COMPLEX MULTIPLICATION AND REDUCTION AT AN INERT PRIME

Prerequisites. Chapter 12, *Complex tori, theta functions and periods*, Section 12.1: the Weierstrass functions, Problems 12.1.6 and 12.1.7, and the lemniscatic lattice $\varpi\mathbb{Z}[\mathrm{i}]$ of the curve $E\colon y^2 = x^3 - x$. Orders in imaginary quadratic fields. Elliptic curves over a field at the level of [Si1, Ch. III], and the statements, not the proofs, of [Si1, Ch. IV, §§V.1–V.4, Ch. VI].

14.1. Complex multiplication

Which tori have endomorphisms other than $u \mapsto nu$? Every holomorphic map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ that fixes 0 is $u \mapsto \alpha u$ with $\alpha\Lambda \subseteq \Lambda$ [Si1, Thm. VI.4.1]. So if E corresponds to Λ, then $\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$, and we write $[\alpha]$ for $u \mapsto \alpha u$.

Problem 14.1.1. If $\mathrm{End}(E) \neq \mathbb{Z}$, then $K := \mathbb{Q}(\alpha)$ is imaginary quadratic for every $\alpha \in \mathrm{End}(E) \smallsetminus \mathbb{Z}$, $\mathrm{End}(E)$ is an order in K, and Λ is homothetic to a lattice contained in K.

We then say that E has *complex multiplication* by that order.

Problem 14.1.2. $\mathrm{End}(\mathbb{C}/\mathbb{Z}[\mathrm{i}]) = \mathbb{Z}[\mathrm{i}]$, $\mathrm{End}(\mathbb{C}/\mathbb{Z}[2\mathrm{i}]) = \mathbb{Z}[2\mathrm{i}]$, and $\mathrm{End}(\mathbb{C}/\mathbb{Z}[\rho]) = \mathbb{Z}[\rho]$ with $\rho = e^{2\pi\mathrm{i}/3}$.

Problem 14.1.3. For $\alpha \in \mathrm{End}(E)$, $\alpha \neq 0$, the kernel of $[\alpha]$ on $\mathbb{C}/\Lambda$ has $|\alpha|^2$ elements.

The function $\wp(\alpha u)$ is even and elliptic for Λ, so it is a rational function of $\wp(u)$, and $[\alpha]$ is a rational map of the curve.

Problem 14.1.4. For the lemniscatic lattice, $\wp((1+\mathrm{i})u) = \dfrac{\wp(u)^2 - 1}{2\mathrm{i}\,\wp(u)}$.

Problem 14.1.5. On $E\colon y^2 = x^3 - x$, $[\mathrm{i}](x, y) = (-x, \mathrm{i}y)$. For every $\alpha \in \mathrm{End}(E)$, $[\alpha]^*(dx/2y) = \alpha\, dx/2y$.

Problem 14.1.6. For $a, b \in \mathbb{C}^\times$, the curve $y^2 = x^3 + ax$ has complex multiplication by $\mathbb{Z}[\mathrm{i}]$, and $y^2 = x^3 + b$ has complex multiplication by $\mathbb{Z}[\rho]$.

The endomorphisms of $E\colon y^2 = x^3 - x$ have coefficients in $\mathbb{Z}[\mathrm{i}, \frac{1}{2}]$, so they can be reduced modulo an odd prime p. What do they look like near the origin? There an endomorphism is a power series in a local parameter, and this is the formal group.

14.2. The formal group

Let E be given by a Weierstrass equation over a ring R, and let $z := -x/y$. The group law, written in z, is a formal group law $F(z_1, z_2) \in R[[z_1, z_2]]$, and every endomorphism defined over R becomes a series $[\alpha](z) \in R[[z]]$ [Si1, §§IV.1–IV.2]. The invariant differential becomes $\omega(z) = \sum_{n\geq 1} c_n z^{n-1}\, dz$ with $c_1 = 1$ and

Date: November 24, 2026.

c_n integral over the coefficients, and the *logarithm* $\ell(z) := \sum_{n\ge1} c_n z^n/n$ satisfies $F(z_1,z_2) = \ell^{-1}(\ell(z_1)+\ell(z_2))$ [Si1, §§IV.4–IV.5]. Over $\mathbb{C}$, $\ell(z(u)) = u$. The *invariant derivation* is $D := d/du = \ell'(z)^{-1}\,d/dz$.

For a one-parameter formal group over $\mathbb{Z}_p$, either $[p](z) \equiv 0 \pmod p$ or $[p](z) \equiv g(z^{p^h}) \pmod p$ with $g'(0) \not\equiv 0$; the integer h is the *height* [Si1, §IV.7]. For an elliptic curve with good reduction at p, $h \in \{1,2\}$, and $h = 2$ exactly when the reduction is supersingular [Si1, Thm. V.3.1]. The two extreme models are $\hat G_a(X,Y) = X+Y$ and $\hat G_m(X,Y) = X+Y+XY$.

Problem 14.2.1. For $\hat G_m$, $\ell(X) = \log(1+X)$, $[p](X) \equiv X^p \pmod p$, and the height is 1.

Problem 14.2.2. As operators on $\mathbb{Z}_p[[X]]$ modulo p: for $\hat G_a$, $D^p \equiv 0$; for $\hat G_m$, $D = (1+X)\,d/dX$ and $D^p \equiv D$.

For any formal group over $\mathbb{Z}_p$ one has $D^p \equiv \lambda D \pmod p$ for a constant λ; Problems 16.3.1 and 16.3.2 of Chapter 16 prove this for the lemniscate, and their proofs apply to any formal group. Which constant is λ?

Problem 14.2.3. Let $\hat G$ be the formal group of a Weierstrass equation over $\mathbb{Z}_{(p)}$, with $D^p \equiv \lambda D \pmod p$. Then $(D^n z)(0) = n!\,[u^n]\,\ell^{-1}(u)$ for every n, and $\lambda \equiv c_p \pmod p$.

Problem 14.2.4. For $\hat G$ as in Problem 14.2.3, the coefficient of z^p in $[p](z)$ is congruent to c_p modulo p. Hence the height is 1 exactly when $p \nmid c_p$.

Now we compute c_n for $E\colon y^2 = x^3 - x$. Let $w := -1/y$.

Problem 14.2.5. For $y^2 = x^3 - x$, $w + zw^2 = z^3$, and $\omega(z) = dz/\sqrt{1+4z^4}$.

Problem 14.2.6. For $y^2 = x^3 - x$, $\ell(z) = \sum_{m\ge0} (-1)^m \binom{2m}{m} z^{4m+1}/(4m+1)$. For odd n, c_n is the coefficient of x^{n-1} in $(x^3-x)^{(n-1)/2}$.

For a curve $y^2 = f(x)$ over $\mathbb{F}_p$ with f cubic, the coefficient A_p of x^{p-1} in $f^{(p-1)/2}$ is the *Hasse invariant*, and the curve is supersingular exactly when $A_p = 0$ [Si1, Thm. V.4.1(a)]. By Problem 14.2.6, $c_p = A_p$ for $y^2 = x^3 - x$, and Problems 14.2.3 and 14.2.4 recover the criterion for this curve. When $c_p = 0$, the first term of $[p](z)$ modulo p lies beyond z^p. To find it one needs the Frobenius endomorphism.

14.3. Reduction at an inert prime

Which primes are supersingular for a curve with complex multiplication? Deuring's answer [Deu]: if E has complex multiplication by an order in K and good reduction at a prime above p, the reduction is supersingular if and only if p does not split in K. For $y^2 = x^3 - x$ these are the $p \equiv 3 \pmod 4$. We check this by hand.

Problem 14.3.1. Let $p \equiv 3 \pmod 4$. Then $\#E(\mathbb{F}_p) = p+1$, that is, $a_p := p + 1 - \#E(\mathbb{F}_p) = 0$.

Problem 14.3.2. For $p = 4m+1$, $A_p = (-1)^m \binom{2m}{m} \not\equiv 0 \pmod p$. For $p \equiv 3 \pmod 4$, $A_p = 0$.

For $p \equiv 1 \pmod 4$ one has $a_p = \gamma + \bar\gamma$, where $\gamma \in \mathbb{Z}[\mathrm{i}]$ has $\gamma\bar\gamma = p$ and $\gamma \equiv 1 \pmod{2+2\mathrm{i}}$ [IR, Ch. 18].

Problem 14.3.3. $a_5 = -2$ and $a_{13} = 6$, in agreement with $\gamma = -1 + 2\mathrm{i}$ and $\gamma = 3 + 2\mathrm{i}$.

Now let $p \equiv 3 \pmod 4$, let $\phi(x, y) := (x^p, y^p)$ be the Frobenius endomorphism of E over $\mathbb{F}_p$, and reduce [i] modulo p into $\mathbb{F}_{p^2}$.

Problem 14.3.4. $\phi^2 = [-p]$ and $\phi \circ [\mathrm{i}] = [-\mathrm{i}] \circ \phi$. Hence $\mathrm{End}(E_{\mathbb{F}_p})$ is not commutative.

Problem 14.3.5. Let $p \equiv 3 \pmod 4$. In the parameter $z = -x/y$, $[p](z) \equiv -z^{p^2} \pmod p$, and $[\mathrm{i}](z) = \mathrm{i}z$.

For instance $[3](z) \equiv -z^9 \pmod 3$. So modulo p the multiplication by $-p$ is exactly the p^2-power map. This is the situation of Lubin and Tate [LT]. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, with uniformizer π and residue field of order q. Lubin and Tate prove: (i) each $f \in \mathcal{O}[[X]]$ with $f(X) \equiv \pi X \bmod X^2$ and $f(X) \equiv X^q \bmod \pi$ is an endomorphism of a unique formal group F_f over $\mathcal{O}$; (ii) each $a \in \mathcal{O}$ gives a unique endomorphism $[a]_f$ of F_f with linear term aX, and $a \mapsto [a]_f$ is a ring homomorphism; (iii) for two such f, g there is a unique isomorphism $\theta\colon F_f \to F_g$ over $\mathcal{O}$ with linear term X, and it commutes with the $[a]$. By Hazewinkel's functional-equation lemma [Ha, I.2.2], the *model logarithm* $\ell_\pi(X) := X + X^q/\pi + X^{q^2}/\pi^2 + \cdots$ is the logarithm of such an F_f.

Let $p \equiv 3 \pmod 4$ and $\mathcal{O} := \mathbb{Z}_p[\mathrm{i}]$, so that $\pi := -p$ is a uniformizer and $q = p^2$.

Problem 14.3.6. The series $f := [-p]$ satisfies the hypotheses of (i), the formal group $\hat{E}$ of $y^2 = x^3 - x$ is F_f, and $[a]_f$ extends $\alpha \mapsto [\alpha]$ from $\mathbb{Z}[\mathrm{i}]$ to $\mathcal{O}$.

Problem 14.3.7. There is $\theta \in z + z^2\mathcal{O}[[z]]$ with $\ell = \ell_{-p} \circ \theta$. Consequently the coefficients of ℓ in degrees less than p^2 are p-integral, and $p \cdot [z^{p^2}]\,\ell \equiv -1 \pmod p$.

For $p = 3$: $[z^9]\,\ell = \frac{2}{3}$, and $3 \cdot \frac{2}{3} \equiv -1 \pmod 3$. Chapter 16 proves the same congruence for the lemniscate with binomial coefficients (Problem 16.4.2).

In the model logarithm the denominators occur only in the degrees $q, q^2, \ldots$, and there they are $p, p^2, \ldots$. Divisibility of derivatives at inert primes comes from this sparseness. The functions whose derivatives one needs are not functions on E, however; they are theta functions. Chapter 15 uses D^p in a single determinant; theta functions are the subject of Chapters 16 and 17.

Hints

§14.1.

14.1.1: Write $\alpha\omega_1 = a\omega_1 + b\omega_2$ and $\alpha\omega_2 = c\omega_1 + d\omega_2$ with integers a, b, c, d. Then α is a root of $x^2 - (a + d)x + ad - bc$. If $\alpha \notin \mathbb{R}$, then $\omega_2/\omega_1 \in \mathbb{Q}(\alpha)$; if $\alpha \in \mathbb{R}$, then $b = c = 0$.

14.1.2: $\alpha \cdot 1 \in \Lambda$.

14.1.3: The kernel is $\alpha^{-1}\Lambda/\Lambda$. Its order is the index of $\alpha\Lambda$ in Λ, a determinant.

14.1.4: Apply Problem 12.1.6 with $v = \mathrm{i}u$, using Problem 12.1.7 and $\wp'^2 = 4\wp^3 - 4\wp$.

14.1.5: $x = \wp(u)$ and $y = \wp'(u)/2$.

14.1.6: Find automorphisms of the curves of order 4 and 3.

§14.2.

14.2.1: $[p](X) = (1+X)^p - 1$.

14.2.2: $D(1+X)^k = k(1+X)^k$. For $\hat{G}_a$, $(d/dX)^p X^n = n(n-1)\cdots(n-p+1)X^{n-p}$.

14.2.3: $D = d/du$ in the coordinate $u = \ell(z)$. For λ, apply $D^p \equiv \lambda D$ to the truncated logarithm $u_p := \sum_{n<p} c_n z^n/n$, for which $Du_p = 1 - c_p z^{p-1} + O(z^p)$; evaluate at 0 and use $(p-1)! \equiv -1$.

14.2.4: Compare $\ell([p](z)) = p\,\ell(z)$ modulo (p, z^{p+1}).

14.2.5: Substitute $x = z/w$ and $y = -1/w$. Solve the quadratic for w, and compute $dx/2y = -\frac{z}{2}\,d\log x$.

14.2.6: The binomial series of $(1+4z^4)^{-1/2}$. For the second statement, $(x^3 - x)^{2m} = x^{2m}(x^2-1)^{2m}$.

§14.3.

14.3.1: $x^3 - x$ is odd, and -1 is not a square modulo p.

14.3.2: Problem 14.2.6. For the non-vanishing, $2m < p$.

14.3.3: Count the solutions of $y^2 = x^3 - x$ over $\mathbb{F}_5$ and $\mathbb{F}_{13}$.

14.3.4: $\phi^2 - a_p\phi + p = 0$ in $\mathrm{End}(E)$ [Si1, §V.2], and Problem 14.3.1. For the second relation, $\mathrm{i}^p = -\mathrm{i}$ in $\mathbb{F}_{p^2}$.

14.3.5: In the parameter z, ϕ acts on the formal group over $\mathbb{F}_p$ by $z \mapsto z^p$, and $[-1](z) = -z$.

14.3.6: Problem 14.3.5. For the last statement, use the uniqueness in (ii).

14.3.7: Use (iii). A formal group over a $\mathbb{Q}$-algebra has only one logarithm with linear term z. For the consequence, expand $\ell_{-p}(\theta(z))$ up to degree q.

References

[Deu] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[Ha] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[LT] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.