

CM ELLIPTIC CURVES – A CRASH COURSE FOR CRYPTOGRAPHERS

MATTHEW GREENBERG

These are informal notes of lectures delivered at the summer school preceding ECC 2009 in Calgary. The goal of these lectures was to introduce participants to theory of complex multiplication of elliptic curves, emphasizing the objects and computational applications which are of interest in cryptography, e.g., modular polynomials, Hilbert class polynomials, and the CM method for constructing elliptic curves with a known number of points. In these notes, I'm assuming a basic familiarity with the basic algebraic theory of elliptic curves, in particular over finite fields. In particular, the notions like j -invariant, isogeny, and trace of Frobenius will be used freely. These fundamental notions were the subject of a minicourse run concurrently by Larry Washington. Being informal notes, this document is likely full of typos, errors and inconsistencies. I would appreciate it very much if readers who find such could let me know so I can make the relevant corrections.

1. COMPLEX TORI

A *complex torus* is a space of the form $T = \mathbb{C}/L$, where L is a lattice in \mathbb{C} , i.e., a free \mathbb{Z} -submodule of \mathbb{C} which spans \mathbb{C} as an \mathbb{R} -vector space. It follows that L has rank two over \mathbb{Z} . Endowing T with the unique complex structure such that the canonical projection $\mathbb{C} \rightarrow T$ is analytic, T becomes a Riemann surface, i.e., a complex manifold of dimension one.

Let L_1 and L_2 be lattices in \mathbb{C} and let $T_1 = \mathbb{C}/L_1$ and $T = \mathbb{C}/L_2$. An analytic map $f : T_1 \rightarrow T_2$ which is also a group homomorphism is called an *isogeny*. A bijective isogeny of complex tori is an isomorphism.

Example 1. Let $\alpha \in \mathbb{C}$ be such that $\alpha L_1 \subset L_2$. Then the map $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto \alpha z$, descends to an isogeny denoted $\alpha : T_1 \rightarrow T_2$. If $\alpha L_1 = L_2$, then the map α is an isomorphism.

Proposition 2. *Every isogeny $T_1 \rightarrow T_2$ is given by multiplication by α , for some $\alpha \in \mathbb{C}$ with $\alpha L_1 \subset L_2$.*

Proof. Let $f : T_1 \rightarrow T_2$ be an isogeny. Since $\mathbb{C} \rightarrow \mathbb{C}/L_2$ is the universal cover and \mathbb{C} is simply connected, there is a unique $F : \mathbb{C} \rightarrow \mathbb{C}$ such that $F(0) = 0$ and

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{F} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/L_1 & \xrightarrow{f} & \mathbb{C}/L_2 \end{array}$$

commutes. Since $\mathbb{C} \rightarrow \mathbb{C}/L_1$ is a local homeomorphism, F is entire. Let $\omega \in L_1$. Then for all $z \in \mathbb{C}$,

$$\Delta(z, \omega) := F(z + \omega) - F(z)$$

belongs to L_2 . Since $\Delta(\cdot, \omega)$ is continuous and L is discrete, Δ must be a function of ω alone, i.e., there is a function $\delta : L_1 \rightarrow \mathbb{C}$ such that $\Delta(z, \omega) = \delta(\omega)$ for all z . We note that δ is a group homomorphism:

$$\begin{aligned} \delta(\omega + \omega') &= F(z + \omega + \omega') - F(z) \\ &= F((z + \omega) + \omega') - F(z + \omega) + F(z + \omega) - F(z) \\ &= \Delta(z + \omega, \omega') + F(z, \omega) \\ &= \delta(\omega') + \delta(\omega). \end{aligned}$$

Let $\{\omega_1, \omega_2\}$ be a basis of L_1 . Let $z \in \mathbb{C}$. There there are integers a_1 and a_2 such that, setting $\omega_z = a_1\omega_1 + a_2\omega_2$, $z - \omega$ belongs to the closed parallelogram \mathcal{F}_{L_1} with vertices $0, \omega_1, \omega_2$ and $\omega_1 + \omega_2$. Since δ is a group homomorphism, $|\omega_z| = O(|z|)$ and $z - \omega_z$ belongs to the compact set \mathcal{F}_{L_1} , we have

$$\begin{aligned} |F(z)| &\leq |F(z - \omega_z)| + |\delta(\omega_z)| \\ &= |F(z - \omega_z)| + O(|\omega_z|) \\ &= |F(z - \omega_z)| + O(|z|) \\ &= O(|z|). \end{aligned}$$

It is a basic result in complex analysis that an entire function $F(z)$ satisfying $|F(z)| = O(|z|)$ must have the form $\alpha z + \beta$. Since $F(0) = 0$, $\beta = 0$ and $F(z) = \alpha z$, as desired. \square

Define the equivalence relation *homothety* on the set of lattices in \mathbb{C} by saying that two lattices L_1 and L_2 are homothetic if there is a complex number $\alpha \in \mathbb{C}^\times$ such that $L_2 = \alpha L_1$.

Corollary 3. *The mapping $L \mapsto \mathbb{C}/L$ extends to a bijection*

$$(set\ of\ lattices\ in\ \mathbb{C})/homothety \longleftrightarrow (set\ of\ complex\ tori)/isomorphism.$$

2. WEIERSTRASS UNIFORMIZATION

The goal of this section is to prove that the categories of complex tori and Weierstrass models of elliptic curves over \mathbb{C} are equivalent. Let L be a lattice in \mathbb{C} . We wish to write down an analytic isomorphism of the complex torus \mathbb{C}/L onto an elliptic curve in $\mathbb{P}^2(\mathbb{C})$. This coordinatization exploits the *Weierstrass elliptic function* \wp_L associated to L :

$$\wp_L(z) := z^{-2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} ((z - \omega)^{-2} - \omega^{-2}).$$

Lemma 4.

(1) *Let k be an integer. Then sum*

$$G_k(L) := \sum_{\omega \in L} \omega^{-k}$$

converges absolutely if $k > 2$.

(2) *The function \wp_L converges absolutely and uniformly on compact sets $K \subset \mathbb{C}$ with $K \cap L = \emptyset$. Therefore, \wp_L is a meromorphic function on \mathbb{C} whose singularities consist of a double poles at each $\omega \in L$.*

Sketch of proof. There are positive constants c and C such that

$$c\sqrt{a_1^2 + a_2^2} \leq |a_1\omega_1 + a_2\omega_2| \leq C\sqrt{a_1^2 + a_2^2}$$

for all $a_1, a_2 \in \mathbb{Z}$. Therefore, $G_k(L)$ converges absolutely if and only if $G_k(L_i)$ converges. Comparing the sum to an integral, $G_k(L_i)$ converges if and only if the integral

$$\iint_{x^2+y^2 \geq R} (x^2 + y^2)^{-k/2} dx dy = \iint_{r > R} r^{-k} (r dr d\theta)$$

converges. This happens when $k > 2$, proving (1).

Statement (2) follows from (1), together with the fact that for each compact K with $K \cap L = \emptyset$, we have

$$|(z - \omega)^{-2} - \omega^{-2}| = O(|\omega|^{-3}),$$

where the implied constant depends only on K and not on ω . \square

The change of variable $z \mapsto -z$ induces a permutation of the terms in the summation defining \wp_L :

$$(z - \omega)^{-2} - \omega^{-2} \mapsto (z - (-\omega))^{-2} - (-\omega)^{-2}.$$

Since the sum is absolutely convergent, we conclude that \wp_L is even:

$$\wp_L(-z) = \wp_L(z).$$

Another consequence of the absolute convergence of \wp_L is that its derivative may be computed term-by-term:

$$\wp'_L(z) = -2 \sum_{\omega \in L} (z - \omega)^{-3}.$$

This sum being absolutely convergent, it follows that \wp'_L is L -periodic, i.e., invariant under translation by elements L :

$$\wp'_L(z + \omega) = \wp'_L(z) \quad \text{for all } \omega \in L.$$

Lemma 5. *The Weierstrass function \wp_L is L -periodic.*

Proof. let $\omega \in L$. Its derivative being zero by the translation invariance of \wp'_L , the function $\wp_L(z + \omega) - \wp_L(z)$ is constant, say $\wp_L(z + \omega) - \wp_L(z) = c_\omega$. Setting $z = -\omega/2$, we have $\wp_L(\omega/2) - \wp_L(-\omega/2) = c_\omega$. Since \wp_L is even, $c_\omega = 0$. \square

Proposition 6. *The Weierstrass function \wp satisfies the differential equation*

$$(\wp')^2 = 4\wp^3 - 60G_4(L)\wp - 140G_6(L).$$

Proof. Set

$$F = (\wp'_L)^2 - 4\wp_L^3 - 60G_4(L)\wp_L - 140G_6(L).$$

We wish to compute the Laurent expansion of F about $z = 0$. Suppose $|z| < |\omega|$ for all $\omega \in L - \{0\}$.

$$(z - \omega)^{-2} - \omega^{-2} = \omega^{-2}((1 - z/\omega)^{-2} - 1) = \sum_{n=1}^{\infty} (n+1)z^n \omega^{-(n+2)}.$$

Therefore,

$$\begin{aligned}
\wp_L(z) &= z^{-2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \sum_{n=1}^{\infty} (n+1) z^n \omega^{-(n+2)} \\
&= z^{-2} + \sum_{n=1}^{\infty} (n+1) \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-(n+2)} \\
&= z^{-2} + \sum_{n=1}^{\infty} (n+1) G_{n+2}(L) z^n \\
&= z^{-2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(L) z^{2n},
\end{aligned}$$

where the last equality follows from the fact that $G_k(L) = 0$ for k odd, $k > 2$. Differentiating,

$$\wp'_L(z) = -2z^{-3} + \sum_{n=1}^{\infty} 2n(2n+1) G_{2n+2}(L) z^{2n-1}.$$

Computing the first few terms of these expansions, we have

$$\wp_L(z) = z^{-2} + 3G_4z^2 + 5G_6z^4 + \dots, \quad \wp'_L(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + \dots.$$

One may now compute directly that the Laurent expansion of F about $z = 0$ has the form $c_1z + c_2z^2 + \dots$. Since this expansion has no terms with negative powers, it follows from the L -periodicity of F that F is an entire, L -periodic. Such a function bounded and therefore constant. Since the expansion of F around $z = 0$ has no constant term, $F = 0$. \square

Let E_L/\mathbb{C} be the projective plane curve given by

$$E_L : zy^2 = 4x^3 - g_2(L)xz^2 - g_6(L)z^3,$$

where $g_2(L) := 60G_4(L)$ and $g_3 = 140G_6(L)$. That E_L is an elliptic curve follows from the following result:

Lemma 7. *For any lattice L in \mathbb{C} , the quantity*

$$\Delta(L) := g_2(L)^3 - 27g_3(L)^2$$

is nonzero.

By Proposition 6, we may define the *Weierstrass uniformization*

$$\Phi_L : \mathbb{C} \longrightarrow E_L(\mathbb{C}) \quad \text{by} \quad \Phi_L(z) = \begin{cases} (\wp_L(z) : \wp'_L(z) : 1), & \text{if } z \notin L, \\ (0 : 1 : 0), & \text{if } z \in L. \end{cases}$$

By the periodicity of \wp_L and \wp'_L , Φ_L descends to an analytic map

$$\Phi_L : \mathbb{C}/L \longrightarrow E_L(\mathbb{C})$$

Proposition 8. *The mapping Φ_L is a group isomorphism.*

Theorem 9 (Uniformization theorem). *Suppose A and B are unique complex numbers such that $A^3 - 27B^2 \neq 0$. Then there is a unique lattice L in \mathbb{C} such that*

$$g_2(L) = A \quad \text{and} \quad g_3(L) = B.$$

Thus, all Weierstrass models of elliptic curves arise from lattice as described above. We summarize this discussion with the following commutative diagram

$$\begin{array}{ccc}
 \begin{array}{c} \text{lattices in } \mathbb{C} \\ = \text{complex tori} \end{array} & \xrightarrow{\hspace{10em}} & \begin{array}{c} \text{nonsingular Weierstrass equations} \\ \text{of the form } y^2 = 4x^3 - Ax - B \end{array} \\
 \downarrow & & \downarrow \\
 \begin{array}{c} \text{lattices up to homothety} \\ = \text{complex tori up to isomorphism} \end{array} & \xrightarrow{\hspace{10em}} & \begin{array}{c} \text{Weierstrass equations up to} \\ \text{admissible change of variable} \\ = \text{elliptic curves over } \mathbb{C} \text{ up to isomorphism} \end{array}
 \end{array}$$

in which the horizontal arrows are bijections.

The j -invariant of E_L is given by

$$j(E_L) = 1728g_2(L)^3/\Delta(L).$$

3. ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Let T_1 and T_2 be the complex tori corresponding to lattices L_1 and L_2 . Write $\text{Isog}(T_1, T_2)$ for the set of isogenies from T_1 to T_2 . If $f, g \in \text{Isog}(T_1, T_2)$, then $(f + g)(z) = f(z) + g(z)$ is also an isogeny. Thus, $\text{Isog}(T_1, T_2)$ is an abelian group. For a complex torus $T = \mathbb{C}/L$, let $\text{End } T = \text{Isog}(T, T)$. By Proposition 2, $\text{End } T$ is naturally identified with the ring

$$\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subset L\} \subset \mathbb{C}.$$

We call $\mathcal{O}(L)$ the *ring of multipliers of L* . Evidently, $\mathbb{Z} \subset \mathcal{O}(L)$.

Let D be a fundamental discriminant and let K be the unique quadratic field with discriminant D . Write \mathcal{O}_D for the ring of integers of K . Let $f > 0$ be an integer. We define the *order in K of conductor f* to be the rank-two ring

$$\mathcal{O}_{f^2D} = \mathbb{Z} + f\mathcal{O}_D \subset \mathcal{O}_D.$$

It has index f in \mathcal{O}_D as an abelian group and it has discriminant f^2D .

Proposition 10. *The ring $\mathcal{O}(L)$ is either \mathbb{Z} or isomorphic to an order \mathcal{O}_{f^2D} with $D < 0$.*

Proof. Suppose $\alpha \in \mathcal{O}(L)$, $\alpha \notin \mathbb{Z}$. Let $\{\omega_1, \omega_2\}$ be a basis of L , there is a matrix $M(\alpha) \in M_2(\mathbb{Z})$ such that

$$\alpha \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = M(\alpha) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

It follows that α is an eigenvalue of $M(\alpha)$. Since $\alpha \notin \mathbb{Z}$, the matrix $M(\alpha)$ is not diagonal. Since ω_1 and ω_2 are \mathbb{R} -linearly dependent, $\alpha \notin \mathbb{R}$. Therefore, α is an algebraic integer and $\mathbb{Q}(\alpha)$ is an imaginary quadratic field. Let $\beta \in \mathcal{O}(L)$. We claim that $\beta \in \mathbb{Q}(\alpha)$. For suppose not. Then $\mathbb{Z}[\alpha, \beta]$ has rank four over \mathbb{Z} , implying that M induces a surjection $\mathbb{Q}(\alpha, \beta) \twoheadrightarrow M_2(\mathbb{Q})$. But no such surjection can exist as $\mathbb{Q}(\alpha, \beta)$ is commutative and $M_2(\mathbb{Q})$ is not. Therefore, $\text{End } T$ is an order in a quadratic field. \square

If E/\mathbb{C} is an elliptic curve with $\text{End } E = \mathcal{O}_{f^2D}$, we say that E has CM by \mathcal{O}_{f^2D} .

Proposition 11. *Let L be a lattice in \mathbb{C} . Then $\mathcal{O}(L) = \mathcal{O}_{f^2D}$ if and only if L is homothetic to an invertible ideal of \mathcal{O}_{f^2D} .*

Proof. We give the proof under the assumption $f = 1$. Suppose αL is an ideal of \mathcal{O}_D . (Since \mathcal{O}_D is the full ring of integers of K_D , all ideals of \mathcal{O}_D are invertible.) Then $\mathcal{O}_D \subset \mathcal{O}(L)$. Since $\mathcal{O}(L)$ is an order and \mathcal{O}_D is maximal, this inclusion must be an equality. Conversely, suppose $\mathcal{O}(L) = \mathcal{O}_D$. Let $\{\omega_1, \omega_2\}$ be a basis of L and let $\alpha \in \mathcal{O}_D - \mathbb{Z}$. Then there are integers a_1 and a_2 such that

$$\alpha\omega_2 = a_1\omega_1 + a_2\omega_2.$$

Since $\alpha \notin \mathbb{Z}$, $\alpha - a_2 \neq 0$ and

$$\omega_2/\omega_1 = a_1/(\alpha - a_2) \in K.$$

Letting n be such that $n\omega_2/\omega_1 \in \mathcal{O}$, we have

$$n\omega_1^{-1}L = n\omega_1^{-1}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \subset \mathcal{O}_D. \quad \square$$

We write Cl_{f^2D} for the class group of \mathcal{O}_{f^2D} and $h_{f^2D} := |\text{Cl}_{f^2D}|$ for the class number of \mathcal{O}_{f^2D} .

Corollary 12. *There are bijections*

$$\left(\begin{array}{l} \text{isomorphism classes of elliptic} \\ \text{curves } E/\mathbb{C} \text{ with } \text{End } E = \mathcal{O}_{f^2D} \end{array} \right) \longleftrightarrow \left(\begin{array}{l} \text{homothety classes of lattices} \\ L \text{ with } \mathcal{O}(L) = \mathcal{O}_{f^2D} \end{array} \right) \longleftrightarrow \text{Cl}_{f^2D}.$$

Set

$$J_{f^2D} = \{j(E) : E \text{ is defined over } \mathbb{C} \text{ and } \text{End } E = \mathcal{O}_{f^2D}\}.$$

Corollary 13. $|J_{f^2D}| = h_{f^2D}$.

Corollary 14. *Let E/\mathbb{C} be an elliptic curve with complex multiplication. Then $j(E)$ is algebraic.*

Proof. Suppose $j \in J_{f^2D}$ and Let E/\mathbb{C} ,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{C},$$

be an elliptic curve with $j(E) = j$. Let $\sigma \in \text{Aut } \mathbb{C}$ and let E^σ be the elliptic curve given by

$$y^2 = x^3 + A^\sigma x + B^\sigma.$$

As $\text{End } E^\sigma = \text{End } E = \mathcal{O}_{f^2D}$

$$j(E^\sigma) = j(E)^\sigma \in J_{f^2D}.$$

It follows that J_{f^2D} is stable under $\text{Aut } \mathbb{C}$ and, thus, is contained in $\overline{\mathbb{Q}}$. □

Theorem 15. *Let E/\mathbb{C} be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

We will indicate a proof of this theorem in the next section. Set

$$H_{f^2D}(x) = \prod_{j \in J_{f^2D}} (x - j).$$

Since J_{f^2D} is a set of algebraic integers which is stable under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$H_{f^2D}(x) \in \mathbb{Z}[x].$$

The polynomial H_{f^2D} is called the *Hilbert class polynomial associated to the order \mathcal{O}_{f^2D}* .

Theorem 16.

- (1) H_{f^2D} is irreducible over K_D .
- (2) For any $j \in \{j_1, \dots, j_{h(\mathcal{O})}\}$, $K_D(f) := K_D(j)$ is an abelian, Galois extension of K_D which is unramified away from f . H_{f^2D} splits into linear factors over $K_D(f)$.
- (3) Let $I_K(f)$ be the group of fractional ideals of K which are prime to f . Then the mapping $I_K(f) \rightarrow \text{Gal}(K(f)/K)$ given by $\mathfrak{a} \mapsto \text{Fr}_{\mathfrak{a}}$ descends to an isomorphism $\text{Cl}_{f^2D} \rightarrow \text{Gal}(K(f)/K)$.

Corollary 17. *Suppose E is an elliptic curve with CM which is defined over \mathbb{Q} and suppose $\text{End } E = \mathcal{O}_{f^2D}$. Then \mathcal{O}_{f^2D} has class number one. There are exactly thirteen such discriminants f^2D and, thus, thirteen $\overline{\mathbb{Q}}$ -isomorphism classes of CM elliptic curves defined over \mathbb{Q} .*

4. MODULAR POLYNOMIALS AND THE INTEGRALITY OF j

In this section, we indicate how one proves Theorem 15. Let E/\mathbb{C} be an elliptic curve with CM by the \mathcal{O}_{f^2D} . We have seen that the monic minimal polynomial of $j(E)$ is $H_{f^2D}(x)$. Therefore, the integrality of $j(E)$ is equivalent to that of $H_{f^2D}(x)$. The Hilbert class polynomial, though is a fairly unwieldy object. Therefore, we proceed by finding another monic polynomial in $\mathbb{Z}[x]$ (not necessarily irreducible) which has $j(E)$ as a root.

Let L be a lattice. For $n > 0$, let $L_1, \dots, L_{t(n)}$ be the set of index n sublattices of L , and define

$$\Phi_n(x, L) := \prod_{i=1}^{t(n)} (x - j(L_i)).$$

For each i , the canonical map $\mathbb{C}/L_i \rightarrow \mathbb{C}/L$ is an isogeny of degree n . Conversely, if $\mathbb{C}/L' \rightarrow \mathbb{C}/L$ is an isogeny of degree n , then L' is homothetic to L_i for some i . If E and E' are elliptic curve over \mathbb{C} , write $E \sim_n E'$ if there is an isogeny of degree n from E' to E . Similarly, if j and j' are complex numbers, write $j \sim_n j'$ if there are elliptic curves E and E' such that $j(E) = j$, $j(E') = j'$ and $E \sim_n E'$. It follows that

$$\Phi_n(x, L) = \prod_{j \sim_n j(L)} (x - j).$$

Theorem 18.

- (1) *There is a polynomial $\Phi_n \in \mathbb{Z}[x, y]$ such that for all lattice L ,*

$$\Phi_n(x, j(L)) = \Phi_n(x, L).$$

- (2) *If n is not a perfect square, then*

$$H_n(x) := \Phi_n(x, x)$$

is nonconstant and has leading coefficient ± 1 .

Thus, Φ_n has the “isogeny detecting” property that

$$\Phi_n(j(E_1), j(E_2)) = 0 \iff E_1 \text{ is } n\text{-isogenous to } E_2.$$

Φ_n is called the n -th modular polynomial. Theorem 18 may be used to prove Theorem 15:

Proof of Theorem 15. Let E/\mathbb{C} be an elliptic curve with CM \mathcal{O}_{f^2D} . Let L be a lattice in \mathbb{C} with $j(L) = j(E)$ and let $\alpha \in \mathcal{O}_{f^2D}$ be such that $n := N_{K/\mathbb{Q}}(\alpha)$ is not a perfect square. Then αL is a sublattice of L of index n , so $\Phi_n(j(L), j(\alpha L)) = 0$. But since the lattices L and αL are homothetic, $j(\alpha L) = j(L)$. Therefore,

$$H_n(j(L)) = \Phi_n(j(L), j(L)) = \Phi_n(j(L), j(\alpha L)) = 0.$$

By Theorem 18, $\pm H_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$, and the result follows. \square

5. COMPUTING HILBERT CLASS POLYNOMIALS

There are several approaches to computing H_{f^2D} in practice:

- floating point method
- CRT method
- p -adic method

We will discuss the first two. The first step in computing $H_{\mathcal{O}}$ is computing lattices $\{L_1, \dots, L_{h_{f^2D}}\}$ such that

$$\{j(L_1), \dots, j(L_{h_{f^2D}})\} = J_{f^2D}.$$

This is best accomplished using *binary quadratic forms*:

Theorem 19. *There is a bijection*

$$\begin{aligned} \text{Cl}_{f^2D} &\longleftrightarrow \left\{ \begin{array}{l} \text{primitive, reduced binary quadratic} \\ \text{forms of discriminant } f^2D \end{array} \right\} \\ \text{class of } (2a, -b + f\sqrt{D}) &\longleftrightarrow ax^2 + bxy + cy^2. \end{aligned}$$

Computing primitive, reduced binary quadratic forms of discriminant D is well understood. Suppose $L = (2a, -b + f\sqrt{D})$. Using q -expansions and the formula

$$j(L) = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2},$$

$j(L)$ can be computed to high precision. Since H_{f^2D} has integral coefficients, it can be recognized by rounding off a sufficiently accurate floating point approximation. It can be shown that

$$\log |j(L)| = O(f\sqrt{|D|}/a).$$

Thus, the numbers $j(L_i)$ must be computed to enormous precision to recognize the coefficients of H_{f^2D} . Let B be the maximum of the absolute values of the coefficients of H_{f^2D} . Then

$$\log B = \tilde{O}(f\sqrt{|D|}).$$

Another approach is to compute $H_{f^2D} \bmod p$ for many “small” primes p and then recover H_{f^2D} using the Chinese remainder theorem. Before discussing this CRT-based approach, we must further develop some characteristic p theory.

6. ORDINARY ELLIPTIC CURVES

Let E/\mathbb{F}_q be an elliptic curve with $q = p^r$.

Theorem 20. *The ring $\text{End } E$ is isomorphic to either an order in an imaginary quadratic field or to a maximal order in the quaternion \mathbb{Q} -algebra ramified precisely at p and ∞ .*

Definition 21. If $\text{End } E$ is isomorphic to an order in an imaginary quadratic field, we say E is *ordinary*. If $\text{End } E$ is isomorphic to an order in a quaternion algebra, we say E is *supersingular*.

The ring \mathcal{O}_{f^2D} is endowed with an involution given by the action of the nontrivial element of $\text{Gal}(K_D/\mathbb{Q})$. Similarly, a maximal order in a quaternion algebra has a canonical involution. The endomorphism ring of an elliptic curve also has a canonical involution which matches with the above under the identifications of Theorem 20. If $\alpha : E \rightarrow E$ is an endomorphism, then there is canonical *dual isogeny* $\bar{\alpha} : E \rightarrow E$ such that

- $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ and $\overline{\bar{\alpha}} = \alpha$;
- $\bar{\alpha} = \alpha$ if and only if $\alpha \in \mathbb{Z}$
- $\deg \alpha = \alpha\bar{\alpha}$;

The fact that $\text{End } E$ is a *involutive algebra* is crucial for the proof of Theorem 20, which has two steps. First one shows that $\text{End } E$ is an integral domain, free over \mathbb{Z} of rank at most 4. One then shows that the only involutive integral domains of at most 4 are \mathbb{Z} , orders in imaginary quadratic fields, and orders in quaternion \mathbb{Q} -algebras.

We will frequently make use of the fact that if E is ordinary, then any choice of ring isomorphism $\text{End } E \cong \mathcal{O}_{f^2D}$ (there are always two choices) respects involutions. In particular, if $\alpha \in \text{End } E$ corresponds to the element $u + vf\sqrt{D}$ with $u, v \in \mathbb{Q}$, then $\text{tr } \alpha := \alpha + \bar{\alpha} = 2u$.

Ordinariness and supersingularity can be characterized using the p -torsion subgroup of E :

Proposition 22. *If $n \geq 1$, then*

$$E[p^n](\overline{\mathbb{F}}_p) \cong \begin{cases} \mathbb{Z}/p^n\mathbb{Z}, & \text{if } E \text{ is ordinary;} \\ 0, & \text{if } E \text{ is supersingular.} \end{cases}$$

Proposition 23. *Suppose E is ordinary and that $\text{End } E = \mathcal{O}_{f^2D}$ with $p \nmid f$. Then*

- (1) p splits in \mathcal{O}_{f^2D} , i.e., $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ where \mathfrak{p} and \mathfrak{p}' are ideals of \mathcal{O}_{f^2D} of norm p .
- (2) $\varphi\mathcal{O}_{f^2D} = \mathfrak{p}^r$ or \mathfrak{p}'^r , where φ is q -th power Frobenius endomorphism of E .
- (3) There are integers u, v such that $4q = u^2 + v^2f^2|D|$.
- (4) $|E(\mathbb{F}_q)| = q + 1 \pm u$.

Proof. Letting the endomorphism ring \mathcal{O}_{f^2D} of E act on $E[p]$, we obtain a homomorphism

$$\mathcal{O}_{f^2D} \rightarrow \text{End } E[p] = \text{End } \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}.$$

Since \mathcal{O}_{f^2D} admits a (necessarily surjective) homomorphism to $\mathbb{Z}/p\mathbb{Z}$, we see the ring \mathcal{O}_{f^2D} has an ideal of norm p . Therefore, \mathfrak{p} is either split or ramified in \mathcal{O}_{f^2D} . Suppose that p ramifies in \mathcal{O}_{f^2D} , i.e., $p\mathcal{O} = \mathfrak{p}^2$. Since φ has norm $q = p^r$, we must have $\varphi = \mathfrak{p}^r$. Therefore, $p^r = \alpha\varphi^2$ for some $\alpha \in \mathcal{O}_{f^2D}^\times$. But, treating p^r and $\alpha\varphi^2$ as endomorphisms of E , we obtain the nonsensical chain of equalities:

$$0 = \ker \alpha\varphi^2 = \ker p^r = \mathbb{Z}/p^r\mathbb{Z}.$$

Therefore, p must split in \mathcal{O}_{f^2D} .

To prove (2), we note first that φ is an element of \mathcal{O}_{f^2D} of norm $q = p^r$. Therefore, $\varphi \mathcal{O}_{f^2D} = \mathfrak{p}^s \mathfrak{p}'^t$, where $r = s + t$. If $s > 0$ and $t > 0$, then $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ divides φ . Therefore, $\varphi = \psi p$ for some $\psi \in \mathcal{O}_{f^2D}$, implying

$$0 = \ker \varphi = \ker \psi p \supset \ker p = \mathbb{Z}/p\mathbb{Z},$$

a contradiction. Therefore, (2) must hold.

To prove (3), suppose first that $D \equiv 0 \pmod{4}$. Then $d := D/4f^2$ is squarefree and $\mathcal{O}_{f^2D} = \mathbb{Z}[f\sqrt{d}]$. Thus, we may write $\varphi = u' + vf\sqrt{d}$. Setting $u = 2u'$, we have $2\varphi = u + vf\sqrt{d}$. Taking norms, we obtain the relation $4q = u^2 + v^2 f^2 |D|$. (4) follows from (3) upon observing that $\text{tr } \varphi = 2u' = u$. The analysis in the case $D \equiv 1 \pmod{4}$ is similar. \square

Corollary 24. *Let E/\mathbb{F}_q be an ordinary elliptic curve such that $\text{End } E = \mathcal{O}_{f^2D}$ with $p \nmid f$ and $\mathcal{O}_D = \{\pm 1\}$ ($\Leftrightarrow D \neq -3, -4$). Let E'/\mathbb{F}_q be an elliptic curve such that such that $j(E') = j(E)$ and $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. Then E and E' are isomorphic over \mathbb{F}_q .*

Proof. Since E has no extra automorphisms, there are two \mathbb{F}_q -isomorphism classes of elliptic curves with j -invariant equal to $j(E)$ — that of E and that of its twist E^{tw} . The traces of Frobenius a and a^{tw} of E and E^{tw} , respectively, are related by $a^{\text{tw}} = -a$. Since E is ordinary, $a \neq 0$. Therefore, E and E' are isomorphic over \mathbb{F}_q if and only if their j -invariants and traces of Frobenius match. \square

7. REDUCTIONS OF CM ELLIPTIC CURVES AND HILBERT CLASS POLYNOMIALS MOD p

Let E/\mathbb{C} be an elliptic curve with CM by \mathcal{O}_{f^2D} . Then E may be defined over $K_D(f)$. Let $p \nmid f$ be a rational prime and let \mathfrak{P} be a prime of $K_D(f)$ above p with residue field \mathbb{F}_q , $q = p^r$. Suppose that E has good reduction at \mathfrak{P} and let \tilde{E}/\mathbb{F}_q be the corresponding reduction.

Proposition 25. *The elliptic curve \tilde{E}/\mathbb{F}_q is ordinary if and only if p splits in K_D .*

Proof. Suppose \tilde{E} is ordinary. It is a general fact that the natural map is injective. Together with the ordinarity of E , this fact implies that $\text{End } E = \mathcal{O}_{f^2D}$ for some conductor $f > 0$. By part (1) of Proposition 23, p splits in K_D . If \tilde{E} is supersingular, then $\text{End } \tilde{E} \cong R_{p,\infty}$, where $R_{p,\infty}$ is a maximal order in a quaternion \mathbb{Q} -algebra $B_{p,\infty}$ ramified at p and ∞ . Since the natural map $\text{End } E \rightarrow \text{End } \tilde{E}$ is injective, we obtain an embedding $K_D \hookrightarrow B_{p,\infty}$. It is a general fact a quadratic field K embeds into a quaternion algebra B if and only if every prime at B ramifies is inert in B . Therefore, p is inert in K_D . \square

It is a remarkable fact that every ordinary elliptic curve arises in this way:

Theorem 26 (Deuring). *Let \tilde{E} be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$ with $\text{End } \tilde{E} = \mathcal{O}_{f^2D}$ with $p \nmid f$. Then \tilde{E} lifts to a CM elliptic curve $E/\overline{\mathbb{Q}}$ with $\text{End } E = \mathcal{O}_{f^2D}$. If E' is another such lift, then $j(E) = j(E')$.*

Letting

$$\overline{J}_{f^2D} = \{j(E) : E/\overline{\mathbb{F}}_p \text{ ordinary with } \text{End } E = \mathcal{O}_{f^2D}\},$$

we obtain the following:

Corollary 27. $\overline{J}_{f^2D} = \{\overline{j} : j \in J_D\}$.

Corollary 28. *Let p be a prime which splits in K_D .*

$$H_{f^2D}(x) \equiv \prod_{\bar{j} \in \bar{J}_{f^2D}} (x - \bar{j}) \pmod{p}$$

Let p be a prime which splits in K_D . To compute $H_{f^2D} \pmod{p}$, it suffices to compute the set \bar{J}_{f^2D} . If $p > 3$ is small, this may be accomplished as follows. For computational purposes, it is convenient to restrict to primes $p \nmid f$ which split in K_D into principal ideals or, equivalently, to primes p such that $4p$ may be written in the form $u^2 + v^2 f^2 |D|$ for integers u, v . This is convenient as, in this case, $\bar{J}_D \subset \mathbb{F}_p$. Since p is small, it is feasible to loop over $j \in \mathbb{F}_p$, checking the membership $j \in \bar{J}_D$ at each step. To check whether j belongs to \bar{J}_D , we consider representative a curve E/\mathbb{F}_p defined over with j -invariant j :

$$E_j : y^2 = x^3 + 3 \frac{j}{1728 - j} x + 2 \frac{j}{1728 - j}.$$

A necessary condition for j to be in \bar{J}_{f^2D} is that $|E(\mathbb{F}_p)| = p + 1 \pm u$. This could be checked by point-counting. In practice, however, it is more efficient to randomly generate points $P \in E(\mathbb{F}_p)$ and check the identity $(p + 1)P = \pm uP$. It follows from the representability of $4p$ in the form $u^2 + v^2 f^2 |D|$ that $\text{End } E \supset \mathcal{O}_{v^2 f^2 D}$. There are efficient ‘‘volcanic’’ algorithms (Kohel, Sutherland, Bisson, ...) to compute a curve E'/\mathbb{F}_p isogenous to E with endomorphism ring \mathcal{O}_{f^2D} . As isogenous curves necessarily have the same trace¹, $j(E') \in \bar{J}_{f^2D}$. According to an analysis by Agashe, Lauter and Venkatesan, to recover H_{f^2D} , one must compute $H_{f^2D} \pmod{p}$ for $\tilde{O}(f\sqrt{D})$ values of p whose sizes are $\tilde{O}(f^2D)$.

This can all be turned around to construct elliptic curves with a known number of points. Suppose now that we know H_{f^2D} . Let $p \nmid f$ be a *big* prime such that p splits into principal ideals in \mathcal{O}_{f^2D} . Thus, we may find integers u and v such that $4p = u^2 + v^2 |D|$. Then H_{f^2D} factors completely over \mathbb{F}_p ; let j be one of its roots. Let E_j be an elliptic curve over \mathbb{F}_p with j -invariant j and let E_j^{tw} be its twist. Then by part (4) of Proposition 23,

$$\{|E_j(\mathbb{F}_p)|, |E_j^{\text{tw}}(\mathbb{F}_p)|\} = \{p + 1 \pm u\}.$$

UNIVERSITY OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, AB, T2N 1N4, CANADA
E-mail address: mgreenbe@ucalgary.ca

¹This can be seen from the following facts: (1) If $\alpha : E_1 \rightarrow E_2$ is a nonzero isogeny and $\ell \nmid \deg \alpha$, then α induces an isomorphism between the ℓ -adic Tate modules of E_1 and E_2 ; (2) The trace of E is the trace of the Frobenius endomorphism of E acting on $T_\ell E$.