On CM and RM constructions of abelian surfaces

David R. Kohel
Institut de Mathématiques de Luminy

CIRM Number Theory and Applications
30 November – 4 December 2009

On CM and RM constructions of abelian surfaces

David R. Kohel
Institut de Mathématiques de Luminy

Belgian Mathematical Society - London Mathematical Society
Algebraic Geometry and Cryptography Special Session
Leuven, 5 December 2009

Contents

1. **Complex multiplication**
   - CM overview
   - Motivation: Number theory
   - Motivation: Cryptography
2. **Real multiplication**
   - RM overview
   - Application: RM zeta functions
   - Application: explicit real endomorphisms
   - Application: explicit RM and point counting

CM Motivation

Let A/k be a simple abelian variety. Then A is said to have *complex multiplication* if $\mathrm{End}(A)$ is an order in a totally imaginary quadratic extension of a totally real field K. Such a field K is called a *CM field*, and is the largest such ring which can occur as the endomorphism ring of an abelian variety.

Question: Why are we interested?

1. *The beauty of the mathematics.*
   It provides a connection between algebraic geometry and constructive class field theory.
2. *The applications to cryptography.*
   There are explicit and very efficient constructions of elliptic curves and abelian varieties with known group orders.

Motivation: Number theory

The abelian varieties (or Jacobians) with CM by $\mathcal{O}$ are determined by a zero dimensional scheme (Galois orbits of points) in the moduli space $\mathcal{A}_g$ of p.p. abelian varieties (or $\mathcal{M}_g$ of curves).

Elliptic curves. For $g = 1$ the coordinate function is the j-invariant, and the scheme is defined by the Hilbert class polynomial $H_D(j)$, e.g.

$$H_{-3}(j) = j = 0, \quad H_{-4}(j) = j - 12^3 = 0,$$

and

$$H_{-23}(j) = j^3 + 3491750j^2 - 5151296875j + 12771880859375 = 0.$$

A root j generates the Hilbert class field $H = K(j)$ over $K = \mathbb{Q}(\sqrt{D})$.

Motivation: Number theory

Level structure. In order to reduce the height of the moduli points, a standard trick is to introduce level structure. For example, $H_{-71}(x)$ is:

$$x^7 + 313645809715x^6 - 3091990138604570x^5 + 9839403881004781204930 2x^4 - 8235342634397307799680913 89x^3 + 513880036645397678032372632 9446x^2 - 42531947394613960327460515 1187659x + 11^9 \cdot 17^6 \cdot 23^3 \cdot 41^3 \cdot 47^3 \cdot 53^3.$$

but if we use a low degree function on $X_0^+(N)$ we find:

$$\begin{aligned}
19: &\quad x^7 + 12x^6 + 64x^5 + 219x^4 + 556x^3 + 974x^2 + 964x + 391\\
29: &\quad x^7 + 4x^6 + 4x^5 - 2x^4 - 2x^3 + x + 1\\
37: &\quad x^7 - 2x^6 + 9x^5 - 10x^4 - x^3 + 8x^2 - 5x + 1\\
43: &\quad x^7 - 3x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - x + 1\\
83: &\quad x^7 - 2x^6 + 4x^5 - 4x^4 + 5x^3 - 4x^2 + 2x - 1\\
89: &\quad x^7 - 4x^6 + 5x^5 - x^4 - 3x^3 + 2x^2 - 1.
\end{aligned}$$

Motivation: Number theory

Genus 2 curves. For $g = 2$, the invariants of a curve is a triple (j_1, j_2, j_3) of Igusa invariants, and the CM subscheme is defined by an ideal in $k[j_1, j_2, j_3]$. E.g. the CM curve $y^2 = x^5 - 1$ (with $K = \mathbb{Q}(\zeta_5)$) has Igusa invariants

$$(j_1, j_2, j_3) = (0, 0, 0).$$

In general, the degree and coefficient size of this ideal grows with the class number and defines a subfield of the Hilbert class field of the reflex field of K.

As in the case $g = 1$, the moduli points encode arithmetic information about the reduction and congruence behavior of the geometric objects, so the heights of the points grows with the discriminant of K.

Motivation: Cryptography

Random curve point counting. The efficient construction of a random abelian surface $A/\mathbb{F}_p$ such that $A(\mathbb{F}_p)$ has known order N over a large prime finite field $\mathbb{F}_p$ is a challenging open problem.

Using an optimized Schoof, Atkin, Elkies algorithm for genus 2 can produce a Jacobian $J/\mathbb{F}_p$ with N prime of cryptographic size (160-256 bits), but may require months of computation. See:

http://chic.gforge.inria.fr/index_en.html

This difficulty fuels the interest in CM curves in cryptography (and efforts to improve the algorithms for random curves).

Motivation: Cryptography

CM curve point counting. In contrast, given a CM curve, it takes a matter of seconds to produce such a Jacobian surface. For example, let p be the prime

$$82868313845568823383146027529869455231.$$

Then the genus 2 curve $C : y^2 = x^5 + 3$ over $\mathbb{F}_p$ has Jacobian whose number N of points:

$$6867157439607693550919607918760021921783195331645921526927337384226808323221$$

is prime. In particular the class $[(1, 2)] - [\infty]$ generates a cyclic group of prime order N.

Explicit CM in genus 2

The known methods for CM constructions in genus 2 are:

1. complex analytic (van Wamelen, Spalleck, Weng, Dupont, Houtmann, etc.),
2. p-adic analytic (G.H.K.R.W., Carls, K., Lubicz),
3. CRT (Lauter et al.).

The CRT method is not yet practical. The 2-adic and 3-adic methods implemented, are limited by the congruence condition on the CM field at p, and finding a suitable input curve, over a small finite field, with endomorphism ring equal to the maximal order. A good general implementation of the complex analytic method is not yet available.

Explicit CM in genus 2

A genus 2 database of CM invariants. The simple form and tiny invariants for the curve in the previous example is deceptive. In general, due to the size of the output, it is a challenging problem to determine defining equations for CM Igusa invariants. See:

http://echidna.maths.usyd.edu.au/kohel/dbs/complex_multiplication2.html

Once a set of defining polynomials are known for given K, it is nevertheless still efficient to sieve for degree one primes (of good ordinary reduction) and and write down a CM curve (using Mestre's algorithm) whose Jacobian has known prime number of points.

Contents

1. **Complex multiplication**
   - CM overview
   - Motivation: Number theory
   - Motivation: Cryptography
2. **Real multiplication**
   - RM overview
   - Application: RM zeta functions
   - Application: explicit real endomorphisms
   - Application: explicit RM and point counting

RM overview

RM moduli. The data of (the maximal order of) a CM field determines a zero dimensional scheme in $\mathcal{A}_g$. For $g = 2$ these comprise a finite set of points in a 3-dimensional space.

If we restrict to the real subring of discriminant D, we determine a 2-dimensional *Humbert surface* $\mathcal{H}_D$ in $\mathcal{A}_2$. This is a new phenomenon not seen in genus 1. As a codimension one subspace of a rational space it is determined by a polynomial equation.

For details of the determination of these Humbert polynomials, especially in covers of $\mathcal{A}_2$ with level structure, see the thesis of D. Gruenewald:

http://echidna.maths.usyd.edu.au/~davidg,

Alternatively, for N. Elkies and A. Kumar approach via K3 surfaces:

http://www.math.harvard.edu/~elkies/banff07.pdf

RM overview

Question: Why are we interested?

1. *Mathematical beauty.*
   The Humbert surfaces are fundamental geometric objects in $\mathcal{A}_2$ (or $\mathcal{M}_2$), with connections to Hilbert modular forms, Shimura curves, etc.
2. *Applications.*
   The real subring determines half of the data of the Frobenius characteristic polynomial and for small discriminants D the endomorphisms on an RM Jacobian can be made effective.

Application: RM zeta functions

RM zeta functions. For small discriminants for which the Humbert surface $\mathcal{H}_D$ has been computed, we obtain a random RM construction over finite fields. If D is known, then the characteristic polynomial of Frobenius factors:

$$\chi(T) = T^4 - tT^3 + sT^2 - ptT^2 + p^2 = \chi_1(T)\chi_2(T),$$

where

$$\chi_i(T) = T^2 - \tau_i T + p \text{ for } \tau_i = \frac{t \pm m\sqrt{D}}{2}.$$

We can then replace the bounds

$$|t| \leq 4\sqrt{p} \text{ and } |s - 2p| \leq 4p,$$

with

$$|t| \leq 4\sqrt{p} \text{ and } |m|\sqrt{D} \leq 4\sqrt{p}.$$

Application: explicit real endomorphisms

Explicit endomorphisms. Let K be a field and C/K the genus 2 family of curves:

$$C : y^2 = x^5 - 5x^3 + 5x + t.$$

If $P = (\xi, \gamma)$ is a generic point on C over its function field $F = K(\xi, \gamma)$, then in Mumford representation, we have

$$[P] - [\infty] = (x - \xi,\ y - \gamma) \in J(F).$$

Then J has real multiplication by $\mathbb{Z}[\eta_5] = \mathbb{Z}[t]/(t^2 - t - 1)$. In particular:

$$[\eta_5](P) = (x^2 + (-\eta_5 + 1)\xi x + \xi^2 - \eta_5 - 2,\ y - \gamma).$$

See K. and Smith, (ANTS 7, Berlin).

Application: explicit RM and point counting

RM torsion decomposition. The use of explicit real multiplication for such families will permit us (for half of the primes ℓ) to determine a decomposition

$$A[\ell] = G_1 \oplus G_2.$$

Since a generic genus 2 divisor is of the form $[P_1] + [P_2] - 2[\infty]$, $G \subset A[\ell]$ is determined by a meet-in-the-middle construction

$$\phi([P_1] - [\infty]) = -\phi([P_2] - [\infty]),$$

where $\phi = n + m\eta$ is a generator for a principal ideal over (ℓ).

Since the order of G_i is ℓ^2 rather than ℓ^4 for $A[\ell]$, this allows one to push the explicit SEA calculation further using larger primes ℓ for a combined random RM and SEA algorithm.

THE END