Class invariants for quartic CM-fields

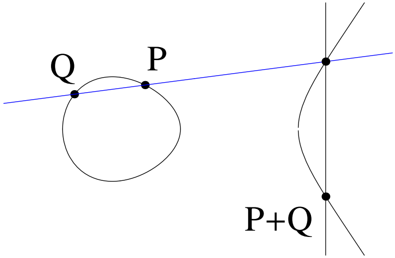
Marco Streng

THE UNIVERSITY OF WARWICK

Number Theory Seminar
Oxford
2 June 2011

Elliptic curves

- An elliptic curve E/k ($\mathrm{char}(k) \neq 2$) is a smooth projective curve
$$y^2 = x^3 + ax^2 + bx + c.$$



- E is a commutative algebraic group

Endomorphisms

- $\mathrm{End}(E) = (\text{ring of algebraic group morphisms } E \to E)$
  - $(\phi + \psi)(P) = \phi(P) + \psi(P)$
  - $(\phi\psi)(P) = \phi(\psi(P))$
- Examples:
  - $\mathbf{Z} \subset \mathrm{End}(E)$ with $n : P \mapsto P + \cdots + P$.
    For "most" E's in characteristic 0, have $\mathrm{End}(E) = \mathbf{Z}$.
  - If $E : y^2 = x^3 + x$ and $i^2 = -1$ in k, then we have
    $$i : (x, y) \mapsto (-x, iy),$$
    and $\mathbf{Z}[i] \subset \mathrm{End}(E)$.
  - If $\#k = q$, we have
    $$\mathrm{Frob} : (x, y) \mapsto (x^q, y^q).$$

The Hilbert class polynomial

The *j*-invariant is

$$j(E) = \frac{2^8 3^3 b^3}{2^2 b^3 + 3^3 c^2} \quad \text{for} \quad E : y^2 = x^3 + bx + c.$$

$$j(E) = j(F) \iff E \cong_{\overline{k}} F$$

Definition

Let K be an imaginary quadratic number field. Its Hilbert class polynomial is

$$H_K = \prod_{\substack{E/\mathbf{C} \\ \mathrm{End}(E) \cong \mathcal{O}_K}} \bigl(X - j(E)\bigr) \quad \in \mathbf{Z}[X].$$

Application 1: roots generate the Hilbert class field of K over K.
Application 2: make elliptic curves with prescribed order over $\mathbf{F}_p$.

Curves with prescribed order

- If $p = \pi\overline{\pi}$ for $\pi \in \mathcal{O}_K$, then $(H_K \bmod p)$ splits into linear factors.
- Let $j_0 \in \mathbf{F}_p$ be a root and let $E_0/\mathbf{F}_p$ have $j(E_0) = j_0$.
- Then a twist E of E_0 has "$\mathrm{Frob} = \pi$".
  Reason:
  - E_0 is the reduction of some $\widetilde{E}$ with $\mathrm{End}(\widetilde{E}) = \mathcal{O}_K$
  - CM theory $\Longrightarrow$ $\mathrm{Frob} \in \mathcal{O}_K$ and $N(\mathrm{Frob}) = p$.
- We get

$$\#E(\mathbf{F}_p) = N(\pi - 1) = p + 1 - \mathrm{tr}(\pi).$$

Computing Hilbert class polynomials (1)

- Any E is complex analytically $\mathbf{C}/\Lambda$ for a lattice Λ
- Endomorphisms induce $\mathbf{C}$-linear maps $\alpha : \mathbf{C} \to \mathbf{C}$ with $\alpha(\Lambda) \subset \Lambda$
- If $\mathrm{End}(E) \cong \mathcal{O}_K$, then $\Lambda = c\mathfrak{a}$ for an ideal $\mathfrak{a} \subset \mathcal{O}_K$ and $c \in \mathbf{C}^*$.
- We get

$$\begin{array}{ccc} \mathrm{Cl}_K & \longleftrightarrow & \dfrac{\{E/\mathbf{C} : \mathrm{End}(E) \cong \mathcal{O}_K\}}{\cong} \\ [\mathfrak{a}] & \longmapsto & \mathbf{C}/\mathfrak{a}. \end{array}$$

Computing Hilbert class polynomials (2)

- Write $\mathfrak{a} = \tau\mathbf{Z} + \mathbf{Z}$ and let $q = \exp(2\pi i\tau)$.
- Let $\theta_0 = 1 + 2\sum_{n=1}^{\infty} q^{\frac{1}{2}n^2}$ and $\theta_1 = 1 + 2\sum_{n=1}^{\infty}(-1)^n q^{\frac{1}{2}n^2}$. Then
$$j(z) = 256\frac{(\theta_0^8 - \theta_0^4\theta_1^4 + \theta_1^8)^3}{\theta_0^8\theta_1^8(\theta_0^4 - \theta_1^4)^2}$$
- Compute
$$H_K = \prod_{[\mathfrak{a}]\in\mathcal{CL}_K} (X - j(\mathbf{C}/\mathfrak{a})) \in \mathbf{Z}[X].$$
- Other algorithms:
  - p-adic, [Couveignes-Henocq 2002, Bröker 2006]
  - Chinese remainder theorem. [Chao-Nakamura-Sobataka-Tsujii 1998, Agashe-Lauter-Venkatesan 2004]

Performance

- The Hilbert class polynomial is huge: the degree h_K grows like $|D|^{\frac{1}{2}}$, as do the logarithms of the coefficients.
- Example: for $K = \mathbf{Q}(\sqrt{-101})$, get

$$
\begin{aligned}
H_K =\,& X^{14} - 2652316292259287225437667968X^{13} - 1365996687301280729477925915809419014840 32X^{12} \\
& -1891475354780093822060552578529754912659822828584 96X^{11} - 26181691797967322135414182137\backslash \\
& 3607961509161995538407779991552X^{10} - 1193885115058826956622248802184209653984472912487\backslash \\
& 3940665420165939 2X^{9} - 19970076081487858762907119018999559036025406760107290495924627270\backslash \\
& 795264X^{8} + 70524492551600286857708450126047595357088538427268967051429368624924170 6496X^{7} \\
& -33872799529198964844915900102578375435327831844475016592225474796536885894184960X^{6} \\
& -28964740677799848606869471095560110578849599906939259716546639301246667627522162688X^{5} \\
& -2256682006851346287910284831850004190305688705440243677279242465209820098759090340102144X^{4} \\
& -20029857140725594241374103253519991803846628029288114898836303084125120135029852242 7064\backslash \\
& 320X^{3} + 4726005776355464384826792760368048790095399865685681356244989969038745364 40493\backslash \\
& 770310317768704X^{2} + 1309385635604955875367012999470271658586864508328051014508458343 39\backslash \\
& 087741520825779034777771311104X - 159432100575370755282929724352954504040081348440017 0\backslash \\
& 063825647603421973516654721364784863808910786 56
\end{aligned}
$$

- Under GRH or heuristics, all three quasi-linear $O(|D|^{1+\epsilon})$.

Curves of genus 2

Definition

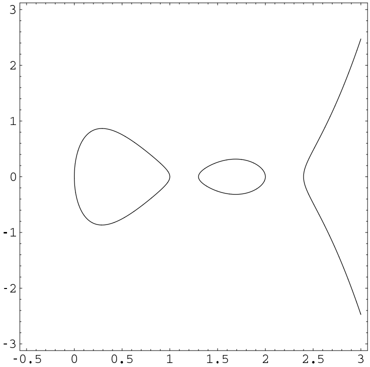
A curve of genus 2 is a smooth geometrically irreducible curve of which the genus is 2.

"Definition" (char.$\neq 2$)

A curve of genus 2 is a smooth projective curve that has an affine model

$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

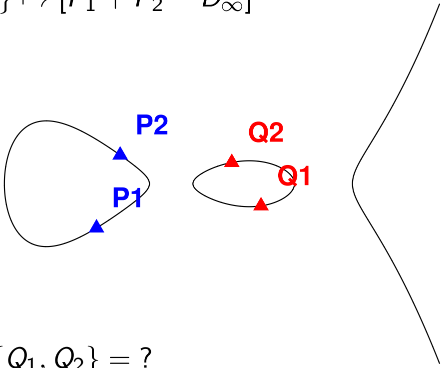
where f has no double roots.



The group law on the Jacobian

The Jacobian: group of equivalence classes of pairs of points.

- More precisely, divisor class group $\mathrm{Pic}^0(C)$
  $\{P_1, P_2\} \mapsto [P_1 + P_2 - D_\infty]$

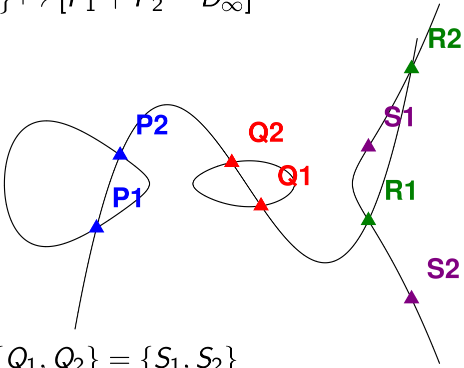


$\{P_1, P_2\} + \{Q_1, Q_2\} = ?$

The group law on the Jacobian

The Jacobian: group of equivalence classes of pairs of points.

- More precisely, divisor class group $\mathrm{Pic}^0(C)$
  $\{P_1, P_2\} \mapsto [P_1 + P_2 - D_\infty]$



$\{P_1, P_2\} + \{Q_1, Q_2\} = \{S_1, S_2\}$

Complex multiplication

- Elliptic curves E have CM if $\mathrm{End}(E)$ is an order in an imaginary quadratic field $K = \mathbf{Q}(\sqrt{r})$ with $r \in \mathbf{Q}$ negative.
- Curves C of genus 2 have CM if $\mathrm{End}(J(C))$ is an order in a CM field K of degree 4, i.e. $K = K_0(\sqrt{r})$ with K_0 real quadratic and $r \in K_0$ totally negative.
- Assume K contains no imaginary quadratic field.

Rosenhain form

- Over algebraically closed fields, we can write any elliptic curve in Legendre form

$$E : y^2 = x(x-1)(x-\lambda).$$

- and any curve of genus 2 in Rosenhain form

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

- The moduli space of elliptic curves is one-dimensional, that of curves of genus 2 is three-dimensional.

Igusa invariants

- Igusa gave a genus-2 analogue of the j-invariant (i.e., a model for the moduli space)
- Mestre's algorithm (available in Magma) constructs an equation for the curve from its invariants.
- This may need an extension of degree 2 over the field of moduli.
- The Igusa class polynomials of a quartic CM field K are a set of polynomials of which the roots are the Igusa invariants of curves C of genus 2 with CM by $\mathcal{O}_K$.

Applications

- Roots generate class fields.
  - not of K, but of its "reflex field" (no problem)
  - not the full Hilbert class field (but we know which field)
  - useful? efficient? (work in progress!)
- If $p = \pi\overline{\pi}$ in $\mathcal{O}_K$, construct curve C with

$$\#J(C)(\mathbf{F}_p) = N(\pi - 1) \quad \text{and} \quad \#C(\mathbf{F}_p) = p + 1 - \mathrm{tr}(\pi).$$

Algorithms

1. Complex analytic [Spallek 1994, Van Wamelen 1999]
2. p-adic [Gaudry-Houtmann-Kohel-Ritzenthaler-Weng 2002, Carls-Kohel-Lubicz 2008]
3. Chinese remainder theorem [Eisenträger-Lauter 2005]

None of these had running time bounds:

- denominators (now bounded by Goren and Lauter)
- not known how to bound $|i_n(C)|$.
- algorithms not explicit enough
- no rounding error analysis for alg. 1 (not even for genus 1!!)

Complex CM surfaces

- $K \otimes \mathbf{R} \cong \mathbf{C}^2$ as $\mathbf{R}$-algebra
- let Φ be an isomorphism and $\mathfrak{a} \subset K$ an $\mathcal{O}_K$-ideal
- Then $\mathbf{C}^2/\Phi(\mathfrak{a})$ has CM by $\mathcal{O}_K$
  (also need a polarization ξ, which we'll ignore)
- Can enumerate triples $(\Phi, \mathfrak{a}, \xi)$ up to isomorphism.
- By choosing the right kind of basis, get $\mathbf{C}^2/(\tau\mathbf{Z}^2 + \mathbf{Z})$ with $\tau \in \mathrm{Mat}_2(\mathbf{C})$ symmetric with positive definite imaginary part.

Theta constants

Thomae's formula [1870] gives a model for C, given τ.
For $c_1, c_2 \in \mathbf{Q}^g$, let

$$\theta[c_1, c_2](\tau) = \sum_{v \in \mathbf{Z}^g} \exp(\pi i (v + c_1)\tau(v + c_1)^{\mathrm{t}} + 2\pi i (v + c_1) c_2^{\mathrm{t}}).$$

For $c_1 = \frac{1}{2}(a, b)$, $c_2 = \frac{1}{2}(c, d)$, write $\theta_{a+2b+4c+8d} = \theta[c_1, c_2]$. Let

$$\lambda_1 = \frac{\theta_0^2 \theta_1^2}{\theta_2^2 \theta_3^2}, \quad \lambda_2 = \frac{\theta_1^2 \theta_{12}^2}{\theta_2^2 \theta_{15}^2}, \quad \lambda_3 = \frac{\theta_0^2 \theta_{12}^2}{\theta_3^2 \theta_{15}^2}.$$

Then the polarized ab. surface corresponding to τ is $\mathrm{Jac}(C)$ with

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

Igusa invariants in terms of theta

- Write out, get [Bolza 1887, Igusa 1967]

$$i_k(\tau) = \frac{\text{pol. in } \theta\text{'s}}{\prod \theta^4}, \qquad \text{e.g.} \qquad i_2(\tau) = \frac{(\sum \theta^8)^5}{\prod \theta^4},$$

  sums and products taken over $\theta[c_1, c_2]$ with $c_i \in \{0, \frac{1}{2}\}^2$ and $2c_1^t c_2 \in \mathbf{Z}$.
- Evaluate Igusa class polynomials numerically.
- Bound absolute values by bounding entries of τ.

Thesis result

Theorem

Algorithm computes the Igusa class polynomials of K in time less than

$$\mathrm{cst.}(D_1^{7/2} D_0^{11/2})^{1+\epsilon},$$

where $D_0 = \operatorname{disc} K_0$ and $D_1 D_0^2 = \operatorname{disc} K$. The bit size of the output is between

$$\mathrm{cst.}(D_1^{1/2} D_0^{1/2})^{1-\epsilon} \quad \text{and} \quad \mathrm{cst.}(D_1^{2} D_0^{3})^{1+\epsilon}.$$

Bottlenecks:

1. quasi-quadratic time theta evaluation (quasi-linear method not proven [Dupont 2006])
2. denominator bounds not optimal (special cases/conjectures [Bruinier-Yang 2006, Yang (preprint)])

A cube root of j with $K = \mathbf{Q}(\sqrt{-101})$

$$
\begin{aligned}
H_K = {} & X^{14} - 26523162922592872254376679 68X^{13} - 136599668730128072947792591580941901484032X^{12} \\
& -18914753547800938220605525785297549126598228 2858496X^{11} - 2618169179796732213541418 2137\backslash \\
& 360796150916199553840777999 1552X^{10} - 119388511505882695662224880218420965398447291 2487\backslash \\
& 3940665420165 9392X^{9} - 199700760814878587629071190189995590360254067601072904959246272 70\backslash \\
& 795264X^{8} + 705244925516002868577084501260475953570885384272689670514293686249241706496X^{7} \\
& -3387279952919896484491590010257837543532783184447501659222547479653688589418496 0X^{6} \\
& -28964740677799848606869471095560110578849599906939259716546639301246667627522162688X^{5} \\
& -2256682006851346287910284831850004190305688705440243677279242465209820098759090340102144X^{4} \\
& -2002985714072559424137410325351999180384662802928811489883630308412512013502985224270 64\backslash \\
& 320X^{3} + 4726005776355464384826792760368048790095399865685681356244989969038745364404 93\backslash \\
& 770310317768704X^{2} + 13093856356049558753670129994702716585868645083280510145084583433 9\backslash \\
& 0877415208257790347777713111 04X - 159432100575370755282929724352954504040081348440017 0\backslash \\
& 06382564760342197351665472136478486380891078656
\end{aligned}
$$

But $\sqrt[3]{j} \in \mathcal{H}_K$, with minimal polynomial

$$
\begin{aligned}
& x^{14} - 1384191268x^{13} - 54409559932784x^{12} - 109975523484025600x^{11} - 6497263664420010 9056x^{10} \\
& - 93870013855499653529 6x^{9} - 301077128582729878118400x^{8} - 12465371501488887595892736x^{7} \\
& - 46994916157152578945115750 4x^{6} - 109510996089590350647624990 72x^{5} \\
& - 825985238745823051483950612 48x^{4} + 130539260721880851394736213196 8x^{3} \\
& + 143977048189883901779330025390 08x^{2} - 40695014697105469250394793181184x \\
& - 542240463480639621593647374401536
\end{aligned}
$$

The Hilbert class field

- The Hilbert class field $\mathcal{H}_K$ of K is the largest unramified abelian extension of K.
  - CM fact: $\mathcal{H}_K = K[X]/H_K$
- There is a natural isomorphism $\mathrm{Cl}_K \to \mathrm{Gal}(\mathcal{H}_K/K)$.
  - CM fact: $[\mathfrak{b}] \cdot j(\mathbf{C}/\mathfrak{a}) = j(\mathbf{C}/\mathfrak{b}^{-1}\mathfrak{a})$.
- A class invariant is a value $f(\tau) \in \mathcal{H}_K$ of a modular function f in a point $\tau \in K$.
  - Example: $j(\omega)$ with $\mathcal{O}_K = \mathbf{Z} + \tau\mathbf{Z}$
  - Example: on previous slide, also $j(\omega)^{1/3}$
- Weber (around 1900) studied "smaller" class invariants.

Modular functions

- For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q})$, let $A\tau = \frac{a\tau+b}{c\tau+d}$.
- A modular form of weight k and level n is a holomorphic map $f : \mathcal{H} \to \mathbf{C}$ satisfying

$$f(A\tau) = (c\tau + d)^k f(\tau)$$

  for all $A \in \Gamma(n) = \ker(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}))$, and a convergence condition at the cusps.
- Example: linear combination of products of $2k$ theta's
- Has a Fourier expansion $f(\tau) = \sum_{k=0}^{\infty} a_k q^{k/n}$ with $q = e^{2\pi i \tau}$.
- Let $\mathcal{F}_n = \{\frac{f}{g} : f, g$ of weight k, level n, coefficients in $\mathbf{Q}(\zeta_n)\}$
- $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathcal{F}_n$ by $f^A(\tau) := f(A\tau)$, induces action of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$.

Modular functions

- Let $\mathcal{F}_n = \{\frac{f}{g} : f, g \text{ of weight } k, \text{ level } n, \text{ coefficients in } \mathbf{Q}(\zeta_n)\}$
- $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathcal{F}_n$ by $f^A(\tau) := f(A\tau)$,
  induces action of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$.
- $(\mathbf{Z}/n\mathbf{Z})^* = \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ acts on $\mathcal{F}_n$ by acting on coeffs.
- Let $(\mathbf{Z}/n\mathbf{Z})^* \subset \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ via $v \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)$.
- Fact: $\mathcal{F}_1 = \mathbf{Q}(j)$, $\mathrm{Gal}(\mathcal{F}_n/\mathcal{F}_1) = \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}$

Shimura's reciprocity law

- Let $\mathcal{O}_K = \omega\mathbf{Z} + \mathbf{Z}$.
- The values $f(\omega)$ for $f \in \mathcal{F}_n$ generate the ray class field $\mathcal{H}_K^n$ of K of conductor n.
- $\mathrm{Gal}(\mathcal{H}_K^n/\mathcal{H}_K) = (\mathcal{O}_K/n\mathcal{O}_K)^*$.
- Shimura's reciprocity law gives a map $g = g_\omega : (\mathcal{O}_K/n\mathcal{O}_K)^* \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ such that $f(\omega)^x = f^{g(x)}(\omega)$.
- $g(x)^{\mathrm{t}}$ is the matrix of multiplication by x with respect to the basis ω, 1 of $\mathcal{O}_K$.

Shimura's reciprocity law

- $\mathrm{Gal}(\mathcal{H}_K^n/\mathcal{H}_K) = (\mathcal{O}_K/n\mathcal{O}_K)^*$.
- Shimura's reciprocity law gives a map
  $g = g_\omega : (\mathcal{O}_K/n\mathcal{O}_K)^* \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$
  such that $f(\omega)^x = f^{g(x)}(\omega)$.
- $g(x)^{\mathrm{t}}$ is the matrix of multiplication by x wrt $\omega, 1$.
- If f is fixed under $g_\omega((\mathcal{O}_K/n\mathcal{O}_K)^*)$, then $f(\omega) \in \mathcal{H}_K$, that is, $f(\omega)$ is a class invariant
- Any example gives a whole family of number fields that are examples!
- A more general version of g gives the orbit of $f(\omega)$ under $\mathrm{Gal}(\mathcal{H}_K/K)$.

Shimura reciprocity for dimension > 1

- Shimura's reciprocity law for dimension > 1 can be made as explicit as on the previous slide (just more complicated).
- The action of $\mathrm{Sp}_{2g}(\mathbf{Z})$ on the θ's is also explicit.
- Example: $\lambda_1 = \frac{\theta_0^2\theta_1^2}{\theta_2^2\theta_3^2}$ is a class invariant if 2 splits completely in K
- Example:

$$e^{5\pi i/4}\frac{\theta_2\theta_3\theta_4}{\theta_8\theta_9\theta_{15}}$$

  is a class invariant for a certain τ for $K = \mathbf{Q}(\alpha)$ with $\alpha^4 + 54\alpha^2 + 521 = 0$.

Example

The Hilbert class field of $K = \mathbf{Q}(\alpha)$ with $\alpha^4 + 54\alpha^2 + 521 = 0$ is given by

$$\begin{aligned}
&10201X^7 + (15520516211635864775 5w + 55960017022093888711 0)X^6 \\
&+(1524076876974601951759207505355941525 50w \\
&\quad +5495137327680949562589706361181928594 00)X^5 \\
&+\tfrac{1}{2}(22019095800305237302726238484345380483178345138 75w \\
&\quad +79390978947354318441530190893209731530112108821 25)X^4 \\
&+(1047175262927393182849164587480891367594710449395570625w \\
&\quad +3775644104882200832865729346429752069380200097845736875)X^3 \\
&+\tfrac{1}{2}(907392914800494855136752991106041311116404713247380607234375w \\
&\quad +327165168130591119268893142372375309476346120037916993828437 5)X^2 \\
&+(1501416604965651986004588022297124411339065052590506998745406250 0w \\
&\quad +5413434555036719078560598444558693989308353185140536597841106250 0)X \\
&+\tfrac{1}{2}(32085417029115132212877701052175189051312077050549053777767632898437 5w \\
&\quad +11568561629312006703870932114432428501257096676832654599179872792968 75)
\end{aligned}$$

$w = \sqrt{13} = \frac{1}{4}(\alpha^2 + 27) \in \mathbf{Q}(w)[X]$

But also by

$$\begin{aligned}
&32724y^7 + \big(-2565\alpha^3 + 41958\alpha^2 - 19305\alpha + 543996\big)y^6 \\
&+\big(157041\alpha^3 - 874980\alpha^2 + 1982817\alpha - 10998810\big)y^5 \\
&+\big(86247\alpha^3 - 3144210\alpha^2 + 1090035\alpha - 39544356\big)y^4 \\
&+\big(929411\alpha^3 + 2159184\alpha^2 + 11694475\alpha + 27138894\big)y^3 \\
&+\big(1679697\alpha^3 + 14532218\alpha^2 + 21122613\alpha + 182787868\big)y^2 \\
&+\big(-3975265\alpha^3 + 28878240\alpha^2 - 50000345\alpha + 363226614\big)y \\
&-2905827\alpha^3 - 3366054\alpha^2 - 36548895\alpha - 42337548
\end{aligned}$$