Complex Multiplication: Part 2

July 13, 2009

In this part we will prove that the j-invariant of a CM elliptic curve is an algebraic integer, and prepare for the proof that these algebraic integers generate certain class fields of K. Recall that the j-invariant is an invariant function for the group $\Gamma = SL_2(Z)$ which is holomorphic on the upper half plane and has a Fourier expansion $q^{-1} + \dots$ at infinity.

1 The modular equation

Let n be a positive integer, and let Δ_n^* denote the set of integral 2×2 matrices with determinant n and entries with no common factor. Then one has the following elementary result:

Proposition 1 (Exercise, using the elementary divisor theorem) *We have the decomposition* $\Delta_n^* = \Gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \Gamma$ *and* $\Delta_n^* = \bigcup \Gamma \alpha_i$ *where* α_i *runs over matrices of the form*

$$\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $0 < a, 0 \le b < d$*, and* $ad = n$*.*

Lemma 2 *Suppose f is a holomorphic function on the upper half plane which is invariant under the action of Γ by fractional linear transformations and which is meromorphic at infinity. Then f is a polynomial in the function $j(z)$, with coefficients in the $\mathbf{Z}$-module generated by the Fourier coefficients of f.*

Proof. Let us write $f = c_{-m}q^{-m} + \dots$. Then $f - c_{-m}j^m$ has the properties in the statement of the theorem, and has a pole of order at most $m-1$ at infinity. Repeating this process, we find a polynomial P in j with coefficients that are linear combinations of the coefficients of f such that $f - P(j)$ vanishes at infinity and is holomorphic on the upper half plane. It follows that $f - P(j)$ is identically zero, which proves our assertion.

Now let n be a positive integer and let α_i be representatives for the right cosets of Δ_n^* as in the proposition above. Consider the formal product

$$\Phi_n(X) = \prod(X - j \circ \alpha_i).$$

This is a polynomial in the variable X with coefficients that are holomorphic functions on the upper half plane.

Lemma 3 *The coefficients of $\Phi_n(X)$ are invariant under the action of Γ. They are meromorphic at infinity and holomorphic on the upper half plane.*

Proof. By definition, the coefficients of Φ_n are elementary symmetric functions of the $j \circ \alpha_i$. Since the action of Γ permutes the cosets $\Gamma\alpha_i$ in Δ_n^*, the first assertion follows. It is clear that each function $j \circ \alpha_i$ is holomorphic on the upper half plane since j is so, and the meromorphy at infinity comes from the explicit formula for $\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, which shows in fact that $j \circ \alpha_i$ has a Laurent expansion in $q^{1/d}$ (and that it has coefficients in $\mathbf{Q}(\zeta_d)$).

Corollary 4 *The coefficients of $\Phi_n(X)$ are polynomials in j with coefficients lying in $\mathbf{Z}$. Thus we may write $\Phi_n(X) = \Phi_n(X, j) \in \mathbf{Z}[X, j]$.*

Proof. It is clear that the coefficients of $\Phi_n(X)$ are polynomials in j of degree dividing n with coefficients lying in the cyclotomic field $\mathbf{Q}(\zeta_n)$. Thus we may view the coefficients of Φ_n as elements of the Laurent series field $\mathbf{Q}(\zeta_n)((q))$. One checks that the automorphisms of $\mathbf{Q}(\zeta_n)$ acting on the roots of unity permute the power series expansions of the functions $j \circ \alpha_i$, and this shows in fact that these power series, being expansions of functions symmetric in the $j \circ \alpha_i$, in fact have coefficients in $\mathbf{Q}$. That these coefficients are integral follows from the fact that the coefficients of the functions j and $j \circ \alpha_i$ are so.

Theorem 5 *The polynomial $\Phi_n(X, j)$ is irreducible over $\mathbf{C}(j)$, is symmetric in X and j, and if n is not a perfect square, then $\Phi_n(j, j)$ is a polynomial in j of degree greater than 1 and has leading coefficient ± 1.*

Proof. The first assertion follows from the fact that Γ permutes the functions $j \circ \alpha_i$ transitively.

As for the symmetry, observe that $j(z/n)$ is a root of $\Phi_n(X, j)$, since one of the matrices α_i is equal to $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, so that $\Phi_n(j(z/n), j(z))$ is identically zero. It follows then that $\Phi(j(z), j(nz))$ is identically zero as well. Thus $j(nz)$ is a root of the polynomial $\Phi_n(j, X)$. On the other hand, taking $\alpha_i = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ shows that $j(nz)$ is also a root of $\Phi_n(X, j)$. Since $\Phi_n(X, j)$ is irreducible and has a common root with $\Phi_n(j, X)$ it follow that $\Phi_n(X, j)$ divides $\Phi_n(j, X)$. By Gauss' Lemma, we must have

$$\Phi_n(j, X) = g(j, X)\Phi_n(X, j)$$

in $\mathbf{Z}[j, X]$ and hence $\Phi_n(j, X) = g(j, X)g(X, j)\Phi_n(j, X)$. It follows that $g(j, X) = \pm 1$. If $g(j, X) = -1$ then we get $\Phi_n(j, j) = -\Phi_n(j, j) = 0$, which contradicts the fact that $\Phi_n(X, j)$is irreducible over $\mathbf{Z}[j]$. Thus $g = 1$ and we get the second statement.

To get the last part, assume that n is not a square, so that in the given form for the matrices α_i we have $a \neq d$. Then we have

$$j - j \circ \alpha_i = (\frac{1}{q} + \dots) - (\frac{1}{\zeta_d^b q^{a/d}})$$

and there is no cancellation in the leading terms of the two pieces. Thus the leading coefficient of the Laurent expansion is a root of unity, and the expansion for $\Phi_n(j, j)$ starts with $\frac{\pm 1}{q^m}$, since this leading coefficient is both an integer and a root of unity. Thus $\Phi_m(j, j)$ is a polynomial in j with leading coefficient ± 1 as claimed.

Lemma 6 (exercise) *If τ is an element of the upper half plane and E is the elliptic curve corresponding to the lattice $\mathbf{Z} + \mathbf{Z}\tau$, then the roots of $\Phi_n(X, j(\tau))$ are precisely the j-invariants of elliptic curves E' such that there exists a cyclic isogeny $E \to E'$ of degree n.*

We also have the following simple observation:

Lemma 7 (Exercise) *Let $\tau \in K$ and let E denote the elliptic curve corresponding to the lattice $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ as above. Then there exists an n such that there is a cyclic endomorphism $E \to E$ of degree n.*

Granting these facts for the moment, we can give the proof of the following basic result:

Theorem 8 *If τ is an element of an imaginary quadratic field, then $j(\tau)$ is an algebraic integer.*

Proof. Let $\tau \in K$ and E be as in the statement of the lemma above. Then we find that there exists a non-square n such that $j(\tau)$ satisfies the equation $\Phi_n(j(\tau), j(\tau))) = 0$. But $\Phi_n(X, X)$ is a polynomial with integer coefficients and leading coefficient ± 1, so the theorem follows.

2 Points of finite order on elliptic curves

Let $\Gamma = SL_2(\mathbf{Z})$ as before. Let $\Gamma(N)$ be the subgroup of Γ which is the kernel of reduction modulo N.

Lemma 1 (Exercise) *The reduction map $\Gamma \to SL_2(\mathbf{Z}/N\mathbf{Z})$ is surjective.*

Now let f be a meromorphic function on the upper half plane, invariant under $\Gamma(N)$. Let $q^{1/N} = e(2\pi i\tau/N)$ as usual; then we see in the usual way that f has a Fourier expansion in powers of $q^{1/N}$. We say that f is modular of level N if $f \circ \gamma$ has a finite-tailed Laurent expansion in $q^{1/N}$ at infinity for every $\gamma \in \Gamma$. We let F_N denote the field (over $\mathbf{C}$) of modular functions of level N. Then clearly there is an action of the finite group $\Gamma/\Gamma(N)$ on the field F_N where Γ acts by composition.

Theorem 2 (Exercise) *We have $F_1 = \mathbf{C}(j)$.*

A more interesting question is to determine generators of the field F_N. Let $a = (r, s)$ denote an element of $(\frac{1}{N}\mathbf{Z}/\mathbf{Z})^2$ and define the Fricke by

$$f_a(\tau) = -2^7 3^5 \frac{g_2(\tau) g_3(\tau)}{\Delta(\tau)} \mathcal{P}(r + s\tau; \tau). \tag{1}$$

Thus $f_a(\tau)$ is a normalized x-coordinate for the point $r + s\tau$ of order N in E_τ. It is clear that if $\gamma \in \Gamma$ then

$$f_{\gamma a}(\tau) = f_a(\tau) \circ \gamma.$$

This implies in particular that f_a is a modular function of level N (since the q-expansions of each f_a can be checked to be finite-tailed at infinity, using the results stated in Lecture 1). We note also that if Λ is an arbitrary lattice, then we can also define numbers

$$f_a(\Lambda)$$

where $\frac{1}{N}\Lambda/\Lambda$ by means of the formula above.

Theorem 3 *We have* $F_N = \mathbf{C}(j, f_a)$ *where* a *runs through the elements of* $(\frac{1}{N}\mathbf{Z}/\mathbf{Z})^2$.

Proof. Let L denote the field in the statement of the theorem. Then it is clear that $\Gamma/\pm\Gamma(N)$ acts as a group of automorphisms of $L/\mathbf{C}(j)$ (note ± 1 acts trivially since the $\mathcal{P}$-function is even). Furthermore, if γ in Γ acts trivially on L, then one checks that $\gamma \in \Gamma(N)$. Thus the Galois group of L over $\mathbf{C}(j)$ is $\Gamma/\pm\Gamma(N)$ and the result follows.

This corollary says that over $\mathbf{C}$, the generic elliptic curve with transcendental j has the property that the X-coordinates of its division points of order N generate an extension of $\mathbf{C}(j)$ with Galois group $SL_2(\mathbf{Z}/N\mathbf{Z})$. This is in sharp contrast with the case of CM curves, where (as we shall see) the values of the f_a at imaginary quadratic τ generate certain ray class fields. Actually, if $j(E)$ is algebraic and E is *not* a CM elliptic curve, then the field generated by the coordinates of the division points of E over the field of definition $j(E)$ is typically large, with Galois group containing $SL_2(\mathbf{Z}/N\mathbf{Z})$. However, this is not obvious!