Lower Dimensional Complex Multiplication

David R. Kohel
Institut de Mathématiques de Luminy

Complex multiplication of abelian varieties

An abelian variety A/k over a field k is a complete, projective group scheme. An abelian variety A/k is said to have CM if $\mathcal{O} = \mathrm{End}(A)$ is an order in a CM field K of degree $2g = 2\dim(A)$ over $\mathbb{Q}$. Such a number field has a unique automorphism which agrees with complex conjugation on any complex embedding. Consequently there exists a unique totally real subfield F of degree g over $\mathbb{Q}$.

The simplest example of an abelian variety is an elliptic curve, which can be described by the projective closure of a Weierstrass cubic:

$$E : y^2 + xy = x^3 - \frac{36}{(j - 1728)}x - \frac{1}{(j - 1728)},$$

which has an associated invariant $j = j(E)$. An elliptic curve with CM is the projective image of $\mathbb{C}/\mathfrak{a}$ where $\mathfrak{a}$ is an ideal in a CM order $\mathcal{O}$ embedded in $\mathbb{C}$.

Complex abelian varieties

For general $A/\mathbb{C}$ we have $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for a Hermitian lattice Λ, and

$$\mathrm{End}(A) \cong \mathrm{End}(\mathbb{C}^g/\Lambda) \subseteq \mathbb{M}_g(\mathbb{C}).$$

Generically, we have $\mathrm{End}(A) = \mathbb{Z}$. We can write

$$\Lambda = \Omega_1\mathbb{Z}^g + \Omega_2\mathbb{Z}^g \cong \mathbb{Z}^g + \Omega_2^{-1}\Omega_1\mathbb{Z}^g,$$

such that $\tau = \Omega_2^{-1}\Omega_1$ is an element of Siegel upper half space:

$$\mathbb{H}_g = \{\tau \in \mathbb{M}_g(\mathbb{C}) \,|\, \tau^t = \tau \text{ and } \Im(\tau) > 0\}.$$

The set of isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ of dimension g are in bijection with

$$\mathcal{A}_g(\mathbb{C}) = \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g,$$

where $\mathcal{A}_g$ is the (course) moduli space of p.p. abelian varieties.

Moduli of abelian varieties

In the case $g = 1$, the discrete group $\mathrm{Sp}_2(\mathbb{Z})$ equals $\mathrm{SL}_2(\mathbb{Z})$, and we recover the j-line $\mathbb{A}^1(\mathbb{C}) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, where

$$\mathbb{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\},$$

which is an affine line with coordinate function j. We would like to determine an algebraic description of the special values of $j = j(E)$ for which $\mathrm{End}(E)$ is a CM order. E.g. for $\mathcal{O} = \mathbb{Z}[(1+\sqrt{-23})/2]$, such j satisfy:

$$j^3 + 3491750j^2 - 5151296875j + 12771880859375 = 0.$$

In general for a fixed CM order $\mathcal{O}$ there are a finite number of such points in $\mathcal{A}_g(\mathbb{C})$ which lie in $\mathcal{A}_g(\overline{\mathbb{Q}})$.

Explicit moduli

In higher dimension we need a suitable moduli space of curves $\mathcal{M}_g$ or of p.p. abelian varieties $\mathcal{A}_g$ with known coordinate functions. For lower dimension $g \leq 3$, the map from curves to their Jacobians maps $\mathcal{M}_g$ to a dense open subvariety of $\mathcal{A}_g$ (invariants of nondecomposable abelian varieties).

Assumptions:

1. Some functions $x_1, \ldots, x_n$ on $\mathcal{M}_g$ (or $\mathcal{A}_g$) are known which determine the function field of $\mathcal{M}_g$ (or $\mathcal{A}_g$).
2. Given a curve C/k (or abelian variety A/k) we can compute the point $P = (x_1, \ldots, x_n)$ in $\mathcal{M}_g(k)$ (or $\mathcal{A}_g(k)$), which determines C (or A) up to $\bar{k}$-isomorphism,
3. Conversely, from P we can find such a C (or an A).

For dimension $g \leq 3$ there exist explicitly computable invariants of curves, but for $g = 3$, there remains work to describe an algorithm for assumed property 3.

Explicit CM constructions

GOAL: Determine moduli of CM curves (or p.p. abelian varieties), as a set of polynomial relations determining CM points in $\mathcal{M}_g$ (or $\mathcal{A}_g$), associated to an order $\mathcal{O}_K$.

Motivation:

1. Fundamental mathematical interest: generation of abelian extensions, explicit class field theory.
2. Cryptographic applications: the zeta function of a CM curve or abelian variety over a finite field is determined (up to finitely many possibilities) by $\mathcal{O}_K$.

Algorithmic considerations

1. Choice of a moduli space X with low degree map $X \to \mathbb{P}^n$.
2. Complex analytic, p-adic, or CRT methods.
   - 2.1 Construction of special CM points.
   - 2.2 Reconstruction of defined polynomials (ideals) over $\mathbb{Z}$.
3. Galois theoretic properties of these points coming from CFT.

Explicit invariant theory

We have at our disposal the following explicit invariants:

g	$\dim(\mathcal{H}_g)$	$\dim(\mathcal{M}_g)$	$\dim(\mathcal{A}_g)$	Invariants
1		1	1	j
2	3	3	3	Igusa/Clebsch
3	5	6	6	Dixmier-Ohno/Shioda
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
g	$2g-1$	$3g-3$	$g(g+1)/2$	Theta constants

Genus 1:
In the case of $g = 1$ we have $\mathcal{M}_1 (= \mathcal{A}_1) = \mathrm{Spec}(\mathbb{Q}[j]) = \mathbb{A}^1$.
Genus 2:
In the case of $g = 2$ we have a rational parametrization of $\mathcal{M}_2$, given by a (noncanonical choice of) triple of Igusa invariants (j_1, j_2, j_3). Thus $\mathcal{M}_2$ is birational to $\mathbb{A}^3$.

Explicit invariant theory

Genus 3:
For $g = 3$, Shioda described the ring of projective invariants for the hyperelliptic locus $\mathcal{H}_3$, as $\mathbb{Q}[J_2, J_3, \ldots, J_{10}]$ such that J_2, J_3, $\ldots$, J_7 are algebraically independent and $\mathbb{Q}[J_2, \ldots, J_{10}]$ is a free $\mathbb{Q}[J_2, \ldots, J_7]$-module of rank 5, generated by $\{1, J_8, J_9, J_{10}, J_9^2\}$.

On the generic space $\mathcal{M}_3$, Dixmier described 7 algebraically independent projective invariants, such that $\mathcal{M}_3 \to \mathbb{P}^6$ is a finite cover of degree 60. Invariants of Ohno complete the description of the full ring of projective invariants.

Potential improvements:
For $g \geq 2$, we may replace $\mathcal{A}_g$ of dimension $g(g+1)/2$ by the smaller Hilbert moduli space of dimension g, whose points have endomorphisms by a fixed totally real subring $\mathcal{O}_F$.

At the risk of replacing a geometrically simple moduli space with a more complicated one, we consider finite covers of $\mathcal{M}_g$ or $\mathcal{A}_g$ by adding a level structure.

Level structure in genus 1

In terms of the j-function, we saw that even for the small order $\mathbb{Z}[(1+\sqrt{-23})/2]$ the Hilbert class polynomial (minimal polynomial of CM j-invariants) has relatively large coefficient size:

$$j^3 + 3491750j^2 - 5151296875j + 12771880859375.$$

Using a Legendre model $y^2 = x(x-1)(x-t)$, with full parametrized 2-torsion subgroup, we find a class polynomial

$$t^6 - 3t^5 + 13651t^4 - 27297t^3 + 8016t^2 + 5632t + 4096.$$

Here t is a generator for the function field of $X(2)$, and $j = 2^8(t^2-t+1)^3/(t(t-1))^2$. The coefficient size is reduced at the expense of finding a degree $2h$ polynomial.
By adding a level-48 structure, a suitable Weber function (such that $j = (u^{24}-16)^3/u^{24}$) gives class polynomial:

$$u^3 - u^2 + 1.$$

Level structure in genus 2

In analogy with the Legendre model for an elliptic curve, a genus 2 curve with a full level 2 structure can be expressed by a Rosenhain model:

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

The six points with $y = 0$ or $y = \infty$ are Weierstrass points, whose differences give the 2-torsion points of $J = Jac(C)$. The action of S_6 on (pairs of) Weierstrass points is isomorphic to the symplectic group $\mathrm{Sp}_4(\mathbb{F}_2)$ action on $J[2]\backslash\{0\}$.

The triple (t_0, t_1, t_2) represents a point on $\mathcal{M}_g(2)$, the moduli space of curves with will level 2 structure (on their Jacobian). This triple of functions give candidates for CM invariants of smaller height. If $(2) = \mathfrak{p}_1\mathfrak{p}_2\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2$ splits completely in $\mathcal{O}_K$, then

$$J[2] = J[\mathfrak{p}_1] \oplus J[\mathfrak{p}_2] \oplus J[\bar{\mathfrak{p}}_1] \oplus J[\bar{\mathfrak{p}}_2].$$

However, the Galois action on $\{\mathfrak{p}_i, \bar{\mathfrak{p}}_i\}$ results in a nontrivial action on the 2-torsion, hence on these invariants. Thus the degrees of the class polynomials are greater than those for (j_1, j_2, j_3).

Level structure in genus 2

A Richelot is determined by the ordered factorization

$$y^2 = G_0(x)G_1(x)G_2(x),$$

where $G_0(x) = x(x - t_0)$, $G_1(x) = (x - 1)(x - t_1)$, $G_2(x) = t - t_2$. This data is equivalent to specifying a split $(2,2)$-subgroup of $J[2]$. In terms of the action of S_6, this represents a quotient by the subgroup

$$\langle (1,4), (2,5), (3,6) \rangle,$$

under the ordering

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ (0,0) & (0,1) & \infty & (t_0,0) & (t_1,0) & (t_2,0) \end{array}$$

The quotient space of this group is a $\Gamma_1(2)$ level structure:

$$\Gamma_1(p) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}) \,:\, C \equiv 0 \bmod p \text{ and } A \equiv 1 \bmod p \right\}.$$

Level structure in genus 2

To find invariants of this quotient we find the representation of the S_6 action in $\mathrm{Aut}(\mathbb{Q}(t_0, t_1, t_2))$. For instance the cycle $(1, 2, 3, 4, 5, 6)$ determines

$$(t_0, t_1, t_2) \longmapsto \left(\frac{(1 - t_1)}{(t_0 - t_1)}, \frac{(1 - t_2)}{(t_0 - t_2)}, \frac{1}{t_0} \right),$$

by applying the permutation of points, followed by a linear fractional transformation to send the first three to $(0, 1, \infty)$. Noting that the degenerate loci $t_i - t_j = 0$ must be permuted, we find an action on exponent vectors in $\mathbb{Z}^9$ in terms of the factor basis

$$\{t_0, t_1, t_2, t_0 - 1, t_1 - 1, t_2 - 1, t_0 - t_1, t_0 - t_2, t_1 - t_2\}.$$

We find forms in the $+1$ eigenspace of $(1, 4)$, $(2, 5)$, and $(3, 6)$:

$$u_1 = \frac{t_2(t_0 - t_2)}{t_0^2}, u_2 = \frac{(t_2 - 1)(t_1 - t_2)}{(t_1 - 1)^2}, u_3 = \frac{t_1(t_0 - 1)(t_0 - t_1)}{t_0^2(t_1 - 1)^2}.$$

First example in genus 2

Consider the quartic CM field $\mathbb{Q}[x]/(x^2+10x+17)$ of class number 1 (with real subfield of discriminant 8). One set of minimal polynomials for Rosenhain invariants (t_0, t_1, t_2) is:

$$
\begin{aligned}
&2^4x^4 - 28x^3 + 13x^2 + 2x - 2,\\
&2^4x^8 + 20x^7 + 465x^6 - 950x^5 + 723x^4 - 232x^3 + 19x^2 + 2x + 1,\\
&2^{10}x^8 - 3904x^7 + 6196x^6 - 4984x^5 + 1776x^4 + 52x^3 - 171x^2 - 4x + 2^4
\end{aligned}
$$

The Richelot invariants (u_1, u_2, u_3) corresponding to the $\mathcal{O}_K$-isogeny determined by $\mathfrak{p}_1\mathfrak{p}_2 \mid \mathfrak{p}_1^2\mathfrak{p}_2^2 = 2\mathcal{O}_K$ have minimal polynomials:

$$
\begin{aligned}
&16x^2 + 4x - 1,\\
&256x^4 - 16\cdot 11x^3 + 8\cdot 17x^2 - 75x + 16,\\
&256x^4 + 16\cdot 11x^3 + 8\cdot 17x^2 + 75x + 16
\end{aligned}
$$

By comparison, the minimal polynomials of Igusa invariants are:

$$
\begin{aligned}
&j_1^2 - 531441j_1 + 55788550416,\\
&j_2^2 - 4374j_2 - 76527504,\\
&16j_4^2 - 8667j_4 - 3359232
\end{aligned}
$$

Second example in genus 2

The field $\mathbb{Q}[x]/(x^2 + 38x + 89)$ with real subfield of discriminant 17 is one of two non-normal quartic CM fields of class number 7 in which 2 splits completely (the other being its reflex field). This is the smallest class number for which this occurs.

For this field there exists a single set of split Richelot invariants of the same degree ($= 14$) as the Igusa invariants (the rest have degree 28). The corresponding Richelot isogeny is not one of the six $\mathcal{O}_K$-isogenies determined by the factorization of 2. For this example, the size of the minimal polynomials for these invariants is strikingly small (in comparison to those of the Igusa invariants):

$$
\begin{aligned}
&5^8x^{14} - 26606920000x^{13} + 65586675772096x^{12} \\
&+177740304205952x^{11} + 248039128327680x^{10} + 208159900349440x^9 \\
&+385595201712128x^8 - 191023627468800x^7 + 297310545969152x^6 \\
&-283298980691968x^5 + 107307397545984x^4 - 18493869129728x^3 \\
&+1372963471360x^2 - 29729226752x + 2^{28},
\end{aligned}
$$

$$
\begin{aligned}
&5^8x^{14} - 137748840000x^{13} + 12962437435616x^{12} \\
&+94672625668736x^{11} + 2543612904653568x^{10} - 5738421484984320x^9 \\
&+5526999453577216x^8 - 2038583246651392x^7 + 392532678737920x^6 \\
&-107927186178048x^5 + 31648890486784x^4 - 5490033557504x^3 \\
&+617669984256x^2 - 19595788288x + 2^{28},
\end{aligned}
$$

$$
\begin{aligned}
&5^4 11^4 x^{14} - 1116231216x^{13} + 2287896896x^{12} \\
&-544552666944x^{11} - 748232547840x^{10} - 10793935284224x^9 \\
&+37781775106048x^8 - 27811400695808x^7 - 13407189270528x^6 \\
&+9054522703872x^5 + 6717607772160x^4 + 1516031180800x^3 \\
&+134637158400x^2 + 3892314112x + 2^{28}
\end{aligned}
$$

There are similarly two non-normal quartic CM fields of class number 10 and two of class number 11 for which 2 splits completely. Taking one of the latter we find the following minimal polynomials of Richelot invariants:

We note again that there is a unique choice among the 15 such invariants (up to permutation) such that the degree is 22 (and not 44), and this does not correspond to one of the six $\mathcal{O}_K$-isogenies.

$$
\begin{aligned}
&5^8x^{22} + 295323445000x^{21} + 6857290679649907536x^{20} - 25244737244319200055 04x^{19} \\
&+20238375563623631300 5056x^{18} - 25682587323012011077 46816x^{17} + 15003082194028844457512960x^{16} \\
&-5710696089307744098 2302720x^{15} + 1455661440738433814 67807744x^{14} - 115438127941825876291223552x^{13} \\
&+360273699982053896 28243968x^{12} + 200109560536324137 17233664x^{11} + 137499396947386051 22519040x^{10} \\
&-535670244526960072 14366720x^{9} + 429512191373175964 71230464x^{8} - 181240660581510641 28978944x^{7} \\
&+506534252950098308 1304064x^{6} - 109311665663791607 2640512x^{5} + 189799205941359117 598720x^{4} \\
&-232696541969893535 25248x^{3} + 146759934873512915 7632x^{2} + 31660657224135475 2x + 2^{44},
\end{aligned}
$$

$$
\begin{aligned}
&5^{12}31^4x^{22} - 241664598090625000x^{21} + 6589373758567507 0000x^{20} \\
&-8839083142975465017 6x^{19} - 2103465281888678425344x^{18} + 1949312817245894310912x^{17} \\
&+2748807433452985189 9904x^{16} + 1311597012843177484 2880x^{15} - 8446903971224795407 9744x^{14} \\
&+3295786194987463475 200x^{13} + 8144498195866845498 5728x^{12} - 3963108680097360510 9760x^{11} \\
&-8426403160138344038 400x^{10} + 9916587822249332965 376x^{9} - 1316073487063607934 976x^{8} \\
&-6863529846561675673 60x^{7} + 2606233508429829242 88x^{6} - 2882552501971084902 4x^{5} \\
&-5436984668916285 44x^{4} + 2164314422242181 12x^{3} + 4174845650665472x^{2} + 43980465111040x + 2^{44},
\end{aligned}
$$

$$
\begin{aligned}
&5^8x^{22} + 1111785000x^{21} + 242723405136x^{20} - 110278699886016x^{19} \\
&-24786540857223680x^{18} + 2316736614120654848x^{17} + 82668386737701575 8848x^{16} \\
&-16167405833026381922304x^{15} + 8614618842114775862 4768x^{14} - 3363238207961227591 6800x^{13} \\
&+12961121054741692835 4304x^{12} + 3870228138417967144 63232x^{11} + 2243852123207584291 22560x^{10} \\
&+1237485561393660821504x^{9} + 2224298494599242973 1840x^{8} + 6306746589916581330 9440x^{7} \\
&+2946114732297178998 3744x^{6} + 3303427266641999691 776x^{5} + 2368560434080278118 40x^{4} \\
&+1027533885770039296 0x^{3} + 2439805306918666 24x^{2} + 3034652092661760x + 2^{44}
\end{aligned}
$$