22 Ring class fields and the CM method

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D, let $K = \mathbb{Q}(\sqrt{D})$, and let L be the splitting field of the Hilbert class polynomial $H_D(X)$ over K. In the previous lecture we 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 $H_D(X)$ (the j-invariants of elliptic curves with CM by $\mathcal{O}$). To complete the proof of the the First Main Theorem of Complex Multiplication, which asserts that Ψ is an isomorphism, we need to show that Ψ is surjective; this is equivalent to showing the $H_D(X)$ is irreducible over K.

At the end of the last lecture we introduced the Artin map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$, which sends each unramified prime $\mathfrak{p}$ of K to the unique automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ for which

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

for all $x \in \mathcal{O}_L$ and primes $\mathfrak{q}$ of L dividing $\mathfrak{p}\mathcal{O}_L$ (recall that $\sigma_{\mathfrak{p}}$ is independent of $\mathfrak{q}$ because $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{cl}(\mathcal{O})$ is abelian). Equivalently, $\sigma_{\mathfrak{p}}$ is the unique element of $\mathrm{Gal}(L/K)$ that fixes $\mathfrak{q}$ and induces the Frobenius automorphism $x \mapsto x^{\mathrm{N}\mathfrak{p}}$ of $\mathbb{F}_q := \mathcal{O}_L/\mathfrak{q}$, which is a generator for $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, where $\mathbb{F}_p := \mathcal{O}_K/\mathfrak{p}$.

Note that if $E/\mathbb{C}$ has CM by $\mathcal{O}$ then $j(E) \in L$, and this implies that E can be defined by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathcal{O}_L$. For each prime $\mathfrak{q}$ of L, so long as $\Delta(E) = -16(4A^3 + 27B^2)$ does not lie in $\mathfrak{q}$, equivalently, the image of $\Delta(E)$ in $\mathbb{F}_q = \mathcal{O}_L/\mathfrak{q}$ is nonzero, we can reduce E modulo $\mathfrak{q}$ to get 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 $\mathfrak{q}$, which holds for all but finitely many primes $\mathfrak{q}$ of L, since the unique factorization of $\Delta(E)\mathcal{O}_L$ into prime ideals of $\mathcal{O}_L$ is finite.

22.1 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 $\alpha \in \mathrm{cl}(\mathcal{O})$ for which $j(E)^\sigma = \alpha j(E)$ holds for all $j(E) \in \mathrm{Ell}_{\mathcal{O}}(L)$ is a group isomorphism that commutes with the actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(L)$.*

Proof. We have already shown that Ψ is well defined, injective, and commutes with the group actions of $\mathrm{Gal}(L/K)$ and $\mathrm{cl}(\mathcal{O})$ (see Theorem 21.13 and the discussion preceding it). It remains only to show that Ψ is surjective.

So let α be an arbitrary element of $\mathrm{cl}(\mathcal{O})$, and let $\mathfrak{p}$ be a prime of K that satisfies the following conditions:

(i) $\mathfrak{p} \cap \mathcal{O}$ is a proper $\mathcal{O}$-ideal of prime norm p contained in α;

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

Andrew V. Sutherland

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

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

By Theorem 21.10, 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 a prime of K or 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 an equivalence class of $\mathcal{O}$-ideals).

Let us now consider a prime $\mathfrak{q}$ of L dividing $\mathfrak{p}\mathcal{O}_L$ and curve E/L with CM by $\mathcal{O}$ that has good reduction modulo $\mathfrak{q}$, and let $\overline{E}/\mathbb{F}_{\mathfrak{q}}$ denote the reduction of E modulo $\mathfrak{q}$. Since $\mathfrak{p}$ is unramified in L (by (ii)), we can apply the Artin map to obtain $\sigma_{\mathfrak{p}}$, which by (1) corresponds to the p-power Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, since $\mathrm{N}\mathfrak{p} = p$. This induces an isogeny $\pi\colon \overline{E} \to \overline{E^{\sigma}} = \overline{E}^{(p)}$ 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 $\mathfrak{p}$ corresponds to an isogeny $\phi_{\mathfrak{p}}\colon E \to \mathfrak{p}E$ of degree $\mathrm{N}\mathfrak{p} = p$, that induces an isogeny $\overline{\phi}_{\mathfrak{p}}\colon \overline{E} \to \overline{\mathfrak{p}E}$ of the reduced curves that also has degree p; here we are using the fact that E and $\mathfrak{p}E$ both have good reduction modulo $\mathfrak{q}$, by (iii). The isogeny $\overline{\phi}_{\mathfrak{p}}$ is obtained by reducing the coefficients of the rational map $(u(x)/v(x), s(x)/t(x)y)$ that defines $\phi_{\mathfrak{p}}$ modulo $\mathfrak{q}$; we can assume $u, v, s, t \in \mathcal{O}_L[x]$ because E and $\mathfrak{p}E$ are both defined over L, and that u is monic (so its degree does not change after reduction) and that the reduction of v is nonzero (because $\mathfrak{p}E$ has good reduction).

If ϕ is inseparable, then $\phi = \phi_{\mathrm{sep}} \circ \pi$, by Corollary 5.16, and $\deg \phi = p = \deg \pi$ implies $\deg \phi_{\mathrm{sep}} = 1$, which means that ϕ_{sep} is an isomorphism, so $\overline{\mathfrak{p}E} \simeq \overline{E^{\sigma_{\mathfrak{p}}}}$. We then have $j(\overline{\mathfrak{p}E}) = j(\overline{E^{\sigma_{\mathfrak{p}}}})$ and therefore $j(\mathfrak{p}E) = j(E^{\sigma_{\mathfrak{p}}})$, by (iv). 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 $\mathrm{Ell}_{\mathcal{O}}(L)$.

Now suppose $\phi\colon \overline{E} \to \overline{\mathfrak{p}E}$ is separable.[1] Then $\Psi(\sigma_{\mathfrak{p}}) \neq [\mathfrak{p}]$, but we claim that in this case $\Psi(\sigma_{\mathfrak{p}}^{-1}) = [\mathfrak{p}]$. Indeed, if ϕ is separable then the reduction of the isogeny $E \to \mathfrak{p}E$ must be separable no matter which E we pick. This implies that the reduction of the dual isogeny $\mathfrak{p}E \to E$ corresponding to the action of $\overline{\mathfrak{p}}$ must be inseparable, since the composition of the reductions of these isogenies is the multiplication-by-p map which we recall is inseparable in characteristic p; note that $\mathfrak{p} \neq \overline{\mathfrak{p}}$ since p is unramified in K, by (ii). This implies $\Psi(\sigma_{\mathfrak{p}}) = [\overline{\mathfrak{p}}]$ and therefore $\Psi(\sigma_{\mathfrak{p}}^{-1}) = [\mathfrak{p}]$, since $[\mathfrak{p}]^{-1} = [\overline{\mathfrak{p}}]$. □

Corollary 22.2. *The Hilbert class polynomial $H_D(x)$ is irreducible over $K = \mathbb{Q}(\sqrt{D})$ and each of its roots $j(E)$ generates an abelian extension $K(j(E))/K$ with Galois group isomorphic to* $\mathrm{cl}(\mathcal{O})$.

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 therefore the minimal polynomial of each of its roots. The degree of H_D is equal to the class number $h(D)$, and we have $h(D) = |\mathrm{cl}(\mathcal{O})| = |\mathrm{Gal}(L/K)| = [L : K]$, so we must have $L = K(j(E))$ for every root $j(E)$ of $H_D(X)$. And we have $\mathrm{Gal}(L/K) \simeq \mathrm{cl}(\mathcal{O})$ by Theorem 22.1, which is an abelian group. □

[1] In fact, with the normalized identification $\mathrm{End}(E) = \mathcal{O}$ discussed in §17.2 this never happens. We defined $\mathfrak{p}E = E_{\mathfrak{p}^{-1}}$ rather than $\mathfrak{p}E = E_{\mathfrak{p}}$ precisely so that we would always have $\Psi(\sigma_{\mathfrak{p}}) = [\mathfrak{p}]$; but we don't need to prove this so we won't.

The splitting field L of $H_D(X)$ over K is known as the *ring class field* of the imaginary quadratic order $\mathcal{O}$ with discriminant D. For any number field L, we say that an integer prime p is unramified in L if the ideal $p\mathcal{O}_L$ factors into distinct prime ideals $\mathfrak{q}$, and we say that p *splits completely* in L if the prime ideals $\mathfrak{q}$ are distinct and all have norm $\mathrm{N}\mathfrak{q} = p$ (such prime ideals $\mathfrak{q}$ are called degree-1 primes, since the degree of the residue field extension $\mathbb{F}_\mathfrak{q}/\mathbb{F}_p$ is 1). We say that a polynomial in *splits completely* in $\mathbb{F}_p[x]$ if it is a product of distinct linear polynomials in $\mathbb{F}_p[x]$.

Theorem 22.3. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D and ring class field L. Let p be a prime not dividing D that is unramified in L.*[2] *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 completely in $\mathbb{F}_p[X]$;*

(iii) *p splits completely in L;*

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

Proof. Let $K = \mathbb{Q}(\sqrt{D})$ be the fraction field of $\mathcal{O}$ and let $\mathcal{O}_K = [1, \omega]$ be the maximal order (ring of integers of K). By Theorem 17.14 we may write $D = u^2 D_K$, where $u = [\mathcal{O}_K : \mathcal{O}]$ and $D_K = \mathrm{disc}(\mathcal{O}_K)$ is a fundamental discriminant, and then $\mathcal{O} = [1, u\omega]$.

(i)⇒(iv): Let (λ) be a principal $\mathcal{O}$-ideal of norm p. Then $[1, \lambda]$ is a suborder of $\mathcal{O}$ with discriminant $v^2u^2D_K = v^2D$, where $v = \big[\mathcal{O} : [1, \lambda]\big]$. Let $t := \lambda + \bar{\lambda}$ so that $x^2 - t\lambda + p$ is the minimal polynomial of λ. By Lemma 22.4 below, this polynomial has discriminant $t^2 - 4p = v^2D$, so (iv) holds with $t \not\equiv 0 \bmod p$ since p does not divide D.

(iv)⇒(i): If $4p = t^2 - v^2D$ then the polynomial $x^2 - tx + p$ with discriminant v^2D has a root $\lambda \in \mathcal{O}$ because the order $[1, \lambda]$ has discriminant v^2D and therefore lies in $\mathcal{O}$.

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

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

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

(ii)⇒(iii): If $\left(\frac{D}{p}\right) = 1$, then $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits into distinct primes of norm p in K, by Lemma 22.5, and if $H_D(X)$ splits completely over $\mathbb{F}_p$, 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 $\mathfrak{q}$ of L lying above $\mathfrak{p}$. So p splits completely in L.

(iii)⇒(i): If $p\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ with the $\mathfrak{q}_i$ distinct $\mathcal{O}_L$-ideals of norm p, then we have $\mathbb{F}_\mathfrak{q} := [\mathcal{O}_L : \mathfrak{q}] = \mathbb{F}_p$ for all primes $\mathfrak{q}$ that divide p. If $\mathfrak{p}$ is any prime of K dividing $p\mathcal{O}_K$ then $\mathfrak{p}\mathcal{O}_L$ divides $p\mathcal{O}_L$ and is divisible by some $\mathfrak{q}$ dividing $p\mathcal{O}_L$. The inclusions $\mathbb{Q} \subseteq K \subseteq L$ imply $\mathbb{F}_p \subseteq \mathbb{F}_\mathfrak{p} \subseteq \mathbb{F}_\mathfrak{q}$, 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 $\sigma_\mathfrak{p} \in \mathrm{Gal}(L/K)$ is the identity, and so is $[\mathfrak{p} \cap O] \in \mathrm{cl}(\mathcal{O})$, 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 u). Thus $\mathfrak{p} \cap \mathcal{O}$ is a principal $\mathcal{O}$-ideal of norm $[\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O}_K : \mathfrak{p}] = p$. □

[2] In fact if p does not divide D then it is guaranteed to be unramified in L, but we have not proved this (nor do we plan to) so it is included as a hypotheses.

Lemma 22.4. *Let $\mathcal{O} = [1, \omega]$ be an imaginary quadratic order of discriminant D. Then D is the discriminant of the minimal polynomial $x^2 - (\omega + \overline{\omega})x + \omega\overline{\omega} \in \mathbb{Z}[x]$ of ω over $\mathbb{Q}$.*

Proof. We have

$$\operatorname{disc}([1, \omega)| = \det \begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix}^2 = (\overline{\omega} - \omega)^2 = D. \qquad \square$$

Lemma 22.5. *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 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*

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

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

We say p is *split*, *ramified*, or *inert*, according to $\left(\frac{D}{p}\right) = 1, 0, -1$, respectively.

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 $\mathfrak{p}\overline{\mathfrak{p}} = (\mathrm{N}\mathfrak{p}) = (p)$. 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 $[o, \omega - s]$ are clearly distinct.

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

$$(\omega + \overline{\omega})^2 - 4\omega\overline{\omega} = (\omega - \overline{\omega})^2 = \det \begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix}^2 = \operatorname{disc}(\mathcal{O}_K) = D, \qquad (2)$$

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. $\square$

Corollary 22.6. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K with discriminant. If p divides the conductor $[\mathcal{O}_K : \mathcal{O}]$ then 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, where $D = \operatorname{disc}(\mathcal{O}_K)$.*

22.2 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 Galois extensions. A famous 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 to fields other than $\mathbb{Q}$ 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[3] of K, and it satisfies $\mathrm{Gal}(L/K) \simeq \mathrm{cl}(\mathcal{O}_K)$. This conjecture was proved shortly thereafter by Furtwängler, and the field L is known as the *Hilbert class field* of K. While its existence was 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).

After $\mathbb{Q}$, the simplest fields K to consider are imaginary quadratic fields. As a generalization of the Hilbert class field, rather than requiring L/K to be unramified at every prime of K, we might instead only require L/K to be unramified at primes that are proper $\mathcal{O}$-ideals, for some order $\mathcal{O} \subseteq \mathcal{O}_K$. As proved in problem 3 of Problem Set 9, this excludes only finitely many primes of K, namely, those whose norms divide the conductor $[\mathcal{O}_K : \mathcal{O}]$ of the order $\mathcal{O}$. This leads to the definition of the *ring class field* $K_{\mathcal{O}}$ of the order $\mathcal{O}$. The ring class field of $\mathcal{O}_K$ is then the Hilbert class field.

The ring class field $K_{\mathcal{O}}$ is uniquely characterized by the infinite set $\mathcal{S}_{K_{\mathcal{O}}/\mathbb{Q}}$ of rational primes p that split completely in $K_{\mathcal{O}}$, and with finitely many exceptions, these are precisely the primes that satisfy the equation $4p = t^2 - v^2D$ for some $t, v \in \mathbb{Z}$, where $D = \mathrm{disc}(\mathcal{O})$; see [2, Thm. 9.2, Ex, 9.3]. The Chebotarev density theorem implies that any extension M/K for which the set $\mathcal{S}_{M/\mathbb{Q}}$ matches $\mathcal{S}_{K_{\mathcal{O}}/\mathbb{Q}}$ with only finitely many exceptions must in fact be equal to $K_{\mathcal{O}}$, by [2, Thm. 8.19]. Thus we have the following corollary of Theorem 22.3, which completely solves the problem of explicitly constructing the Hilbert class field (and ring class fields), in the case that K is an imaginary quadratic field.

Corollary 22.7. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D with fraction field K. The splitting field of $H_D(X)$ over K is the ring class field of the order $\mathcal{O}$.*

Ring class fields allow us to explicitly construct infinitely many abelian extensions of a given imaginary quadratic field K. One might then ask whether every abelian extension of K is contained in a ring class field. This is not the case, but by extending ring class fields $K_{\mathcal{O}}$ by adjoining the x-coordinates of the n-torsion points of any elliptic curve with CM by $\mathcal{O}$ (or powers of them when $D = -3, -4$), one obtains what are known as *ray class fields* (which vary with 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 as explicit as they are in the imaginary quadratic case.

[3]This includes not only all prime $\mathcal{O}_K$-ideals, but also the "infinite primes" of K, which correspond to embeddings of K into $\mathbb{C}$. Only real infinite primes (embeddings of K into $\mathbb{R}$) can ramify, so for imaginary quadratic fields K this imposes no additional restrictions the Hilbert class field L.

22.3 The CM method

The equation

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

in part (iv) of Theorem 22.3 is known as the *norm equation*, since it arises from the principal ideal of norm p given by part (i). For $D < -4$, the integers t^2 and v^2 are uniquely determined by p and D. If the norm equation is satisfied and $j(E)$ is a root of $H_D(X)$ over $\mathbb{F}_p$, then the Frobenius endomorphism π of $E/\mathbb{F}_p$ corresponds to a root of the characteristic polynomial

$$x^2 - (\operatorname{tr}\pi)x + p.$$

Viewing π as an element of $\operatorname{End}(E) \simeq \mathcal{O}$, we can apply the quadratic formula to compute

$$\pi = \frac{\operatorname{tr}(\pi) \pm \sqrt{\operatorname{tr}(\pi)^2 - 4p}}{2},$$

where $\sqrt{\operatorname{tr}(\pi)^2 - 4p}$ lies in $\mathcal{O}$ and can written as $v\sqrt{D}$ for some integer v. It follows that $\operatorname{tr}\pi = \pm t$. The two possible signs correspond to quadratic twists of E.

Given the Hilbert class polynomial $H_D(X)$ and a prime p for which the norm equation holds, we can compute a root j_0 of $H_D(X)$ over $\mathbb{F}_p$ 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 $B = 2j(1728 - j)^2$. The Frobenius endomorphism π_E then satisfies $\operatorname{tr}\pi_E = \pm t$, and by Hasse's theorem we have

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

The sign of $\operatorname{tr}\pi_E$ can be uniquely determined using the formulas in [5]. A more expedient method is to 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 $\operatorname{tr}\pi$ is determined. By Mestre's theorem (see Theorem 8.5), for $p > 229$ this is guaranteed that to work for either E or its quadratic twist, for most of the random points P we pick (when p is large the first random point P that we try is almost certain to work).

This method of constructing an elliptic curve $E/\mathbb{F}_p$ using a root of the Hilbert class polynomial is known as the *CM method*. Its key virtue is that $\#E(\mathbb{F}_p) = p + 1 - t$ is known in advance. This has many applications, one of which is an improved version of elliptic curve primality proving developed by Atkin and Morain [1]; see Problem Set 12 for details.

The main limitation of the CM method is that it requires computing (or having precomputed) 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 $h(D)$, which is asymptotically on the order of $\sqrt{|D|}$, and the size of its largest coefficient is on the order of $\sqrt{|D|}\log|D|$ bits.[4] 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 (in general, $|D|$ may be as large as the prime p we are working with). 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 [7]. Using class polynomials associated to alternative modular functions (which may be smaller then H_D by a large constant factor), discriminants up to $|D| \approx 10^{15}$ can be readily addressed [3]; with more advanced techniques, even $|D| \approx 10^{16}$ is feasible [8].

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

22.4 Summing up the theory of complex multiplication

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

E	L	$\mathfrak{a}$	$ax^2+bxy+cy^2$
↓ isomorphism	↓ homethety	↓ mod principal ideals	↓ $\mathrm{SL}_2(\mathbb{Z})$-equivalence
$j(E)$	$j(L)$	$[\mathfrak{a}]$	reduced form
↓	↓	↓	↓
$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$	$\{j(L) : \mathcal{O}(L) = \mathcal{O}\}$	$\mathrm{cl}(\mathcal{O})$	$\mathrm{cl}(D)$

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. Primitive positive definite binary quadratic forms $ax^2 + bxy + cy^2$ 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 prinicipal 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 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \mathrm{Ell}_{\mathcal{O}}(K_{\mathcal{O}})$. This action is free and transitive, so that $\mathrm{Ell}_{\mathcal{O}}(K_{\mathcal{O}})$ is a $\mathrm{cl}(\mathcal{O})$-torsor.

The integer polynomials $H_D(X)$ and $\Phi_N(X,Y)$ allow us to explicitly realize this torsor over any field k containing $\sqrt{D}$ in which $H_D(X)$ splits completely: the roots of $H_D(X)$ form the set $\mathrm{Ell}_{\mathcal{O}}(k)$, and the action of $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ sends $j(E) \in \mathrm{Ell}_{\mathcal{O}}(k)$ to a root of $\Phi_{N(\mathfrak{a})}(j(E), Y)$ that also lies in $\mathrm{Ell}_{\mathcal{O}}(k)$, via a cyclic isogeny of degree $\mathrm{N}\mathfrak{a}$.

References

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

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

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

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

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

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

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

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