Complex Multiplication: Part 3

July 15, 2009

Our present goal is to prove that the j-invariants of the elliptic curves of conductor 1 generate the Hilbert class field of K. More generally, we want to show that the invariants of the curves of conductor c generate the ring class field of conductor c.

1 Summary of the situation

Let us recall the basic set-up. We fix a positive integer c.

- There are $h = h_c$ non-isomorphic CM curves E_i of conductor c, where h_c is the class number of the order $R = R_c = \mathcal{O}_{K,c}$.
- The curves E_i may be decribed as $E_i \cong \mathbf{C}/\mathfrak{a}_i$ where $\mathfrak{a}_i$ runs over a set of representatives of the ideal classes of R.
- There is an action of the ideal class group $G = G_c$ of R on the set of isomorphism classes of curves of conductor c induced by multiplication of ideals: if $\mathfrak{b}$ in an ideal of R and $E_i = \mathbf{C}/\mathfrak{a}_i$ then $[\mathfrak{b}] \cdot E_i$ is the elliptic curve $\mathbf{C}/\mathfrak{a}_i\mathfrak{b}$, and one sees that this passes to equivalence classes of ideals $\mathfrak{b}$ and isomorphism classes of curves.
- The value of the j-invariant on each ideal class of R is an algebraic integer.

In view of the last two items above, and the identification of G with the Galois group $\mathrm{Gal}(K(c)/K)$, it seems reasonable to hope that the j-invariants of the E_i generate $K(c)$ and that the multiplication of ideals giving the action on curves goes over to the Galois action on j-invariants. This is what we shall prove below.

2 The key ingredient: Kronecker congruence

We first dispose of the case where $c = 1$, leaving the case of general c for the adelic formulation of our results, which will come later. Thus we take $R = \mathcal{O}_K$ and G to be the usual ideal class group of K.

Let p denote a rational prime number which is split in K. Let L/K denote the Galois closure of the field generated by the j-invariants $j(\mathfrak{a}_i)$. Let $\mathfrak{a} = \mathfrak{a}_i$ be fixed. Then if $\mathfrak{p}$ is a factor of p in K, consider the elliptic curve $\mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a}$. We will show that for all but finitely split primes p, we have

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{P}} \tag{1}$$

where $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in L. Observe that the statement above assumes the fact that the j-invariants in question are algebraic integers.

Let us assume this congruence for the moment.

Theorem 1 *The field L is the Hilbert class field of K.*

Proof. Let $\mathrm{Frob}(\mathfrak{P}) \in \mathrm{Gal}(L/K)$ denote the Frobenius automorphism of $\mathfrak{P}$. Then the congruence (1) may be restated as

$$\mathrm{Frob}(\mathfrak{P})(j(\mathfrak{a})) \equiv j(\mathfrak{p}^{-1}\mathfrak{a}) \pmod{\mathfrak{P}}.$$

Since there are only finitely many ideal classes $[a_i]$ and consequently only finitely many j-invariants $j(\mathfrak{a}_i)$ to consider, we may assume that p is relatively prime to the finitely many numbers obtained by taking differences of the conjugates of the $j(\mathfrak{a}_i)$. Then the the congruence above is in fact an equality:

$$\mathrm{Frob}(\mathfrak{P})(j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a}).$$

But now we are done, since this implies already that all the numbers $j(\mathfrak{a}_i)$ are conjugate over K. Indeed, we can find infinitely many split primes p in any ideal class of K, so that the set $\mathfrak{p}^{-1}\mathfrak{a}$ runs over all the ideal classes. Furthermore, $\mathrm{Frob}(\mathfrak{P})$ is trivial precisely when $\mathfrak{p}$ is principal, since $\mathfrak{p}^{-1}\mathfrak{a}$ is in the same ideal class as $\mathfrak{a}$ precisely for principal $\mathfrak{p}$. Thus the primes of degree 1 in K splitting in E are the ones which are principal. It follows that L is the Hilbert class field of K.

Corollary 2 *We have $H = K(j(\mathfrak{a}))$ for any ideal $\mathfrak{a}$ of K.*

3 Proof of the Kronecker congruence

The proof of the key congruence is not hard, although it is somewhat technical. Thus far we have been able to get away with viewing the curves E_i as being defined over **C**, but the free ride is over, and we have to deal with them as elliptic curves defined over number fields and wrestle with what reduction modulo a prime actually means.

For the purposes of this course, we will proceed formally, and assume that reduction modulo a prime works the way one would like, at least if we avoid a finite set of primes of bad reduction. We will state what we need, but we emphasize that the results we use all follow from a systematic development of Néron models.

So let us briefly state what is required. Let E_1 and E_2 denote elliptic curves over a number field L and let $\mathfrak{P}$ denote a prime of L. We assume that there exist Weierstrass models for E_i/L which have the property that the corresponding discriminants are prime to $\mathfrak{P}$. Let let R be the localization of the ring of integers of L at $\mathfrak{P}$, and let $\mathbf{F}$ denote the residue field of R at $\mathfrak{P}$. Then let $\overline{E}_i$ denote the elliptic curves over $\mathbf{F}$ defined by reducing the coefficients of the given equations of the E_i. Under our assumptions, the curves $\overline{E}_i$ are elliptic curves over $\mathbf{F}$.

The key property is the following. Let $A_i = H^0(E_i, \Omega^1)_L$ denote the 1-dimensional L-space of differentials on E_i. Then A_i is contravariantly functorial: if there is an isogeny $\mu : E_1 \to E_2$, then there is an induced map $A_2 \to A_1$. If $E_1 = E_2$ then there is an endomorphism $A \to A$, induced by multiplication by an element $a(\mu) \in L$, since A is a 1-dimensional space.

Similarly, let $\overline{A}_i = H^0(\overline{E}_i, \Omega^1)_{\overline{\mathbf{F}}_p}$ denote the corresponding object over $\mathbf{F}_p$. Then each $\overline{A}_i$ is a 1-dimensional space over $\overline{\mathbf{F}}_p$, and, if $\overline{\mu}$ is an isogeny $E_1 \to E_2$, then there is an induced map $\overline{A}_2 \to \overline{A}_1$.

The key property of good reduction that we need is the following.

Theorem 1 (See Silverman's book) *Let the hypotheses be as above. Then there exist rank 1 free R-modules $\mathbf{A}_i$ such that the following properties hold:*

- $A_i = \mathbf{A}_i \otimes L$
- $\overline{A}_i = \mathbf{A}_i \otimes R/\mathfrak{P}S$
- *If $\mu : E_1 \to E_2$ is an isogeny, then there is a canonical isogeny $\overline{\mu} : \overline{E}_1 \to \overline{E}_2$ called the reduction of μ, and there is a canonical map $\mathbf{A}_2 \to \mathbf{A}_1$ which is compatible via the above tensor product with the corresponding maps on A_i and $\overline{A}_i$.*

- *The degree of $\overline{\mu}$ is the same as the degree of μ.*

Corollary 2 *Suppose $E_1 = E_2$ and μ is an endomorphism of E. Then the induced map $H^0(E,\Omega^1)_L \to H^0(E,\Omega^1)_L$ is induced by multiplication by an element $a(\mu) \in S$. The endomorphism of $H^0(\overline{E},\Omega^1)_{\overline{\mathbf{F}}_p}$ induced by $\overline{\mu}$ is simply multiplication by the image of $a(\mu)$ in $S/\mathfrak{P}S$.*

With this in hand, we proceed as follows. For each ideal class $[\mathfrak{a}_i]$ of K, we pick a Weierstrass model of E_i over the Galois closure of the field generated by the $j(\mathfrak{a}_i)$ over K. We pick a split prime $\mathfrak{p}$ of K which is relatively prime to the following quantities:

- The differences of the conjugates of the $j(\mathfrak{a}_i)$

- The discriminants of the selected Weierstrass models of the E_i

- The discriminant of L.

Since $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$, we have a natural map

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a}.$$

Note that this map has degree p. Let $\mathfrak{b}$ denote an ideal of $\mathcal{O}_K$ such that $\mathfrak{p}\mathfrak{b} = (\alpha)$ is principal. We may assume that $\mathfrak{b}$ is prime to p. Then multiplication by α followed by the natural projection gives a map

$$\mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a} \to \mathbf{C}/\mathfrak{b}\mathfrak{a} \to \mathbf{C}/\mathfrak{a}.$$

The composite map

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a} \to \mathbf{C}/\mathfrak{b}\mathfrak{a} \to \mathbf{C}/\mathfrak{a} \tag{2}$$

is clearly induced by multiplication by α, as can be seen by tracing around the effect on $\mathbf{C}$. Furthermore, the first arrow above has degree p as was previously remarked, the second arrow is an isomorphism, and the third arrow has degree equal to the norm of $\mathfrak{b}$, which is prime to p.

We now want to reduce the endomorphism $[\alpha]$ modulo $\mathfrak{P}$, and we claim that the reduction of α is inseparable in characteristic p. We remark here that since α is contained in $K \subset L$, the endomorphism $[\alpha]$ is indeed defined over L.

Now note that over $\mathbf{C}$ we have that if ω is the differential dz on $E = \mathbf{C}/\Lambda$, then the pullback $[\alpha]^*\omega = \alpha\omega$. In other words, μ induces multiplication by α on the 1-dimensional complex vector space $H^0(E,\Omega^1)$ over $\mathbf{C}$. Thus $[\alpha]$ induces multiplication by α on $H^0(E,\Omega^1)_L$, so we see that in characteristic p, the reduction of $[\alpha]$ induces multiplication by $\overline{\alpha}$ on $H^0(E,\Omega^1)$ over $\overline{\mathbf{F}}_p$, and that this is zero, since α is divisible by $\mathfrak{p}$.

On the other hand, μ factors as a composite of two maps, one of degree p, and the other of degree prime to p. Enlarging the field L if neccesary, we may assume that each of these isogenies is defined over L. Since the reduction of the second map is separable, it follows that the the reduction of the former is purely inseparable and since it has degree p, it must be the Frobenius map raising to p-th powers, up to an automorphism of the reduced curve. Thus we get

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{P}}$$

as required. (Note that this conclusion is not affected by any possible extension of the field L effected for purposes of the proof above; the conclusion holds in any Galois extension of K containing the j-invariants in question.)

Corollary 3 (exercise) *The Hilbert class field of K is generated by $j(E)$ where E is any one elliptic curve of conductor* 1.

4 Points of order N

We now want to look at the field generated by adding the coordinates of points of order N together with the j-invariants. However, this will require a certain precision about the exact models we choose for our elliptic curves, which we have thus far been able to avoid. So let E be an elliptic curve over $\mathbf{C}$ with $E \cong \mathbf{C}/\Lambda$ for some Λ. As we have seen above, the choice of Λ leads to a Weierstrass model for E:

$$E : Y^2 = 4X^3 - g_2(\Lambda)X - g_3.$$

At first glance, there is no particularly canonical choice of Λ.[1] Since the coordinates of points evidently depend on the model, we are led to seek an isomorphism invariant quantity. Let us define the Weber function h of E as follows. If $j(E) \neq 0, 1728$

$$h_E = -2^7 3^5 \frac{g_2 g_3}{\Delta} \cdot X.$$

[1] Actually, there is a canonical choice, but it comes from considerations which are not particularly useful here.

Here we view g_2 and g_3 as constants, and X as a rational function on E. Recall also that in terms of the complex analytic incarnation of E, the function X is just the Weierstrass $\mathcal{P}$ function. Thus, h is just a constant multiple of the $\mathcal{P}$-function, once the choice of Λ is fixed. Note also that h_E vanishes identically if $g_2 g_3 = 0$; this is excluded by our assumption that $j(E) \neq 0, 1728$, since there are the values of the j-invariant corresponding to $g_2 g_3 = 0$.

If $g_2 = 0$ we put

$$h_E = \frac{g_2^3}{\Delta} x^2$$

and if $j(E) = 1728$ we put

$$h_E = \frac{g_3}{\Delta} x^3.$$

Then in every case, h_E is a rational function on E. Observe also that the values of h_E at points of finite order coincide with the values of the Fricke functions f_a defined previously.

Proposition 1 (exercise) *The Weber function gives a rational function $E \to \mathbf{P}^1$. If u and u' are points on E, we have $h_E(u) = h_E(u')$ if and only if there is an automorphism σ of E such that $\sigma(u) = u'$.*

The starting point is the following observation. We know from the foregoing considerations that the canonical projection $E = \mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a} = E^\sigma$ for $\sigma = \mathrm{Frob}(\mathfrak{p})$ reduces to a purely inseparable map of degree p in characteristic p. Such a map is equal to Frobenius, at least up to an automorphism of $\overline{E^\sigma}$.

Lemma 2 (exercise) *We may compose the natural map $E = \mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a} = E^\sigma$ with an automorphism of E^σ so that the deduced map $E \to E^\sigma$ reduces precisely to the Frobenius map.*

Theorem 3 *Let E be a CM elliptic curve of conductor 1. Then the field L generated over K by $j(\mathfrak{a})$ and the numbers $h_E(u)$ for u running over the points of order N in E is the ray class field of conductor N.*

Proof. We will show that a degree 1 prime of K splits completely in L if and only if it is principal, generated by an element congruent to 1 modulo N. Thus suppose $\mathfrak{p} = (\alpha)$ is such a prime and $\alpha \equiv 1 \pmod{N}$. We assume again that $\mathfrak{p}$ is away from a finite set of bad primes. Then let $\mathfrak{a}$ denote and ideal of K and consider the map

$$\mu : E = \mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a} = E^\sigma$$

where $\sigma = \mathrm{Frob}(\mathfrak{P})$ for a prime $\mathfrak{P}$ above $\mathfrak{p}$. Since α is principal, the previous results on the Hilbert class field show that in fact $E^{\sigma} = E$.

Using the lemma above, we can assume that the reduction of μ is the Frobenius endomorphism. Now if u is a point of order N on E, then u^{σ} is a point of order N on E^{σ} and u^{σ} reduces to $\mathrm{Frob}(\overline{u})$ on the reduced curve $\mathrm{Frob}(\overline{E})$. Thus $\mu(u)$ and u^{σ} reduce to the same point modulo $\mathfrak{P}$, so that $\mu(u) = \sigma(u)$ for each point of order N.

Then consider the composite

$$\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\alpha^{-1}\mathfrak{a} \to \mathbf{C}/\mathfrak{a}$$

where the second arrow is induced by multiplication by α. The composite is the endomorphism of $\mathbf{C}/\mathfrak{a}$ induced by multiplication by α. Under our hypothesis on α, this endomorphism acts as the identity on the points of order N. Furthermore, as endomorphisms of E, the multiplication-by-α map and the the map μ are equal up to an automorphism (multiplication by a root of unity in $\mathcal{O}_K^{\times}$). Since the numbers $h_E(u)$ are invariant under automorphisms, it follows that σ acts as the identity on each $h_E(u)$, which shows that $\mathrm{Frob}(\mathfrak{P})$ is trivial on L, so $\mathfrak{p}$ splits completely.

As for the converse, suppose $\mathfrak{p}$ is a prime that has trivial Frobenius in L. Then in particular $\mathrm{Frob}(\mathfrak{P})$ is trivial in the $K(j(\mathfrak{a}))$ which is the Hilbert class field, so $\mathfrak{p} = (\alpha)$ is principal, and, with notation as above, $E^{\sigma} = E$ for $E = \mathbf{C}/\mathfrak{a}$ and $E^{\sigma} = \mathbf{C}/\mathfrak{p}^{-1}\mathfrak{a}$. Then if u is a point of order N corresponding to to $u \in K/\mathfrak{a}$, we have $h_E(u)^{\sigma} = h_E(u)$ since σ is trivial on L. Furthermore, we can argue as in the previous case to see that the multiplication-by-α endomorphism acts via σ on the points of order N. But now $h_E^{\sigma} = h_E$ since h_E is defined over $K(j(E))$ whence we get $(h_E(u))^{\sigma} = h_E^{\sigma}(u^{\sigma}) = h_E(u^{\sigma}) = h_E(\alpha u)$. It follows that $h_E(u) = h_E(\alpha u)$ for each u, so that u and αu differ by an automorphism of E. Thus there exists a root of unity ϵ (perhaps dependent on u) such that $\alpha u = \epsilon u$. Changing the generator α by this root of unity we get $\alpha u = u$, and since $E[N]$ is principal as a module over $\mathcal{O}_K/N\mathcal{O}_K$, we find that the $\alpha u = u$ for all u in $E[N]$. Thus $\alpha \equiv 1 \pmod{N}$.