An $\ell$-adic CM method for genus 2

David R. Kohel
The University of Sydney

Journées Arithmétiques, Marseille, 5 July 2005
Moduli of Genus 2 Curves

A genus 2 curve $X/k$ (in char$(k) = \ell \neq 2$) is defined by a Weierstrass equation

$$y^2 = f(x),$$

where $f(x)$ is a polynomial of degree 6. Over an algebraic closure, we have

$$X : f(x) = \prod_{i=1}^{6}(x - u_i).$$

The points $(u_i, 0)$ are then both the Weierstrass points and the fixed points of the hyperelliptic involution.

The absolute Igusa invariants $(j_1, j_2, j_3)$ of $X$ are defined either in terms of $f(x)$ or, equivalently, by symmetric functions on the set $\{u_i\}$.

N.B. The projective Igusa invariants are weighted invariants $J_2, J_4, J_6, J_8, J_{10}$, where

$$4J_8 = J_2J_6 - J_4^2$$

and $J_{10}$ is the discriminant of $f(x)$. The absolute invariants are defined by

$$j_1 = \frac{J_2^5}{J_{10}}, \quad j_2 = \frac{J_2^3J_4}{J_{10}}, \quad j_3 = \frac{J_2^2J_6}{J_{10}}.$$ 

The triple $(j_1, j_2, j_3)$ determines a point of the moduli space $\mathcal{M}_2$ of genus 2 curves, a space birational to $\mathbb{A}^3$. 
Moduli of Genus 2 Curves with Level Structure

Beginning with the curve $X : y^2 = \prod(x - u_i)$ as above, a linear fractional transformation of the $x$-line $\mathbb{P}^1$ sends three of the $u_i$ to 0, 1, and $\infty$. This determines an isomorphism with a curve in Rosenhain from:

$$y^2 = x(x - 1)(x - t_0)(x - t_1)(x - t_2).$$

The triple $(t_0, t_1, t_2)$ is determined by an ordering on the Weierstrass points, and such a linear fractional transformation. The Weierstrass points generate the 2-torsion subgroup, and an ordered 6-tuple of Weierstrass points determines a full 2-level structure on the Jacobian of $X$.

N.B. A map $\mathcal{M}_g \to \mathcal{A}_g$, from the moduli space of genus $g$ curve to the moduli space of principally polarised abelian varieties of dimension $g$ is induced by sending a curve to its Jacobian. The map to $\mathcal{A}_g$ allows us to define moduli spaces of curves together with a level structure on their Jacobians.

For $g = 2$ this map is a birational isomorphism, and we identify the triple $(t_0, t_1, t_2)$ with a point in the moduli space $\mathcal{M}_2(2)$, classifying genus 2 curves together with a full 2-level structure. The forgetful morphism

$$\mathcal{M}_2(2) \longrightarrow \mathcal{M}_2$$

$$(t_0, t_1, t_2) \longmapsto (j_1, j_2, j_3)$$

is a Galois covering of degree 720, with Galois group $S_6 \cong \text{Sp}_4(\mathbb{F}_2)$. The former group naturally acts on the Weierstrass points (the first three of which must then be renormalised to $(0, 1, \infty)$). The isomorphic group $\text{Sp}_4(\mathbb{F}_2)$ is that which naturally acts on the 2-torsion subgroup.
The Richelot Correspondence

Given a genus two curve

\[ X_1 : y^2 = G_0(x)G_1(x)G_2(x) \]

where each \( G_i(x) \) has degree at most 2, we define a second curve

\[ X_2 : t^2 = \delta H_0(z)H_1(z)H_2(z), \]

by the equations

\[ H_i(x) = G'_{i+1}(x)G_{i+2}(x) - G_{i+1}(x)G''_{i+2}(x), \]

and an explicit constant \( \delta \). Then there exists a Richelot correspondence

\[ C \longrightarrow X_1 \times X_2, \]

where the curve \( C \) is defined by

\[
C : \begin{cases} 
    G_0(x)H_0(z) + G_1(x)H_1(z) = 0, \\
    y^2 = G_0(x)G_1(x)G_2(x), \\
    t^2 = \delta H_0(z)H_1(z)H_2(z), \\
    yt = G_0(x)H_0(z)(x - z). 
\end{cases}
\]

The correspondence determines a \((2, 2)\)-isogeny \( J_1 \rightarrow J_2 \) of Jacobians. More importantly from our point of view, it will let us determine a correspondence of moduli:

\[ \mathcal{X} \longrightarrow \mathcal{M}_2(2) \times \mathcal{M}_2(2). \]
The Richelot Correspondence on Moduli

Associated to a point \((t_0, t_1, t_2) \in \mathcal{M}_2(2)\), we can write down a curve

\[ X_1 : y^2 = f(x) = x(x - 1)(x - t_0)(x - t_1)(x - t_2). \]

A Richelot isogeny is determined setting \(f(x) = G_0(x)G_1(x)G_2(x)\), where the \(G_i(x)\) are:

\[
G_0(x) = x(x - t_0), \quad G_1(x) = (x - 1)(x - t_1), \quad G_2(x) = x - t_2.
\]

The curve \(X_2 : y^2 = \delta H_0(x)H_1(x)H_2(x)\) is then determined by the triple of polynomials:

\[
H_0(x) = x^2 - 2t_2x + t_1t_2 - t_1 + t_2,
H_1(x) = -(x^2 - 2t_2x + t_0t_2),
H_2(x) = (t_0 - t_1 - 1)x^2 + 2t_1x - t_0t_1,
\]

and \(\delta = t_0t_2 - t_1t_2 + t_1 - t_2\).

Let \((u_0, u_1, u_2)\) be a triple of solutions to \(H_i(u_i) = 0\), and set

\[
(v_0, v_1, v_2) = (2t_2 - u_0, 2t_2 - u_1, 2t_1/(t_0 - t_1 - 1) - u_2)
\]

equal to the conjugate solutions. Then

\[ X_2 : y^2 = \delta H_0(z)H_1(z)H_2(z) = \delta \prod_{i=0}^{2} (x - u_i)(x - v_i), \]

and a linear fraction transformation sending \((u_0, u_1, u_2)\) to \((0, 1, \infty)\), maps \((v_0, v_1, v_2)\) to a new triple \((s_0, s_1, s_2) \in \mathcal{M}_2(2)\).
The Richelot Modular Correspondence

We summarise by writing down the defining set of polynomials for the previous correspondence. First we have the relations between the \( t_i \)'s and \( u_i \)'s:

\[
\begin{align*}
\Phi_0(T_0, T_1, T_2, U_0, U_1, U_2) &= U_0^2 - 2T_2U_0 + T_1T_2 - T_1 + T_2, \\
\Phi_1(T_0, T_1, T_2, U_1) &= U_1^2 - 2T_2U_1 + T_0T_2, \\
\Phi_2(T_0, T_1, T_2, U_2) &= (T_0 - T_1 - 1)U_2^2 + 2T_1U_2 - T_0T_1.
\end{align*}
\]

That is, we find \( \mathcal{X} \to \mathcal{M}_2(2) \times \mathbb{A}^3 \)

\[\Phi(x, u) = (\Phi_0(x, u), \Phi_1(x, u), \Phi_2(x, u)) = (0, 0, 0).\]

where \( x = (t_0, t_1, t_2) \) and \( u = (u_0, u_1, u_2) \).

Then we define the second projection to \( \mathcal{M}_2(2) \):

\[\psi : \mathcal{M}_2(2) \times \mathbb{A}^3 \xrightarrow{\psi} \mathcal{M}_2(2)\]

by letting \( \psi \) be the map \((t_0, t_1, t_2), (u_0, u_1, u_2) \mapsto (u_0, u_1, u_2, v_0, v_1, v_2)\), followed by the transformation

\[(s_0, s_1, s_2) = (S(v_0), S(v_1), S(v_3)), \text{ where } S(z) = \frac{(u_1 - u_2)(z - u_0)}{(u_1 - u_0)(z - u_2)}.\]

Then the image of \( \mathcal{X} \) in \( \mathcal{M}_2(2) \times \mathbb{A}^3 \times \mathcal{M}_2(2) \) is defined by

\[
\Phi_i(T_0, T_1, T_2, U_0, U_1, U_2) = \Psi_j(T_0, T_1, T_2, U_0, U_1, U_2, S_j) = 0.
\]
The Richelot Modular Correspondence

In summary, for \((x, u, y) \in \mathcal{M}_2(2) \times \mathbb{A}^3 \times \mathcal{M}_2(2)\) we have

\[
\Phi(x, u) = (\Phi_0(x, u), \Phi_1(x, u), \Phi_2(x, u)) = (0, 0, 0),
\]

\[
\Psi(x, u, y) = (\Psi_0(x, u, y), \Psi_0(x, u, y), \Psi_0(x, u, y)) = (0, 0, 0),
\]

whose zero set \(\mathcal{X}\) admits two finite covers of \(\mathcal{M}_2(2)\).

We are interested in pairs \(x = (t_0, t_1, t_2)\) and \(y = (s_0, s_1, s_2)\) such that \(y = x^\sigma\) for some automorphism \(\sigma\) of the base field \(k\). We then set \(x_i = x\) and \(x_{i+1} = y\). Since each \(x_i\) corresponds to a Richelot isogeny \(J_i \to J_{i+1}\), the Galois action determines a cycle of isogenies:

\[
\begin{array}{c}
J_1 \xrightarrow{x_1} J_2 \xrightarrow{x_2} \\
\phantom{x_1} \downarrow x_5 \downarrow \phantom{x_5} \uparrow \uparrow \uparrow \uparrow \uparrow \uparrow \\
J_6 \xleftarrow{x_5} J_5 \xleftarrow{x_4} J_3 \\
\phantom{x_5} \uparrow \uparrow \uparrow \uparrow \uparrow \uparrow \downarrow x_3 \downarrow x_5 \uparrow \\
J_4 \xleftarrow{x_4} J_3 \xleftarrow{x_3} J_2 \xleftarrow{x_2} J_1 \\
\end{array}
\]

In fact, with the map \(\psi\) as defined above, the point \(y = (s_0, s_1, s_2)\) determines the dual isogeny, which can only be the Galois conjugate of \(x = (t_0, t_1, t_2)\) if it determines a 2-cycle:

\[
\begin{array}{c}
J_1 \xrightarrow{x} J_2 \\
\phantom{x} \downarrow y \downarrow \phantom{y} \\
J_1 \xleftarrow{y} J_2 \\
\end{array}
\]

Instead we modify \(\psi\), and \(\Psi_i\), by composing with a permutation of \((u_0, u_1, u_2, v_0, v_1, v_2)\) to find a Galois conjugate 2-level structure. This corresponds to an isomorphism of the curve

\[
X_2 : y^2 = \delta x(x - 1)(x - s_0)(x - s_1)(x - s_2),
\]

to another in Rosenhain form.
**Canonical Lifting**

Suppose that $A/k$ is an ordinary, simple abelian variety over a finite field of characteristic $\ell$. Let $R$ be the unramified extension of $\mathbb{Z}_\ell$ such that $[R : \mathbb{Z}_\ell] = [k : \mathbb{F}_\ell]$. A **canonical lift** is an abelian variety $\tilde{A}/R$ such that

$$\tilde{A}/R \times_R k = A/k \text{ and } \text{End}(\tilde{A}) = \text{End}(A).$$

The main theorem of complex multiplication describes the relation between (certain) ideal classes of a maximal order $O_K$, isogenies of an abelian variety $A/\overline{\mathbb{Q}}$ with $\text{End}(A) = O_K$, and the action of Galois on the conjugates of $A$. We say that an isogeny $\varphi$ **splits** $A[n]$ if $\ker(\varphi)$ is a proper subgroup of $A[n]$ and $\ker(\varphi) \not\subseteq A[m]$ for any $m \mid n$. The canonical lift of $A/k$ is determined by:

- A cycle of isogenies $\tilde{A}_1 \to \tilde{A}_2 \to \cdots \to \tilde{A}_r \to \tilde{A}_1$ with $\tilde{A}_1 \times_R k = A$ such that the compositum is an endomorphism of $\tilde{A}_1$ whose kernel splits $\tilde{A}_1[n]$; or
- An isogeny $\varphi : \tilde{A}_1 \to \tilde{A}_2$ with $\tilde{A}_1 \times_R k = A$ such that $\tilde{A}_2 = \tilde{A}_1^\sigma$ with $\ker(\varphi)$ splitting $\tilde{A}_1[n]$.

The latter condition, exploiting the Galois action, yeilds a better algorithmic solution to the construction of the canonical lift. As a constructive CM method, we only need to solve for the canonical lift of a moduli point in $\mathcal{M}_2(R)$, and solve a system of equations $\Phi(x, x^\sigma) = 0$ for $x \in \mathcal{M}_2(R)$. 
Canonical Lifts of Moduli

Recall that we derived a set of defining equations in $\mathcal{M}_2(2) \times \mathbb{A}^3 \times \mathcal{M}_2(2)$,

\[
\Phi(x, u) = (\Phi_0(x, u), \Phi_1(x, u), \Phi_2(x, u)) = (0, 0, 0),
\]

\[
\Psi(x, u, y) = (\Psi_0(x, u, y), \Psi_0(x, u, y), \Psi_0(x, u, y)) = (0, 0, 0),
\]

where

\[x = (t_0, t_1, t_2) \in \mathcal{M}_2(2), \quad u = (u_0, u_1, u_2) \in \mathbb{A}^3, \quad y = (s_0, s_1, s_2) \in \mathcal{M}_2(2).\]

In order to preserve the simplicity of these defining equations, we refrain from eliminating $u \in \mathbb{A}^3$ to find relations only in $\mathcal{M}_2(2) \times \mathcal{M}_2(2)$. Also we work with moduli in $\mathcal{M}_2(2)(R)$, with 2-level structure, rather than $\mathcal{M}_2(R)$, and only afterwards compute the image under $\mathcal{M}_2(2) \to \mathcal{M}_2$.

We can solve this system of equations by Hensel’s Lemma, first for $u$, given $x$, such that

\[
\Phi(x, u) = (0, 0, 0),
\]

and then for $y$ satisfying

\[
\Psi(x, u, y) = (0, 0, 0).
\]

However, the resulting $y$ need not converge to $x^\sigma$. For this purpose we adapt a method of Harley from the one-dimensional setting (of moduli of genus 1 curves) to higher dimension.
The Method of Harley

In the one-dimensional setting, Harley developed a means of solving a generalised $p$-adic AGM recursion, determined by a geometric correspondence of moduli:

$$\Phi(x, x^\sigma) = 0,$$

where $\sigma$ is the Frobenius automorphism. In particular, if $x$ is such a solution, and $x_i \equiv x \mod p^i$, then we set

$$\delta = \frac{1}{p^i}(x - x_i).$$

We observe that

$$\frac{1}{p^i} \Phi(x_i, y_i) + \delta \Phi_x(x_i, x_i^\sigma) + \delta^\sigma \Phi_x(x_i, x_i^\sigma) \equiv \Phi(x, y) \mod p^i \equiv 0 \mod p^i.$$

Thus it comes down to determining $\delta$ such that

$$\delta^\sigma \alpha + \delta \beta + \gamma = 0 \mod p^i.$$

The additional condition $v_p(\beta) > 0$ implies that a unique $p$-adic solution is determined. 

N.B. Such an equation $\Phi(x, y) = 0$ arises as the defining equations for the image modular curve

$$X_0(Np) \longrightarrow X_0(N) \times X_0(N),$$

where $X_0(N)$ is a modular curve of genus 0.
Generalised Method of Harley

In place of a single modular equation \( \Phi(x, x^\sigma) = 0 \), we need to generalise the method to the multivariate setting. For a solution \((x, u, y)\) with \( y = x^\sigma \) to the system of equations

\[
\Phi(x, u) = \Psi(x, u, y) = 0,
\]

we set \( x_i \equiv x \mod \ell^i \). Then

\[
\frac{1}{\ell^i} \Phi(x_i, u_i) + \Delta_x \cdot D_x \Phi(x_i, u_i) + \Delta_u \cdot D_u \Phi(x_i, u_i) \equiv 0 \mod \ell^i,
\]

where

\[
\Delta_x = \frac{1}{\ell^i} (x - x_i) \quad \text{and} \quad \Delta_u = \frac{1}{\ell^i} (u - u_i),
\]

and

\[
D_x \Phi(x, u) = \begin{pmatrix}
\frac{\partial \Phi_0(x, u)}{\partial t_0} & \frac{\partial \Phi_1(x, u)}{\partial t_0} & \frac{\partial \Phi_2(x, u)}{\partial t_0} \\
\frac{\partial \Phi_0(x, u)}{\partial t_1} & \frac{\partial \Phi_1(x, u)}{\partial t_1} & \frac{\partial \Phi_2(x, u)}{\partial t_1} \\
\frac{\partial \Phi_0(x, u)}{\partial t_2} & \frac{\partial \Phi_1(x, u)}{\partial t_2} & \frac{\partial \Phi_2(x, u)}{\partial t_2}
\end{pmatrix}
\]

and

\[
D_u \Phi(x, u) = \begin{pmatrix}
\frac{\partial \Phi_0(x, u)}{\partial u_0} & \frac{\partial \Phi_1(x, u)}{\partial u_0} & \frac{\partial \Phi_2(x, u)}{\partial u_0} \\
\frac{\partial \Phi_0(x, u)}{\partial u_1} & \frac{\partial \Phi_1(x, u)}{\partial u_1} & \frac{\partial \Phi_2(x, u)}{\partial u_1} \\
\frac{\partial \Phi_0(x, u)}{\partial u_2} & \frac{\partial \Phi_1(x, u)}{\partial u_2} & \frac{\partial \Phi_2(x, u)}{\partial u_2}
\end{pmatrix}.
\]

And also

\[
\frac{1}{p^i} \Psi(x_i, u_i, x_i^\sigma) + \Delta_x \cdot D_x \Psi(x_i, u_i, x_i^\sigma) + \Delta_u \cdot D_u \Psi(x_i, u_i, x_i^\sigma) + \Delta_x^\sigma \cdot D_y \Psi(x_i, u_i, x_i^\sigma) \equiv 0 \mod p^i,
\]

where \( D_x \Psi, D_u \Psi, \) and \( D_y \Psi \) are the similarly defined Jacobian matrices.
Generalised Method of Harley

We solve for $u_i$ such that $\Phi(x_i, u_i) \equiv 0 \mod \ell^{2i}$, then, assuming $D_u \Phi$ is invertible, we may eliminate $\Delta_u$ to find an equation

$$\Delta_x^\sigma \cdot A + \Delta_x \cdot B + C \equiv 0 \mod \ell^i.$$

where

$$A = D_y \Psi,$$
$$B = D_x \Phi - D_x \Phi D_u \Phi^{-1} D_u \Psi,$$
$$C = \frac{1}{\ell^i(\Psi)} - \frac{1}{\ell^i(\Phi)} D_u \Phi^{-1} D_u \Psi \equiv \frac{1}{\ell^i(\Psi)} \mod \ell^i.$$

We apply this for input $x_i$, correct to precision $\ell^i$, and $u_i$ such that $\Phi(x_i, u_i) = 0$. This provides a matrix equation which we can solve for the deficiency $\Delta_x \mod \ell^i$, and set $x_{i+1} = x_i + \ell^i \Delta_x$.

We note that when $B \not\equiv 0 \mod \ell$, there will generally be multiple solutions to the matrix equation, and we must determine which solution extends to the canonical lift.

This gives a convergent Hensel lifting algorithm for the CM moduli, in which precision doubles with each iteration.

An algebraic relation can be recovered over $\mathbb{Z}$ by means of LLL reduction of the lattice dependency relations between powers of $j_1$, $j_2$, and $j_3$. 
A 3-Adic Example

Let \( \mathbb{F}_{27} = \mathbb{F}_3[w]/(w^3 - w + 1) \), and set \( x = (t_0, t_1, t_2) = (w^{14}, w^8, 2) \), determining a Galois cycle of length 3. The point \( y = (s_0, s_1, s_2) = (w^{16}, w^{24}, 2) \) is the image of \( x \) under Frobenius, and defines a second curve related to the first by a Richelot correspondence. Then the 3-adic lifts of these invariants map to a triple of absolute Igusa invariants \((j_1, j_2, j_3)\), satisfying:

\[
10460353203j_1^6 - 20644606194972313680j_1^5 + 1584797903444725069000181184j_1^4 - \\
57934203669971774729663594299868672j_1^3 - \\
4757210399363959986030325710967612515648j_1^2 - \\
2319410019701066580457483440392962776928771637248j_1 - \\
1633610752539414651637667693318669910064037028972986368,
\]

\[
19683j_2^6 - 3154427913690j_2^5 + 1301845828705642175j_2^4 - \\
9011847196705020909893875j_2^3 - \\
4691292251238152998837057320000j_2^2 + \\
1371934443680672253419375717574400000j_2 - \\
42517234157035811590789580667261104120000000,
\]

\[
531441j_3^6 - 80079819760854j_3^5 + 681652231356458824713j_3^4 - \\
1621537231026449336569333993j_3^3 - \\
1566137192004297839675972173376896j_3^2 - \\
1479377322341359891148215922582439772160j_3 - \\
93993702130655707607384087330217698726510592.
\]