22 Ring class fields and the CM method

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D, and let

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E) \in \mathbb{C} : \mathrm{End}(E) = \mathcal{O}\}.$$

In the previous lecture we proved that the Hilbert class polynomial

$$H_D(X) := H_{\mathcal{O}}(X) := \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} \big(X - j(E)\big)$$

has integer coefficients. We then defined L to be the splitting field of $H_D(X)$ over the field $K = \mathbb{Q}(\sqrt{D})$, and showed that there is an injective group homomorphism

$$\Psi\colon \mathrm{Gal}(L/K) \hookrightarrow \mathrm{cl}(\mathcal{O})$$

that commutes with the group actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$ on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \mathrm{Ell}_{\mathcal{O}}(L)$ of roots of $H_D(X)$. To complete the proof of the the First Main Theorem of Complex Multiplication, which asserts that Ψ is an isomorphism, we just need to show that Ψ is surjective, equivalently, that $H_D(X)$ is irreducible over K.

To do this we need to introduce the Artin map (named after Emil Artin), which allows us to associate to each $\mathcal{O}$-ideal $\mathfrak{p}$ of prime norm satisfying certain constraints an automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ whose action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ corresponds to the action of $[\mathfrak{p}]$. In order to define the Artin map we need to briefly delve into a bit of algebraic number theory. We will restrict our attention to the absolute minimum that we need. Those who would like to know more may wish to consult one of [7, 8] or these 18.785 lecture notes; those who do not may treat the Artin map as a black box.

22.1 The Artin map

Let L be a finite Galois extension of a number field K. Nonzero prime ideals $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ are called "primes of K".[1] The $\mathcal{O}_L$-ideal $\mathfrak{p}\mathcal{O}_L$ is typically not a prime ideal, but it can be uniquely factored as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

where the $\mathfrak{q}_i$ are not-necessarily-distinct primes of L (prime ideals of $\mathcal{O}_L$) that are characterized by the property $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$. The primes $\mathfrak{q}_i$ are said to "lie above" the prime $\mathfrak{p}$, and it is standard to write $\mathfrak{q}_i|\mathfrak{p}$ as shorthand for $\mathfrak{q}_i|\mathfrak{p}\mathcal{O}_L$ and use $\{\mathfrak{q}|\mathfrak{p}\}$ to denote the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$.

We should note that the ring $\mathcal{O}_L$ is typically *not* a unique factorization domain, but it is a *Dedekind domain*, and this implies unique factorization of ideals.[2]

When the $\mathfrak{q}_i$ are distinct, we say that $\mathfrak{p}$ is *unramified* in L, which is true for all but finitely many primes $\mathfrak{p}$. If we apply an automorphism $\sigma \in \mathrm{Gal}(L/K)$ to both sides of the equation above, the LHS must remain the same: σ fixes every element of $\mathfrak{p} \subseteq K$, and it maps algebraic integers to algebraic integers, so it preserves the set $\mathcal{O}_L$. For the RHS, it is

[1] This is an abuse of terminology: as a ring, K does not have any nonzero prime ideals (it is a field).

[2] There are several equivalent definitions of Dedekind domains: it is an integral domain with unique factorization of ideals, and it also an integral domain in which every nonzero fractional ideal is invertible. We have seen that the latter applies to rings of integers in number fields (at least for imaginary quadratic fields), so the former must as well (this equivalence is a standard result from commutative algebra).

clear that σ must map $\mathcal{O}_L$-ideals to $\mathcal{O}_L$-ideals, and since the $\mathfrak{q}_i$ are all prime ideals, σ must permute them. Thus the Galois group $\mathrm{Gal}(L/K)$ acts on the set $\{\mathfrak{q}_1,\dots,\mathfrak{q}_n\} = \{\mathfrak{q}|\mathfrak{p}\}$; one can show that this action is transitive, but it is typically not faithful.

For each $\mathfrak{q}|\mathfrak{p}$, the stabilizer of $\mathfrak{q}$ under this action is a subgroup

$$D_{\mathfrak{q}} := \{\sigma \in \mathrm{Gal}(L/K) : \mathfrak{q}^\sigma = \mathfrak{q}\} \subseteq \mathrm{Gal}(L/K)$$

known as the *decomposition group* of $\mathfrak{q}$. Each $\sigma \in D_{\mathfrak{q}}$ fixes $\mathfrak{q}$ and therefore induces an automorphism $\bar\sigma$ of the quotient $\mathbb{F}_{\mathfrak{q}} := \mathcal{O}_L/\mathfrak{q}$ defined by $\bar\sigma(\bar x) = \overline{\sigma(x)}$, where $x \mapsto \bar x$ is the quotient map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q}$. The quotient $\mathcal{O}_L/\mathfrak{q}$ is a field (in a Dedekind domain every nonzero prime ideal is maximal), and $\mathfrak{q}$ has finite index $\mathrm{N}\mathfrak{q} := [\mathcal{O}_L : \mathfrak{q}]$ in $\mathcal{O}_L$, so it is a finite field of cardinality $\mathrm{N}\mathfrak{q}$ (which must be a prime power). The image of $\mathcal{O}_K$ under the quotient map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q} = \mathbb{F}_q$ is $\mathcal{O}_K/(\mathfrak{q}\cap\mathcal{O}_K) = \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}}$, thus the finite field $\mathbb{F}_{\mathfrak{p}}$ is a subfield of $\mathbb{F}_{\mathfrak{q}}$ (and necessarily has the same characteristic). It follows that $\bar\sigma \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$, and we have a group homomorphism

$$\begin{aligned} D_q &\to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \\ \sigma &\mapsto \bar\sigma. \end{aligned}$$

This homomorphism is surjective [8, Prop. I.9.4], and when $\mathfrak{p}$ is unramified it is also injective [8, Prop. I.9.5], and therefore an isomorphism, which we now assume.

The group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic, generated by the Frobenius automorphism $x \to x^{\mathrm{N}\mathfrak{p}}$, where $\mathrm{N}\mathfrak{p} = [\mathcal{O}_K : \mathfrak{p}] = \#\mathbb{F}_{\mathfrak{p}}$. The unique $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}}$ for which $\bar\sigma_{\mathfrak{q}}$ is the Frobenius automorphism is called the *Frobenius element* of $\mathrm{Gal}(L/K)$ at $\mathfrak{q}$. In general the Frobenius element $\sigma_{\mathfrak{q}}$ depends on our choice of $\mathfrak{q}$, but the $\sigma_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$ are all conjugate, since if $\tau(\mathfrak{q}_i) = \mathfrak{q}_j$ then we must have $\sigma_{\mathfrak{q}_j} = \tau^{-1}\sigma_{\mathfrak{q}_i}\tau$. This implies that the $\bar\sigma_{\mathfrak{q}}$ all have the same order, hence the extensions $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ all have the same degree and are thus isomorphic.

In the case we are interested in, $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{cl}(\mathcal{O})$ is abelian, so conjugacy implies equality, and the $\sigma_{\mathfrak{q}}$ are all the same. Thus when $\mathrm{Gal}(L/K)$ is abelian, each prime $\mathfrak{p}$ of K determines a unique Frobenius element that we denote $\sigma_{\mathfrak{p}}$. The map

$$\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$$

is known as the *Artin map* (it extends multiplicatively to all $\mathcal{O}_K$-ideals that are products of unramified primes ideals, but this is not relevant to us). The automorphism $\sigma_{\mathfrak{p}}$ is uniquely characterized by the fact that

$$\sigma_{\mathfrak{p}}(x) \equiv x^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{q}, \tag{1}$$

for all $x \in \mathcal{O}_L$ and primes $\mathfrak{q}|\mathfrak{p}$.

If $E/\mathbb{C}$ has CM by $\mathcal{O}$ then $j(E) \in L$, and this implies that (up to isomorphism) E can be defined by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathcal{O}_L$. Indeed, as in the proof of Theorem 14.12, for $j(E) \neq 0, 1728$ we can take $A = 3j(E)(1728 - j(E))$ and $B = 2j(E)(1728 - j(E))^2$.

For each prime $\mathfrak{q}$ of L, so long as the discriminant $\Delta(E) := -16(4A^3 + 27B^2)$ does not lie in $\mathfrak{q}$, equivalently, the image of $\Delta(E)$ under the quotient map $\mathcal{O}_L \to \mathcal{O}_L/q = \mathbb{F}_q$ is nonzero, reducing modulo $\mathfrak{q}$ yields an elliptic curve $\bar E/\mathbb{F}_{\mathfrak{q}}$ defined by $y^2 = x^3 + \bar A x + \bar B$. We then say that E has good reduction modulo $\mathfrak{q}$. This holds for all but finitely many primes $\mathfrak{q}$ of L, since the principal ideal $(\Delta(E))$ is divisible by only finitely many prime ideals.

22.2 The First Main Theorem of Complex Multiplication

With the Artin map in hand, we can now complete our proof of the First Main Theorem of Complex Multiplication.

Theorem 22.1. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and let L be the splitting field of $H_D(X)$ over $K := \mathbb{Q}(\sqrt{D})$. The map $\Psi\colon \mathrm{Gal}(L/K) \to \mathrm{cl}(\mathcal{O})$ that sends each $\sigma \in \mathrm{Gal}(L/K)$ to the unique $\alpha_\sigma \in \mathrm{cl}(\mathcal{O})$ such that $j(E)^\sigma = \alpha_\sigma j(E)$ for all $j(E) \in \mathrm{Ell}_{\mathcal{O}}(L)$ is a group isomorphism compatible with the actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(L)$.*

Proof. In the previous lecture we showed that Ψ is well-defined, injective, and commutes with the group actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$; see Theorem 21.14 and the discussion preceding it. It remains only to show that Ψ is surjective.

Fix $\alpha \in \mathrm{cl}(\mathcal{O})$, and let $\mathfrak{p}$ be a prime of K such that the following hold:

(i) $\mathfrak{p} \cap \mathcal{O}$ is a proper $\mathcal{O}$-ideal of prime norm p such that $[\mathfrak{p}] = \alpha$;

(ii) p is unramified in K and $\mathfrak{p}$ is unramified in L;

(iii) Each $j(E) \in \mathrm{Ell}_{\mathcal{O}}(L)$ is the j-invariant of an elliptic curve E/L that has good reduction modulo every prime $\mathfrak{q}|\mathfrak{p}$ (prime ideals $\mathfrak{q}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}\mathcal{O}_L$).

(iv) The $j(E) \in \mathrm{Ell}_{\mathcal{O}}(L)$ are distinct modulo every prime $\mathfrak{q}|\mathfrak{p}$.

By Theorem 21.11, there are infinitely many $\mathfrak{p}$ for which (i) holds, and conditions (ii)-(iv) prohibit only finitely many primes, so such a $\mathfrak{p}$ exists. To ease the notation, we will also use $\mathfrak{p}$ to denote the $\mathcal{O}$-ideal $\mathfrak{p} \cap \mathcal{O}$; it will be clear from context whether we are viewing $\mathfrak{p}$ as an $\mathcal{O}_K$-ideal as an $\mathcal{O}$-ideal (in particular, anytime we write $[\mathfrak{p}]$ we must mean $[\mathfrak{p} \cap \mathcal{O}]$, since we are using $[\,\cdot\,]$ to denote equivalence classes of $\mathcal{O}$-ideals).

Let us now consider a particular prime $\mathfrak{q}|\mathfrak{p}$ and curve E/L with CM by $\mathcal{O}$ that has good reduction modulo $\mathfrak{q}$, defined by $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathcal{O}_L$ and $\mathfrak{q} \nmid \Delta(E)$. Put $\mathbb{F}_\mathfrak{q} := \mathcal{O}_L/\mathfrak{q}$, and let $\overline{E}/\mathbb{F}_\mathfrak{q}$ be the reduction of E modulo $\mathfrak{q}$, defined by $\overline{E}\colon y^2 = x^3 + \bar{A}x + \bar{B}$. The Frobenius element $\sigma_\mathfrak{p}$ induces the p-power Frobenius automorphism $\overline{\sigma}_\mathfrak{p} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_p)$, since $\mathrm{N}\mathfrak{p} = p$, and we have a corresponding isogeny

$$\pi\colon \overline{E} \to \overline{E^{\sigma_\mathfrak{p}}} = \overline{E}^{\bar{\sigma}_p} = \overline{E}^{(p)}$$

defined by $(x, y) \mapsto (x^p, y^p)$, where $\overline{E}^p$ is the curve $y^2 = x^3 + \bar{A}^p x + \bar{B}^p$. The isogeny π is purely inseparable of degree p.

The CM action of the proper $\mathcal{O}$-ideal $\mathfrak{p} \cap \mathcal{O}$ corresponds to an isogeny $\phi_\mathfrak{p}\colon E \to \mathfrak{p}E$ of degree $\mathrm{N}\mathfrak{p} = p$, with $\mathfrak{p}E$ of good reduction modulo $\mathfrak{q}$, by (iii), which we can assume is defined by a rational map $(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ where $u, v, s, t \in \mathcal{O}_L[x]$, with u monic and v nonzero modulo $\mathfrak{q}$. The isogeny $\phi\colon \overline{E} \to \overline{\mathfrak{p}E}$ obtained by reducing the coefficients of u, v, s, t modulo $\mathfrak{q}$ has the same degree p as the isogeny π (we can assume $\deg v < \deg u$ and u is monic so its degree doesn't change when it is reduced). The composition of ϕ with its dual $\hat{\phi}$ is the multiplication-by-p map on $\overline{E}$, which is inseparable since $\mathbb{F}_\mathfrak{q}$ has characteristic p. This implies that at least one of ϕ and $\hat{\phi}$ is inseparable. Without loss of generality we may assume ϕ is inseparable: if not, we can replace E by $\mathfrak{p}E$ and $\mathfrak{p}$ by its complex conjugate $\bar{\mathfrak{p}}$, which also satisfies (i)-(iv) and induces the dual isogeny $\hat{\phi}_\mathfrak{p}\colon \mathfrak{p}E \to E$ (up to an isomorphism), since the ideal $\bar{\mathfrak{p}}\mathfrak{p} = (\mathrm{N}\mathfrak{p}) = (p)$ induces the multiplication-by-p map on E, and reducing the rational maps defining $\hat{\phi}_\mathfrak{p}$ yields the dual isogeny $\hat{\phi}\colon \overline{\mathfrak{p}E} \to \overline{E}$.

By Corollary 6.4, we can decompose the inseparable isogeny ϕ of degree p as $\phi = \phi_{\text{sep}} \circ \pi$, where ϕ_{sep} has degree 1 and must be an isomorphism. Thus $\overline{\mathfrak{p}E} \simeq \overline{E^{\sigma_\mathfrak{p}}}$ and therefore $j(\overline{\mathfrak{p}E}) = j(\overline{E^{\sigma_\mathfrak{p}}})$, and (iv) implies $j(\mathfrak{p}E) = j(E^{\sigma_\mathfrak{p}})$. It follows that $\Psi(\sigma_\mathfrak{p}) = [\mathfrak{p}] = \alpha$, since each element of $\mathrm{cl}(\mathcal{O})$ is determined by its action on any element of the $\mathrm{cl}(\mathcal{O})$-torsor $\mathrm{Ell}_\mathcal{O}(L)$. □

Corollary 22.2. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D. The Hilbert class polynomial $H_D(x)$ is irreducible over $K = \mathbb{Q}(\sqrt{D})$ and for any elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}$ the field $K(j(E))$ is a finite abelian extension of K with $\mathrm{Gal}(K(j(E))/K) \simeq \mathrm{cl}(\mathcal{O})$.*

Proof. Let L be the splitting field of $H_D(X)$ over K. The class group $\mathrm{cl}(\mathcal{O})$ acts transitively on the roots of $H_D(X)$ (the set $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$), hence by Theorem 22.1, the Galois group $\mathrm{Gal}(L/K)$ also acts transitively on the roots of $H_D(X)$, which implies that $H_D(X)$ is irreducible over K and is the minimal polynomial of each of its roots. The degree of H_D is equal to the class number $h(D) = \#\,\mathrm{cl}(\mathcal{O}) = \#\mathrm{Gal}(L/K) = [L : K]$, so we $L = K(j(E))$ for every root $j(E)$ of $H_D(X)$, equivalently, every $j(E) \in \mathrm{Ell}_\mathcal{O}(\mathbb{C}) = \{j(E) : \mathrm{End}(E) = \mathcal{O}\}$. We have $\mathrm{Gal}(L/K) \simeq \mathrm{cl}(\mathcal{O})$ by Theorem 22.1, which is abelian. □

22.3 The ring class field of an imaginary quadratic order

Definition 22.3. Let O be an imaginary quadratic order with discriminant D. The splitting field of the Hilbert class polynomial of $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$, equivalently, the extension of K generated by the j-invariant of any elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}$, is known as the *ring class field* of the imaginary quadratic order $\mathcal{O}$ with discriminant D.

We say that an integer prime p is *unramified* in a number field L if the ideal $p\mathcal{O}_L$ factors into distinct prime ideals $\mathfrak{q}$ in $\mathcal{O}_L$, and we say that p *splits completely* in L if the prime ideals $\mathfrak{q}|p$ are distinct and have minimal norm $\mathrm{N}\mathfrak{q} = p$.

For an imaginary quadratic field K of discriminant D there are three possibilities for the factorization of the ideal $p\mathcal{O}_K$ in $\mathcal{O}_K$: it either *splits* (completely into two distinct prime ideals), *ramifies* (is the square of a prime ideal), or remains *inert* (the ideal $p\mathcal{O}_K$ is already prime). These are distinguished by the *Kronecker symbol* $\left(\frac{D}{p}\right)$, which is 1, 0, -1, respectively, in these three cases (as proved in Lemma 22.6 below).

Definition 22.4. Let p be a prime and D an integer. For $p > 2$ the *Kronecker symbol* is

$$\left(\frac{D}{p}\right) := \#\{x \in \mathbb{F}_p : x^2 = D\} - 1.$$

For $p = 2$, we define $\left(\frac{D}{p}\right)$ to be 1 for $D \equiv \pm 1 \bmod 8$, zero if $p|D$, and -1 for $D \equiv \pm 3 \bmod 8$.

Theorem 22.5. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D and ring class field L. Let $p \nmid D$ be an odd prime unramified in L.*[3] *The following are equivalent:*

(i) *p is the norm of a principal $\mathcal{O}$-ideal;*

(ii) *$\left(\frac{D}{p}\right) = 1$ and $H_D(X)$ splits into linear factors in $\mathbb{F}_p[X]$;*

(iii) *p splits completely in L;*

(iv) *$4p = t^2 - v^2 D$ for some integers t and v with $t \not\equiv 0 \bmod p$.*

[3] If p does not divide D then it must be unramified in L, but we have not proved this yet, so we include it as a hypothesis which will be removed in Corollary 22.8.

Proof. Let $K := \mathbb{Q}(\sqrt{D})$, let $\mathcal{O}_K = [1, \omega]$ be the ring of integers of K. By Theorem 18.18, we may write $D = u^2 D_K$, where $u = [\mathcal{O}_K : \mathcal{O}]$ and $D_K = \operatorname{disc} \mathcal{O}_K$ is a fundamental discriminant, and we then have $\mathcal{O} = [1, u\omega]$.

(i)⇒(iv): Let (λ) be a principal $\mathcal{O}$-ideal of norm p. Then $[1, \lambda]$ is a suborder of $\mathcal{O}$ with discriminant $v^2 u^2 D_K = v^2 D$, where $v = [\mathcal{O} : [1, \lambda]]$. Let $t := \lambda + \bar{\lambda}$ so that $x^2 - tx + p$ is the minimal polynomial of λ, with discriminant $\operatorname{disc}[1, \lambda] = t^2 - 4p = v^2 D$. Then (iv) holds with $t \not\equiv 0 \bmod p$ because $p \nmid D$ (if $p|t$ then $p|v$ and $p^2|4p$, a contradiction for $p \neq 2$).

(iv)⇒(i): If $4p = t^2 - v^2 D$ then the polynomial $x^2 - tx + p$ with discriminant $v^2 D$ has a root $\lambda \in \mathcal{O}_K$; the order $[1, \lambda]$ has discriminant $v^2 D$ and therefore lies in $\mathcal{O}$, by Theorem 18.18, so $\lambda \in \mathcal{O}$, and (λ) is a principal $\mathcal{O}$-ideal of norm $\lambda\bar{\lambda} = p$.

(i)⇒(ii): Since (i)⇒(iv) we have $4p = t^2 - v^2 D$ for some $t, v \in \mathbb{Z}$ with $t \not\equiv 0 \bmod p$, and

$$\left(\frac{D}{p}\right) = \left(\frac{v^2 D}{p}\right) = \left(\frac{t^2 - 4p}{p}\right) = 1,$$

since $t^2 \not\equiv 0 \bmod p$. If $\mathfrak{p}$ is a principal $\mathcal{O}$-ideal of norm p, then $\mathfrak{p}$ is unramified in L (since $p = \mathfrak{p}\bar{\mathfrak{p}}$ is unramified in L), and $\mathfrak{p}$ is principal, so $[\mathfrak{p}]$ and therefore $\sigma_{\mathfrak{p}}$ acts trivially on the roots of $H_D(X)$, by Theorem 22.1. The roots of $H_D(X)$ mod p must therefore lie in $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_p$ and $H_D(X)$ splits into linear factors in $\mathbb{F}_p[X]$.

(ii)⇒(iii): If $(\frac{D}{p}) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ splits into distinct primes of norm p in K, by Lemma 22.6, and if $H_D(X)$ splits into linear factors in $\mathbb{F}_p[x]$, then its roots are all fixed by $\sigma_{\mathfrak{p}}$. This implies $[\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] = 1$, and therefore $\mathrm{N}\mathfrak{q} = [\mathcal{O}_L : \mathfrak{q}] = [\mathcal{O}_K : \mathfrak{p}] = p$ for every prime $\mathfrak{q}|\mathfrak{p}$, so $\mathfrak{p}$ splits completely in L (it must be unramified, since p is). If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$, then $\bar{\mathfrak{p}}\mathcal{O}_L = \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_n$ (note that $\bar{\mathcal{O}}_L = \mathcal{O}_L$), and $p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_n$ splits completely in L (the $\mathfrak{q}_i$ and $\bar{\mathfrak{q}}_i$ must all be distinct since p is unramified in L).

(iii)⇒(i): If $p\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ with the $\mathrm{N}\mathfrak{q}_1 = \cdots \mathrm{N}\mathfrak{q}_n = p$ then $\mathbb{F}_{\mathfrak{q}} := [\mathcal{O}_L : \mathfrak{q}] = \mathbb{F}_p$ for all primes $\mathfrak{q}$ dividing $p\mathcal{O}_L$. If $\mathfrak{p}$ is a prime of K dividing $p\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L$ divides $p\mathcal{O}_L$ must be divisible by some prime ideal $\mathfrak{q}$ dividing $p\mathcal{O}_L$. The inclusions $\mathbb{Q} \subseteq K \subseteq L$ imply $\mathbb{F}_p \subseteq \mathbb{F}_{\mathfrak{p}} \subseteq \mathbb{F}_{\mathfrak{q}} = \mathbb{F}_p$, where $\mathbb{F}_p := [\mathcal{O}_K : \mathfrak{p}]$, so $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_p$, and $\mathfrak{p}$ has norm p. The extension $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ is trivial, so the Frobenius element $\sigma_{\mathfrak{p}} \in \operatorname{Gal}(L/K)$ is the identity, and so is $[\mathfrak{p} \cap O] \in \operatorname{cl}(\mathcal{O})$, by Theorem 22.1 (note: $\mathfrak{p} \cap \mathcal{O}$ is a proper $\mathcal{O}$-ideal because $\mathrm{N}\mathfrak{p} = p$ does not divide $D = u^2 D_K$). Thus $\mathfrak{p} \cap \mathcal{O}$ is a principal $\mathcal{O}$-ideal of norm $[\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O}_K : \mathfrak{p}] = p$. □

Lemma 22.6. *Let K be an imaginary quadratic field of discriminant D with ring of integers $\mathcal{O}_K = [1, \omega]$ and let p be prime. Every $\mathcal{O}_K$-ideal of norm p is of the form $\mathfrak{p} = [p, \omega - r]$, where $r \in \mathbb{Z}$ is a root of the minimal polynomial of ω modulo p. The number of such ideals $\mathfrak{p}$ is $1 - \left(\frac{D}{p}\right) \in \{0, 1, 2\}$ and the factorization of the principal $\mathcal{O}_K$-ideal into prime ideals is*

$$(p) = \begin{cases} \mathfrak{p}\bar{\mathfrak{p}} & \text{if } (\frac{D}{p}) = 1, \\ \mathfrak{p}^2 & \text{if } (\frac{D}{p}) = 0, \\ (p) & \text{if } (\frac{D}{p}) = -1. \end{cases}$$

with $\mathfrak{p} \neq \bar{\mathfrak{p}}$ when $\left(\frac{D}{p}\right) = 1$.

Proof. Let $f(x) = x^2 - (\omega + \overline{\omega})x + \omega\overline{\omega} \in \mathbb{Z}[x]$ be the minimal polynomial of ω and let $\mathfrak{p}$ be an $\mathcal{O}_K$-ideal of norm p. Every nonzero $\mathcal{O}_K$-ideal is invertible, so by Theorem 18.9 we have $\mathfrak{p}\bar{\mathfrak{p}} = (\mathrm{N}\mathfrak{p}) = (p)$. Thus $p \in \mathfrak{p}$, and every integer $n \in \mathfrak{p}$ must be a multiple of p because otherwise $\gcd(n, p) = 1 \in \mathfrak{p}$ would imply $\mathfrak{p} = \mathcal{O}_K$ has norm $1 \neq p$. Therefore $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

We can thus write $\mathfrak{p} = [p, a\omega - r]$ for some $a, r \in \mathbb{Z}$, and $[\mathcal{O}_K : \mathfrak{p}] = p$ then implies $a = 1$. The ideal $\mathfrak{p}$ is closed under multiplication by $\mathcal{O}_K$, so in particular it must contain

$$(\overline{\omega} - r)(\omega - r) = \overline{\omega}\omega - (\overline{\omega} + \omega)r + r^2 = f(r),$$

which is both an integer and an element of $\mathfrak{p}$, hence a multiple of p. Thus r must be a root of $f(x) \bmod p$. Conversely, if r is any root of $f(x) \bmod p$, then $[p, \omega - r]$ is an $\mathcal{O}_K$-ideal of norm p, and if $f(x) \bmod p$ has roots r and s that are distinct modulo p, then the $\mathcal{O}_K$-ideals $[p, \omega - r]$ and $[p, \omega - s]$ are clearly distinct.

It follows that the number of $\mathcal{O}_K$-ideals of prime norm p is equal to the number of distinct roots of $f(x) \bmod p$. The discriminant of $f(x)$ is

$$(\omega + \overline{\omega})^2 - 4\omega\overline{\omega} = (\omega - \overline{\omega})^2 = \operatorname{disc} \mathcal{O}_K = D, \tag{2}$$

and when p is odd it follows from the quadratic equation that the number of distinct roots of $f(x) \bmod p$ is $1 - \left(\frac{D}{p}\right)$, since this is the number of distinct square-roots of D modulo p.

For $p = 2$, we first note that if $D \equiv 0 \bmod 4$ then (2) implies that $\omega + \overline{\omega}$ is even, so $f(x) \equiv x^2 \bmod 2$ has $1 = 1 - \left(\frac{D}{2}\right)$ distinct roots. If $D \equiv 1 \bmod 4$ then $\omega + \overline{\omega}$ must be odd. If $D \equiv 1 \bmod 8$ then (2) implies that $\omega\overline{\omega}$ must be even (since $(\omega + \overline{\omega})^2 \equiv 1 \bmod 8$), and then $f(x) \equiv x^2 + x \bmod 2$ has $2 = 1 - \left(\frac{D}{2}\right)$ distinct roots. If $D \equiv 5 \bmod 8$ then $\omega\overline{\omega}$ must be odd, and then $f(x) \equiv x^2 + x + 1 \bmod 2$ has $0 = 1 - \left(\frac{D}{2}\right)$ distinct roots. □

Corollary 22.7. *Let $\mathcal{O}$ be an order of discriminant D in an imaginary quadratic field K, and let p be a prime. When p divides the conductor $[\mathcal{O} : \mathcal{O}_K]$ there are no proper $\mathcal{O}$-ideals of norm p and otherwise there are $1 - \left(\frac{D}{p}\right) = 0, 1, 2$, depending on whether p is inert, ramified, or split in K, respectively*

22.4 Class field theory

The theory of complex multiplication was originally motivated not by the study of elliptic curves, but as a way to construct abelian extensions of imaginary quadratic fields. A celebrated theorem of Kronecker and Weber states that every finite abelian extension of $\mathbb{Q}$ lies in a cyclotomic field (a field of the form $\mathbb{Q}(\zeta_n)$, for some nth root of unity ζ_n). The effort to generalize this result led to the development of *class field theory*, a branch of algebraic number theory that was one of the major advances of early 20th century number theory.

In 1898 Hilbert conjectured that every number field K has a unique maximal abelian extension L/K that is unramified at every prime[4] of K, for which $\operatorname{Gal}(L/K) \simeq \operatorname{cl}(\mathcal{O}_K)$. This conjecture was proved shortly thereafter by Furtwängler, and the field L is now known as the *Hilbert class field* of K. While its existence was quickly proved, the problem of explicitly constructing L, say by specifying a generator for L in terms of its minimal polynomial over K, remained an open problem (and for general K it still is).

The field $\mathbb{Q}$ has no nontrivial unramified extensions (let along abelian ones), so its Hilbert class field is not interesting (it is just $\mathbb{Q}$). After $\mathbb{Q}$, the simplest fields K to consider are imaginary quadratic fields. For an imaginary quadratic field K of discriminant D, the splitting field L of the Hilbert class polynomial $H_D(X)$ over K; it is a Galois extension of K with Galois group $\operatorname{Gal}(L/K) \simeq \operatorname{cl}(O_K)$. It follows from class field theory that L must be the Hilbert class field of K. The Hilbert class field of an imaginary quadratic field K can

[4]This includes not only all prime $\mathcal{O}_K$-ideals, but also "infinite primes" of K, corresponding to embeddings of K into $\mathbb{C}$. For imaginary quadratic fields K this imposes no additional restrictions.

also be characterized as the minimal extension L/K over which there exists an elliptic curve E with CM by $\mathcal{O}_K$; in other words, $L = K(j(E))$.

What about the splitting field L of a Hilbert class polynomial $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$ when D is the discriminant of a non-maximal order $\mathcal{O} \subsetneq \mathcal{O}_K$? These are called *ring class fields*. They are abelian extensions of K with Galois group $\mathrm{Gal}(L/K) \simeq \mathrm{cl}(\mathcal{O})$, but unlike the Hilbert class field of K, they are necessarily ramified at some primes. It follows from class field theory that ramified primes are not proper $\mathcal{O}$-ideals.

The ring class field L is characterized by the infinite set $\mathcal{S}_{L/\mathbb{Q}}$ of primes that split completely in L, and with finitely many exceptions, these are precisely the primes p that satisfy the equation $4p = t^2 - v^2 D$ for some $t, v \in \mathbb{Z}$, with $D = \mathrm{disc}(\mathcal{O})$; see [4, Thm. 9.2, Ex. 9.3]. Any extension M/K for which the set $\mathcal{S}_{M/\mathbb{Q}}$ matches $\mathcal{S}_{L/\mathbb{Q}}$ with only finitely many exceptions must in fact be equal to L, by [4, Thm. 8.19]. We thus have the following corollary of Theorem 22.5, which removes the assumption that p is unramified in L.

Corollary 22.8. *Let $\mathcal{O}$ be order of discriminant D in an imaginary quadratic field K. The splitting field L of $H_D(X)$ over K is unramified at all primes that do not divide the conductor of $\mathcal{O}$. In particular, every rational prime $p \nmid D$ is unramified in L.*

Ring class fields allow us to explicitly construct infinitely many abelian extensions of a given imaginary quadratic field K. One might ask whether every abelian extension of K is contained in a ring class field. This is not the case, but by extending the ring class field of on order $\mathcal{O}$ by adjoining the x-coordinates of the n-torsion points of an elliptic curve with CM by $\mathcal{O}$ (or powers of them, when $\mathrm{disc}\,\mathcal{O} \in \{-3, -4\}$), one obtains what are known as *ray class fields*, which depend on the choice of both $\mathcal{O}$ and n. These are analogs of the cyclotomic extensions of $\mathbb{Q}$ (which is its own Hilbert class field because it has no unramified extensions). An analog of the Kronecker-Weber theorem then holds: every abelian extension of an imaginary quadratic field is contained in a ray class field. One can define ring class fields and ray class fields for arbitrary number fields, and obtain a similar result (this was started by Weber and finished by Takagi around 1920), but the constructions are not nearly as explicit as they are in the imaginary quadratic case.

22.5 The CM method

The equation

$$4p = t^2 - v^2 D$$

in part (iv) of Theorem 22.5 is known as the *norm equation*; it arises from the principal $\mathcal{O}$-ideal (λ) of norm p given by part (i), generated by a root $\lambda \in \mathcal{O} \subseteq \mathcal{O}_K$ of $x^2 - tx + p$, which has norm p and trace t. By the quadratic equation

$$\lambda = \frac{-t \pm \sqrt{t^2 - 4p}}{2} = \frac{-t \pm v\sqrt{D}}{2}.$$

Clearing denominators and taking norms yields the equation $\mathrm{N}(2\lambda) = 4\lambda\bar{\lambda} = 4p = t^2 - v^2 D$.

Let us assume this equation holds with $p \nmid D$ odd and $D < -4$. The prime p splits completely in the ring class field L for the order $\mathcal{O}$ of discriminant D, and we can completely factor $H_D(X)$ in both $\mathcal{O}_L[x]$ and $\mathbb{F}_p[x]$. If we now fix a prime $\mathfrak{q}$ lying above p, then $\mathrm{N}\mathfrak{q} = p$, by Theorem 22.5, we have a reduction map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q} \simeq \mathbb{F}_p$ that we can apply to the roots of $H_D(X)$, equivalently, to the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \{j(E) \in \mathbb{C} : \mathrm{End}(E) \simeq \mathcal{O}\}$.

It follows that the j-invariant $j(E)$ of any elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}$ can be reduced (modulo $\mathfrak{q}$) to the j-invariant of an elliptic curve $\overline{E}/\mathbb{F}_p$ that is the reduction of E: we can always pick a model $y^2 = x^3 + Ax + B$ for E with $A, B \in \mathcal{O}_L$ such that $\mathfrak{q} \nmid \Delta(E)$ because p is odd and the denominator of $j(E)$ has to be nonzero modulo $\mathfrak{q}$. Now we know that $\mathrm{End}(E) \simeq \mathcal{O}$, but what about $\mathrm{End}(\overline{E})$?

If $\varphi \in \mathrm{End}(E) \simeq \mathcal{O}$ is a nonzero endomorphism of E, then we can reduce the coefficients of the rational functions defining φ modulo $\mathfrak{q}$ to obtain a corresponding endomorphism $\bar{\varphi} \in \mathrm{End}(\overline{E})$. The endomorphism $\bar{\varphi}$ is nonzero because it must satisfy the characteristic equation $x^2 - [\mathrm{tr}\,\varphi]x + [\deg\varphi] = 0$ in $\mathrm{End}(\overline{E})$: multiplication-by-$n$ maps $[n]$ can always be reduced to from $\mathrm{End}(E)$ to $\mathrm{End}(\overline{E})$, so $[\mathrm{tr}\,\varphi]$ and $[\deg\varphi]$ reduce to maps $[\mathrm{tr}\,\bar{\varphi}]$ and $[\deg\bar{\varphi}]$ that represent multiplication by the same integers. It follows that the reduction map induces an injective ring homomorphism

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(\overline{E}). \tag{3}$$

In fact this map is an isomorphism (see §22.6), but for the moment we will content ourselves with showing that it at least induces an isomorphism of endomorphism algebras. By Corollary 14.19 we know that $\mathrm{End}^0(\overline{E})$ is either an imaginary quadratic field or a quaternion algebra, depending on whether $\overline{E}$ is ordinary or supersingular.

Corollary 22.9. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D and ring class field L, and let $p \nmid D$ be an odd prime satisfying $4p = t^2 - v^2D$. Every $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is the j-invariant of an elliptic curve E/L with good reduction $\overline{E}$ modulo a prime $\mathfrak{q}$ of L lying above p. Provided $j(\overline{E}) \neq 0, 1728$, we have $\mathrm{tr}\,\pi_{\overline{E}} = \pm t \not\equiv 0 \bmod p$ and $\overline{E}$ is ordinary.*[5]

Proof. By Theorem 22.5 and its proof, p is the norm of a principal $\mathcal{O}$-ideal $\mathfrak{p} := (\lambda)$, where λ has norm p and trace t. As in the proof of Theorem 22.1, one of the isogenies $\phi_{\mathfrak{p}} \colon E \to \mathfrak{p}E$ and $\phi_{\bar{\mathfrak{p}}} \colon E \to \bar{\mathfrak{p}}E$ induces a purely inseparable isogeny $\phi \colon \overline{E} \to \overline{E}^{(p)} = \overline{E}$, which up to an automorphism, must be the Frobenius endomorphism $\pi_{\overline{E}}$. We have $\mathrm{tr}\,\phi = \mathrm{tr}\,\phi_{\mathfrak{p}} = \mathrm{tr}\,\phi_{\bar{\mathfrak{p}}} = t$, with $t \not\equiv 0 \bmod p$ by part (iv) of Theorem 22.5. For $j(\overline{E}) \neq 0, 1728$ the only automorphisms of $\overline{E}$ are ± 1, so $\mathrm{tr}\,\pi_{\overline{E}} = \pm\,\mathrm{tr}\,\phi = \pm t \not\equiv 0 \bmod p$ and $\overline{E}$ is ordinary. □

Corollary 22.9 gives us an explicit method for constructing elliptic curves over finite fields with a prescribed number of rational points. Let $D < -4$ be an imaginary quadratic discriminant and let $p \nmid D$ be an odd prime. In this case the norm equation $4p = t^2 - v^2D$ determines t (and v) up to a sign, and we can efficiently compute a solution (t, v) using Cornacchia's algorithm (see Problem Set 2). Given the Hilbert class polynomial $H_D(X)$, we can efficiently compute a root j_0 of $H_D(X)$ over $\mathbb{F}_p$ (using a randomized root-finding algorithm) and then write down the equation $y^2 = x^3 + Ax + B$ of an elliptic curve E with $j(E) = j_0$, using $A = 3j(1728 - j)$ and $B = 2j(1728 - j)^2$ (assuming $j_0 \neq 0, 1728$).

The Frobenius endomorphism π_E then satisfies $\mathrm{tr}\,\pi_E = \pm t$, and by Hasse's theorem,

$$\#E(\mathbb{F}_p) = p + 1 - \mathrm{tr}(\pi_E).$$

The sign of $\mathrm{tr}\,\pi_E$ depends can be explicitly determined using the formulas in [9]. Alternatively, one can simply pick a random point $P \in E(\mathbb{F}_p)$ and check whether $(p+1-t)P = 0$ or $(p+1+t)P = 0$ both hold (at least one must); if only one of these equations is satisfied, then $\mathrm{tr}\,\pi$ is determined (for large p this will almost always happen with the first P we try). Note that we can always change the sign of $\mathrm{tr}\,\pi$ be replacing E with its quadratic twist.

[5] In fact $\overline{E}$ is also ordinary when $j(\overline{E}) \in \{0, 1728\}$, but this takes more work to prove.

Now suppose that wish to construct an elliptic curve E over some finite field $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = N$, for some positive integer N. Provided we can factor N (typically N is prime and this is easy), we can use Cornacchia's algorithm to find a solution (a, v) to

$$4N = a^2 - v^2 D$$

for any particular imaginary quadratic discriminant D, whenever such a solution exists.[6] Given a solution (a, v), we put $t := a + 2$ and check whether $p := N - 1 + t$ is prime. If not, or if no solution (a, v) can be found, we just try a different discriminant D. In practice this will happen quite quickly; see [3] for a heuristic complexity analysis.

Once we have $p = N - 1 + t$ prime, we then observe that

$$4p = 4N - 4 + 4t = a^2 - v^2 D - 4 + 4a + 8 = (a + 2)^2 - v^2 D = t^2 - v^2 D,$$

so the norm equation is satisfied, and we can construct an elliptic curve $E/\mathbb{F}_p$ with $\operatorname{tr} \pi_E = \pm t$ using the Hilbert class polynomial $H_D(X)$ as described above, taking a quadratic twist if necessary to get $\operatorname{tr} \pi_E = t$. We then have $\#E(\mathbb{F}_p) = p + 1 - t = N$ as desired.

This method of constructing an elliptic curve $E/\mathbb{F}_p$ is known as the *CM method*. The CM method has many applications, one of which is an improved version of elliptic curve primality proving developed by Atkin and Morain [1]; see Problem Set 11.

Remark 22.10. It can happen that $H_D(X)$ has roots in $\mathbb{F}_p$ even when p does not split completely in the ring class field L. These roots cannot be j-invariants of elliptic curves $E/\mathbb{F}_p$ with $\operatorname{End}(E) = \mathcal{O}$, we must have $\mathcal{O} \subsetneq \operatorname{End}(E)$, and in fact the fraction field K of $\mathcal{O}$ must be properly contained in $\operatorname{End}^0(E)$. This means that $\operatorname{End}^0(E)$ has to be a quaternion algebra that contains the imaginary quadratic field K. This cannot happen when $p = \mathfrak{p}\overline{\mathfrak{p}}$ splits in K (which occurs exactly when $\left(\frac{D}{p}\right) = 1$), because L/K is Galois and the residue field extensions $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ all have the same degree (so $H_D \bmod p$ either has no roots at all or splits completely and in the latter case p must split completely in the ring class field for $\mathcal{O}$). But if p is inert in K then $H_D(X)$ can easily have roots modulo p that must be j-invariants of supersingular elliptic curves. This actually provides a very efficient method for constructing supersingular elliptic curves; see [2] for details.

Remark 22.11. We have restricted our attention to prime fields $\mathbb{F}_p$ in order to simplify the exposition, but everything we have done generalizes to arbitrary finite fields $\mathbb{F}_q$ of prime power order q. If $\mathcal{O}$ is an imaginary quadratic order of discriminant D with ring class field L, in Theorem 22.5 we can replace $p \nmid D$ with $q \perp D$, replace $\left(\frac{D}{p}\right) = 1$ with the requirement that D is a square in $\mathbb{F}_q$ (automatic when q is a square), and rather than requiring p to split completely in L we require q to be the norm of a prime ideal $\mathfrak{q}$ in $\mathcal{O}_L$. The norm equation then becomes $4q = t^2 - v^2 D$ with $t \perp q$, and if it is satisfied with $D < -4$ the Hilbert class polynomial $H_D(X)$ splits completely in $\mathbb{F}_q[x]$ and its roots are j-invariants of elliptic curves $E/\mathbb{F}_q$ with $\operatorname{tr} \pi_E = \pm t$ (which in fact have $\operatorname{End}(E) = \mathcal{O}$).

The main limitation of the CM method is that it requires computing the Hilbert class polynomial $H_D(X)$, which becomes very difficult when $|D|$ is large. The degree of $H_D(X)$ is the class number $h(D) \approx \sqrt{|D|}$, and the size of its largest coefficient is on the order of

[6] We need to be able to factor N because Cornacchia's algorithm requires a square root of D modulo N; computing square roots modulo primes is easy, and if we know the factorization of N we can use the CRT to reduce to this case; in general, computing square roots modulo N is as hard as factoring N.

$\sqrt{|D|}\log|D|$ bits.[7] Thus the total size of $H_D(X)$ is on the order of $|D|\log|D|$ bits, which makes it impractical to even write down if $|D|$ is large. An efficient algorithm for computing $H_D(X)$ is outlined in Problem Set 11, and with a suitably optimized implementation, it can practically handle discriminants with $|D|$ as large as 10^{13}, for which the size of $H_D(X)$ is several terabytes [11]. Using class polynomials associated to other modular functions discriminants up to $|D| \approx 10^{15}$ can be readily addressed [5], and with more advanced techniques, even $|D| \approx 10^{16}$ is feasible [12].

22.6 The Deuring lifting theorem

As noted in the previous section, the injective ring homomorphism $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\overline{E})$ given by (3), where $\overline{E}/\mathbb{F}_p$ is the reduction of an elliptic curve E/L with CM by $\mathcal{O}$ over its ring class field L modulo an unramified prime $\mathfrak{q}$ of norm p, is actually an isomorphism. Moreover, every elliptic curve over $\mathbb{F}_p$ with CM by $\mathcal{O}$ arises as the reduction of an elliptic curve E/L, and this correspondence is a bijective at the level of j-invariants. These facts follow from results of Deuring that we won't take the time to prove, but record here for reference.

Theorem 22.12 (Deuring)**.** *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D with ring class field L, and let q be the norm of a prime ideal in $\mathcal{O}_L$ with $q \perp D$. Then $H_D(X)$ splits into distinct linear factors in $\mathbb{F}_q[X]$ and its roots form the set*

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) := \{j(E) \in \mathbb{F}_q : \mathrm{End}(E) \simeq \mathcal{O}\}.$$

of j-invariants of elliptic curves $E/\mathbb{F}_q$ with CM by $\mathcal{O}$.

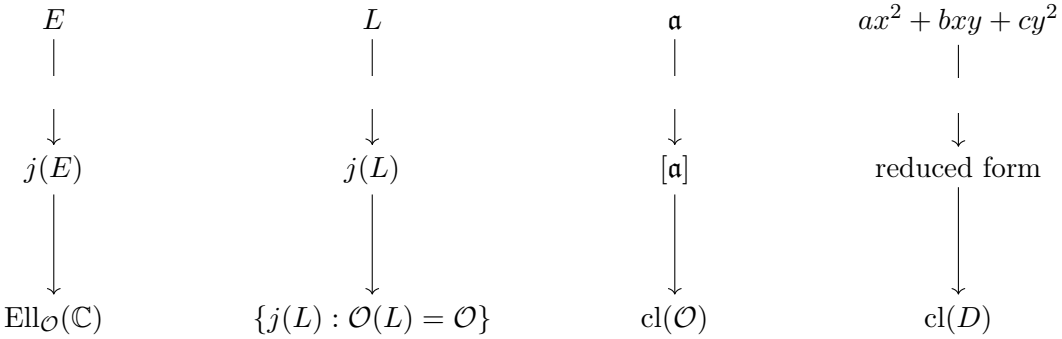
Proof. This follows from [6, Thm. 13]. □

Theorem 22.13 (Deuring lifting theorem)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field and let $\phi \in \mathrm{End}(E)$ be nonzero. There exists an elliptic curve E^* over a number field L with an endomorphism $\phi^* \in \mathrm{End}(E^*)$ such that E^* has good reduction modulo a prime $\mathfrak{q}$ of L with residue field $\mathcal{O}_L/\mathfrak{q} \simeq \mathbb{F}_q$and E and ϕ are the reductions modulo $\mathfrak{q}$ of E^* and ϕ^*.*

Proof. See [6, Thm. 14]. □

22.7 Summing up the theory of complex multiplication

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D.



[7] Under the Generalized Riemann Hypothesis, these bounds are accurate to within an $O(\log\log|D|)$ factor.

The figure above illustrates four different objects that have been our focus of study for the last several weeks:

1. Elliptic curves $E/\mathbb{C}$ with CM by $\mathcal{O}$.
2. Lattices L (which define tori $\mathbb{C}/L$ that correspond to elliptic curves).
3. Proper $\mathcal{O}$-ideals $\mathfrak{a}$ (which may be viewed as lattices).
4. Reduced primitive positive definite binary quadratic forms of discriminant D (which correspond to proper $\mathcal{O}$-ideals of norm a).

In each case we defined a notion of equivalence: isomorphism, homethety, equivalence modulo principal ideals, and equivalence modulo an $\mathrm{SL}_2(\mathbb{Z})$-action, respectively. Modulo this equivalence, we obtain a finite set of objects with the cardinality $h(\mathcal{O}) = h(D)$ in each case. The two sets on the right, $\mathrm{cl}(\mathcal{O})$ and $\mathrm{cl}(D)$, are finite abelian groups that act on the two sets on the left, both of which are equal to $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. This action is free and transitive, so that $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-torsor.

References

[1] A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), 29–68.

[2] R. Bröker, *Constructing supersingular elliptic curves*, Journal of Combinatorics and Number Theory **1** (2009), 269–273.

[3] R. Bröker and P. Stevenhagen, *Efficient CM-constructions of elliptic curves over finite fields*, Mathematics of Computation **76** (2007), 2161–2179.

[4] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, 1989.

[5] A. Enge and A.V. Sutherland, *Class invariants by the CRT method*, ANTS IX, LNCS 6197, Springer, 2010, pp. 142-156.

[6] S. Lang, *Elliptic functions*, Springer, 1987.

[7] J. S. Milne, *Algebraic number theory*, course notes, 2014.

[8] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[9] K. Rubin and A. Silverberg, *Choosing the correct elliptic curve in the CM method*, Mathematics of Computation **79** (2010), 545–561.

[10] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.

[11] A.V. Sutherland, *Computing Hilbert class polynomials with the Chinese Remainder The-orem*, Mathematics of Computation **80** (2011), 501–538.

[12] A.V. Sutherland, *Accelerating the CM method*, LMS Journal of Computation and Math-ematics **15** (2012), 172–204.

18.783 Elliptic Curves

Spring 2019