Computing modular polynomials in dimension 2
ECC 2015, Bordeaux

Enea Milio

29/09/2015

Computing modular polynomials

1. Dimension 1 : elliptic curves

2. Dimension 2 : abelian surfaces
   - Computation of the modular polynomials
   - Smaller invariants

3. Real Multiplication : cyclic isogenies

Computing modular polynomials

Motivation

An **isogeny** between two elliptic curves E_1 and E_2 is a surjective map with finite kernel. The **degree** of the isogeny is the cardinality of the kernel.

Many applications :

- Theory ;
- Cryptography : transfert the DLP ;
- SEA algorithm ;
- Class polynomials ;
- Graph of isogenies.

Motivation

For cryptography, we work over finite fields.

Here, we work on $\mathbb{C}$.

- The theory is "easy" on $\mathbb{C}$;
- Numerical computation ;
- The modular polynomials can be reduced modulo p.

Complex elliptic curves

Let $\mathcal{H}_1 = \{a + \imath b : b > 0\} \subset \mathbb{C}$ be the **Poincaré half plane**.

Proposition

Let $E/\mathbb{C}$ be an elliptic curve.
Then there exists a lattice

$$\Lambda = \mathbb{Z} + \tau\mathbb{Z}, \qquad \textit{where} \quad \tau \in \mathcal{H}_1$$

and a complex analytic isomorphism $E \simeq \mathbb{C}/\Lambda$ of complex Lie groups.

Isomorphism

Modular group : $\mathrm{SL}_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}, ad - bc = 1\}$

Group action :

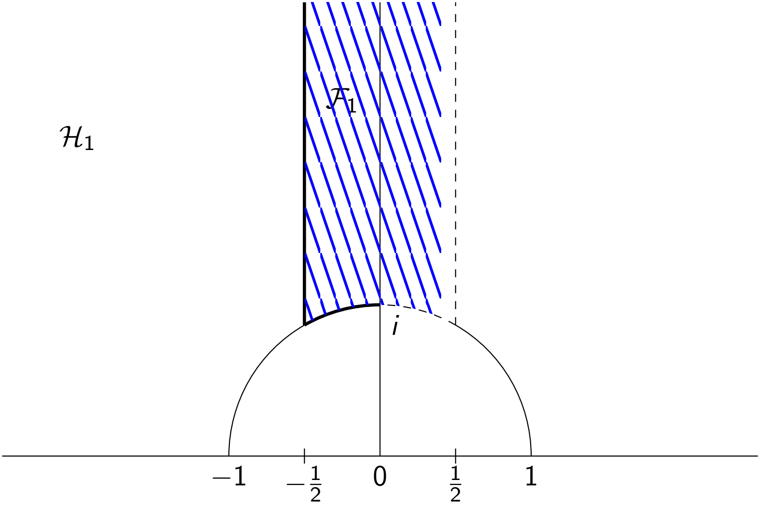
$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H}_1 & \longrightarrow & \mathcal{H}_1 \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \tau & = & \frac{a\tau+b}{c\tau+d} \end{array}$$

Proposition

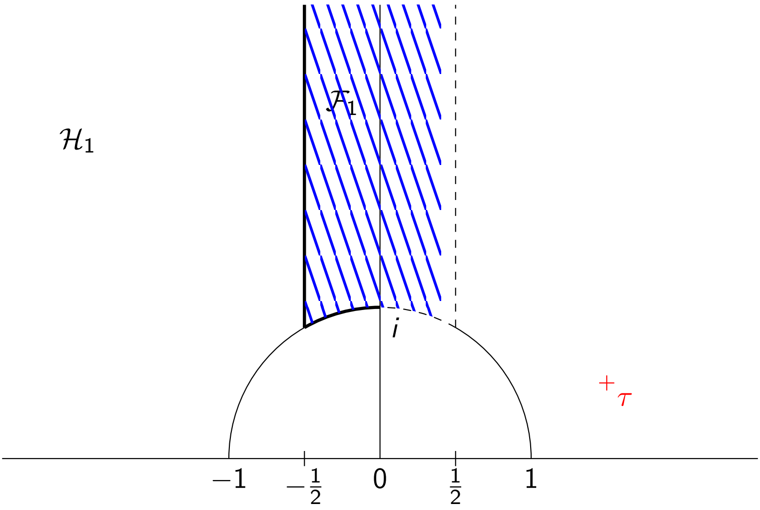
Two elliptic curves E_1 and E_2 over $\mathbb{C}$ corresponding to the lattices $\Lambda_1 = \mathbb{Z} + \tau_1\mathbb{Z}$ and $\Lambda_2 = \mathbb{Z} + \tau_2\mathbb{Z}$ are **isomorphic** *if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_2 = \gamma\tau_1$.*

$\Longrightarrow$ change of basis of the lattice.

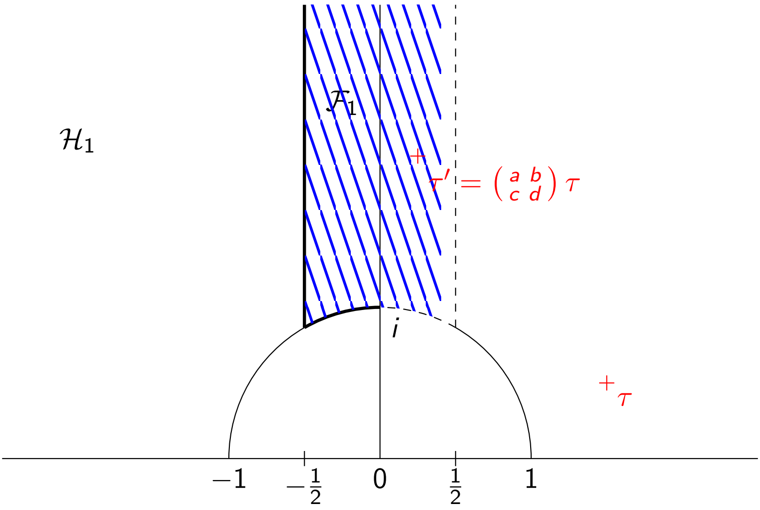
Fundamental domain $\mathcal{F}_1$



Fundamental domain $\mathcal{F}_1$



Fundamental domain $\mathcal{F}_1$



Modular function

Let p be a prime and

$$\Gamma_0(p) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod p \right\}.$$

Definition

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of finite index.
$f : \mathcal{H}_1 \to \mathbb{C}$ is a **modular function** *for Γ if*

1. *f is meromorphic on $\mathcal{H}_1$ (and on the cusps);*
2. *for all $\gamma \in \Gamma$ and $\tau \in \mathcal{H}_1$, $f(\gamma\tau) = f(\tau)$.*

Example

- *$j(\tau)$ is a modular function for $\mathrm{SL}_2(\mathbb{Z})$;*
- *$j_p(\tau) := j(p\tau)$ is a modular function for $\Gamma_0(p)$.*

Modular function

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of finite index. Denote by $\mathbb{C}_\Gamma$ the field of modular functions for Γ. Then

Theorem

- $\mathbb{C}_{\mathrm{SL}_2(\mathbb{Z})} = \mathbb{C}(j)$;
- $\mathbb{C}_{\Gamma_0(p)} = \mathbb{C}(j, j_p)$.

Isogeny

We are interested in the isogenies of degree p.

Let C_p be a set of representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(p)$.

The isogenous points of degree p are : $p\gamma\tau$, $\gamma \in \mathrm{C}_p$.

Theorem

The field extension $\mathbb{C}_{\Gamma_0(p)}/\mathbb{C}_{\mathrm{SL}_2(\mathbb{Z})} = \mathbb{C}(j, j_p)/\mathbb{C}(j)$ *is algebraic of degree* $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$.

Conjugate functions of j_p in $\mathbb{C}_{\Gamma_0(p)}/\mathbb{C}_{\mathrm{SL}_2(\mathbb{Z})}$: $j_p^\gamma(\tau) := j(p\gamma\tau)$, $\gamma \in \mathrm{C}_p$.

Modular polynomial

The **classical modular polynomial** of index p is the polynomial Φ_p that parameterizes isomorphism classes of elliptic curves together with an isogeny of degree p :

$$\Phi_p(X, j(E)) = \prod_{E' \; p-\text{isogenous to } E} (X - j(E')).$$

It is also the minimal polynomial of j_p for the extension $\mathbb{C}_{\Gamma_0(p)}/\mathbb{C}_{\mathrm{SL}_2(\mathbb{Z})}$, thus

$$\Phi_p(X, j) = \prod_{\gamma \in \mathrm{C}_p} (X - j_p^{\gamma}) \in \mathbb{Z}[X, j].$$

Algorithm

Computation of the modular polynomials by evaluation/interpolation (Enge 2009).

$$\Phi_p(X,j) = \prod_{\gamma\in \mathrm{C}_p} (X - j_p^{\gamma}) = X^{p+1} + \sum_{i=0}^{p} c_i(j)X^i.$$

- Evaluate :

$$\prod_{\gamma\in \mathrm{C}_p} (X - j(p\gamma\tau)) = X^{p+1} + \sum_{i=0}^{p} c_i(j(\tau))X^i;$$

$\Rightarrow$ Evaluate in $\deg_j(\Phi_p) + 1 = (p+1) + 1$ values τ.

- Interpolate c_i.

Evaluation of j in $\tilde{O}(N)$ at precision N digits (Dupont 2006) ; Algorithm quasi-linear : $\tilde{O}(p^3)$.

Examples

$p = 2$ $\Phi_2(X, Y) = X^3 + (-Y^2 + 1488Y - 162000)X^2 + (1488Y^2 + 40773375Y + 8748000000)X + (Y^3 - 162000Y^2 + 8748000000Y - 157464000000000)$

$p = 3$ $\Phi_3(X, Y) = X^4 + (-Y^3 + 2232Y^2 - 1069956Y + 36864000)X^3 + (2232Y^3 + 2587918086Y^2 + 8900222976000Y + 452984832000000)X^2 + (-1069956Y^3 + 8900222976000Y^2 - 770845966336000000Y + 1855425871872000000000)X + (Y^4 + 36864000Y^3 + 452984832000000Y^2 + 1855425871872000000000Y)$

$p = 5$ $\Phi_5(X, Y) =$
$X^6 + (-Y^5 + 3720Y^4 - 4550940Y^3 + 2028551200Y^2 - 246683410950Y + 1963211489280)X^5 + (3720Y^5 + 1665999364600Y^4 + 107878928185336800Y^3 + 383083609779811215375Y^2 + 128541798906828816384000Y + 1284733132841424456253440)X^4 + (-4550940Y^5 + 107878928185336800Y^4 - 441206965512914835246100Y^3 + 26898488858380731577417728000Y^2 - 192457934618928299655108231168000Y + 280244777828439527804321565297868800)X^3 + (2028551200Y^5 + 383083609779811215375Y^4 + 26898488858380731577417728000Y^3 + 5110941777552418083110765199360000Y^2 + 36554736583949629295706472332656640000Y + 6692500042627997708487149415015068467200)X^2 + (-246683410950Y^5 + 128541798906828816384000Y^4 - 192457934618928299655108231168000Y^3 + 36554736583949629295706472332656640000Y^2 - 264073457076620596259715790247978782949376Y + 53274330803424425450420160273356509151232000)X + (Y^6 + 1963211489280Y^5 + 1284733132841424456253440Y^4 + 280244777828439527804321565297868800Y^3 + 6692500042627997708487149415015068467200Y^2 + 53274330803424425450420160273356509151232000Y + 141359947154721358697753474691071362751004672000)$

Other invariants : Schläfli, Weber, theta functions.

Schläfli 1870, $p = 5$: $x^6 - x^5y^5 + 4xy + y^6$.

Computing modular polynomials

Computing modular polynomials

Motivation

Dimension 2 : principally polarized abelian surfaces (ppas) $\implies$ Jacobian of hyperelliptic curves of genus 2 (or product of elliptic curves) ;

Cryptography : competitive with elliptic curves ;

$\implies$ we want to do the same thing !

Siegel space

Siegel upper half-space $\mathcal{H}_2$ the set of 2×2 symmetric matrices over $\mathbb{C}$ with positive definite imaginary part.

Ppas on $\mathbb{C}$: $A \simeq \mathbb{C}^2/\Lambda$ where $\Lambda = \mathbb{Z}^2 + \Omega\mathbb{Z}^2$, with $\Omega \in \mathcal{H}_2$ (**period matrix**).

Let $J = \begin{pmatrix} 0 & Id_2 \\ -Id_2 & 0 \end{pmatrix}$. **Symplectic group :**

$$\mathrm{Sp}_4(\mathbb{Z}) = \{\gamma \in \mathrm{GL}_4(\mathbb{Z}) : \, {}^t\gamma J \gamma = J\}.$$

Group action : $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \Omega = (A\Omega + B)(C\Omega + D)^{-1}$.

We have a fundamental domain $\mathcal{F}_2$.

Siegel modular threefold : $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$.

Modular forms and functions

Let Γ be a subgroup of finite index of $\mathrm{Sp}_4(\mathbb{Z})$ and $k \in \mathbb{Z}$.

Definition

A **Siegel modular form** *of weight k for Γ is a function $f : \mathcal{H}_2 \to \mathbb{C}$ such that :*

1. *f is holomorphic on $\mathcal{H}_2$;*
2. $f(\gamma\Omega) = \det(C\Omega + D)^k f(\Omega)$, $\quad \forall \gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ *and* $\Omega \in \mathcal{H}_2$.

Definition

Siegel modular function *for Γ : $f = \frac{f_1}{f_2}$ quotient of Siegel modular forms of same weight. Thus,* $f(\gamma\Omega) = f(\Omega)$.

Theta functions

Theta functions (of characteristic $\frac{1}{2}$) :

Define for $a = (a_0, a_1)$ and $b = (b_0, b_1)$ in $\{0,1\}^2$:

$$\theta_{b_0+2b_1+4a_0+8a_1}(\Omega) = \sum_{n \in \mathbb{Z}^2} \exp(\imath\pi\, {}^t(n+\frac{a}{2})\Omega(n+\frac{a}{2}) + \imath\pi\, {}^t(n+\frac{a}{2})b)$$

- 16 theta functions ;
- 6 are identically zero ;
- $\mathcal{P} = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$;
- θ_i^2 = Siegel modular form of weight 1 for $\Gamma(2,4)$.

$$\Gamma(2,4) = \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) : \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv Id_4 \bmod 2, B_0 \equiv C_0 \equiv 0 \bmod 4 \right\}.$$

Theta functions

Let

$$h_{10} = \prod_{i \in \mathcal{P}} \theta_i^2,$$

$$h_4 = \sum_{i \in \mathcal{P}} \theta_i^8,$$

$$h_6 = \sum_{60 \text{ triples } (i,j,k) \in \mathcal{P}^3} \pm(\theta_i \theta_j \theta_k)^4,$$

$$h_{12} = \sum_{15 \text{ tuples } (i,j,k,l,m,n) \in \mathcal{P}^6} (\theta_i \theta_j \theta_k \theta_l \theta_m \theta_n)^4.$$

$\Rightarrow$ h_i is a Siegel modular form of weight i for the group $\mathrm{Sp}_4(\mathbb{Z})$.

Generalization of the j-invariant

Definition

We call **Igusa invariants**, *or j-invariants, the Siegel modular functions j_1, j_2, j_3 for $\mathrm{Sp}_4(\mathbb{Z})$ defined by*

$$j_1 := \frac{h_{12}^5}{h_{10}^6}, \quad j_2 := \frac{h_4 h_{12}^3}{h_{10}^4}, \quad j_3 := \frac{(h_{12}h_4 - 2h_6 h_{10})h_{12}^2}{3h_{10}^4}.$$

Theorem (Igusa 1962, Spallek 1994)

The field of Siegel modular functions invariant by $\mathrm{Sp}_4(\mathbb{Z})$ is $\mathbb{C}(j_1, j_2, j_3)$.

Generically, two ppas have the same j-invariants if and only if they are isomorphic.

Isogeny

The functions

$$j_{\ell,p}(\Omega) := j_\ell(p\Omega), \quad \ell = 1, 2, 3,$$

are Siegel modular functions for $\Gamma_0(p)$, where

$$\Gamma_0(p) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) \in \mathrm{Sp}_4(\mathbb{Z}) : C \equiv 0 \bmod p \right\}$$

is of index $[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0(p)] = p^3 + p^2 + p + 1$.

Ppas (p, p)-isogenous to Ω : $p\gamma\Omega$, where $\gamma \in \mathrm{C}_p = \mathrm{Sp}_4(\mathbb{Z})/\Gamma_0(p)$.

Theorem (Bröker-Lauter 2009)

The field of Siegel modular functions invariant by $\Gamma_0(p)$ is $\mathbb{C}(j_1, j_2, j_3, j_{1,p})$.

We define

$$j^{\gamma}_{\ell,p}(\Omega) := j_\ell(p\gamma\Omega), \quad \ell = 1, 2, 3.$$

Modular polynomials in dimension 2

$$\Phi_{1,p}(X) = \prod_{\gamma \in \mathrm{C}_p} (X - j_{1,p}^{\gamma}),$$

(minimal polynomial of the extension $\mathbb{C}(j_1, j_2, j_3, j_{1,p})/\mathbb{C}(j_1, j_2, j_3)$),

$$\text{and for } \ell = 2, 3, \qquad \Psi_{\ell,p}(X) = \sum_{\gamma \in \mathrm{C}_p} j_{\ell,p}^{\gamma} \prod_{\gamma' \in \mathrm{C}_p \setminus \{\gamma\}} (X - j_{1,p}^{\gamma'}).$$

Proposition (Bröker-Lauter 2009)

$\Phi_{1,p}, \Psi_{2,p}, \Psi_{3,p} \in \mathbb{Q}(j_1, j_2, j_3)[X]$.

We have $j_{\ell,p}^{\gamma}(\Omega) =$
$\Psi_{\ell,p}(j_{1,p}^{\gamma}(\Omega), j_1(\Omega), j_2(\Omega), j_3(\Omega))/\Phi'_{1,p}(j_{1,p}^{\gamma}(\Omega), j_1(\Omega), j_2(\Omega), j_3(\Omega))$.

Algorithm

How to compute the modular polynomials ?

Evaluation/interpolation :

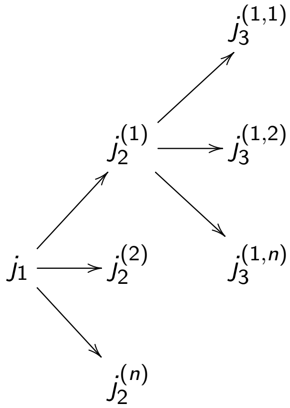
$$\Phi_{1,p}(X, j_1(\Omega), j_2(\Omega), j_3(\Omega)) = X^{p^3+p^2+p+1} + \sum_{i=0}^{p^3+p^2+p} c_i(j_1(\Omega), j_2(\Omega), j_3(\Omega))X^i.$$

where $c_i \in \mathbb{Q}(j_1, j_2, j_3)$.

Problem : Interpolation of trivariate rational fractions.

Interpolation

We can not choose the matrices Ω as we want !



Complexity

Inversion : $(j_1(\Omega), j_2(\Omega), j_3(\Omega)) \longrightarrow \Omega$ in $\tilde{O}(N)$ (Dupont 2006).

Fast evaluation of the Igusa invariants : $\tilde{O}(N)$ (Dupont 2006, Enge–Thomé 2014).

Complexity of the computation of the modular polynomials : $\tilde{O}(d_{j_1} d_{j_2} d_{j_3} p^3 N)$.

Streng invariants

The modular polynomials have been computed by Dupont for $p = 2$ only. For $p = 3$ they are too big.

Other invariants?

$\Rightarrow$ Streng 2010 :

$$i_1 := \frac{h_4 h_6}{h_{10}}, \quad i_2 := \frac{h_4^2 h_{12}}{h_{10}^2}, \quad i_3 := \frac{h_4^5}{h_{10}^2}.$$

while Igusa :

$$j_1 := \frac{h_{12}^5}{h_{10}^6}, \quad j_2 := \frac{h_4 h_{12}^3}{h_{10}^4}, \quad j_3 := \frac{(h_{12} h_4 - 2 h_6 h_{10}) h_{12}^2}{3 h_{10}^4}.$$

Theorem

The field of Siegel modular functions is $\mathbb{C}(j_1, j_2, j_3) = \mathbb{C}(i_1, i_2, i_3)$.

Comparison

For $p = 3 : \Phi_{1,3}(X, f_1, f_2, f_3) = X^{40} + \sum_{i=0}^{39} c_i(f_1, f_2, f_3)X^i$.

i	j_1	i_1	j_2	i_2	j_3	i_3
0	394	61	288	32	278	32
1	302	61	286	32	276	31
2	302	61	286	32	276	31
⋮	⋮		⋮			⋮
37	268	41	382	22	253	21
38	263	36	375	21	248	19
39	257	31	367	20	243	17

Memory space :

- $p = 2$: 2.1 MB against 57 MB.
- $p = 3$: 890 MB.

Denominators

- Denominators for Igusa invariants for $p = 2$:

$$j_1^\alpha D_2(j_1, j_2, j_3)^6 \text{ (}\alpha\text{ ranging between 5 and 21)}$$

- Denominators for Streng invariants for $p = 2$:

$$i_3^\alpha D_2(i_1, i_2, i_3) \text{ and } i_3^\alpha D_2(i_1, i_2, i_3)^2 \text{ (}\alpha\text{ varies from 0 to 3)}$$

- Denominators for Streng invariants for $p = 3$:

$$i_3^\alpha D_3(i_1, i_2, i_3)^2 \text{ and } i_3^\alpha D_3(i_1, i_2, i_3)^4 \text{ (}\alpha\text{ varies from 0 to 4)}$$

Examples

$D_2(Ig) = 236196 j_1^5 + (-972 j_2^2 + (5832 j_3 + 19245600) j_2 + (-8748 j_3^2 - 104976000 j_3 + 125971200000)) j_1^4 + (j_2^4 + (-12 j_3 - 77436) j_2^3 + (54 j_3^2 + 870912 j_3 - 507384000) j_2^2 + (-108 j_3^3 - 3090960 j_3^2 + 2099520000 j_3) j_2 + (81 j_3^4 + 349920 j_3^3)) j_1^3 + (78 j_2^5 + (-1332 j_3 + 592272) j_2^4 + (8910 j_3^2 - 4743360 j_3) j_2^3 + (-29376 j_3^3 + 9331200 j_3^2) j_2^2 + 47952 j_3^4 j_2 - 31104 j_3^5) j_1^2 + (-159 j_2^6 + (1728 j_3 - 41472) j_2^5 - 6048 j_3^2 j_2^4 + 6912 j_3^3 j_2^3) j_1 + (80 j_2^7 - 384 j_3 j_2^6).$

$D_2(Str) = (24576 i_3 i_1^5 + (96 i_2^3 - 4608 i_3 i_2) i_1^4 + (-6220800 i_3 i_2 - 12288 i_3^2) i_1^3 + (-23328 i_2^4 - 48 i_3 i_2^3 + 1088640 i_3 i_2^2 + 2304 i_3^2 i_2 + 24883200 i_3^2) i_1^2 + (93312 i_3 i_2^3 + 419904000 i_3 i_2^2 - 5909760 i_3^2 i_2 + (1536 i_3^3 - 8398080000 i_3^2)) i_1 + (1417176 i_2^5 - 5832 i_3 i_2^4 + (6 i_3^2 - 94478400 i_3) i_2^3 + 287712 i_3^2 i_2^2 + (-288 i_3^3 + 1154736000 i_3^2) i_2 + (-248832 i_3^3 + 755827200000 i_3^2))).$

$D_3(Str) = 1073741824i_1^{13}i_2i_3 + 1048576i_1^{12}i_2^4 - 100663296i_1^{12}i_2^2i_3 -$
$805306368i_1^{12}i_3^2+23653961957376i_1^{11}i_2^2i_3-1610612736i_1^{11}i_2i_3^2+391378894848i_1^{11}i_3^2+$
$23123460096i_1^{10}i_2^5-1572864i_1^{10}i_2^4i_3-2220871385088i_1^{10}i_2^3i_3+150994944i_1^{10}i_2^2i_3^2+$
$1912538199490560i_1^{10}i_2i_3^2+1207959552i_1^{10}i_3^3-39627113103360i_1^{10}i_3^2+1885039755264i_1^9i_2^4i_3+$
$217027664414244864i_1^9i_2^3i_3-113664992477184i_1^9i_2^2i_3^2+1006632960i_1^9i_2i_3^3-$
$152617815730248744960i_1^9i_2i_3^2-1448199755661312i_1^9i_3^3+212468467875840i_1^8i_2^6+$
$65691648000i_1^8i_2^5i_3+983040i_1^8i_2^4i_3^2-169468806884327424i_1^8i_2^4i_3-6305124188160i_1^8i_2^3i_3^2-$
$94371840i_1^8i_2^2i_3^3 + 552004832446119936i_1^8i_2^2i_3^2 - 853581062209536i_1^8i_2i_3^3 +$
$2192102843693456141844480i_1^8i_2i_3^2-754974720i_1^8i_3^4+115173392856354127872i_1^8i_3^3-$
$13232363778146304i_1^7i_2^5i_3-784286613504i_1^7i_2^4i_3^2+3201946631712311279616i_1^7i_2^4i_3+$
$1917038253511802880i_1^7i_2^3i_3^2+21388245073920i_1^7i_2^2i_3^3+1907360734639457917992960i_1^7i_2^2i_3^2-$
$335544320i_1^7i_2i_3^4+298045608749759987712i_1^7i_2i_3^3+602576730980352i_1^7i_3^4-$
$16997813388479467440046080i_1^7i_3^3+10412017268255539 20i_1^6i_2^7+634990989219840i_1^6i_2^6i_3-$
$52624982016i_1^6i_2^5i_3^2+28332185178888128102 4i_1^6i_2^5i_3-327680i_1^6i_2^4i_3^3+220052660032438272i_1^6i_2^4i_3^2+$
$5051361263616i_1^6i_2^3i_3^3-190938200244582471892992i_1^6i_2^3i_3^2+31457280i_1^6i_2^2i_3^4-$
$38286251079255982080i_1^6i_2^2i_3^3 - 7784410537473661314263900160i_1^6i_2^2i_3^2 -$
$81096968503296i_1^6i_2i_3^4-6268888273473709362118656i_1^6i_2i_3^3+251658240i_1^6i_3^5-$
$215987170489694945280i_1^6i_3^4+8046545760301777811295436 80i_1^6i_3^3-15017559155950054809 6i_1^5i_2^6i$
$10569523360776192i_1^5i_2^5i_3^2-4638615481599896235073536i_1^5i_2^5i_3-118674948096i_1^5i_2^4i_3^3+$
$9503957409357763952640i_1^5i_2^4i_3^2+2941904259840540672i_1^5i_2^3i_3^3+3618779438490652637954187264i$
$22887256817664i_1^5i_2^2i_3^4+1557150937623844175609856i_1^5i_2^2i_3^3+62914560i_1^5i_2i_3^5-$
$86670799689200173056i_1^5i_2i_3^4+78210945482001523924713209856i_1^5i_2i_3^3+$
$91081207185408i_1^5i_3^5+4566207265162884601085952i_1^5i_3^4-80900957611133776805681037312i_1^5i_3^3+$
$2870105097548602679040i_1^4i_2^8+896261713716314880i_1^4i_2^7i_3+1880971493524992i_1^4i_2^6i_3^2+$
$2559594048233864351947776i_1^4i_2^6i_3+11221327872i_1^4i_2^5i_3^3+780494067727704797184i_1^4i_2^5i_3^2+$
$61440i_1^4i_2^4i_3^4-273088658240188416i_1^4i_2^4i_3^3-398708239387678826603145984i_1^4i_2^4i_3^2-$
$1077088223232i_1^4i_2^3i_3^4+8443058316853636251648i_1^4i_2^3i_3^3+465201647880516504082693373644 8i_1^4i_2^3i$
$5898240i_1^4i_2^2i_3^5-13387967790199603 2i_1^4i_2^2i_3^4-36831815040167945837868423168i_1^4i_2^2i_3^3+$
$82081531035648i_1^4i_2i_3^5+2449653429540496482238464i_1^4i_2i_3^4-1811217712379191892949216756695$
$47185920i_1^4i_3^6+71004250037730410496i_1^4i_3^5-56148085403579776990704795648i_1^4i_3^4-$
$193303195584228338932224i_1^3i_2^7i_3+90123759266066684928i_1^3i_2^6i_3^2+86253682640195233723228416$
$7400456973692928i_1^3i_2^5i_3^3-13398162297286395745575936i_1^3i_2^5i_3^2+88576229376i_1^3i_2^4i_3^4-$
$14192373000496360845312i_1^3i_2^4i_3^3-28914635435703118905668650905 60i_1^3i_2^4i_3^2+$
$8830817872221634 56i_1^3i_2^3i_3^4+5995098052733571847066939392i_1^3i_2^3i_3^3-8811853774848i_1^3i_2^2i_3^5-$
$1400003098553579221647360i_1^3i_2^2i_3^4+97479251470446402968352866672640i_1^3i_2^2i_3^3-$
$6291456i_1^3i_2i_3^6+33166148344289427456i_1^3i_2i_3^5+19743632405446596697071747072i_1^3i_2i_3^4+$
$105529273322620022295815917468569600i_1^3i_2i_3^3-68018900041728i_1^3i_3^6-$
$2349627765367941191172096i_1^3i_3^5+160080105674658429821334465478656i_1^3i_3^4+$
$4219485009161078228590656i_1^2i_2^9-46639207835164793534 40i_1^2i_2^8i_3-8349593486170324608i_1^2i_2^7i_3^2-$
$2594927222047499837745975552i_1^2i_2^7i_3+168462522797184i_1^2i_2^6i_3^3+3615767749123322594310432i_1^2$
$300837888i_1^2i_2^5i_3^4-215921145233199135744i_1^2i_2^5i_3^3+616229927403745317212702913984i_1^2i_2^5i_3^2-$
$6144i_1^2i_2^4i_3^5+10665677157580800i_1^2i_2^4i_3^4-487539271451605190224113792i_1^2i_2^4i_3^3+$
$597249336471120770783168754827136i_1^2i_2^4i_3^2+28860530688i_1^2i_2^3i_3^5+186470378203297558376448i_1^2$
$16808787545488790224850857944576i_1^2i_2^3i_3^3+589824i_1^2i_2^2i_3^6-2882413394767282176i_1^2i_2^2i_3^5-$
$249601482395717764722799104i_1^2i_2^2i_3^4-547750487312356146660294997708396 80i_1^2i_2^2i_3^3-$
$9840529244160i_1^2i_2i_3^6+1200618490930489311952896i_1^2i_2i_3^5-5716111833495176039610782117068 8$
$4718592i_1^2i_3^7-2059885059165860 6592i_1^2i_3^6+1756148202989834383269273600i_1^2i_3^5-$
$146528474346150169055177586688358400i_1^2i_3^4+317226969698885826116654304i_1i_2^8i_3-$
$178977835709619524148384i_1i_2^7i_3^2+3124836357738656041461702205440i_1i_2^7i_3+$
$80327353040040889728i_1i_2^6i_3^3-52049511457475420205500787648i_1i_2^6i_3^2-$
$171351407729664i_1i_2^5i_3^4+31066479848877793459524864i_1i_2^5i_3^3-17182126661344900461156343499$
$9835831296i_1i_2^4i_3^5-7865818063161388895232i_1i_2^4i_3^4+1084885263822875380568914521600i_1i_2^4i_3^3+$
$26769697166776320i_1i_2^3i_3^5-350507041737785106690571776i_1i_2^3i_3^4+854063297390456990431843334$
$859222867968i_1i_2^2i_3^6-158918678997153812471808i_1i_2^2i_3^5+6034098811311665176411960989696i_1i$
$8219687635411560887978987415249552000i_1i_2^2i_3^3+262144i_1i_2i_3^7-1758652150455042048i_1i_2i_3^6-$
$1374354304441055536139034624i_1i_2i_3^5+44067183709700749413582229123077120i_1i_2i_3^4+$
$7553536229376i_1i_3^7-311886510373696391479296i_1i_3^6-5938917592170743659134396997632i_1i_3^5+$
$44934202777922750168136710661864960000i_1i_3^4+2584698285924232982401063716i_2^{10}-$
$10764481642689341617256844i_2^9i_3+11471581029841035951969i_2^8i_3^2-364122297955518385909414$
$551124377010071568i_2^7i_3^3+1366656586959783418027410924i_2^7i_3^2+10122995873376i_2^6i_3^4-$
$1396299980777369520070152i_2^6i_3^3+10083133967459042825973517961268i_2^6i_3^2-$
$83047680i_2^5i_3^5-3420729739797762816i_2^5i_3^4-23288737190432645290652458416i_2^5i_3^3+$
$58879180974264105377458087129861488i_2^5i_3^2+256i_2^4i_3^6-2818796161673088i_2^4i_3^5+$
$19128585162994430843368656i_2^4i_3^4-249217801853496426807044659839576i_2^4i_3^3+$
$7973572608i_2^3i_3^6+58267829903861357475 84i_2^3i_3^5-14850932330520519874373790144i_2^3i_3^4-$
$412301901384482808596505385031449200i_2^3i_3^3-24576i_2^2i_3^7+169510614703349760i_2^2i_3^6+$
$227795857854991291357100928i_2^2i_3^5-2175526599854742507306371238190944i_2^2i_3^4+$
$63764692992i_2i_3^7+43405460712485963808768i_2i_3^6+1477862393729354088693012596736i_2i_3^5-$
$5673335901704124338996627108519232000i_2i_3^4-196608i_3^8+1418239425570766848i_3^7-$
$6324413850721664271452160i_3^6+1498018164069949798113492863030784i_3^5-$
$3883782492464424496895506065638925150000i_3^4$

Computing modular polynomials

Alternative invariants

$\Rightarrow$ look at modular functions for another group.

$b_i(\Omega) := \frac{\theta_i(\Omega/2)}{\theta_0(\Omega/2)}$, $i = 1, 2, 3$.

Modular functions for $\Gamma(2,4)$.

Modular polynomials with b_1, b_2, b_3

Theorem (Mumford, Manni)

The field of modular functions invariant by $\Gamma(2,4)$ is $\mathbb{C}(b_1, b_2, b_3)$.

We look at $\mathrm{C}_p = \Gamma(2,4)/(\Gamma_0(p) \cap \Gamma(2,4))$, $p > 2$.

The index is still $p^3 + p^2 + p + 1$.

Proposition

The field of modular functions invariant by $\Gamma_0(p) \cap \Gamma(2,4)$ is $\mathbb{C}(b_1, b_2, b_3, b_{1,p})$.

We compute $\Phi_{1,p}(X, b_1, b_2, b_3) = \prod_{\gamma \in \mathrm{C}_p} (X - b_{1,p}^{\gamma})$ and $\Psi_{\ell,p}(X, b_1, b_2, b_3) = \sum_{\gamma \in \mathrm{C}_p} b_{\ell,p}^{\gamma} \prod_{\gamma' \in \mathrm{C}_p \setminus \{\gamma\}} (X - b_{1,p}^{\gamma'})$. They are in $\mathbb{Q}(b_1, b_2, b_3)[X]$.

Algorithm

- Evaluation of the b_i in $\tilde{O}(N)$ (Dupont 2006, Enge–Thomé 2014).

- Inversion : $(b_1, b_2, b_3)(\Omega) \longrightarrow \Omega$?

$(b_1, b_2, b_3)(\Omega) \longrightarrow (j_1, j_2, j_3)(\Omega) \longrightarrow \Omega \bmod \mathrm{Sp}_4(\mathbb{Z})$.

Problem : we want Ω mod $\Gamma(2, 4)$!

Solutions :

- Compute $b_i(\gamma\Omega)$ for $\gamma \in \mathrm{Sp}_4(\mathbb{Z})/\Gamma(2, 4)$. But index 11520 !
- Use of functional equation of the theta functions.

Denominators with the theta functions

Polynomials computed for $p = 3, 5, 7$.

Always D_p in the denominator.

$$D_3(b_1, b_2, b_3) = 64(b_1^2 b_2^2 b_3^2)(16 b_1^4 b_2^4 b_3^4 + 1)(b_1^4 + b_2^4 + b_3^4)$$
$$-32(48 b_1^4 b_2^4 b_3^4 + 16 b_1^2 b_2^2 b_3^2 + 1)(b_1^4 b_2^4 + b_1^4 b_3^4 + b_2^4 b_3^4)+$$
$$256(b_1^8 b_2^8 + b_1^8 b_3^8 + b_2^8 b_3^8) + 32(b_1^4 b_2^4 b_3^4)(-24 b_1^4 b_2^4 b_3^4 + 80 b_1^2 b_2^2 b_3^2 + 13) + 1.$$

It is symmetric and there are relations modulo 2 and 4 between the exponents.

Symmetries

Theorem (M. 2014)

For all prime p, we have $\Phi_{1,p}(X, b_1, b_2, b_3) = \Phi_{1,p}(X, b_1, b_3, b_2)$ *and* $\Psi_{2,p}(X, b_1, b_3, b_2) = \Psi_{3,p}(X, b_1, b_2, b_3)$.

Proof : there always exist $\gamma \in \mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$ such that for all $\Omega \in \mathcal{H}_2$:

$$\begin{array}{rcl} b_1(\gamma\Omega) & = & b_1(\Omega) \\ b_2(\gamma\Omega) & = & b_3(\Omega) \\ b_3(\gamma\Omega) & = & b_2(\Omega) \end{array} \quad \text{and} \quad \begin{array}{rcl} b_{1,p}(\gamma\Omega) & = & b_{1,p}(\Omega) \\ b_{2,p}(\gamma\Omega) & = & b_{3,p}(\Omega) \\ b_{3,p}(\gamma\Omega) & = & b_{2,p}(\Omega) \end{array}$$

$\Phi_{1,p}$ is a minimal polynomial.
$\Psi_{\ell,p}(b_{1,p}) = b_{\ell,p}\Phi'_{1,p}(b_{1,p})$ for $\ell = 2, 3$. Action on $\Psi_{2,p}(X)$:

$$\Psi_{2,p}(b_{1,p}, b_1, b_3, b_2) = b_{3,p}\Phi'_{1,p}(b_{1,p}, b_1, b_2, b_3) := \Psi_{3,p}(b_{1,p}, b_1, b_2, b_3).$$

Relations modulo 2 and 4

We look at matrices γ such that

$$\begin{array}{rcl} b_1(\gamma\Omega) & = & i^{\alpha_1} b_1(\Omega) \\ b_2(\gamma\Omega) & = & i^{\alpha_2} b_2(\Omega) \\ b_3(\gamma\Omega) & = & i^{\alpha_3} b_3(\Omega) \end{array} \quad \text{and} \quad \begin{array}{rcl} b_{1,p}(\gamma\Omega) & = & i^{\alpha_4} b_{1,p}(\Omega) \\ b_{2,p}(\gamma\Omega) & = & i^{\alpha_5} b_{2,p}(\Omega) \\ b_{3,p}(\gamma\Omega) & = & i^{\alpha_6} b_{3,p}(\Omega) \end{array}$$

Comparison

For $p = 3$:

i	j_1	i_1	b_1	j_2	i_2	b_2	j_3	i_3	b_3
0	394	61	40	288	32	10	278	32	10
1	302	61	37	286	32	12	276	31	12
2	302	61	38	286	32	14	276	31	14
$\vdots$		$\vdots$			$\vdots$			$\vdots$	
37	268	41	17	382	22	16	253	21	16
38	263	36	14	375	21	14	248	19	14
39	257	31	13	367	20	12	243	17	12

- $p = 3$: 175 KB $= \sim$ 5000 smaller than Streng ;
- $p = 5$: 200 MB ;
- $p = 7$: 30 GB ;

Computing modular polynomials

1. Dimension 1 : elliptic curves
2. Dimension 2 : abelian surfaces
   - Computation of the modular polynomials
   - Smaller invariants
3. Real Multiplication : cyclic isogenies

Hilbert space

Let $D \in \mathbb{Z}^{>0}$ and $K = \mathbb{Q}(\sqrt{D})$ a real quadratic field. We take $D \in \{2, 5\}$ for simplicity.
The group $\mathrm{SL}_2(O_K)$ acts on $\mathcal{H}_1^2$.

Proposition

The **Hilbert modular surface** $\mathcal{H}_1^2/\mathrm{SL}_2(O_K)$ *is a moduli space for isomorphism classes of ppas with real multiplication by* O_K*.*

Let p a prime number such that

$$p = \beta\overline{\beta}, \quad \beta \in O_K^+.$$

β-isogenous surfaces : $\beta\gamma z$, $z \in \mathcal{H}_1^2$ and $\gamma \in \mathrm{C}_p = \mathrm{SL}_2(O_K)/\Gamma_0(\beta)$;
$\#\mathrm{C}_p = p + 1$.

Hilbert and Humbert

The following diagram is commutative :

$$\begin{array}{ccc} \mathcal{H}_1^2 & \xrightarrow{\phi} & \mathcal{H}_2 \\ \downarrow & & \downarrow \\ \mathcal{H}_1^2/\mathrm{SL}_2(O_K) & \xrightarrow{\rho} & \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z}) \end{array}$$

where ρ is generically of degree 2 onto the Humbert surface H_{Δ_K}.

Hilbert modular function

Gundlach invariants : J_1 and J_2 for $D = 2$ and 5 only.

Two modular polynomials Φ_β and Ψ_β in $\mathbb{Q}(J_1, J_2)[X]$.

Algorithm

For $D = 5$, we have (Resnikoff 1974, Lauter–Yang 2011)

$$\begin{aligned} j_1 \circ \phi &= 8J_1(3J_2^2/J_1 - 2)^5; \\ j_2 \circ \phi &= \tfrac{1}{2}J_1(3J_2^2/J_1 - 2)^3; \\ j_3 \circ \phi &= 2^{-3}J_1(3J_2^2/J_1 - 2)^2(4J_2^2/J_1 + 2^5 3^2 J_2/J_1 - 3). \end{aligned}$$

These equations can be inverted by Gröbner basis.

Fast evaluation of the Gundlach invariants :

$$z \to \phi(z) = \Omega \to (j_1(\Omega), j_2(\Omega), j_3(\Omega)) \to (J_1(z), J_2(z)).$$

Inversion of the Gundlach invariants :

$$(J_1(z), J_2(z)) \to (j_1(\phi(z)), j_2(\phi(z)), j_3(\phi(z))) \to \phi(z) \to z.$$

Results

D=2

p	2	7	17	23	31	41
Memory space	$8.5KB$	$172KB$	$5.8MB$	$21MB$	$70MB$	$225MB$

D=5

p	5	11	19	29	31
Memory space	$22KB$	$3.5MB$	$33MB$	$188MB$	$248MB$

Theta functions

Other invariants?

$$\tilde{j}_i = j_i \circ \phi, \quad i = 1, 2, 3$$

or

$$\tilde{b}_i = b_i \circ \phi, \quad i = 1, 2, 3.$$

Works for any D. Three invariants for a space of dimension 2 : need the equation P of the Humbert component (Gruenewald 2008).

Interpolation : $\mathbb{Q}(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)/(P) = \mathbb{Q}(\tilde{b}_1, \tilde{b}_2)[\tilde{b}_3]/(P)$.

Conclusion

- Implementation and generalization of the algorithm of Dupont ;
- Used smaller invariants and proved properties with them ;
- Definition and computation of modular polynomials with cyclic isogenies.

Perspectives

- Compute more modular polynomials ;
- Release the code ;
- Applications of the polynomials.