Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Chapter 1

Preliminaries

This chapter consists mainly of standard definitions and results. It is advised to consult it mainly for reference and to skip (at least) to Chapter 2. The reader familiar with isogeny-based cryptography can immediately skip to Chapter 3, where the main contributions of this work are highlighted. Chapters 4, 5, 6, and 7 have been individually published as research papers.

1.1 Elliptic Curves

Our main references for this section are [2, 4].

1.1.1 Definition and Weierstrass models

Let k be a field. An *algebraic group* over k is an algebraic variety G/k together with a specified point $e \in G(k)$, and morphisms of varieties $G \times G \to G$ (multiplication), and $G \to G$ (inversion), which induce a group structure on $G(\overline{k})$ with respect to which e is the identity element. A morphism of algebraic groups is a morphism of algebraic varieties that is also a homomorphism of groups. Projective connected algebraic groups are called *abelian varieties*; their group structure is always commutative. Abelian varieties of dimension one are called *elliptic curves*. Any smooth projective geometrically irreducible algebraic curve C over k of genus one together with a specified point $e \in C(k)$ admits the structure of an elliptic curve with e as an identity element. Every morphism of varieties between elliptic curves that respects the identity element is a morphism (of algebraic groups). An elliptic curve E over k admits a k-rational isomorphism to a smooth projective planar curve with affine model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

sending the specified point $e \in E(k)$ to the unique point at infinity. A curve of this form is called a *Weierstrass curve*. If the characteristic of k is not 2 or 3, there furthermore exists an isomorphism to one for which $a_1 = a_2 = a_3 = 0$; i.e. to a *short Weierstrass curve*, whose affine model is given by an equation of the form

$$y^2 = x^3 + Ax + B. \tag{1.2}$$

The *j-invariant* of an elliptic curve E/k is an explicit element of k that can be defined by a rational function in the coefficients of its long Weierstrass model [4, III.1]. For the case of a short Weierstrass equation it is $j(E) := (2^8 \cdot 3^3 \cdot A^3)/(4A^3 + 27B^2)$. Two elliptic curves over an algebraically closed field are isomorphic if and only if their j-invariants are equal.

1.1.2 Isogenies between elliptic curves

Morphisms of elliptic curves that are not constant, or equivalently, have finite kernel, are called *isogenies*. Associated to an isogeny $\varphi : E \to E'$ is the field extension $\varphi^* : \overline{k}(E') \hookrightarrow \overline{k}(E)$ of function fields given by the pull-back map $\varphi^* : f \mapsto f \circ \varphi$. The degree $\deg(\varphi)$ of an isogeny is the degree of this field extension, and an isogeny is called *separable* if this is a separable field extension. An isogeny of degree ℓ is also called an *ℓ-isogeny*. For $N \in \mathbf{Z}$ we denote by $[N] : E \to E$, $P \mapsto NP$ the multiplication-by-N map, and its kernel, which consists of the N-torsion points, by $E[N]$. For every isogeny $\varphi : E \to E'$ there exists a unique isogeny $\hat{\varphi} : E' \to E$, called the *dual isogeny*, such that $\varphi \circ \hat{\varphi} = [\deg \varphi]$. The degree of $[N]$ is N^2. For a field $L \supseteq k$, we write $\mathrm{End}_L(E)$ for the set of endomorphisms of E defined over L, and write $\mathrm{End}(E) := \mathrm{End}_{\bar{k}}(E)$ for the *(full) endomorphism ring*. The set $\mathrm{End}_L(E)$ admits a ring structure, where the multiplication is given by composition and the addition is given (pointwise) by the group operation. This ring is isomorphic to either [4, Cor. III.9.4]

(i) the integers $\mathbf{Z}$;

(ii) an order $\mathcal{O}$ in an imaginary quadratic number field K;

(iii) a maximal order $\mathcal{O}$ in $B_{p,\infty}$, the unique quaternion algebra over $\mathbf{Q}$ ramified at p and infinity, where $p > 0$ equals the characteristic of k.

The ring $\mathrm{End}^0_L(E) := \mathrm{End}_L(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ is called the *endomorphism algebra* of E *over* L. We denote by $\mathrm{End}^0(E) := \mathrm{End}_{\bar{k}}(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ the *(full) endomorphism algebra* of E. Any non-integer endomorphism of an elliptic curve is an imaginary quadratic number, whose norm over $\mathbf{Q}$ as an algebraic integer is equal to its degree as an isogeny.

Lemma 1.1.1 *Let $E/\overline{k}$ be an elliptic curve and let H be a finite subgroup of E. Then there exists a separable isogeny $\varphi : E \to E'$ with domain E and kernel H. This isogeny is unique up to post-composition with an isomorphism. The curve E' is necessarily unique up to isomorphism and we denote it by E/H.*

Proof. [4, Prop. III.4.12]. □

There is a set of formulae by Vélu [6] that can be used to explicitly compute a Weierstrass model for E/H, as well as a description of the associated isogeny $\varphi : E \to E/H$.

Proposition 1.1.2 (Vélu, [6]) *Let $E/\overline{k}$ be an elliptic curve in long Weierstrass form*

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

together with a finite subgroup $H \subseteq E$. Denote by $0 \in E$ the point at infinity. Partition $H \setminus \{0\} = H_2 \sqcup H^+ \sqcup H^-$, where $H_2 = H[2] \setminus \{0\}$ and H^+ and H^- are such that for any $P \in H^+$ it holds that $-P \in H^-$. Write $S = H_2 \cup H^+$, and for $P \in S$ define

$$\begin{aligned}
g_P^x &= 3x(P)^2 + 2a_2x(P) + a_4 - a_1y(P),\\
g_P^y &= -2y(P) - a_1x(P) - a_3,\\
u_P &= (g_P^y)^2, \quad v_P = \begin{cases} g_P^x & \text{if} \quad P \in H_2,\\ 2g_P^x - a_1g_P^y & \text{else,}\end{cases}\\
v &= \sum_{P\in S} v_P, \quad w = \sum_{P\in S}(u_P + x(P)v_P),\\
A_1 &= a_1, \quad A_2 = a_2, \quad A_3 = a_3,\\
A_4 &= a_4 - 5v, \quad A_6 = a_6 - (a_1^2 + 4a_2)v - 7w.
\end{aligned}$$

Then an equation for $E' = E/H$ is given by

$$E' : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6. \tag{1.3}$$

Furthermore, there exists a separable isogeny $\varphi : E \to E'$ with kernel H that satisfies

$$\begin{aligned}
x(\varphi(Q)) &= x(Q) + \sum_{P\in H\setminus\{0\}} (x(Q+P) - x(P))\\
y(\varphi(Q)) &= y(Q) + \sum_{P\in H\setminus\{0\}} (y(Q+P) - y(P)).
\end{aligned}$$

for all $Q \in E$.

1.1.3 Elliptic curves over finite fields

Let $\mathbf{F}_q$ be a finite field with q elements of characteristic $p := \mathrm{char}(\mathbf{F}_q)$, and let $E/\mathbf{F}_q$ be an elliptic curve with long Weierstrass model $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. The q-Frobenius endomorphism $\pi \in \mathrm{End}(E)$ is given by the map $(x, y) \mapsto (x^q, y^q)$. If $N := \#E(\mathbf{F}_q)$, then we define by $t := q + 1 - N$ the *trace* of $E/\mathbf{F}_q$, also called the *trace of Frobenius*. The *characteristic polynomial* of Frobenius is the polynomial $f := X^2 - tX + q$. It always has π as a root. An elliptic curve for which $p \mid t$ is called *supersingular*, otherwise E is called *ordinary*. If $\pi \notin \mathbf{Z}$, which is guaranteed if E is ordinary, then the characteristic polynomial is the minimal polynomial of π as an algebraic integer. The full endomorphism ring $\mathrm{End}(E)$ of an ordinary elliptic curve is an order in an imaginary quadratic number field. For a supersingular elliptic curve it is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbf{Q}$ ramified at p and ∞.

1.2 Orientations and CM

Our main references for this subsection are [1, 3, 5].

1.2.1 Imaginary quadratic orders

An imaginary quadratic order $\mathcal{O}$ is an order (i.e. a full-rank $\mathbf{Z}$-lattice that is also a subring) in an imaginary quadratic number field K. It is always of the form $\mathcal{O} = \mathbf{Z}[\sigma]$ for some $\sigma \in K$; such σ is called a *generator* for $\mathcal{O}$. The *discriminant* $\mathrm{Disc}(\mathcal{O})$ of $\mathcal{O}$ is the discriminant of σ as an imaginary quadratic number. The discriminant is always a negative integer that is congruent to 0 or 1 (mod 4); such integers are also called *imaginary quadratic discriminants*. For every imaginary quadratic discriminant there exists, up to ring isomorphism, a unique imaginary quadratic order with that discriminant. An imaginary quadratic discriminant that corresponds to a maximal order (i.e. the ring of integers of its field K) is called a *fundamental discriminant*. If $\mathcal{O}_1 \subseteq \mathcal{O}_2$ is an inclusion of imaginary quadratic orders, then $\mathrm{Disc}(\mathcal{O}_1) = v^2 \mathrm{Disc}(\mathcal{O}_2)$, where $v = [\mathcal{O}_2 : \mathcal{O}_1]$ is the index of $\mathcal{O}_1$ in $\mathcal{O}_2$ as an additive abelian group. A *proper* $\mathcal{O}$-ideal $\mathfrak{a}$ is an $\mathcal{O}$-ideal for which $\{\beta \in K \mid \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}$ (cf. [5, Def. 17.9]). We call two proper $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ *equivalent* if there exists $\beta \in K$ for which $\beta\mathfrak{a} = \mathfrak{b}$. The (ideal) *class group* $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is the multiplicative group of proper $\mathcal{O}$-ideals up to equivalence.

1.2.2 Elliptic curves over C

Let $\Lambda \subseteq \mathbf{C}$ be a $\mathbf{Z}$-lattice of rank 2. We define a morphism $\Lambda_1 \to \Lambda_2$ of two such lattices as a complex number $\alpha \in \mathbf{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$, that is

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) := \{\alpha \in \mathbf{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}.$$

Under this notion of morphism, there is an equivalence of categories

$$\Big\{\text{Elliptic curves over } \mathbf{C}\Big\} \rightleftarrows \Big\{\text{Full rank } \mathbf{Z}\text{-lattices } \Lambda \subseteq \mathbf{C}\Big\}$$

Any lattice is isomorphic to one of the form $\Lambda = \mathbf{Z} + \tau\mathbf{Z} = \langle 1, \tau \rangle$ for some τ in the complex upper half plane $\mathbf{H}$, and any two such lattices $\Lambda_1 = \langle 1, \tau_1 \rangle, \Lambda_2 = \langle 1, \tau_2 \rangle$ are isomorphic if and only if τ_1 and τ_2 are in the same $\mathrm{SL}_2(\mathbf{Z})$-orbit, i.e. if and only if there exist integers $a, b, c, d \in \mathbf{Z}$ for which $ad - bc = 1$ and such that $\tau_2 = (a\tau_1 + b)/(c\tau_1 + d)$. This happens if and only if τ_1 and τ_2 admit the same value under the *modular j-function* $j : \mathbf{H} \to \mathbf{C}$.

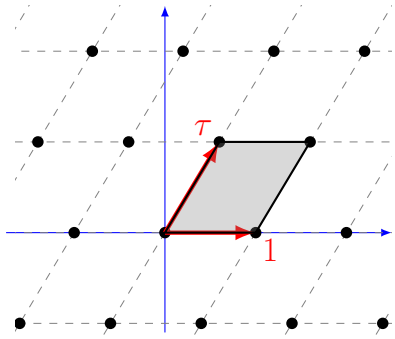

Figure 1.1: A rank two $\mathbf{Z}$-lattice in $\mathbf{C}$ spanned by 1 and $\tau \in \mathbf{H}$.

For most lattices $\Lambda = \langle 1, \tau \rangle$, hence for most elliptic curves over $\mathbf{C}$, we have $\mathrm{End}(\Lambda) \cong \mathbf{Z}$. The exception to this is precisely the special case where τ satisfies a (necessarily imaginary) quadratic equation

$$a\tau^2 + b\tau + c = 0, \quad \text{for some coprime } a, b, c \in \mathbf{Z}, a > 0.$$

In that case, $\mathrm{End}(\Lambda) = \mathbf{Z}[a\tau]$, and we say that Λ has *complex multiplication* by the imaginary quadratic order $\mathcal{O} := \mathbf{Z}[a\tau] \subseteq K := \mathbf{Q}(\tau)$. The field $K(j(\tau))$ depends only on $\mathcal{O}$ and is called the *ring class field* of $\mathcal{O}$. The field extension $K(j(\tau))/K$ is abelian and its Galois group is isomorphic to the class group $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$. The *Hilbert class polynomial* associated to τ is

$$\begin{aligned} H_\tau(X) &:= \prod_{\sigma \in \mathrm{Gal}(K(j(\tau))/K)} (X - \sigma(j(\tau))) \\ &= \prod_{\substack{E/\mathbf{C} \text{ ell. curve} \\ \mathrm{End}(E) \cong \mathcal{O}}} (X - j(E)). \end{aligned}$$

The Hilbert class polynomial has integer coefficients and only depends on (the isomorphism class of) $\mathcal{O}$; sometimes it also denoted $H_{\mathcal{O}}(X)$ or $H_D(X)$, where $D := \mathrm{Disc}(\mathcal{O})$.

1.2.3 The CM method

Hilbert class polynomials can be used to construct elliptic curves over finite fields with a prescribed number of points through a procedure known as the *CM method*. Elliptic curves over finite fields always have complex multiplication, in the sense that their endomorphism ring is never isomorphic to $\mathbf{Z}$. Let $E/\mathbf{F}_q$ be an ordinary elliptic curve over a field of characteristic $p > 0$, and let $\pi \in \mathrm{End}(E)$ denote the q-Frobenius endomorphism. Then the minimal polynomial of π is $X^2 - tX + q$, where $N := \#E(\mathbf{F}_q) = q + 1 - t$. Since $\mathrm{End}(E)$ contains the imaginary quadratic order $\mathbf{Z}[\pi]$, it

follows that

$$t^2 - 4q = \mathrm{Disc}(\mathbf{Z}[\pi]) = v^2 \,\mathrm{Disc}(\mathrm{End}(E)), \quad \text{for some } v \in \mathbf{Z}.$$

This motivates the following algorithm

Algorithm 1.2.1 (CM method) Given a prime power $q = p^e$ and an integer $t \in \mathbf{Z}$ coprime to q for which $t^2 - 4q < 0$, find the j-invariant of an elliptic curve $E/\mathbf{F}_q$ with trace of Frobenius t.

1. Find $v \in \mathbf{Z}$ and an imaginary quadratic discriminant D such that $v^2 D = t^2 - 4q$.
2. Compute the Hilbert class polynomial $H_D(X) \in \mathbf{Z}[X]$.
3. Extract a root $j_0 \in \mathbf{F}_q$ of $H_D \pmod p$.

The root $j_0 \in \mathbf{F}_q$ corresponds to an $\overline{\mathbf{F}_q}$-isomorphism class of elliptic curves. If one wants to find a curve over $\mathbf{F}_q$ with an exact prescribed trace, one could first construct a curve over $\mathbf{F}_q$ with the j-invariant j_0 output by the above algorithm. Then a twist of this curve will have the desired trace.

1.2.4 Orientations

Let $\mathcal{O} \subseteq K$ be an imaginary quadratic order in an imaginary quadratic number field, and let E be an elliptic curve over a field k. Throughout, we assume that k is perfect. A *K-orientation* on E is an injective ring homomorphism $\iota : K \to \mathrm{End}^0(E)$. An *$\mathcal{O}$-orientation* is a K-orientation for which $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. We say that an $\mathcal{O}$-orientation is *primitive* if there does not exist a strict superorder $\mathcal{O}' \supsetneq \mathcal{O}$ in K for which it is also an $\mathcal{O}'$-orientation. This is equivalent to $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$; this last equation associates to each K-oriented elliptic curve a unique order $\mathcal{O}$, called the *primitive order*, with respect to which the orientation is primitive. Given a K-oriented curve (E, ι) and an isogeny $\varphi : E \to E'$, we obtain an induced K-orientation on E' given by

$$\varphi_*(\iota)(\alpha) = \frac{1}{\deg \varphi} \varphi \iota(\alpha) \hat{\varphi}. \tag{1.4}$$

A morphism $(E, \iota) \to (E', \iota')$, also called a *($K$-oriented) isogeny*, of K-oriented elliptic curves is an isogeny $\varphi : E \to E'$ such that $\varphi_*(\iota) = \iota'$.

Lemma 1.2.2 *Let ℓ be a prime number different from* $\mathrm{char}\, k$. *Let $\varphi : (E, \iota) \to (E', \iota')$ be a K-oriented isogeny of degree ℓ, and let $\mathcal{O}, \mathcal{O}'$ be the respective primitive orders. Then exactly one of the following is true.*

(i) $\mathcal{O} \subsetneq \mathcal{O}'$ and $[\mathcal{O}' : \mathcal{O}] = \ell$, in which case φ is called ascending*;*

(ii) $\mathcal{O} \supsetneq \mathcal{O}'$ and $[\mathcal{O} : \mathcal{O}'] = \ell$, in which case φ is called descending*;*

(iii) $\mathcal{O} = \mathcal{O}'$, in which case φ is called horizontal.

1.3 Bibliography

[1] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptolology*, 14(1):414–437, 2020.

[2] James S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017.

[3] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields Appl.*, 69:Paper No. 101777, 18, 2021.

[4] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009.

[5] Andrew Sutherland. Course notes on elliptic curves, 2017. `https://math.mit.edu/classes/18.783/2017/lectures.html`.

[6] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences, Série I*, 273:238–241, 1971.