}{k^c}\right)^i$ converges and therefore $g(t) = O(t^c(\log t)^d)$. The lemma follows from $\gamma(n) = g\left(n + \frac{kl}{k-1}\right)$.

REFERENCES

1. Abel, N. H., *Recherches sur les fonctions elliptiques*, J. Reine Angew. Math. 2 (1827), 101–181.
2. Aho, A. V., Hopcroft, J. E., Ullman, J. D., *The design and analysis of computer algorithms*, Reading, Mass., Addison-Wesley pub. 1974.
3. Cassels, J. W. S., *Lectures on elliptic curves*, London Math. Soc. Stud. Texts 24 (1991).
4. Chudnovsky, D. V., Chudnovsky, G. V., *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. 7 (1986), 385–434.
5. Durst, L. K., *The apparition problem for equianharmonic divisibility sequences*, Proc. Nat. Acad. Sci. U.S.A. 38 (1952), 330–333.
6. Joux, A., Morain, F., *Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe*, J. Number Theory 55 (1995), 108–128.
7. Koblitz, N., *Constructing elliptic curve cryptosystems in characteristic 2*, in *Advances in cryptology, CRYPTO 90*, ed. A. J. Menezes and S. A. Vanstone, Lecture Notes in Comput. Sci. 537 (1991), 156–167.
8. McKee, J., *Computing division polynomials*, Math. Comp. 63 (1994), 767–771.
9. Oshikawa, K., *On formal groups over complete discrete valuation rings with application to a theorem of Lutz*, J. Reine Angew. Math. 334 (1982), 79–90.
10. Silverman, J. H., *The arithmetic of elliptic curves*, Grad. Texts in Math. 106 (1985).
11. Silverman, J. H., *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. 151 (1994).
12. Stark, H. M., *Class-numbers of complex quadratic fields*, in *Modular functions of one variable, I* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math. 320 (1973), 153–174.
13. Zariski, O., Samuel, P., *Commutative Algebra, I, II*, Princeton, New Jersey, D. Van Nostrand Company, Inc. 1958, 1960 (reprint, Grad. Texts in Math. 28–29 (1975)).

CURRENT ADDRESS:
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
TOKYO INSTITUTE OF TECHNOLOGY
OH-OKAMAYA, MEGURO-KU, TOKYO
152-8551 JAPAN
E-mail: tsatomcd@mathpc-satoh.math.titech.ac.jp