

Modular polynomials for genus 2

Reinier Bröker

joint work with Kristin Lauter

Microsoft Research

University of Washington

April 2008

Modular polynomials for genus 1

For $N \geq 1$, put $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N} \right\}$.

The Riemann surface $Y_0(N) \stackrel{\mathrm{def}}{=} \Gamma_0(N) \backslash \mathbf{H}$ has the structure of an *affine curve*.

The function field $\mathbf{C}(Y_0(N))$ equals $\mathbf{C}(j, j_N)$ with $j : \mathbf{H} \rightarrow \mathbf{C}$ the ‘classical’ j -function and $j_N(\tau) = j(N\tau)$.

Definition. *The minimal polynomial $\Phi_N \in \mathbf{C}(j)[X]$ of j_N over $\mathbf{C}(j)$ is called the modular polynomial.*

Modular polynomials for genus 1

Properties of Φ_N :

- $\deg(\Phi_N) = N \prod_{p|N} (1 + 1/p)$
- $\Phi_N \in \mathbf{Z}[j, X]$
- $\Phi_N(j, X) = \Phi_N(X, j)$.

Moduli interpretation:

The roots of $\Phi_N(j(E), X) \in \mathbf{C}[X]$ are the j -invariants of elliptic curves that are N -isogenous to E/\mathbf{C} .

Modular polynomials for genus 1

Knowledge of Φ_p for small primes p speeds up

- point counting for elliptic curves over finite fields
- computation of the Hilbert class polynomial
 - ◇ primality proving (ECPP)
 - ◇ constructing ‘crypto curves’.

Example: $\Phi_2 =$

$$\begin{aligned} &X^3 - X^2j^2 + 1488X^2j - 162000X^2 + 1488Xj^2 + 40773375Xj + \\ &+ 8748000000X + j^3 - 162000j^2 + 8748000000j \\ &- 15746400000000. \end{aligned}$$

Genus 1 \longrightarrow Genus 2

Gaudry, Schost: tailor-made variant of Φ_N for point counting.
Idea is similar to Atkin-Elkies' improvements to Schoof's algorithm.

Today's talk: *Direct generalization of Φ_N to genus 2. Definitions, properties, examples.*

Genus 2: symplectic group

A 2-dimensional principally polarized abelian variety (p.p.a.v.) A/\mathbf{C} can be given as \mathbf{C}^2/L with L a polarized lattice. Every p.p.a.v. arises this way.

The Hermitian form $L \times L \rightarrow \mathbf{Z}$ is given by the matrix

$$J = \begin{pmatrix} 0 & 1_2 \\ -1_2 & 0 \end{pmatrix}$$

for a suitably chosen basis.

The group

$$\mathrm{Sp}(4, \mathbf{Z}) = \{M \in \mathrm{GL}(4, \mathbf{Z}) \mid MJM^T = J\}$$

that respects the form is the *symplectic group*.

Genus 2: isomorphism classes

The group $\mathrm{Sp}(4, \mathbf{Z})$ acts on $\mathbf{H}_2 = \{\tau \in \mathrm{Mat}_2(\mathbf{C}) \mid \tau^T = \tau, \mathrm{Im}(\tau) > 0\}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau \stackrel{\mathrm{def}}{=} \frac{a\tau + b}{c\tau + d}.$$

The quotient $\mathrm{Sp}(4, \mathbf{Z}) \backslash \mathbf{H}_2$ is in bijection with the isomorphism classes of 2-dimensional p.p.a.v.'s via

$$\tau \mapsto A_\tau \stackrel{\mathrm{def}}{=} \mathbf{C}^2 / (\mathbf{Z}^2 + \mathbf{Z}^2 \tau).$$

Isotropic subspaces

The p -torsion of A/\mathbf{C} has rank 4 as \mathbf{F}_p -vector space. The space $A[p]$ is symplectic: the polarization of A induces a non-degenerate skew-symmetric bilinear (*symplectic*) form v .

A subspace $G \subset A[p]$ is called *isotropic* if $v|_G = 0$.

One-dimensional subspaces are always isotropic; not true for two-dimensional.

The kernel of a (p, p) -isogeny $A \rightarrow A'$ of p.p.a.v.'s is a 2-dimensional isotropic subspace of $A[p]$.

The subgroup of $\mathrm{GL}(4, \mathbf{F}_p)$ that respects v is $\mathrm{Sp}(4, \mathbf{F}_p)$.

Isotropic subspaces

Set $\Gamma^{(2)}(p) = \text{Ker}(\text{Sp}(4, \mathbf{Z}) \rightarrow \text{Sp}(4, \mathbf{F}_p))$ and

$$\Gamma_0^{(2)}(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Sp}(4, \mathbf{Z}) \mid c \equiv 0_2 \pmod{p} \right\} \supset \Gamma^{(2)}(p).$$

Lemma. *The index $[\text{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)]$ equals the number of 2-dimensional isotropic subspaces of \mathbf{F}_p^4 .*

Proof. Map $\Gamma_0^{(2)}(p)$ to $H \subset \text{Sp}(4, \mathbf{F}_p)$. The group H is parabolic and is (Borel-Tits) the stabilizer of a 2-dimensional isotropic subspace.

By Witt's extension theorem, $\text{Sp}(4, \mathbf{F}_p)$ permutes the 2-dimensional isotropic subspaces transitively. □

Isotropic subspaces

Set $S(p) = \{(A, G) \mid G \subset A[p] \text{ 2-dimensional and isotropic}\} / \cong$.

Theorem. *The map $\Gamma_0^{(2)}(p) \backslash \mathbf{H}_2 \rightarrow S(p)$ sending τ to the pair $(A_\tau, \langle (1/p, 0, 0, 0), (0, 1/p, 0, 0) \rangle)$ is bijective.*

Proof. Well-defined and injective: clear.

Surjective: every 2-dimensional p.p.a.v. occurs as some A_τ . Now apply the lemma. \square

The analogue of $Y_0(p)$ in genus 1 is

$$Y_0^{(2)}(p) \stackrel{\text{def}}{=} \Gamma_0^{(2)}(p) \backslash \mathbf{H}_2.$$

Baily-Borel: $Y_0^{(2)}(p)$ is a quasi-projective variety.

Igusa functions

Igusa: $Y_0^{(2)}(1) = \mathcal{A}_2$ has dimension 3 and function field $\mathbf{C}(j_1, j_2, j_3)$.

The functions $j_i : \mathbf{H}_2 \rightarrow \mathbf{P}^1(\mathbf{C})$ are rational functions in the 2-dimensional Eisenstein series. They have poles at τ corresponding to products of elliptic curves.

Definition. For $i = 1, 2, 3$ define $j_{i,p} : \mathbf{H}_2 \rightarrow \mathbf{P}^1(\mathbf{C})$ by $j_{i,p}(\tau) = j_i(p\tau)$.

The functions $j_{i,p}$ are $\Gamma_0^{(2)}(p)$ -invariant and satisfy

$$j_i(A_\tau / \langle (1/p, 0, 0, 0), (0, 1/p, 0, 0) \rangle) = j_i(A_{p\tau}) = j_{i,p}(\tau).$$

Igusa functions

Lemma. *The function field of $Y_0^{(2)}(p)$ equals $\mathbf{C}(j_1, j_2, j_3, j_{i,p})$ for every $i = 1, 2, 3$.*

Proof. General theory: the function field of $Y_0^{(2)}(p)$ has degree $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)]$ over $\mathbf{C}(j_1, j_2, j_3)$.

It suffices to show that the functions $j_{i,p}(\alpha\tau)$ are distinct for $\alpha \in \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$.

If two of them are equal, the stabilizer of $j_{i,p}$ is *larger* than $\Gamma_0^{(2)}(p)$.

The image of $\Gamma_0^{(2)}(p)$ inside $\mathrm{Sp}(4, \mathbf{F}_p)$ is *maximal* by Borel-Tits. \square

Modular polynomials for genus 2

Definition. *The minimal polynomial P_p of $j_{1,p}$ over $\mathbf{C}(j_1, j_2, j_3)$ is called the modular polynomial for j_1 .*

The functions $j_{2,p}$ and $j_{3,p}$ are contained in $\mathbf{C}(j_1, j_2, j_3)[j_{1,p}]$. Write

$$j_{2,p} = Q_p(j_{1,p}) \quad j_{3,p} = R_p(j_{1,p})$$

with $Q_p, R_p \in \mathbf{C}(j_1, j_2, j_3)[X]$ monic and of minimal degree.

Definition. *The polynomials Q_p and R_p are the modular polynomials for $j_{2,p}$ and $j_{3,p}$.*

Properties in genus 1

Properties of Φ_p :

- $\deg(\Phi_p) = p + 1$
- $\Phi_p \in \mathbf{Z}[j, X]$
- $\Phi_p(j, X) = \Phi_p(X, j)$.

Moduli interpretation:

The roots of $\Phi_p(j(E), X) \in \mathbf{C}[X]$ are the j -invariants of elliptic curves that are p -isogenous to E/\mathbf{C} .

Properties in genus 2: degree

Lemma. *We have $[\mathrm{Sp}(4, \mathbf{Z}) : \Gamma_0^{(2)}(p)] = (p^4 - 1)/(p - 1)$.*

Proof. We need to count the number of 2-dimensional isotropic subspaces of \mathbf{F}_p^4 .

Any two-dimensional subspace contains $(p^2 - 1)/(p - 1)$ lines.

Any line is contained in $(p^2 - 1)/(p - 1)$ isotropic subspaces.

The number of lines equals $(p^4 - 1)/(p - 1)$. □

Properties in genus 2: field of definition

The Igusa functions are rational functions in the *Eisenstein series* E_k for $k = 4, 6, 10, 12$.

The E_k 's have a Fourier series expansion

$$E_k(\tau) = \sum_T a(T) \exp(2\pi i \operatorname{Tr}(T\tau))$$

with $T \in \operatorname{Mat}_2(\frac{1}{2}\mathbf{Z})$ symmetric with integer diagonal entries.

The coefficients $a(T)$ are zero unless T is positive semi-definite.

The non-zero $a(T)$ can be given in terms of generalized Bernoulli-numbers. They are *rational*.

Properties in genus 2: field of definition

The Eisenstein series have a Laurent series expansion in q_1, q_2, q_3 .

The denominator of j_1, j_2, j_3 is a power of the *cuspidal form*

$$\chi_{10} = E_4 E_6 - E_{10}.$$

Every term of the expansion of χ_{10} is divisible by $q_1 q_2 q_3$.

Consequence. *The Igusa functions have a Laurent series expansion in q_1, q_2, q_3 with rational coefficients.*

Hence: $P_p, Q_p, R_p \in \mathbf{Q}(j_1, j_2, j_3)[X]$.

Properties in genus 2: moduli interpretation

The roots of $P_p(j_1(A), j_2(A), j_3(A), X)$ are j_1 -invariants of p.p.a.v.'s that are (p, p) -isogenous to A .

For such a root x , the triple

$$\begin{array}{c} x \\ Q_p(j_1(A), j_2(A), j_3(A), x) \\ R_p(j_1(A), j_2(A), j_3(A), x) \end{array}$$

determines a p.p.a.v. that is (p, p) -isogenous to A .

All (p, p) -isogenous p.p.a.v.'s arise in this way.

Explicit computations

Set $S = \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$. We have $P_p = \prod_{M \in S} (X - j_{1,p}(M\tau))$.

The polynomials

$$F_{k,p} = \sum_{M \in S} \left(\prod_{\substack{B \in S \\ B \neq M}} \frac{X - j_{1,p}(B\tau)}{j_{1,p}(M\tau) - j_{1,p}(B\tau)} \right) j_{k,p}(M\tau)$$

satisfy $F_{k,p}(j_{1,p}(M\tau)) = j_{k,p}(M\tau)$ for $k = 2, 3$ and all $M \in S$.

The coefficients of $F_{k,p}$ live in $\mathbf{Q}(j_1, j_2, j_3)$, and hence: $R_p = F_{2,p}$ and $Q_p = F_{3,p}$.

Explicit computations

Set

$$\tilde{F}_{k,p} = \sum_{M \in S} \left(\prod_{\substack{B \in S \\ B \neq M}} X - j_{1,p}(B\tau) \right) j_{k,p}(M\tau) \in \mathbf{Q}(j_1, j_2, j_3)[X].$$

We have $R_p = \tilde{F}_{2,p}/P'_p$ and $Q_p = \tilde{F}_{3,p}/P'_p$.

Conclusion: need to compute P_p , $\tilde{F}_{2,p}$ and $\tilde{F}_{3,p}$.

Explicit computations: denominators

A Jacobian A is (p, p) -split if A is (p, p) -isogenous to a product of elliptic curves.

The locus \mathcal{L}_p of such A is a 2-dimensional algebraic subvariety of \mathcal{A}_2 .

It is also known as the *Humbert surface* H_{p^2} . It can be given by an equation $L_p = 0$.

Lemma. *The denominators of the coefficients of $P_p, \tilde{F}_{2,p}, \tilde{F}_{3,p}$ are divisible by L_p .*

Explicit computations: denominators

Lemma. *The denominators of the coefficients of $P_p, \tilde{F}_{2,p}, \tilde{F}_{3,p}$ are divisible by L_p .*

Proof sketch. Let $\tau \in \mathbf{H}_2$ correspond to a (p, p) -split Jacobian.

For some $M \in \mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(p)$, the value $j_{1,p}(M\tau)$ is infinite.

The values $j_i(\tau)$ are finite, so the numerator of a coefficient is finite.

The denominator of a coefficient must vanish at τ . □

Computing L_2

Lemma. *If C has $(2, 2)$ -reducible Jacobian, then C can be given by*

$$Y^2 = X^6 - aX^4 + bX^2 - 1.$$

The Igusa-invariants of $\text{Jac}(C)$ are simple expressions in $u = ab$ and $v = a^3 + b^3$, like

$$j_1(\text{Jac}(C)) = \frac{(240 + 16u)^5}{64(27 - 18u - u^2 + 4v)^2}.$$

Compute a Gröbner basis for the $\mathbf{Q}[u, v, a, j_1, j_2, j_3]$ -ideal

$$\langle 64(27 - 18u - u^2 + 4v)^2 j_1 - (240 + 16u)^5, \dots, a64(27 - 18u - u^2 + 4v)^2 - 1 \rangle$$

for an order eliminating u, v, a .

Computing L_2

$$\begin{aligned} L_2 = & 236196j_1^5 - 972j_1^4j_2^2 + 5832j_1^4j_2j_3 + 19245600j_1^4j_2 - 8748j_1^4j_3^2 \\ & - 104976000j_1^4j_3 + 125971200000j_1^4 + j_1^3j_2^4 - 12j_1^3j_2^3j_3 \\ & - 77436j_1^3j_2^3 + 54j_1^3j_2^2j_3^2 + 870912j_1^3j_2^2j_3 - 507384000j_1^3j_2^2 \\ & - 108j_1^3j_2j_3^3 - 3090960j_1^3j_2j_3^2 + 2099520000j_1^3j_2j_3 + 81j_1^3j_3^4 \\ & + 3499200j_1^3j_3^3 + 78j_1^2j_2^5 - 1332j_1^2j_2^4j_3 + 592272j_1^2j_2^4 \\ & + 8910j_1^2j_2^3j_3^2 - 4743360j_1^2j_2^3j_3 - 29376j_1^2j_2^2j_3^3 + 9331200j_1^2j_2^2j_3^2 \\ & + 47952j_1^2j_2j_3^4 - 31104j_1^2j_3^5 - 159j_1j_2^6 + 1728j_1j_2^5j_3 \\ & - 41472j_1j_2^5 - 6048j_1j_2^4j_3^2 + 6912j_1j_2^3j_3^3 + 80j_2^7 - 384j_2^6j_3. \end{aligned}$$

Computing one coefficient c of P_2

It is easy to give a set of coset representatives for $\mathrm{Sp}(4, \mathbf{Z})/\Gamma_0^{(2)}(2)$.

We can compute $P_2(\{j_i(\tau)\}) \in \mathbf{C}[X]$ for any $\tau \in \mathbf{H}_2$.

Idea. Compute $P_2(\{j_i(\tau)\})$ for enough τ 's to reconstruct a coefficient c using *interpolation* techniques.

We need to know the ‘full’ denominator for the interpolation to work.

Dupont’s trick: fix $y, z \in \mathbf{Q}(i)$ and for many $x_k \in \mathbf{Q}(i)$ compute τ with

$$(j_1(\tau), j_2(\tau), j_3(\tau)) = (x_k, y, z).$$

Multivariate \longrightarrow Univariate

With Dupont's trick, we can evaluate the *univariate* function $c(X, y, z)$.

Compute the degree of numerator and denominator of c by computing the solution space of

$$\begin{pmatrix} 1 & \dots & x_1^m & -c(x_1, y, z) & \dots & -c(x_1, y, z)x_1^n \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & \dots & x_{m+n+2}^m & -c(x_{m+n+2}, y, z) & \dots & -c(x_{m+n+2}, y, z)x_{m+n+2}^n \end{pmatrix}$$

for increasing m, n and random $x_k \in \mathbf{Q}(i)$.

Some guessing

The degree in j_2 is 42 for all coefficients and 30 for j_3 . It varies for j_1 .

Guess. The denominator of c is $L_2^6 j_1^{\alpha(c)}$.

We can ‘check’ the guess by looking at the denominator of $c(x, y, z) \in \mathbf{Q}(i)$.

Computing the numerator is now easy: interpolation!

The degrees are large, so it takes a ‘long’ time.

Some results

The constant term of P_2 contains 16975 monomials.

The coefficients have up to 200 decimal digits.

They are *smooth*, like $2^{127} \cdot 3^{58} \cdot 5 \cdot 7 \cdot 13^{26}$, the coefficient of $j_1^{53} j_2 j_3^3$.

It takes 50 Megabytes to store the polynomials P_2, R_2, Q_2 .

Larger primes

Lemma. *If C has $(3, 3)$ -split Jacobian, then C can be given by*

$$Y^2 = (4X^3 + b^2X^2 + 2bX + 1)(X^3 + aX^2 + bX + 1).$$

Use the same Gröbner basis technique as for $p = 2$ to find L_3 .
The result needs more than 10 slides to display.

In principle, we can compute P_3, Q_3, R_3 without too much effort.

For $p \geq 7$ no explicit models for Humbert surfaces are known.

Question. Are these cases *intrinsically* more difficult?