Singular invariants for generators of Atkin-Lehner groups and applications to explicit class field theory

Jay Jorgenson, Lejla Smajlović, Holger Then

Marseilles, February 08, 2023.

1. Classical aspects of the $j-$invariant
2. Canonical generators of function fields
3. Singular invariants
4. Applications to explicit class field theory
5. Examples of modular polynomials

The $j-$invariant - transcendence properties

$$j(z) = \frac{1728E_4^3(z)}{(E_4^3(z) - E_6^2(z))} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + O(q^3). \quad (1)$$

The $j-$invariant - transcendence properties

$$j(z) = \frac{1728E_4^3(z)}{(E_4^3(z) - E_6^2(z))} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + O(q^3). \quad (1)$$

Study initiated in 1937 by T. Schneider. Results are

(i) If z is a quadratic irrational in $\mathbb{H}$ then $j(z)$ is an algebraic integer

(ii) If z is algebraic but not imaginary quadratic then $j(z)$ is transcendental

(iii) Moreover, if z is any element of an imaginary quadratic extension of $\mathbb{Q}$, then $j(z)$ is an algebraic integer, and the field extension $\mathbb{Q}[j(z), z]/\mathbb{Q}[z]$ is abelian which provides the beginning of (explicit) class field theory.

The $j-$invariant and explicit class field theory

Given an imaginary quadratic field K and the order $\mathcal{O}$ in K of discriminant D, to describe explicitly the abelian extension L of K in terms of, possibly, its generating polynomial. The degree of the polynomial equals:

(i) the order of the (gen.) ideal class group $C(\mathcal{O}) \simeq \mathrm{Gal}(L/K)$ (Artin map).

(ii) the class number $h(D)$ of all classes of primitive, positive definite quadratic forms of discriminant D, modulo an $\mathrm{SL}(2,\mathbb{Z})$ action.

Given propert fract. ideal $\mathfrak{a}$ of $\mathcal{O}$, we may define $j(\mathfrak{a}) = j(\tau)$ for a (CM) point $\tau \in \mathbb{H}$ generating a lattice in $\mathbb{Z}$ homothetic to $\mathfrak{a}$.

Note that $f(1,\tau) = 0$ for a primitive, positive definite quadratic form $f(x,y) = ax^2 + bxy + cy^2$ of discriminant D.

Then $j(\mathfrak{a})$ is an algebraic integer and $K[j(\mathfrak{a})]$ is the ring class field of the order $\mathcal{O}$. Specially, $K[j(\mathcal{O}_K)]$ is the Hilbert class field of K (the maximal unramified abelian extension of K).

The $j-$invariant and the class polynomial

What is a minimal polynomial for $j(\mathfrak{a})$? (i.e. the generating polynomial for the ring class field of $\mathcal{O} = [1, \tau]$ over K)

The $j-$invariant and the class polynomial

What is a minimal polynomial for $j(\mathfrak{a})$? (i.e. the generating polynomial for the ring class field of $\mathcal{O} = [1, \tau]$ over K)

An approach from Chen and Yui 1993 - take the product over all conjugates of $j(\tau)$ in the ring class field

$$\mathcal{M}(X) = \prod_{j=1}^{h(\mathcal{O})} (X - j(\tau_{\phi(Q_j)})),$$

where $h(\mathcal{O}) = h(D)$, Q_j, $j = 1, \ldots, h(\mathcal{O})$ form a complete set of representatives of all primitive, positive definite quadratic forms $f_{Q_j}(x, y)$ of discriminant D and $\tau_{Q_j} \in \mathbb{H}$ is the zero of $f_{Q_j}(1, \tau)$.

The value $j(\tau)$ is called the *singular invariant*.

The $j-$invariant and the class polynomial

What is a minimal polynomial for $j(\mathfrak{a})$? (i.e. the generating polynomial for the ring class field of $\mathcal{O} = [1, \tau]$ over K)

An approach from Chen and Yui 1993 - take the product over all conjugates of $j(\tau)$ in the ring class field

$$\mathcal{M}(X) = \prod_{j=1}^{h(\mathcal{O})} (X - j(\tau_{\phi(Q_j)})),$$

where $h(\mathcal{O}) = h(D)$, Q_j, $j = 1, \ldots, h(\mathcal{O})$ form a complete set of representatives of all primitive, positive definite quadratic forms $f_{Q_j}(x, y)$ of discriminant D and $\tau_{Q_j} \in \mathbb{H}$ is the zero of $f_{Q_j}(1, \tau)$.

The value $j(\tau)$ is called the *singular invariant*.

A "small" obstacle - coefficients in the $q-$expansion of the $j-$invariant are quite large thus a generating polynomial of the class field has enormous coefficients, even in case of some moderate N.

The $j-$invariant and explicit class field theory - an example

The generating polynomial of the Hilbert class field of the principal order $\mathbb{Z}[\sqrt{-74}]$ over $K = \mathbb{Q}[\sqrt{-74}]$, i.e. the minimal polynomial of $j(i\sqrt{74})$ over K is

$$\begin{aligned}
\mathbb{M}_{74}(X) = X^{10} &- 2975900215291446968922 72X^9 \\
&+ 16232088775507507309053223033156844 8X^8 \\
&+ 10833723207526124630181274705783365349945344X^7 \\
&+ 72338679964130565973442594357410062611918717420339 2X^6 \\
&- 15114530035213509909886819641017229466515976895827935232X^5 \\
&+ 16169770830829461160527539471604506855164053736484007538851 84X^4 \\
&+ 15494958955563981344176689890872586852428892851110732280427970560X^3 \\
&+ 13842264737918347802944465684738927192017518963597672890309256255897 6 \\
&+ 18285524842876216398405222709573627530438981888953039849580051382979 7 \\
&+ 65537997861811012957774465106804493369424397836065905853257281566511 4
\end{aligned}$$

The $j-$invariant and explicit class field theory - conclusion

First, note that the constant term is of order $\sim 6.6 \cdot 10^{73}$.

Results obtained with the classical $j-$invariant are algebraically beautiful (e.g. $j(\tau)$ being the generator of the Hilbert class field), however, in explicit class field theory (with applications e.g. in cryptography - elliptic curve primality proving) not quite useful.

The $j-$invariant and explicit class field theory - conclusion

First, note that the constant term is of order $\sim 6.6 \cdot 10^{73}$.

Results obtained with the classical $j-$invariant are algebraically beautiful (e.g. $j(\tau)$ being the generator of the Hilbert class field), however, in explicit class field theory (with applications e.g. in cryptography - elliptic curve primality proving) not quite useful.

There are more aspects of the $j-$invariant but for us the following one is most interesting.....

Monstrous moonshine

J. McKay observed that the linear-term coefficient in (1) is the sum of the two smallest irreducible character degrees of the largest of all sporadic simple groups $\mathbb{M}$, "the Fischer-Griess monster".

J. Thompson conjectured that all coefficients in (1) are related to the dimensions of the components of a graded module admitting action by $\mathbb{M}$.

J. Conway and S. Norton posed the "monstrous moonshine" conjectures; proved in the work of I. Frenkel, J. Lepowsky, A. Meurman and R. Borcherds.

The "moonshine" has been extended to other simple groups and other j-invariants associated to certain genus zero Fuchsian groups.

What about higher genus?

Monstrous moonshine

J. McKay observed that the linear-term coefficient in (1) is the sum of the two smallest irreducible character degrees of the largest of all sporadic simple groups $\mathbb{M}$, "the Fischer-Griess monster".

J. Thompson conjectured that all coefficients in (1) are related to the dimensions of the components of a graded module admitting action by $\mathbb{M}$.

J. Conway and S. Norton posed the "monstrous moonshine" conjectures; proved in the work of I. Frenkel, J. Lepowsky, A. Meurman and R. Borcherds.

The "moonshine" has been extended to other simple groups and other j-invariants associated to certain genus zero Fuchsian groups.

What about higher genus?

T. Ganon: "In genus > 0, two functions are needed to generate the function field. A complication facing the development of a higher-genus Moonshine is that, unlike the situation in genus 0 considered here, there is no canonical choice for these generators."

Atkin-Lehner groups

For any square-free integer N, the subset of $\mathrm{SL}(2,\mathbb{R})$ defined by

$$\Gamma_0(N)^+ = \left\{ e^{-1/2} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) : \quad ad - bc = e, \quad a,b,c,d,e \in \mathbb{Z}, \right.$$
$$\left. e \mid N,\ e \mid a,\ e \mid d,\ N \mid c \right\}$$

is an arithmetic subgroup of $\mathrm{SL}(2,\mathbb{R})$, called the Atkin-Lehner group.

Atkin-Lehner groups

For any square-free integer N, the subset of $\mathrm{SL}(2,\mathbb{R})$ defined by

$$\Gamma_0(N)^+ = \left\{ e^{-1/2} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) : \quad ad - bc = e, \quad a,b,c,d,e \in \mathbb{Z}, \right.$$
$$\left. e \mid N,\ e \mid a,\ e \mid d,\ N \mid c \right\}$$

is an arithmetic subgroup of $\mathrm{SL}(2,\mathbb{R})$, called the Atkin-Lehner group.

Questions:

(1) What should be canonical choice of generators in $g \geq 1$ setting?

(2) Once the canonical generators are described what can we say about the singular invariants (values of generators at imaginary quadratic arguments)?

(3) Can those be applied in the explicit class field theory?

Canonical generators - construction

Recall that

$$j(z) = \frac{1728E_4^3(z)}{(E_4^3(z) - E_6^2(z))} = \frac{1728E_4^3(z)}{\Delta(z)}, \quad \Delta(z) = \eta(z)^{24}.$$

Reasonable to assume that generators can be expressed "in terms" of the Eisenstein series on $\Gamma_0(N)^+$ and the analogue of the delta function.

Eisenstein series on $\Gamma_0(N)^+$ of even weight $k = 2m \geq 4$:

$$E_{2m}^{(N)}(z) = \sum_{\gamma \in \Gamma_\infty(N)\backslash\Gamma_0(N)^+} (cz+d)^{-2m} = \frac{1}{\sigma_m(N)} \sum_{v|N} v^m E_{2m}(vz).$$

Delta function analogue - a minimal weight cusp form vanishing at the cusp only

$$\Delta_N(z) = \left(\prod_{v|N} \eta(vz)\right)^{\ell_N}, \quad \ell_N = 2^{1-r}\mathrm{lcm}\left(4,\ 2^{r-1}\frac{24}{(24, \sigma(N))}\right).$$

Canonical generators - the algorithm

For any positive integer M, let $\mathcal{S}_M$ denote the set of functions

$$F_b(z) = \prod_\nu \left(E_{m_\nu}^{(N)}(z)\right)^{b_\nu} \Big/ \left(\Delta_N(z)\right)^M, \quad \sum_\nu b_\nu m_\nu = Mk_N \quad \text{and} \quad b = (b_1, \ldots)$$

Canonical generators - the algorithm

For any positive integer M, let $\mathcal{S}_M$ denote the set of functions

$$F_b(z) = \prod_\nu \left(E_{m_\nu}^{(N)}(z)\right)^{b_\nu} \Big/ \left(\Delta_N(z)\right)^M, \quad \sum_\nu b_\nu m_\nu = Mk_N \quad \text{and} \quad b = (b_1, \ldots)$$

Choose a non-negative integer κ. Let $M = 1$ and set $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_0$.

1. Form the matrix $A_\mathcal{S}$ of coefficients from the q-expansions of all elements of $\mathcal{S}$. Expand each element in $\mathcal{S}$ along a row; each column contains the coefficient of a power of q. Record those out to order q^κ.
2. Apply Gauss elimination to $A_\mathcal{S}$, to get $B_\mathcal{S}$ in row-reduced echelon form.
3. Implement the following decision to determine if the algorithm is complete:

   If the g lowest non-trivial rows at the bottom of $B_\mathcal{S}$ correspond to q-expansions whose lead terms have precisely g gaps in the set $\{q^{-1}, \ldots, q^{-2g}\}$, the algorithm is completed. (Weierstrass gap theorem)

   If the indicator to stop fails, then replace M by $M+1$, $\mathcal{S}$ by $\mathcal{S}_M \cup \mathcal{S}$ and reiterate the algorithm.

Canonical generators - results for $1 \leq g \leq 3$

The function field associated to $\Gamma_0(N)^+$ admits two generators x_N and y_N whose q-expansions have integer coefficients after the lead coefficient has been normalized to equal one.

Moreover, the orders of poles of the generators at $i\infty$ are at most $g+2$. (Minimal poles possible by the W. gap thm.)

As N grows, the coefficients in the $q-$expansions decay significantly :)

We derived the polynomial relations satisfied by the generators.

For example, when $g = 1$, x_N and y_N satisfy the equation

$$y_N^2 = x_N^3 + A_N x_N y_N + B_N x_N^2 + C_N y_N + D_N x_N + E_N, \tag{2}$$

where the integers A_N, B_N, C_N, D_N and E_N are explicitly computed for all genus one levels.

Singular invariants - genus one

If $\Gamma_0(N)^+$ has genus zero, then $j_N(\tau)$ for any CM point $\tau \in \mathbb{H}$ is algebraic (Chen and Yui for non-elliptic CM points and JST for elliptic fixed points).

However, if $\Gamma_0(N)^+$ has genus one, then $\wp_N(\alpha)$ is transcendental for any non-zero algebraic $\alpha \in \mathbb{C}$ (by a corollary of the Schneider-Lang theorem).

Singular invariants - genus one

If $\Gamma_0(N)^+$ has genus zero, then $j_N(\tau)$ for any CM point $\tau \in \mathbb{H}$ is algebraic (Chen and Yui for non-elliptic CM points and JST for elliptic fixed points).

However, if $\Gamma_0(N)^+$ has genus one, then $\wp_N(\alpha)$ is transcendental for any non-zero algebraic $\alpha \in \mathbb{C}$ (by a corollary of the Schneider-Lang theorem).

We see that there are various results which point both in the direction of algebraicity and in the direction of transcendence of values $x_N(\tau)$ and $y_N(\tau)$ for CM points $\tau \in \mathbb{H}$.

Singular invariants - genus one levels, Case 1

$Q = [a, b, c]$, $a > 0$ is a primitive positive definite quadratic form with discriminant $b^2 - 4ac = M^2 d_K < 0$;

$\tau \in \mathbb{H}$ is the complex root of $Q(\tau, 1) = a\tau^2 + b\tau + c = 0$;

$K = \mathbb{Q}[\tau]$ is imaginary quadratic field of discriminant d_K.

Case 1. Assume $(a, N) = 1$. Then, we proved the following:

1. The values $x_N(\tau)$ and $y_N(\tau)$ are algebraic integers and, moreover, the equation (2) which is quadratic in $y_N(\tau)$, factors (i.e. the discriminant of (2) as a quadratic in $y_N(\tau)$ factors in the field $\mathbb{Q}[\tau, x_N(\tau)]$)

2. $x_N(\tau)$ and $y_N(\tau)$ are algebraic integers when evaluated at different other explicitly described $\tau \in \mathbb{H}$ which are fixed points of certain mappings....

Singular invariants - genus one levels, Case 1 cont'

In case of prime N we derive generators of class fields, and for other squarefree N we deduce generators of the subfield of the class field of the order with suitable discriminant.

The generators of subfields, when combined with generators of genus field in cases when the degree of extension is not a power of 2 give rise to generators of class fields as well.

Main ideas in the proof: a careful study of the (generalized) modular polynomial associated to x_N and Shimura reciprocity.

Singular invariants - genus one levels, Case 2

Case 2. $(a, N) > 1$, hence τ is a fixed point of some elliptic element of $\Gamma_0(N)^+$

We utilize the equation (2) and properties of the Schwarzian derivative

$$S(x_N) = \left(\frac{x_N''}{x_N'}\right)' - \frac{1}{2}\left(\frac{x_N''}{x_N'}\right)^2$$

to show that for

$$Q_N(y) = 2\prod_{e\in\mathcal{E}_N}(y - x_N(e))^2\prod_{i=1}^{3}(y - x_N(a_i))^2 := 2h_N(y)^2.$$

the product $Q_N(x_N(z)) \cdot \frac{S(x_N)(z)}{(x_N'(z))^2}$ is a weight zero holomorphic modular form.

Therefore, one can compute polynomials Q_N, $P_{N,0}$ and $P_{N,1}$ such that

$$Q_N(x_N(z)) \cdot \frac{S((x_N)(z))}{(x_N'(z))^2} = -\left(P_{N,0}(x_N(z)) + P_{N,1}(x_N(z))y_N(z)\right).$$

Singular invariants - genus one levels, Case 2

How? We use the $q-$expansions and solve the system

$$\frac{1}{2}Q_N(x_N)\frac{2S(x_N)(x_N')^2}{(2\pi)^4}+(P_{N,0}(x_N)+P_{N,1}(x_N)y_N)\frac{(x_N')^4}{(2\pi)^4}=0.$$

Some further (simple) considerations are needed in case when $x_N(e)=x_N(f)$, for $e,f\in\mathcal{E}_N$ is a root of elliptic equation (2)

$\frac{1}{2}Q_N$ is a full square and equals the product of the square of the W. equation of the curve (2) and the square of a polynomial which gives generators of class fields.

This also suffices to prove that $x_N(\tau)$ and $y_N(\tau)$ are algebraic integers.

A procedure for generating class fields - classical approach

1. Choose a "good" modular function f so that its values at CM points are known to lie in the corresponding class field

2. Identify sufficiently many CM points τ which produce distinct values of $f(\tau)$ in that class field.

(usually some type of Shimura reciprocity - can not be applied to elliptic CM points)

3. Class polynomials are constructed as $\prod_{\tau}(x - f(\tau))$; the number of terms in this product is the class number.

The choice of f is very important in order to get class polynomials of small height. There are a few good candidates presented in the literature, with the most recent and efficient ones given by certain quotients of Dedekind eta functions.

A procedure for generating class fields - elliptic CM points

For prime levels $N = p$ compute a generator of the class field of the order $\mathbb{Z}[\sqrt{-p}]$ when $p \equiv 1 \bmod 4$ and of $\mathbb{Z}[(-p+\sqrt{-p})/2]$ when $p \equiv 3 \bmod 4$, respectively. The procedure we propose is

1. Find canonical generators x_p and y_p with integer coefficients that begin with q^{-a} and q^{-b} resp. by implementing the first algorithm described.

2. Evaluate the polynomial equation $P_p(x_p, y_p) = 0$ satisfied by the generators x_p and y_p by studying their q-expansions, the polynomial is

$$P_p(X, Y) = Y^a - X^b + AY^{a-1}X + BY^{a-2}X^2 + \ldots \tag{3}$$

3. Determine the set $\mathcal{E}_p$ of elliptic fixed points of $\Gamma_0(p)^+$.

4. Solve the system of equations

$$Q_p(x_p(z)) \cdot \frac{S(x_p)(z)}{(x_p'(z))^2} = -\left(\sum_{j=0}^{g_{p,+}} P_{p,j}(x_p(z))(y_p(z))^j\right)$$

A procedure for generating class fields - elliptic CM points

Further details regarding the polynomial $Q_p(y)$ are given in the paper published in Math. Comp. in 2022.

The degree is initially set to be $2(e_p + 3g_{p,+})$, but should to be increased by 4 if $P_p(X, Y)$ is singular.

The factors of Q_p which are equal to a product of terms $(y - x_p(e))^2$ over all distinct degree 2 elements e with the same class number will give the class polynomial:

If $p \equiv 1 \bmod 4$, there is a factor of Q_p that vanishes at the point $x_p(i/\sqrt{p})$; that factor is the generating polynomial of order $\mathbb{Z}[\sqrt{-p}]$ over $\mathbb{Q}[\sqrt{-p}]$.

If $p \equiv 3 \bmod 4$, there is a factor of Q_p that vanishes at $x_p\left(\frac{-2p+2i\sqrt{p}}{p(p+1)}\right)$; that factor is the generating polynomial of order $\mathbb{Z}[(-p + \sqrt{-p})/2]$ over $\mathbb{Q}[\sqrt{-p}]$.

Modular polynomials from elliptic CM points, prime levels

1. Genus $q = 1$, $N = 131$

The generating polynomial of the Hilbert class field of $K = \mathbb{Q}[\sqrt{-131}]$ is:

$$P(x) = x^{15} + 6x^{14} + 8x^{13} - 69x^{12} - 464x^{11} - 1568x^{10} - 3629x^9 - 6298x^8 - 8452x^7 - 8835x^6 - 7140x^5 - 4412x^4 - 1968x^3 - 688x^2 - 160x - 16.$$

2. Genus $q = 2$, $N = 191$

The generating polynomial of the class field $\mathbb{Z}[\sqrt{-191}]$ over $K = \mathbb{Q}[\sqrt{-191}]$ is:

$$x^{13} - 39x^{11} - 204x^{10} - 553x^9 - 903x^8 - 863x^7 - 501x^6 - 721x^5 - 2157x^4 - 3761x^3 - 4019x^2 - 2254x - 539$$

The generating polynomial of the class field $\mathbb{Z}[(-191 + \sqrt{-191})/2]$ is:

$$x^{13} + 12x^{12} + 61x^{11} + 184x^{10} + 363x^9 + 485x^8 + 429x^7 + 227x^6 + 35x^5 - 41x^4 - 33x^3 - 3x^2 + 2x + 1$$

Modular polynomials from elliptic CM points, composite level

$N = 182$, $K = \mathbb{Q}(\sqrt{-182})$, and $D = -4 \cdot 182 = -728$ with the class number 12.

The algorithm produces the polynomial $x^3 - x^2 - 8x - 20$ which generates degree 4 subfield.

This polynomial is irreducible over the genus field $K(\sqrt{-7}, \sqrt{13})$ of K which is a degree four extension of K. Therefore, the degree 12 extension $K(\sqrt{-7}, \sqrt{13}, \alpha)$, where

$$\alpha = \frac{1}{3}\left(1 + (307 - 12\sqrt{546})^{1/3} + (307 + 12\sqrt{546})^{1/3}\right)$$

is the real root of the polynomial $x^3 - x^2 - 8x - 20$, is actually the Hilbert class field of the order $\mathbb{Z}[\sqrt{-182}]$ of K.

The minimal polynomial for the order 12 element $\sqrt{-7} + \sqrt{13} + \alpha$ has considerably smaller height than the class field polynomial constructed using Weber functions (Hajir and Villegas in Duke J. 1997).

Modular polynomials for smaller discriminants from non-elliptic CM points

Our algoritm computes the generating polynomials of $x_N(\tau)$ for a given non-elliptic CM point τ, which is monic, but not necessarily irreducible. Using the numerical value of $x_N(\tau)$ one easily deduces the modular polynomial for $x_N(\tau)$.

Let $K = \mathbb{Q}[\sqrt{-74}]$. The CM point $\tau = i\sqrt{2/37}$ is a root of $37z^2 + 2 = 0$ of discriminant $-4 \cdot 74$. The generating polynomial of $x_{37}(i\sqrt{\frac{2}{37}})$ is

$$(4+x)(5+x)^2(-21904 - 16428x - 4440x^2 - 481x^3 - 10x^4 + x^5).$$

The value $x_{37}(i\sqrt{2/37})$ is a root of the irreducible polynomial $(-21904 - 16428x - 4440x^2 - 481x^3 - 10x^4 + x^5)$ over $\mathbb{Q}$ which is also irreducible over the genus field $K[\sqrt{37}] = \mathbb{Q}[\sqrt{37}, \sqrt{-2}]$ of K.

Therefore, the Hilbert class field of $K = \mathbb{Q}[\sqrt{-74}]$ is $K[x_{37}(i\sqrt{2/37}), \sqrt{37}]$.

Modular polynomials for larger discriminants from non-elliptic CM points

Let $K = \mathbb{Q}(\sqrt{-3})$, take $N = 131$ and $\tau_0 = -1/2 + i\sqrt{3/4}$. Then, $x_{131}(\tau_0)$ generates the ring class field of the order $\mathcal{O}$ of discriminant -51483 and its generating polynomial is (using a different algorithm):

$$\mathbb{M}(X) = X^{44} - 53256X^{43} + 196840X^{42} + 36072876X^{41} + 803257048X^{40} +$$
$$10577231264X^{39} + 100590352674X^{38} + 748632973896X^{37} + 4555739149976X^{36}$$
$$+ 23318268773404X^{35} + 102423385314232X^{34} + 391952935156016X^{33}$$
$$+ 1322270804468655X^{32} + 3969465809330543X^{31} + 10684361372758013X^{30}$$
$$+ 25943442674614481X^{29} + 57112085822866559X^{28} + 114446053134430682X^{27}$$
$$+ 209438932361476177X^{26} + 350930380264189577X^{25} + 539466844518769041X^{24}$$
$$+ 761974549729012805X^{23} + 989916214943538520X^{22} + 1183590765442302788X^{21}$$

Modular polynomials for larger discriminants cont'

$$+ 130266854802652861 7X^{20} + 131948646146292347 9X^{19}$$
$$+ 122927625714839709 9X^{18} + 105226234980688582 5X^{17}$$
$$+ 826414832379528174X^{16} + 594347401804391454X^{15}$$
$$+ 390478569474944807X^{14} + 233647478396655967X^{13}$$
$$+ 126860003405265027X^{12} + 62217820088579087X^{11}$$
$$+ 27409278283935739X^{10} + 10770710093417380X^{9}$$
$$+ 3742297708553468X^{8} + 1136826379892543X^{7}$$
$$+ 297531293754096X^{6} + 65780863462656X^{5}$$
$$+ 11953182938976X^{4} + 1714591604736X^{3}$$
$$+ 182013951744X^{2} + 12700385280X + 435974400.$$

The end

Thank you for your attention!