An algorithm to compute relative cubic fields

Anna Morra

Université Bordeaux 1

GTEM 3rd annual meeting,
September 8, 2009

Introduction

- K a number field

$$\mathcal{F}_{K,n} = \{\text{extensions } L/K, \quad [L:K] = n\}/\simeq$$

Introduction

- K a number field

$$\mathcal{F}_{K,n} \quad = \quad \{\text{extensions } L/K, \quad [L:K] = n\}/\simeq$$

$$N_{K,n}(X) = |\{L \in \mathcal{F}_{K,n}, \quad |\mathcal{N}\mathfrak{d}(L/K)| \leq X\}|.$$

Many questions:

- Exact value of $N_{K,n}(X)$ for fixed (K, n, X).

Many questions:

- Exact value of $N_{K,n}(X)$ for fixed (K, n, X).
- Asymptotics for $N_{K,n}(X)$ for fixed (K, n) and X going to infinity.

Many questions:

- Exact value of $N_{K,n}(X)$ for fixed (K, n, X).
- Asymptotics for $N_{K,n}(X)$ for fixed (K, n) and X going to infinity.
- Tables of number fields in $\mathcal{F}_{K,n}$ up to a fixed bound X on the relative discriminant.

Some asymptotic results

- Asymptotics for relative quadratic extensions (Wright, Cohen-Diaz y Diaz-Olivier)

Some asymptotic results

- Asymptotics for relative quadratic extensions (Wright, Cohen-Diaz y Diaz-Olivier)
- Asymptotics for cubic extensions Davenport-Heilbronn ($K = \mathbb{Q}$) Datskovsky-Wright (K arbitrary);

Some asymptotic results

- Asymptotics for relative quadratic extensions (Wright, Cohen-Diaz y Diaz-Olivier)
- Asymptotics for cubic extensions Davenport-Heilbronn ($K = \mathbb{Q}$) Datskovsky-Wright (K arbitrary);
- Asymptotics for $n = 4, 5$ and $K = \mathbb{Q}$: Bhargava.

Algorithmics

- Quadratic extensions over $\mathbb{Q}$: trivial

Algorithmics

- Quadratic extensions over $\mathbb{Q}$: trivial
- An efficient algorithm for computing a list of cubic fields (over $\mathbb{Q}$) of bounded discriminant by Belabas.

Algorithmics

- Quadratic extensions over $\mathbb{Q}$: trivial
- An efficient algorithm for computing a list of cubic fields (over $\mathbb{Q}$) of bounded discriminant by Belabas.

What about an algorithm for *relative cubic extensions* ?

Main result

Theorem 1

Let K be a number field.

- *There exists an algorithm to list all the cubic extensions of K with bounded discriminant.*
- *If K is imaginary quadratic, with class number 1, this algorithm has polynomial time in the size of the output.*
- *In particular we can prove it works in $\widetilde{O}(X)$.*

Main result

Theorem 1

Let K be a number field.

- *There exists an algorithm to list all the cubic extensions of K with bounded discriminant.*
- *If K is imaginary quadratic, with class number 1, this algorithm has polynomial time in the size of the output.*
- *In particular we can prove it works in $\widetilde{O}(X)$.*

We made an explicit implementation in PARI/GP for the case $K = \mathbb{Q}(i)$ which can be easily adapted for any imaginary quadratic number field with class number 1.

Over $\mathbb{Q}$

Theorem 2 (Levi, Delone-Faddeev, Davenport-Heilbronn, Belabas, Bhargava)

We have a bijection between cubic fields over $\mathbb{Q}$ (up to isomorphism) and classes of irreducible binary cubic forms

$$ax^3 + bx^2y + cxy^2 + dy^3, \quad a, b, c, d \in \mathbb{Z}$$

modulo $\mathrm{GL}_2(\mathbb{Z})$, *such that* $\langle 1, ax, ax^2 + bx \rangle_{\mathbb{Z}}$ *is a maximal subring of* $\mathbb{Q}[x]/(ax^3 + bx^2 + cx + d)$.

Over $\mathbb{Q}$

Theorem 2 (Levi, Delone-Faddeev, Davenport-Heilbronn, Belabas, Bhargava)

We have a bijection between cubic fields over $\mathbb{Q}$ (up to isomorphism) and classes of irreducible binary cubic forms

$$ax^3 + bx^2y + cxy^2 + dy^3, \quad a, b, c, d \in \mathbb{Z}$$

modulo $\mathrm{GL}_2(\mathbb{Z})$, *such that* $\langle 1, ax, ax^2 + bx \rangle_{\mathbb{Z}}$ *is a maximal subring of* $\mathbb{Q}[x]/(ax^3 + bx^2 + cx + d)$.

Belabas's algorithm : uses Dedekind criterion + sieve methods $\Longrightarrow$ we can list the $\mathcal{O}(X)$ fields of discriminants bounded by X using $\mathcal{O}(X)$ operations on integers $\leq X$.

Reduction Theory

To choose a unique representative for every class of binary cubic forms we need a covariant modulo $\mathrm{GL}_2(\mathbb{Z})$.

Reduction Theory

To choose a unique representative for every class of binary cubic forms we need a covariant modulo $\mathrm{GL}_2(\mathbb{Z})$.

To say that $F \longrightarrow H_F$ is a covariant means

$$H_{\gamma \cdot F} = \gamma \cdot H_F, \quad \forall \gamma \in \mathrm{GL}_2(\mathbb{Z})$$

Reduction Theory

To choose a unique representative for every class of binary cubic forms we need a covariant modulo $\mathrm{GL}_2(\mathbb{Z})$.

To say that $F \longrightarrow H_F$ is a covariant means

$$H_{\gamma \cdot F} = \gamma \cdot H_F, \quad \forall \gamma \in \mathrm{GL}_2(\mathbb{Z})$$

If $K = \mathbb{Q}$, the Hessian form of $F = ax^3 + bx^2y + cxy^2 + dy^3$ is such a covariant :

$$H_F = -\frac{1}{4} \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2,$$

where $P = b^2 - 3ac, Q = bc - 9ad, R = c^2 - 3bd$.

Defined binary quadratic form
$\Longrightarrow$ reduction theory (Gauss)
$\Longrightarrow$ bounds on P, Q, R in terms of the discriminant
$\Longrightarrow$ bounds on a, b, c, d.

Defined binary quadratic form
$\Longrightarrow$ reduction theory (Gauss)
$\Longrightarrow$ bounds on P, Q, R in terms of the discriminant
$\Longrightarrow$ bounds on a, b, c, d.

Thanks to Belabas (Davenport) good bounds we can list all fields with discriminant $< X$ in time $\widetilde{\mathcal{O}}(X)$.

Over an arbitrary number field

Let $\mathcal{O}$ be a Dedekind domain.
Let $V = (\mathrm{Sym}^3 \mathcal{O}^2)^*$.

Over an arbitrary number field

Let $\mathcal{O}$ be a Dedekind domain.
Let $V = (\mathrm{Sym}^3 \mathcal{O}^2)^*$.

We can see an element of V as a binary cubic form :

$$F = ax^3 + bx^2y + cxy^2 + d, \quad a, b, c, d \in \mathcal{O}.$$

Over an arbitrary number field

Let $\mathcal{O}$ be a Dedekind domain.
Let $V = (\mathrm{Sym}^3 \mathcal{O}^2)^*$.

We can see an element of V as a binary cubic form :

$$F = ax^3 + bx^2y + cxy^2 + d, \quad a, b, c, d \in \mathcal{O}.$$

Let $\mathcal{C}(\mathcal{O})$ be the set of isomorphism classes of $\mathcal{O}$-algebras wich are projective of rank 3 as $\mathcal{O}$-modules (*cubic algebras*).

Over an arbitrary number field

Let $\mathcal{O}$ be a Dedekind domain.
Let $V = (\mathrm{Sym}^3 \mathcal{O}^2)^*$.

We can see an element of V as a binary cubic form :

$$F = ax^3 + bx^2y + cxy^2 + d, \quad a, b, c, d \in \mathcal{O}.$$

Let $\mathcal{C}(\mathcal{O})$ be the set of isomorphism classes of $\mathcal{O}$-algebras wich are projective of rank 3 as $\mathcal{O}$-modules (*cubic algebras*).

For any fractional ideal $\mathfrak{a}$, we define

$$\mathcal{C}(\mathcal{O}, \mathfrak{a}) = \{R \in \mathcal{C}(\mathcal{O}) \mid \mathrm{St}(R) = \mathfrak{a}\}$$

.

- $G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha \in \mathcal{O} & \beta \in \mathfrak{a}^{-1} \\ \gamma \in \mathfrak{a} & \delta \in \mathcal{O} \end{pmatrix} \middle| \alpha\delta - \beta\gamma \in \mathcal{O}^{\times} \right\}$
- $V_{\mathfrak{a}} = \{F = (a, b, c, d) \mid a \in \mathfrak{a}, b \in \mathcal{O}, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}$

- $G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha \in \mathcal{O} & \beta \in \mathfrak{a}^{-1} \\ \gamma \in \mathfrak{a} & \delta \in \mathcal{O} \end{pmatrix} \middle| \, \alpha\delta - \beta\gamma \in \mathcal{O}^{\times} \right\}$
- $V_{\mathfrak{a}} = \{F = (a, b, c, d) \mid a \in \mathfrak{a}, b \in \mathcal{O}, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}$

Theorem 3 (Taniguchi)

There exists a canonical bijection between $\mathcal{C}(\mathcal{O}, \mathfrak{a})$ and $V_{\mathfrak{a}}/G_{\mathfrak{a}}$ making the following diagram commutative:

$$\begin{array}{ccc} V_{\mathfrak{a}}/G_{\mathfrak{a}} & \longrightarrow & \mathcal{C}(\mathcal{O}, \mathfrak{a}) \\ \Big\downarrow D & & \Big\downarrow \mathfrak{d} \\ \mathfrak{a}^{-2}/(\mathcal{O}^{\times})^2 & \xrightarrow{\times \mathfrak{a}^2} & \{ \text{ integral ideals of } \mathcal{O}\} \end{array}$$

Finding the covariant

Let $\mathcal{O}$ a maximal *imaginary quadratic* order.
Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Finding the covariant

Let $\mathcal{O}$ a maximal *imaginary quadratic* order.
Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

$$F(x, 1) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in \mathbb{C}[x].$$

Finding the covariant

Let $\mathcal{O}$ a maximal *imaginary quadratic* order.
Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

$$F(x, 1) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in \mathbb{C}[x].$$

Thanks to the work of G. Julia, J. Cremona and M. Stoll, we know that a covariant for the action of $\mathrm{GL}_2(\mathcal{O})$ is the binary hermitian form:

$$H_F = t_1^2|x - \alpha_1 y|^2 + t_2^2|x - \alpha_2 y|^2 + t_3^2|x - \alpha_3 y|^2,$$

where $t_i^2 = |a|^2|\alpha_j - \alpha_k|^2 \quad i, j, k$ pairwise distinct.

We can write

$$H_F = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2,$$

We can write

$$H_F = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2,$$

where

$$\begin{cases} P = t_1^2 + t_2^2 + t_3^2 \in \mathbb{R} \\ Q = \alpha_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 \in \mathbb{C} \\ R = |\alpha_1|^2 t_1^2 + |\alpha_2|^2 t_2^2 + |\alpha_3|^2 t_3^2 \in \mathbb{R}. \end{cases}$$

We can write

$$H_F = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2,$$

where

$$\begin{cases} P = t_1^2 + t_2^2 + t_3^2 \in \mathbb{R} \\ Q = \alpha_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 \in \mathbb{C} \\ R = |\alpha_1|^2 t_1^2 + |\alpha_2|^2 t_2^2 + |\alpha_3|^2 t_3^2 \in \mathbb{R}. \end{cases}$$

Let

$$\Delta := PR - |Q|^2 (= 3|D(F)|)$$

The hyperbolic 3-space

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}^+\} \\ &= \{h = z + tj \mid h \in \mathbb{H}, \text{ s.t. the } k - \text{component is } 0, t > 0\}\end{aligned}$$

where $\mathbb{H}$ is the quaternions ring.

The hyperbolic 3-space

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}^+\} \\ &= \{h = z + tj \mid h \in \mathbb{H}, \text{ s.t. the } k - \text{component is } 0, t > 0\}\end{aligned}$$

where $\mathbb{H}$ is the quaternions ring.

The action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$ (quaternion notation)

$$M \cdot (h) = (Ah + B)/(Ch + D),$$

for each $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}), h \in \mathcal{H}_3$.

The hyperbolic 3-space

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}^+\} \\ &= \{h = z + tj \mid h \in \mathbb{H}, \text{ s.t. the } k - \text{component is } 0, t > 0\}\end{aligned}$$

where $\mathbb{H}$ is the quaternions ring.

The action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$ (quaternion notation)

$$M \cdot (h) = (Ah + B)/(Ch + D),$$

for each $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}), h \in \mathcal{H}_3$.

Let $\mathscr{P} = \{$ positive definite binary hermitian forms in $\mathbb{C}\}$ and let $\widetilde{\mathscr{P}} = \mathscr{P}/\mathbb{R}^+$ where $\mathbb{R}^+$ acts on $\mathscr{P}$ by multiplication.

$\Phi : \mathscr{P} \longrightarrow \mathcal{H}_3$ defined by:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

$\Phi : \mathscr{P} \to \mathcal{H}_3$ defined by:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

Φ induces a bijection $\widetilde{\Phi} : \widetilde{\mathscr{P}} \to \mathcal{H}_3$,
wich commutes with the action of $\mathrm{SL}_2(\mathcal{O})$.

$\Phi : \mathscr{P} \to \mathcal{H}_3$ defined by:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

Φ induces a bijection $\widetilde{\Phi} : \widetilde{\mathscr{P}} \to \mathcal{H}_3$,
wich commutes with the action of $\mathrm{SL}_2(\mathcal{O})$.

Fundamental domains of $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ are well-known (Swan, Elstrodt-Grunewald-Mennicke, etc).

- When $h_K = 1$, from the description of the fundamental domain for $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ we get a lower bound $t \geq t_K$ only depending on the discriminant of the number field K, for $z + it \in \mathcal{H}_3$ in the fundamental domain. This allows us to bound $P, Q, R.$, and then a, b, c, d.

- When $h_K = 1$, from the description of the fundamental domain for $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ we get a lower bound $t \geq t_K$ only depending on the discriminant of the number field K, for $z + it \in \mathcal{H}_3$ in the fundamental domain. This allows us to bound $P, Q, R.$, and then a, b, c, d.

- (Work in progress) When $h_K > 1$, there are points of the fundamental domain such that $t = 0$ (cusps), so we need some supplementary group action to send all this points to the one at infinity. Once this action found, it should be possible to bound P, Q, R and to get an explicit algorithm also in the case $h_K \neq 1$.

When $h_K = 1$

$$\{\text{cubic extensions } L/K, \text{ with } \mathfrak{d}(L/K) \leq X\}/\sim$$

When $h_K = 1$

$$\{\text{cubic extensions } L/K, \text{ with } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{binary cubic forms modulo } GL_2(\mathcal{O})\}$$

When $h_K = 1$

$$\{\text{cubic extensions } L/K, \text{ with } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{binary cubic forms modulo } GL_2(\mathcal{O})\}$$
$$\downarrow$$
$$\{\text{(covariant) positive definite binary hermitian forms}\}$$

When $h_K = 1$

$$\{\text{cubic extensions } L/K, \text{ with } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{binary cubic forms modulo } GL_2(\mathcal{O})\}$$
$$\downarrow$$
$$\{\text{(covariant) positive definite binary hermitian forms}\}$$
$$\updownarrow$$
$$\{\text{points of } \mathcal{H}_3 \text{ modulo } GL_2(\mathcal{O})\}.$$

Theorem 4

Let F be a binary cubic form with coefficients in $\mathcal{O}$ which is reduced modulo $\mathrm{SL}_2(\mathcal{O})$ (weaker conditions than $\mathrm{GL}_2(\mathcal{O})$). Then

$$|a| \ll |D|^{1/4}; \quad |b| \ll |D|^{1/4}$$

$$|ad| \ll |D|^{1/2}; \quad |bc| \ll |D|^{1/2}.$$

and so we can loop on all these (a, b, c, d) in time $\widetilde{\mathcal{O}}(X)$.

Proposition 1

Let $F_1 \neq F_2$, two binary cubic forms, $F_2 = M \cdot F_1$ for some $M \in \mathrm{GL}_2(\mathcal{O})$. Let H_{F_1} and H_{F_2} be both reduced hermitian forms. Then two cases are possible:

1. *$H_{F_1} = H_{F_2} = H$ and $M \in \mathrm{Aut}(H)$ (i.e. $M.H = H$);*
2. *$H_{F_1} \neq H_{F_2}$ but they are both on the boundary of the fundamental domain $\mathcal{F}$ and they are in the same orbit modulo $\mathrm{GL}_2(\mathcal{O})$.*

We will call M as in the proposition an automorphism matrix.

Let M be an automorphism matrix. Then its coefficients are explicitly bounded in terms of the bound X on $\mathfrak{d}(L/K)$.

Let M be an automorphism matrix. Then its coefficients are explicitly bounded in terms of the bound X on $\mathfrak{d}(L/K)$.

- We loop on all possible M.

Let M be an automorphism matrix. Then its coefficients are explicitly bounded in terms of the bound X on $\mathfrak{d}(L/K)$.

- We loop on all possible M.
- We obtain a 4×4 system.

Let M be an automorphism matrix. Then its coefficients are explicitly bounded in terms of the bound X on $\mathfrak{d}(L/K)$.

- We loop on all possible M.
- We obtain a 4×4 system.
- we look at the rank of the matrix (allows to directly discard some cases)

Let M be an automorphism matrix. Then its coefficients are explicitly bounded in terms of the bound X on $\mathfrak{d}(L/K)$.

- We loop on all possible M.
- We obtain a 4×4 system.
- we look at the rank of the matrix (allows to directly discard some cases)
- we check that the space of the solutions is in the fundamental domain.

Implementation

- Floating point computations to check if a point is in the fundamental domain.

Implementation

- Floating point computations to check if a point is in the fundamental domain.
- Study of the precision needed

Implementation

- Floating point computations to check if a point is in the fundamental domain.
- Study of the precision needed
- Exact check for points “near” the borders

Implementation

- Floating point computations to check if a point is in the fundamental domain.
- Study of the precision needed
- Exact check for points “near” the borders
- Mahler theorem to check our results are correct.

Another kind of reduction

(from an idea of J. Cremona)

Unimodular transformations $\tau_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $k \in \mathcal{O}$.

Another kind of reduction

(from an idea of J. Cremona)

Unimodular transformations $\tau_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $k \in \mathcal{O}$.

$$\tau_k : (a, b, c, d) \to (a, b+3ak, 3ak^2+2bk+c, ak^3+bk^2+ck+d).$$

$\Longrightarrow$ we can reduce b modulo $3a$.

Another kind of reduction

(from an idea of J. Cremona)

Unimodular transformations $\tau_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $k \in \mathcal{O}$.

$$\tau_k : (a, b, c, d) \to (a, b+3ak, 3ak^2+2bk+c, ak^3+bk^2+ck+d).$$

$\Longrightarrow$ we can reduce b modulo $3a$.

τ_k leave unchanged $P_H = b^2 - 3ac$, and $P \leq 2^{1/3}|D|^{1/2}$ so

$$|c| \leq \frac{|b|^2 + 2^{1/3}X^{1/2}}{3|a|}$$

Another kind of reduction

(from an idea of J. Cremona)

Unimodular transformations $\tau_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $k \in \mathcal{O}$.

$$\tau_k : (a, b, c, d) \to (a, b+3ak, 3ak^2+2bk+c, ak^3+bk^2+ck+d).$$

$\Longrightarrow$ we can reduce b modulo $3a$.

τ_k leave unchanged $P_H = b^2 - 3ac$, and $P \leq 2^{1/3}|D|^{1/2}$ so

$$|c| \leq \frac{|b|^2 + 2^{1/3}X^{1/2}}{3|a|}$$

Same asymptotic time $\widetilde{O}(X)$ but a practical gain : more than 10 times faster !

Some results

X	$N(X)$	t
10^4	276	4 s
$4 \cdot 10^4$	1339	16 s
$9 \cdot 10^4$	3305	44 s
10^6	42692	16 mn 15 s
$4 * 10^6$	181944	1h 45 mn 29s
$9 \cdot 10^6$	421559	5h 50 mn
10^8	4990974	194h 47 mn

(Intel Xeon 5160 dual core, 3.0 GHz)

Conclusions

- Advantages (comparing with ray class field algorithm)

Conclusions

- Advantages (comparing with ray class field algorithm)
- Problems

Conclusions

- Advantages (comparing with ray class field algorithm)
- Problems
- Work in progress

Conclusions

- Advantages (comparing with ray class field algorithm)
- Problems
- Work in progress

Thank you !