

Computing genus 2 curves from invariants on the Hilbert moduli space

Journal of Number Theory, Special Issue on Elliptic Curve
Cryptography

<http://eprint.iacr.org/2010/294>

Kristin Lauter, Microsoft Research

Joint work with: Tonghai Yang, University of Wisconsin

ECC 2010, October 21, 2010

Constructing genus 2 curves for cryptography

C smooth, projective, irreducible genus 2 curve over \mathbb{F}_p .

$J(C)$ the Jacobian variety.

$J(C)(\mathbb{F}_p)$ can be used in cryptography as the group with a hard Discrete Log Problem (DLP) if the group has a subgroup of large prime order (roughly size p^2)

Advantage: p of size 2^{128} instead of 2^{256} as for elliptic curves.

Applications: key exchange, digital signatures, encryption, ...

Challenge:

Generate C/\mathbb{F}_q with $\#J(C)(\mathbb{F}_q) = N$, N a large prime.

Strategy: Construct curves with a known order using complex multiplication (CM) techniques.

1. Given $N_1 = \#C(\mathbb{F}_q)$ and $N_2 = \#C(\mathbb{F}_{q^2})$ \mathbb{F}_p , this determines a quartic CM number field K by the characteristic polynomial of Frobenius.
2. Compute "modular invariants" associated to the field K .
3. Reconstruct the curve from its invariants via Mestre's algorithm.

Computing the CM field K

For an ordinary genus 2 curve C over a prime field \mathbb{F}_q , let $N_1 = \#C(\mathbb{F}_q)$ and $N_2 = \#C(\mathbb{F}_{q^2})$. Then

$$\#J(C)(\mathbb{F}_q) = (N_1^2 + N_2)/2 - q. \quad (1)$$

Set

$$s_1 := q + 1 - N_1$$

and

$$s_2 := \frac{1}{2} (s_1^2 + N_2 - 1 - q^2).$$

Then the quartic polynomial satisfied by the Frobenius endomorphism of the Jacobian is

$$f(t) = t^4 - s_1 t^3 + s_2 t^2 - q s_1 t + q^2.$$

Thus the Jacobian of the curve has endomorphism ring equal to an order in the quartic CM field $K = \mathbb{Q}[t]/(f(t))$.

Genus 2 curves with CM

$K =$ quartic primitive CM field.

A curve C over \mathbb{C} *has CM* by \mathcal{O}_K if \mathcal{O}_K embeds in the endomorphism ring of $\text{Jac}(C)$.

CM points on the moduli space of principally polarized abelian surfaces correspond to isomorphism classes of CM curves.

The Siegel moduli space

The Siegel moduli space \mathcal{A}_2 parameterizes abelian surfaces with principal polarization.

Let $\mathrm{Sp}_2(\mathbb{Z})$ be the symplectic group over \mathbb{Z} of genus two, consisting of 4×4 -integral matrices g satisfying

$$gJg^t = J, \quad J = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$$

where I_2 is the identity matrix of order 2. Let

$$\mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in M_2(\mathbb{C}) : \Im \tau > 0 \right\}$$

be the Siegel upper half-plane of genus two, and let

$$X_2 = \mathrm{Sp}_2(\mathbb{Z}) \backslash \mathbb{H}_2$$

be the open Siegel modular 3-fold.

The Siegel moduli space

Here $\mathrm{Sp}_2(\mathbb{R})$ acts on \mathbb{H}_2 via

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

We can give explicit representatives for all the CM points on $\mathcal{A}_2(\mathbb{C})$:

$$\{\tau : \mathbb{C}^2 / \langle \mathbf{I}_2 \tau \rangle \text{ has CM by } \mathcal{O}_K\} / \mathrm{Sp}_4(\mathbb{Z})$$

Absolute Igusa invariants

Igusa gave 3 Siegel modular functions h_1, h_2, h_3 , the absolute Igusa invariants.

$$h_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6},$$

$$h_2 = \frac{3^3}{2^3} \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4},$$

$$h_3 = \frac{3}{2^5} \left(\frac{\psi_6 \chi_{12}^2}{\chi_{10}^3} + 2^2 \cdot 3 \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4} \right).$$

Igusa class polynomials

Definition

The Igusa class polynomials

$$H_i(x) = \prod_{\substack{\{\tau: \mathbb{C}^2/\langle I_2, \tau \rangle \text{ has CM by } \mathcal{O}_K\} \\ \text{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \quad i = 1, 2, 3.$$

The Hilbert modular surface

$F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with prime discriminant
 $D \equiv 1 \pmod{4}$

$\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$ is the non-trivial Galois conjugate of F
over \mathbb{Q} .

$\epsilon > 0$ is a unit such that $\sigma(\epsilon)\epsilon = -1$.

Let $X = \mathrm{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$ be the open Hilbert modular surface.

For $z = (z_1, z_2)$ and $a \in F$, we denote $z^* = \text{diag}(z_1, z_2)$, and $a^* = \text{diag}(a, \sigma(a))$. We also denote

$$\gamma^* = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}, \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(F).$$

Choose a \mathbb{Z} -basis $\{e_1, e_2\}$ for \mathcal{O}_F :

$$\mathcal{O}_F = \mathbb{Z}e_1 + \mathbb{Z}e_2, \tag{2}$$

and define

$$R = \begin{pmatrix} e_1 & e_2 \\ \sigma(e_1) & \sigma(e_2) \end{pmatrix}. \tag{3}$$

Map between Hilbert and Siegel

We define the maps

$$\phi : \mathbb{H}^2 \rightarrow \mathbb{H}_2, \quad \phi(z) = R^t \text{diag}\left(\frac{\epsilon}{\sqrt{D}} z_1, \sigma\left(\frac{\epsilon}{\sqrt{D}}\right) z_2\right) R, \quad (4)$$

and

$$\phi : \text{SL}_2(F) \rightarrow \text{Sp}_2(\mathbb{Q}), \quad \phi(\gamma) = S \gamma^* S^{-1}, \quad (5)$$

$$S = \text{diag}(R^t, R^{-1}) \text{diag}(I_2, \left(\frac{\sqrt{D}}{\epsilon}\right)^*).$$

$$F = \mathbb{Q}(\sqrt{5})$$

Assume $F = \mathbb{Q}(\sqrt{5})$, and let $\epsilon = \frac{1+\sqrt{5}}{2}$. Let

$$\phi : \mathrm{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2 \rightarrow \mathrm{Sp}_2(\mathbb{Z}) \backslash \mathbb{H}_2,$$

$$\phi(z) = \begin{pmatrix} 1 & 1 \\ \sigma(\epsilon) & \epsilon \end{pmatrix} \begin{pmatrix} \frac{\epsilon}{\sqrt{5}} z_1 & 0 \\ 0 & -\frac{\sigma(\epsilon)}{\sqrt{5}} z_2 \end{pmatrix} \begin{pmatrix} 1 & \sigma(\epsilon) \\ 1 & \epsilon \end{pmatrix} = \begin{pmatrix} \frac{\epsilon}{\sqrt{5}} z_1 - \frac{\sigma(\epsilon)}{\sqrt{5}} z_2 & \frac{z_2 - z_1}{\sqrt{5}} \\ \frac{z_2 - z_1}{\sqrt{5}} & -\frac{\sigma(\epsilon)}{\sqrt{5}} z_1 + \frac{\epsilon}{\sqrt{5}} z_2 \end{pmatrix}$$

be the map defined above, and let $e(z) := e^{2\pi iz}$ and

$$q_1 = e\left(\frac{\epsilon}{\sqrt{5}} z_1 - \frac{\sigma(\epsilon)}{\sqrt{5}} z_2\right) = e\left(\frac{1+\sqrt{5}}{2\sqrt{5}} z_1 - \frac{1-\sqrt{5}}{2\sqrt{5}} z_2\right), \quad q_2 = e\left(\frac{z_2 - z_1}{\sqrt{5}}\right).$$

Then for a holomorphic Siegel modular form f of weight k for $\mathrm{Sp}_2(\mathbb{Z})$, $g = \phi^* f$ is a symmetric holomorphic Hilbert modular form for $\mathrm{SL}_2(\mathcal{O}_F)$ with the Fourier expansion:

$$g(z) = a_f(0) + \sum_{t=a+b\frac{1-\sqrt{5}}{2} \in \mathcal{O}_F^+} a_g(t) q_1^a q_2^b,$$

with

Pullback

$$a_g(t) = \sum_{\text{condition}(*)} a_f \left(\left(\begin{pmatrix} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{pmatrix} \right) \right).$$

Condition (*):

$$\left\{ \begin{array}{l} m_1, m_2 \in \mathbb{Z}^+, \quad m \in \mathbb{Z}, \\ m^2 < 4m_1m_2, \\ m_1 + m_2 = a, \\ m + m_2 = b \end{array} \right. \quad (6)$$

Hilbert Eisenstein series

$$F = \mathbb{Q}(\sqrt{5}) \quad \epsilon = \frac{1+\sqrt{5}}{2}.$$

The Eisenstein series of even weight $k \geq 2$:

$$G_k(z) = 1 + \sum_{t=a+b\frac{1-\sqrt{5}}{2} \in \mathcal{O}_F^+} b_k(t) q_1^a q_2^b, \quad (7)$$

where

$$b_k(t) = \kappa_k \sum_{(\mu) \supset (t)} (\mu)^{k-1}. \quad (8)$$

$$\kappa_k = \frac{(2\pi)^{2k} \sqrt{5}}{(k-1)! 25^k \zeta_F(k)}$$

Coefficients for the Hilbert Eisenstein series

$$0 < a \leq 3, \frac{1 - \sqrt{5}}{2} a < b < \frac{1 + \sqrt{5}}{2} a$$

$$\begin{aligned} G_k(z) = & 1 + \kappa_k(1 + q_2)q_1 + \\ & \kappa_k [q_2^{-1} + (1 + 4^{k-1}) + (1 + 5^{k-1})q_2 + (1 + 4^{k-1})q_2^2 + q_2^3] q_1^2 + \\ & \kappa_k [(1 + 5^{k-1})q_2^{-1} + (1 + 9^{k-1}) + (1 + 11^{k-1})q_2 + (1 + 11^{k-1})q_2^2 \\ & + (1 + 9^{k-1})q_2^3 + (1 + 5^{k-1})q_2^4] q_1^3. \end{aligned}$$

Theta series

$$\text{Let } \theta_6 = -\frac{67}{2^5 3^3 5^2} (G_6 - G_2^3),$$

$$\theta_{10} = 2^{-10} 3^{-5} 5^{-5} 7^{-1} (412751 G_{10} - 5 \cdot 67 \cdot 2293 G_2^2 G_6 + 2^2 \cdot 3 \cdot 7 \cdot 4231 G_2^5),$$

$$\theta_{12} = 2^{-2} (\theta_6^2 - G_2 \theta_{10})$$

Gundlach invariants

Theorem

(Gundlach) (1) The ring of symmetric holomorphic Hilbert modular forms for $SL_2(\mathcal{O}_F)$ is a polynomial ring of G_2 , G_6 , and θ_{10} .
(2) The field of symmetric meromorphic Hilbert modular functions for $SL_2(\mathcal{O}_F)$ are rational functions of

$$J_1 = \frac{\theta_6}{G_2^3} \quad \text{and} \quad J_2 = \frac{G_2^5}{\theta_{10}}.$$

We call J_1 and J_2 the *Gundlach invariants*.

Alternative choices for Gundlach invariants

Use the invariants J_1 and J_3 , where

$$J_3 = J_1 + J_2^{-1} = \frac{\theta_6 G_2^2 + \theta_{10}}{G_2^5}.$$

This choice has the advantage that both invariants are rather small.

Another possible choice is to use invariants J_2 and J_4 where

$$J_4 = J_1 J_2 = \frac{\theta_6 G_2^2}{\theta_{10}}.$$

This choice has the advantage that both invariants have denominator θ_{10} .

Pullback of Igusa invariants to Gundlach invariants

Proposition

$$\phi^* h_1 = 8J_2(3J_1^2 J_2 - 2)^5,$$

$$\phi^* h_2 = \frac{1}{2} J_2(3J_1^2 J_2 - 2)^3,$$

$$\phi^* h_3 = 2^{-3} J_2(3J_1^2 J_2 - 2)^2(4J_1^2 J_2 + 2^5 \cdot 3^2 J_1 - 3).$$

Algorithm for computing Gundlach invariants

Input: K a primitive quartic CM field, p a prime which splits completely into principal ideals in K^* , the reflex of K , and S a collection of 2 or 4 possible group orders for Jacobians of genus 2 curves over \mathbb{F}_p with CM by K .

Output: Gundlach invariants modulo p for genus 2 curves with CM by K and equations for curves C over \mathbb{F}_p with $\#J(C) \in S$.

1. Find $\Delta \in \mathcal{O}_F$ such that Δ is totally negative, $K = F(\sqrt{\Delta})$

$$\mathcal{O}_K = \mathcal{O}_F + \mathcal{O}_F \frac{b_0 + \sqrt{\Delta}}{2}.$$

2. Let $M = \mathbb{Q}(\sqrt{\Delta}, \sqrt{\sigma(\Delta)})$ be the Galois closure of K over \mathbb{Q} .

$$\text{Im}(\sqrt{\Delta}) > 0, \quad \text{Im}(\sqrt{\sigma(\Delta)}) > 0.$$

Algorithm...

3. Find the class number h_K and the ideals generating the class group of K .
4. Write ideal \mathfrak{a} of K in the form

$$\mathfrak{a} = \left[a, \frac{b + \sqrt{\Delta}}{2} \right] = \mathcal{O}_F a + \mathcal{O}_F \frac{b + \sqrt{\Delta}}{2}$$

such that a is totally positive with $a\mathcal{O}_F =_{K/F} \mathfrak{a}$, and that $z = \frac{b + \sqrt{\Delta}}{2a}$.

$$z([\mathfrak{a}], \Phi) = \Phi(z) = (z, \sigma z) \in \mathbb{H}^2$$

is the CM point in $X = \mathrm{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$ associated to the ideal class

$$z([\mathfrak{a}], \Phi') = (\epsilon z, \sigma'(\epsilon z)) \in \mathbb{H}^2$$

is the CM point of CM type Φ' associated to \mathfrak{a} .

Algorithm

5. Compute $J_i(z([\mathfrak{a}], \Phi))$ and $J_i(z([\mathfrak{a}], \Phi'))$. Form the minimal polynomials $P_1(X)$ and $P_2(X)$. Reduce modulo a prime p not dividing the denominators and find roots $(\bmod p)$.
6. Compute $\phi^* h_i \pmod{p}$ via the pull-back formulas. Apply Mestre's algorithm to pairs of roots from step 5 to construct a genus 2 curve over the finite field \mathbb{F}_p .

Why is this better than using Igusa invariants?

- CM points are easier to write down.
- Two variables instead of three (fewer exponentials to evaluate, fewer multiplications)
- Smaller height.
- Two invariants instead of three.
- Good control over precision needed.

Comparison with others' work

Three methods for computing Igusa class polynomials:

- ① Complex analytic method: Spallek, van Wamelen, Weng, Cohn-L, Dupont, Streng
- ② CRT Chinese Remainder Theorem: Eisentraeger-L., Freeman, Broker, Gruenewald, Robert
- ③ p-adic method: Gaudry, Houtmann, Kohel, Ritzenthaler, Weng, Carls, Lubicz

Joint work with Michael Naehrig

- Examples database
- Improvements to the algorithm
- Understanding the factorization of coefficients of class polynomials

$K = \mathbb{Q}(\sqrt{-26 - 2\sqrt{5}})$, non-normal, class number 1

precision: 3000

number of terms in Eisenstein series: 30

Time for computing polynomials: 8.400 s

$$P_2 = X^2 - 2588193X + 1511654400000$$

$$P_4 = X^2 + 1251X + 324000$$

$$c_{2,0} = 2^{13} \cdot 3^{10} \cdot 5^5, \quad c_{2,1} = 3^5 \cdot 10651, \quad c_{2,2} = 1$$

$$c_{4,0} = 2^5 \cdot 3^4 \cdot 5^3, \quad c_{4,1} = 3^2 \cdot 139, \quad c_{4,2} = 1$$

$K = \mathbb{Q}(\sqrt{-5} + \sqrt{5})$, normal, class number 2

precision: 3000

number of terms in Eisenstein series: 20

Time for computing polynomials (Magma): 1.810 s

$$\begin{aligned}P_2 &= 121X^2 - 5716137600000X + 9183300480000000000 \\ &= 121(X - 47239200000)(X - 194400000/121)\end{aligned}$$

$$\begin{aligned}P_4 &= 121X^2 - 29628000X + 54675000000 \\ &= 121(X - 243000)(X - 225000/121)\end{aligned}$$

$$c_{2,0} = 2^{16} \cdot 3^{15} \cdot 5^{10}, \quad c_{2,1} = 2^{10} \cdot 3^5 \cdot 5^5 \cdot 7351, \quad c_{2,2} = 11^2$$

$$c_{4,0} = 2^6 \cdot 3^7 \cdot 5^8, \quad c_{4,1} = 2^5 \cdot 3^2 \cdot 5^3 \cdot 823, \quad c_{4,2} = 11^2$$

$K = \mathbb{Q}(\sqrt{-14 - 2\sqrt{5}})$, non-normal, class number 2

precision: 3000

number of terms in Eisenstein series: 25

Time for computing polynomials (Magma): 7.410 s

$$\begin{aligned} P_2 = & 49X^4 - 217136775168X^3 + 183163100112001695744X^2 \\ & - 17409591332317849190400000X \\ & + 584985350410076160000000000 \end{aligned}$$

$$\begin{aligned} P_4 = & 49X^4 - 5851584X^3 + 148455970560X^2 \\ & - 21859269120000X - 361117440000000 \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-14 - 2\sqrt{5}})$, non-normal, class number 2

$$c_{2,0} = 2^{34} \cdot 3^{20} \cdot 5^{10}$$

$$c_{2,1} = 2^{27} \cdot 3^{15} \cdot 5^5 \cdot 7 \cdot 79 \cdot 5231$$

$$c_{2,2} = 2^{18} \cdot 3^{11} \cdot 37 \cdot 1129 \cdot 94421$$

$$c_{2,3} = 2^{14} \cdot 3^5 \cdot 54539$$

$$c_{2,4} = 7^2$$

$$c_{4,0} = 2^{14} \cdot 3^8 \cdot 5^7 \cdot 43$$

$$c_{4,1} = 2^{12} \cdot 3^6 \cdot 5^4 \cdot 13 \cdot 17 \cdot 53$$

$$c_{4,2} = 2^8 \cdot 3^5 \cdot 5 \cdot 193 \cdot 2473$$

$$c_{4,3} = 2^6 \cdot 3^2 \cdot 10159$$

$$c_{4,4} = 7^2$$

$K = \mathbb{Q}(\sqrt{-66 - 10\sqrt{5}})$, non-normal, class number 3

precision: 3000

number of terms in Eisenstein series: 100

Time for computing polynomials (Magma): 305.360 s

$$\begin{aligned} P_2 = & X^6 - 14361341769X^5 + 48530935318126967414X^4 \\ & - 6753971583972445270702277X^3 \\ & + 1350060851930542237903564800000X^2 \\ & - 134258998051837482119331840000000000X \\ & + 462842014248469426234982400000000000000 \end{aligned}$$

$$\begin{aligned} P_4 = & X^6 + 139611X^5 + 4817153636X^4 - 3802138545451X^3 \\ & + 1557132203428000X^2 - 378359130128000000X \\ & + 44566851776000000000 \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-66 - 10\sqrt{5}})$, non-normal, class number 3

$$\begin{aligned}c_{2,0} &= 2^{42} \cdot 3^9 \cdot 5^{15} \cdot 281^5 \\c_{2,1} &= 2^{26} \cdot 3^6 \cdot 5^{10} \cdot 7 \cdot 479 \cdot 1699 \cdot 49329760913 \\c_{2,2} &= 2^{15} \cdot 3^3 \cdot 5^5 \cdot 6659 \cdot 488743 \cdot 150037582573 \\c_{2,3} &= 13 \cdot 519536275690188097746329 \\c_{2,4} &= 2 \cdot 313 \cdot 77525455779755539 \\c_{2,5} &= 3^3 \cdot 15919 \cdot 33413 \\c_{2,6} &= 1\end{aligned}$$

$$\begin{aligned}c_{4,0} &= 2^{15} \cdot 5^9 \cdot 281^2 \cdot 8819 \\c_{4,1} &= 2^{10} \cdot 5^6 \cdot 7 \cdot 3378206519 \\c_{4,2} &= 2^5 \cdot 5^3 \cdot 389283050857 \\c_{4,3} &= 1621 \cdot 2345551231 \\c_{4,4} &= 2^2 \cdot 673 \cdot 1789433 \\c_{4,5} &= 3 \cdot 173 \cdot 269 \\c_{4,6} &= 1\end{aligned}$$

$K = \mathbb{Q}(\sqrt{-30 - 6\sqrt{5}})$, normal, class number 4

precision: 3000

number of terms in Eisenstein series: 60

Time for computing polynomials (Magma): 52.960 s

$$\begin{aligned} P_2 &= 961X^4 - 10446951283200000X^3 \\ &\quad + 44375383336320000000000X^2 \\ &\quad - 45630255522816000000000000000X \\ &\quad - 176319369216000000000000000000 \\ P_4 &= 961X^4 - 3359976000X^3 + 4518279000000X^2 \\ &\quad + 7145550000000000X - 9274500000000000 \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-30 - 6\sqrt{5}})$, normal, class number 4

$$c_{2,0} = 2^{32} \cdot 3^{16} \cdot 5^{20}$$

$$c_{2,1} = 2^{25} \cdot 3^{12} \cdot 5^{15} \cdot 191 \cdot 439$$

$$c_{2,2} = 2^{16} \cdot 3^9 \cdot 5^{10} \cdot 337 \cdot 10453$$

$$c_{2,3} = 2^{12} \cdot 3^4 \cdot 5^5 \cdot 10076149$$

$$c_{2,4} = 31^2$$

$$c_{4,0} = 2^{12} \cdot 3^4 \cdot 5^{13} \cdot 229$$

$$c_{4,1} = 2^{10} \cdot 3^3 \cdot 5^{11} \cdot 67 \cdot 79$$

$$c_{4,2} = 2^6 \cdot 3^2 \cdot 5^6 \cdot 59 \cdot 67 \cdot 127$$

$$c_{4,3} = 2^6 \cdot 3 \cdot 5^3 \cdot 139999$$

$$c_{4,4} = 31^2$$

$K = \mathbb{Q}(\sqrt{-6 - \sqrt{5}})$, non-normal, class number 4

precision: 3000

number of terms in Eisenstein series: 240

Time to compute polynomials (Magma): 2290.250 s

$$\begin{aligned} P_2 &= 529X^8 - 906756999727104X^7 \\ &\quad + 346158557025018350146158592X^6 \\ &\quad - 564260103063914026233904731521024X^5 \\ &\quad + 201611557172586486774045507195422900224X^4 \\ &\quad + 1188790268775347682307679034847474483200000X^3 \\ &\quad + 14591665686244083042479219252142444380160000000000X^2 \\ &\quad + 13997722293055522697554403116959903252480000000000000000X \\ &\quad + 4716827642114847482995749174606078935040000000000000000000 \\ P_4 &= 529X^8 - 1072514112X^7 + 517120008137216X^6 + 20475755574980608X^5 \\ &\quad - 724812765867541692416X^4 + 434077018652827582464000X^3 \\ &\quad - 199409785438298832896000000X^2 + 41908452090722648064000000000X \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-6 - \sqrt{5}})$, non-normal, class number 4

$$c_{2,0} = 2^{68} \cdot 3^{12} \cdot 5^{20} \cdot 5009^5$$

$$c_{2,1} = 2^{63} \cdot 3^{10} \cdot 5^{15} \cdot 83 \cdot 1014674956751031349$$

$$c_{2,2} = 2^{53} \cdot 3^7 \cdot 5^{10} \cdot 17 \cdot 17583018821 \cdot 253760436053$$

$$c_{2,3} = 2^{45} \cdot 3^4 \cdot 5^5 \cdot 27585937 \cdot 4838744112380831$$

$$c_{2,4} = 2^{35} \cdot 79 \cdot 101 \cdot 163 \cdot 4728433 \cdot 13547767 \cdot 70427869$$

$$c_{2,5} = 2^{30} \cdot 18288367 \cdot 28734559621330853$$

$$c_{2,6} = 2^{19} \cdot 11 \cdot 281 \cdot 347 \cdot 4027 \cdot 388757 \cdot 393203$$

$$c_{2,7} = 2^{11} \cdot 3^2 \cdot 19 \cdot 103 \cdot 25137821$$

$$c_{2,8} = 23^2$$

$$c_{4,0} = 2^{28} \cdot 5^{12} \cdot 947 \cdot 4933 \cdot 5009^2$$

$$c_{4,1} = 2^{34} \cdot 3^2 \cdot 5^9 \cdot 367 \cdot 503 \cdot 751753$$

$$c_{4,2} = 2^{23} \cdot 5^6 \cdot 19 \cdot 97 \cdot 313 \cdot 751 \cdot 3511777$$

$$c_{4,3} = 2^{20} \cdot 3 \cdot 5^3 \cdot 41611 \cdot 26529401939$$

$$c_{4,4} = 2^{15} \cdot 22119530208360037$$

$$c_{4,5} = 2^{14} \cdot 3 \cdot 499 \cdot 2963 \cdot 2817517$$

$K = \mathbb{Q}(\sqrt{-330 + 66\sqrt{5}})$, normal, class number 8

precision: 3000

number of terms in Eisenstein series: 350

Time to compute polynomials (Magma): 5403.030 s

$$\begin{aligned} P_2 = & 8700896126036551483736041X^8 \\ & - 32550875692547568160555206013385025122918400000X^7 \\ & + 125923144169110910076831696022908759633958010880000000000X^6 \\ & - 353230813277970666790763860207721212032445317120000000000000000X^5 \\ & + 1889625861490122991753094938116665836917739392860160000000000000000000X^4 \\ & + 78004698176565486371972347519396339488310620585984000000000000000000 / \\ & 0000000X^3 \\ & - 362973284011776064323611004432898872351089794511536128000000000000000 / \\ & 00000000000000X^2 \\ & + 1733970682309350778884467784690379871686391383826890752000000000000000 / \\ & 00000000000000000000X \\ & + 11206339807172688624297071398862547803665367574773760000000000000000 / \\ & 0000000000000000000000 \end{aligned}$$

$K = \mathbb{Q}(\sqrt{-330 + 66\sqrt{5}})$, normal, class number 8

$$\begin{aligned}P_4 &= 8700896126036551483736041X^8 \\ &+ 529171959706861316033186870106048000X^7 \\ &+ 39711888130001408728642075379641344000000X^6 \\ &+ 661069949180561165913677507650977792000000000X^5 \\ &+ 2807886486943137234407534221470990336000000000000X^4 \\ &- 213560004684431769616781094087032832000000000000000X^3 \\ &- 1047419059359197899357420865772847104000000000000000000X^2 \\ &+ 7853812718487216446731436819900006400000000000000000000X \\ &- 3237734749975898026658584760156160000000000000000000000\end{aligned}$$

P_4 -coefficients:

$$\begin{aligned}c_{4,8} &= 11^4 \cdot 29^2 \cdot 61^2 \cdot 211^2 \cdot 241^2 \cdot 271^2 \\ c_{4,7} &= 2^9 \cdot 3 \cdot 5^3 \cdot 11^3 \cdot 49253 \cdot 26291379817 \cdot 1599084712499 \\ c_{4,6} &= 2^{16} \cdot 3^2 \cdot 5^6 \cdot 11^2 \cdot 53 \cdot 671918858429137008360873343 \\ c_{4,5} &= 2^{25} \cdot 3^3 \cdot 5^9 \cdot 11 \cdot 17 \cdot 53 \cdot 73 \cdot 193 \cdot 797 \cdot 1871 \cdot 1794212865865807 \\ c_{4,4} &= 2^{33} \cdot 3^4 \cdot 5^{12} \cdot 7 \cdot 43 \cdot 127 \cdot 12907 \cdot 482413 \cdot 69446456336729 \\ c_{4,3} &= 2^{44} \cdot 3^5 \cdot 5^{16} \cdot 19 \cdot 23^2 \cdot 73 \cdot 152531 \cdot 29253882917683 \\ c_{4,2} &= 2^{48} \cdot 3^6 \cdot 5^{19} \cdot 7 \cdot 1056061 \cdot 362022885111720449 \\ c_{4,1} &= 2^{60} \cdot 3^7 \cdot 5^{23} \cdot 283 \cdot 923284368270711347\end{aligned}$$