Reducing number field defining polynomials: An application to class group computations

Alexandre Gélin

Laboratoire d'Informatique de Paris 6, UPMC, Sorbonne Universités

09/11/2016

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q}$ $\Rightarrow$ $\exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} = \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q}$ $\Rightarrow$ $\exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} = \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals
- Group of units

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q}$ $\Rightarrow$ $\exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} = \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals
  Quotient by principal ideals $\Rightarrow$ class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$
- Group of units
  Finitely generated $\Rightarrow$ fundamental units

Number fields

$\mathbb{K}$ number field $\Rightarrow$ finite extension of $\mathbb{Q}$ $\Rightarrow$ $\exists T \in \mathbb{Z}[X]$ monic s.t.

$$\mathbb{K} = \mathbb{Q}[X]/(T).$$

T is a defining polynomial of $\mathbb{K}$.

Two interesting structures:

- Group of ideals
  Quotient by principal ideals $\Rightarrow$ class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$
- Group of units
  Finitely generated $\Rightarrow$ fundamental units

Aim: Compute the structure of the class group.

Outline

1. Overview on class groups
   - State of the art
   - General strategy for computation

2. Reducing the defining polynomial
   - Theoretical results
   - Our algorithm

Subexponential L-notation : $L_N(0,c) \approx (\log N)^c \quad L_N(1,c) \approx N^c$

$$L_N(\alpha, c) = \exp\left((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right).$$

1969 Shanks: quadratic number fields in $O(|\Delta_{\mathbb{K}}|^{\frac{1}{5}})$.

1989 Hafner and McCurley: imaginary quadratic number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, \sqrt{2})$.

1990 Buchmann: all number fields with fixed degree in $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2}, 1.7)$.

2014 Biasse and Fieker: all number fields in $L_{|\Delta_{\mathbb{K}}|}(\frac{2}{3} + \varepsilon)$ in general and $L_{|\Delta_{\mathbb{K}}|}(\frac{1}{2})$ if $n \leq \log(|\Delta_{\mathbb{K}}|)^{3/4-\varepsilon}$.

2014 Biasse and Fieker: number fields defined by a *good* polynomial in $L_{|\Delta_{\mathbb{K}}|}(a)$, $\frac{1}{3} \leq a < \frac{1}{2}$.

Index calculus

1. **Factor base**
   Fix a factor base composed of small elements.
2. **Relation collection**
   Collect some relations between those small elements, corresponding to linear equations.
3. **Linear algebra**
   Deduce the sought result performing linear algebra on the system built.

The factor base

$$\mathcal{B} = \{\text{prime ideals in } \mathcal{O}_{\mathbb{K}} \text{ of norm below } B\}$$

B determined so that $\mathcal{B}$ **generates the whole class group**.

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbb{K}} = \sqrt{|\Delta_{\mathbb{K}}|} \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}.$$

Bach's bound: assuming GRH, classes of ideals of norm less than $12(\log|\Delta_{\mathbb{K}}|)^2$ generate the class group.

The factor base

$$\mathcal{B} = \{\text{prime ideals in } \mathcal{O}_{\mathbb{K}} \text{ of norm below } B\}$$

B determined so that $\mathcal{B}$ **generates the whole class group**.

Minkowski's bound: every class contains an ideal of norm smaller than

$$M_{\mathbb{K}} = \sqrt{|\Delta_{\mathbb{K}}|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

Bach's bound: assuming GRH, classes of ideals of norm less than $12(\log|\Delta_{\mathbb{K}}|)^2$ generate the class group.

Practically

$$B = L_{|\Delta_{\mathbb{K}}|}(\beta, c_b).$$

Relation collection

$$\mathcal{B} = (\mathfrak{p}_1, \cdots, \mathfrak{p}_N)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\phi} & \mathcal{I} & \xrightarrow{\pi} & \mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \\ (e_1, \cdots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

$$\mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \simeq \mathbb{Z}^N / \left\{ (e_1, \cdots, e_N) \in \mathbb{Z}^N \mid \prod_i \mathfrak{p}_i^{e_i} = (\alpha)\mathcal{O}_{\mathbb{K}} \right\}$$

Relation collection

$$\mathcal{B} = (\mathfrak{p}_1, \cdots, \mathfrak{p}_N)$$

Surjective morphism:

$$\begin{array}{ccccc} \mathbb{Z}^N & \xrightarrow{\phi} & \mathcal{I} & \xrightarrow{\pi} & \mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \\ (e_1, \cdots, e_N) & \longmapsto & \prod_i \mathfrak{p}_i^{e_i} & \longmapsto & \prod_i [\mathfrak{p}_i]^{e_i} \end{array}$$

$$\mathsf{Cl}(\mathcal{O}_{\mathbb{K}}) \simeq \mathbb{Z}^N / \left\{ (e_1, \cdots, e_N) \in \mathbb{Z}^N \mid \prod_i \mathfrak{p}_i^{e_i} = (\alpha)\mathcal{O}_{\mathbb{K}} \right\}$$

Idea:

1. Pick at random $A = \prod_i \mathfrak{p}_i^{v_i}$.
2. Find a *reduced* ideal A' in the same class.
3. If A' splits on $\mathcal{B}$ ($\Leftrightarrow A' = \prod_i \mathfrak{p}_i^{v'_i}$) then

$$A(A')^{-1} = \prod_i \mathfrak{p}_i^{v_i - v'_i} \quad \text{is principal.}$$

Linear algebra

- Relations stored in a matrix of size about $N \times N$.
- Structure of the class group given by the *Smith Normal Form* of the matrix.
- First compute *Hermite Normal Form* with a premultiplier because we need kernel vectors.
- Storjohann and Labahn algorithm, runtime in $N^{\omega+1}$ ($2 \leq \omega \leq 3$ exponent of matrix multiplication)

Verification

We find a tentative class group H, but the class group $\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.

$\Rightarrow$ Need an approximation of the class number $h_K = |\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Verification

We find a tentative class group H, but the class group $\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.
$\Rightarrow$ Need an approximation of the class number $h_K = |\mathrm{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Class number formula + Euler Product:

$$h_{\mathbb{K}}\mathrm{Reg}_{\mathbb{K}} = \mathrm{EP} \cdot \frac{w_{\mathbb{K}} \cdot \sqrt{|\Delta_{\mathbb{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}.$$

Verification

We find a tentative class group H, but the class group $\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})$ may be only a quotient of H.
$\Rightarrow$ Need an approximation of the class number $h_K = |\mathsf{Cl}(\mathcal{O}_{\mathbb{K}})|$.

Class number formula + Euler Product:

$$h_{\mathbb{K}}\mathsf{Reg}_{\mathbb{K}} = \mathsf{EP} \cdot \frac{w_{\mathbb{K}} \cdot \sqrt{|\Delta_{\mathbb{K}}|}}{2^{r_1} \cdot (2\pi)^{r_2}}.$$

From the relations, we can also deduce a candidate for an approximation of Reg_K and perform the verification step.

Outline

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

Definition

Let $T = \sum a_k X^k \in \mathbb{Z}[X]$. The height of T is defined as the maximal norm of its coefficients, namely

$$H(T) = \max_k |a_k|.$$

What is a *good* polynomial ?

We want a polynomial that defines a fixed number field:

- The degree is fixed,
- We want the coefficients as small as possible.

Definition

Let $T = \sum a_k X^k \in \mathbb{Z}[X]$. The height of T is defined as the maximal norm of its coefficients, namely

$$H(T) = \max_k |a_k|.$$

Proposition

For every defining polynomial T of a degree-n number field $\mathbb{K}$, the discriminants satisfy

$$|\Delta_{\mathbb{K}}| \leq |\Delta(T)| \leq n^{2n} H(T)^{2n-2}.$$

Classes from Biasse and Fieker work

Definition

Let $n_0, d_0 > 0$ and $0 < \alpha < \frac{1}{2}$.

$$\mathcal{C}_{n_0,d_0,\alpha} = \left\{ \mathbb{K} = \mathbb{Q}[X]/(T) \middle| \begin{array}{l} \deg(T) = n_0(\log|\Delta_{\mathbb{K}}|)^{\alpha}(1+o(1)) \\ \log H(T) = d_0(\log|\Delta_{\mathbb{K}}|)^{1-\alpha}(1+o(1)) \end{array} \right\}$$

Theorem

There exists an $L_{|\Delta_{\mathbb{K}}|}(a)$ algorithm for class group computation for

$$a = \max\left(\alpha, \frac{1-\alpha}{2}\right).$$

Minimal height

If $\mathbb{K} \in \mathcal{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbb{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Minimal height

If $\mathbb{K} \in \mathcal{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbb{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbb{K}$, there exists a defining polynomial T s.t.

$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbb{K}}|}{n} \right)^{\frac{n}{2n-2}}.$$

Minimal height

If $\mathbb{K} \in \mathcal{C}_{n_0,d_0,\alpha}$, there exists T such that
$$H(T) = |\Delta_{\mathbb{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbb{K}$, there exists a defining polynomial T s.t.
$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbb{K}}|}{n}\right)^{\frac{n}{2n-2}}.$$

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathcal{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbb{K} = \frac{\mathbb{Q}[X]}{(T)} \middle| \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log|\Delta_{\mathbb{K}}|}{\log\log|\Delta_{\mathbb{K}}|}\right)^{\alpha} \\ \log H(T) \leq d_0 (\log|\Delta_{\mathbb{K}}|)^{\gamma} (\log\log|\Delta_{\mathbb{K}}|)^{1-\gamma} \end{array} \right\}$$

Minimal height

If $\mathbb{K} \in \mathcal{C}_{n_0,d_0,\alpha}$, there exists T such that

$$H(T) = |\Delta_{\mathbb{K}}|^{\frac{\kappa}{n}}, \quad \text{with } \kappa = n_0 d_0 (1 + o(1)).$$

Proposition

For every number field $\mathbb{K}$, there exists a defining polynomial T s.t.

$$H(T) \leq 3^n \left(\frac{|\Delta_{\mathbb{K}}|}{n} \right)^{\frac{n}{2n-2}}.$$

Definition

Let $n_0, d_0 > 0$, $0 < \alpha < 1$ **and** $1 - \alpha \leq \gamma \leq 1$.

$$\mathcal{D}_{n_0,d_0,\alpha,\gamma} = \left\{ \mathbb{K} = \frac{\mathbb{Q}[X]}{(T)} \middle| \begin{array}{l} \deg(T) \leq n_0 \left(\frac{\log |\Delta_{\mathbb{K}}|}{\log \log |\Delta_{\mathbb{K}}|} \right)^{\alpha} \\ \log H(T) \leq d_0 (\log |\Delta_{\mathbb{K}}|)^{\gamma} (\log \log |\Delta_{\mathbb{K}}|)^{1-\gamma} \end{array} \right\}$$

Every number field belongs to such a class $\mathcal{D}_{n_0,d_0,\alpha,\gamma}$.

Prior reduction algorithm

Cohen and Diaz y Diaz minimize the size of $T = \prod(X - \tau_j)$, defined as

$$S(T) = \sum |\tau_j|^2.$$

Equivalent to find a short vector in the lattice $\mathcal{O}_{\mathbb{K}}$, because $\mathcal{O}_{\mathbb{K}}$ is generated by the vectors

$$[\sigma_1(\tau_j), \cdots, \sigma_n(\tau_j)]$$

☺ **Examples:**

Input	Output
$x^3 - 5955x^2 + 18142x - 607593$	$x^3 - x^2 - 2100x + 38117$
$x^3 - 269463x^2 + 752031x - 518157$	$x^3 - x^2 - 1307x - 13359$
$x^3 - 482665x^2 + 773338x - 308749$	$x^3 - x^2 - 3210x + 61325$
$x^3 - 456191x^2 + 958783x - 499681$	$x^3 - x^2 - 936x - 7616$

Prior reduction algorithm

Cohen and Diaz y Diaz minimize the size of $T = \prod(X - \tau_j)$, defined as

$$S(T) = \sum |\tau_j|^2.$$

Equivalent to find a short vector in the lattice $\mathcal{O}_{\mathbb{K}}$, because $\mathcal{O}_{\mathbb{K}}$ is generated by the vectors

$$[\sigma_1(\tau_j), \cdots, \sigma_n(\tau_j)]$$

☹ **Examples:**

Input	Output
$x^3 + 6381x^2 + 4378x - 1216$	$x^3 - x^2 - 3537064x + 2193757452$
$x^3 - 9681x^2 - 5434x - 6901$	$x^3 - 31246021x - 67226458585$
$x^3 - 6665x^2 - 4318x - 2977$	$x^3 + 336681x - 419200237$
$x^3 - 6018x^2 - 1387x + 6161$	$x^3 - 12073495x - 16147208593$

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbb{K}$.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbb{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbb{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathcal{O}_{\mathbb{K}}$.

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbb{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathcal{O}_\mathbb{K}$.

Let $c > 1$ and $b^F = [b_1^F, \cdots, b_n^F]$ defined by $b_j^F = \lceil \log_c |\sigma_j(\theta_F)| \rceil$.
We introduce a *weighted* copy of $\mathcal{O}_\mathbb{K}$ in $\mathbb{C}^n$, generated by:

$$\widetilde{\Omega_i} = \left[\frac{\sigma_1(\omega_i)}{c^{b_1^F}}, \cdots, \frac{\sigma_n(\omega_i)}{c^{b_n^F}} \right].$$

Our algorithm

Goal: Find the monic polynomial T_F of minimal height defining $\mathbb{K}$.

Idea: Introduce weighted lattices and look for small vectors in them.

Let θ_F root of $T_F \longleftrightarrow v(\theta_F) = [\sigma_1(\theta_F), \cdots, \sigma_n(\theta_F)] \in \mathcal{O}_{\mathbb{K}}$.

Let $c > 1$ and $b^F = [b_1^F, \cdots, b_n^F]$ defined by $b_j^F = \lceil \log_c |\sigma_j(\theta_F)| \rceil$.
We introduce a *weighted* copy of $\mathcal{O}_{\mathbb{K}}$ in $\mathbb{C}^n$, generated by:

$$\widetilde{\Omega_i} = \left[\frac{\sigma_1(\omega_i)}{c^{b_1^F}}, \cdots, \frac{\sigma_n(\omega_i)}{c^{b_n^F}} \right].$$

By construction, $|\tilde{v}(\theta_F)_i| \leq 1$ and $\|\tilde{v}(\theta_F)\|_2 \leq \sqrt{n}$.

Differences between the two algorithms

Shape of the vectors found by the algorithm of Cohen:

Shape of the vectors we find:

As the constant coefficient of the polynomial is the product of all the roots, we prefer vectors of the second family.

Final results

- If $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_{\mathbb{K}}|}(\alpha)$.

Final results

- If $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_{\mathbb{K}}|}(\alpha)$.
- If $\gamma = 1 - \alpha$, we can apply the algorithm of Biasse and Fieker and find the class group in $L_{|\Delta_{\mathbb{K}}|}(a)$, $a = \max\left(\alpha, \frac{1-\alpha}{2}\right)$.

Final results

- If $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, we find the minimal defining polynomial T in time $L_{|\Delta_{\mathbb{K}}|}(\alpha)$.
- If $\gamma = 1 - \alpha$, we can apply the algorithm of Biasse and Fieker and find the class group in $L_{|\Delta_{\mathbb{K}}|}(a)$, $a = \max\left(\alpha, \frac{1-\alpha}{2}\right)$.

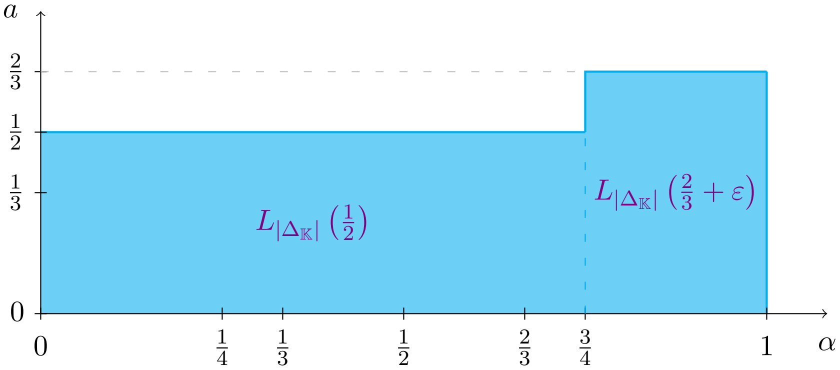
Theorem

Under GRH and smoothness heuristics, for every $\mathbb{K} \in \mathcal{D}_{n_0,d_0,\alpha,\gamma}$, $\alpha < \frac{1}{2}$, there exists an $L_{\Delta_{\mathbb{K}}}(a)$ algorithm for class group computation with

$$a = \max\left(\alpha, \frac{\gamma}{2}\right).$$

State of the art [BF14]

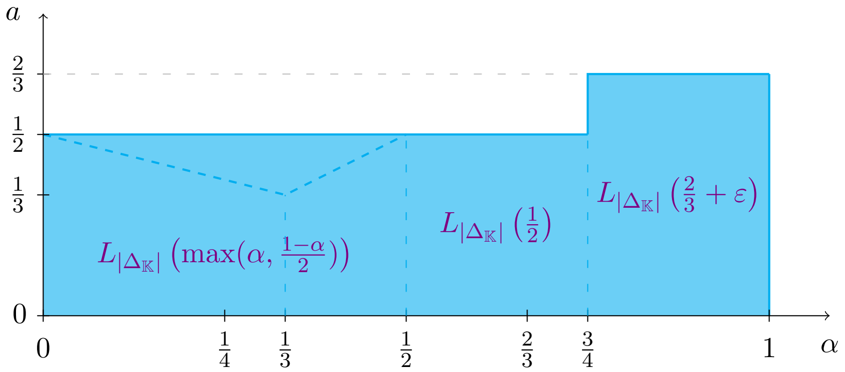
General case:



First general subexponential algorithm.

State of the art [BF14]

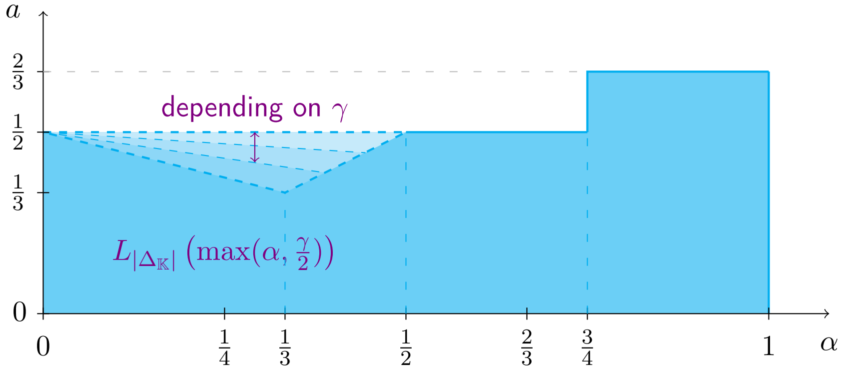
Special case:



Only if $\mathbb{K}$ is defined by T such that $H(T) = L_{|\Delta_{\mathbb{K}}|}(1-\alpha)$.

This work

General case:



Without any condition.

Practically

$\mathbb{K}$ is defined by the polynomial
$x^5 - 2x^4 - 8001397580x^3 - 31542753393650x^2 + 3636653302451131875x + 4818547529425280067500$

Magma V2.22-2 finds the class group – assuming GRH – in about 285 seconds.
With our implementation, we reduce this defining polynomial to

$$T = x^5 - 5843635x^4 + 931633x^2 + 6577x - 8570.$$

Practically

$\mathbb{K}$ is defined by the polynomial
$x^5 - 2x^4 - 8001397580x^3 - 31542753393650x^2 + 3636653302451131875x + 4818547529425280067500$

Magma V2.22-2 finds the class group – assuming GRH – in about 285 seconds.
With our implementation, we reduce this defining polynomial to

$$T = x^5 - 5843635x^4 + 931633x^2 + 6577x - 8570.$$

Magma V2.19-10 has class group computation not as optimized as in V2.22, but works with the input polynomial:

- with T: about 140 seconds,
- with the "reduced" one: about 3240 seconds.

Thanks

Merci