Class group and unit group computation for large degree number fields

Jean-François Biasse

University of Calgary

October 2013
Presentation of the problem

Let $K$ be a number field of degree $n$, $\mathcal{O}_K$ its maximal order and $\mathcal{O} \subseteq \mathcal{O}_K$ an order in $K$.
Let $K$ be a number field of degree $n$, $\mathcal{O}_K$ its maximal order and $\mathcal{O} \subseteq \mathcal{O}_K$ an order in $K$.

We are interested in the following problems:

- Compute the class group $\text{Cl}(\mathcal{O})$ and the unit group $U(\mathcal{O})$ of $\mathcal{O}$. 

Presentation of the problem

Let $K$ be a number field of degree $n$, $\mathcal{O}_K$ its maximal order and $\mathcal{O} \subseteq \mathcal{O}_K$ an order in $K$.

We are interested in the following problems:

- Compute the class group $\text{Cl}(\mathcal{O})$ and the unit group $U(\mathcal{O})$ of $\mathcal{O}$.
- Let $\alpha \subseteq \mathcal{O}$, find $\alpha \in \mathcal{O}$ such that $\alpha = (\alpha)$. 

We mention applications of the resolution of these problems to number theory and cryptography.
Presentation of the problem

Let $K$ be a number field of degree $n$, $\mathcal{O}_K$ its maximal order and $\mathcal{O} \subseteq \mathcal{O}_K$ an order in $K$.

We are interested in the following problems:
- Compute the class group $\text{Cl}(\mathcal{O})$ and the unit group $U(\mathcal{O})$ of $\mathcal{O}$.
- Let $a \subseteq \mathcal{O}$, find $\alpha \in \mathcal{O}$ such that $a = (\alpha)$.
- Let $a \in \text{Cl}(\mathcal{O})$ and $B > 0$, find $p_1, \ldots, p_k$ such that

$$a = p_1 \cdots p_k, \quad \text{with } N(p_i) \leq B$$
Presentation of the problem

Let $K$ be a number field of degree $n$, $\mathcal{O}_K$ its maximal order and $\mathcal{O} \subseteq \mathcal{O}_K$ an order in $K$.

We are interested in the following problems:

- Compute the class group $\text{Cl}(\mathcal{O})$ and the unit group $\text{U}(\mathcal{O})$ of $\mathcal{O}$.
- Let $\alpha \subseteq \mathcal{O}$, find $\alpha \in \mathcal{O}$ such that $\alpha = (\alpha)$.
- Let $\alpha \in \text{Cl}(\mathcal{O})$ and $B > 0$, find $p_1, \ldots, p_k$ such that
  \[ \alpha = p_1 \cdots p_k, \quad \text{with } \mathcal{N}(p_i) \leq B \]

We mention applications of the resolution of these problems to number theory and cryptography.
1 Motivation

2 Class group and unit group computation

3 Complexity aspects

4 Relations in the polarized class group
Computation of $\text{Cl}(\mathcal{O})$ and $U(\mathcal{O})$

Computing the unit group has applications to the resolution of some Diophantine equations.

The Pell equation

For $\Delta > 0$, solving

$$x^2 - \Delta y^2 = 1,$$

is equivalent to finding the unit group for $\mathbb{Q}(\sqrt{\Delta})$. 

Computation of $\text{Cl}(\mathcal{O})$ and $U(\mathcal{O})$

Computing the unit group has applications to the resolution of some Diophantine equations.

**The Pell equation**

For $\Delta > 0$, solving

$$x^2 - \Delta y^2 = 1,$$

is equivalent to finding the unit group for $\mathbb{Q}(\sqrt{\Delta})$.

**Connexion with other equations**

Other Diophantine equations can be solved from solutions to the Pell equation

- Shäffer: $y^2 = 1^k + \cdots + x^k$.
- $y^2 = S_{x-a}^x$.

Where $S$ denotes the Stirling number.
Principal ideal problem

Gentry’s original scheme (and some others) rely on the hardness of finding a small generator of a principal ideal.
Cryptanalysis of homomorphic schemes

Principal ideal problem

Gentry’s original scheme (and some others) rely on the hardness of finding a small generator of a principal ideal.

Alice sets up the schemes. Let $\mathbb{Z}[X]/(X^N + 1) = \mathbb{Z}[\theta]$.

- Alice draws small $\alpha \in \mathbb{Z}[X]/(X^N + 1)$ until $\mathcal{N}(\alpha) = p$ prime.
- Alice displays a $\mathbb{Z}$-basis of $p = (\alpha)$. 
Cryptanalysis of homomorphic schemes

**Principal ideal problem**

Gentry’s original scheme (and some others) rely on the hardness of finding a small generator of a principal ideal.

Alice sets up the schemes. Let $\mathbb{Z}[X]/(X^N + 1) = \mathbb{Z}[\theta]$.

- Alice draws small $\alpha \in \mathbb{Z}[X]/(X^N + 1)$ until $\mathcal{N}(\alpha) = p$ prime.
- Alice displays a $\mathbb{Z}$-basis of $p = (\alpha)$.

Bob wants to encrypt $M \in \{0, 1\}$.

- Bob draws $R \in \mathbb{Z}[X]$ at random.
- Bob sends $M + 2R(\theta) \mod p$. 

To decrypt, it suffices to know a small generator of $p$. 

Biasse (U of C) 

large degree fields 

October 2013
Cryptanalysis of homomorphic schemes

Principal ideal problem

Gentry’s original scheme (and some others) rely on the hardness of finding a small generator of a principal ideal.

Alice sets up the schemes. Let $\mathbb{Z}[X]/(X^N + 1) = \mathbb{Z}[\theta]$.
- Alice draws small $\alpha \in \mathbb{Z}[X]/(X^N + 1)$ until $N(\alpha) = p$ prime.
- Alice displays a $\mathbb{Z}$-basis of $p = (\alpha)$.

Bob wants to encrypt $M \in \{0, 1\}$.
- Bob draws $R \in \mathbb{Z}[X]$ at random.
- Bob sends $M + 2R(\theta) \mod p$.

To decrypt, it suffices to know a small generator of $p$. 
Group action on elliptic curves

- Let $\mathcal{O}$ be a quadratic order, $\mathbb{F}_q$ a finite field and a prime $l \nmid q$.
- Isomorphism classes are represented by $j$-invariants.

$\text{Ell}_{\mathcal{O}, t} := \{ \text{Isomorphism classes of } E(\mathbb{F}_q) \mid \text{End}(E) \simeq \mathcal{O} \text{ and } \text{trace}(E) = t \}$. 
Let $\mathcal{O}$ be a quadratic order, $\mathbb{F}_q$ a finite field and a prime $l \nmid q$.

Isomorphism classes are represented by $j$-invariants.

$$\text{Ell}_{\mathcal{O}, t} := \{ \text{Isomorphism classes of } E(\mathbb{F}_q) \mid \text{End}(E) \cong \mathcal{O} \text{ and trace}(E) = t \}.$$ 

**Group action of $\text{Cl} (\mathcal{O})$ on $\text{Ell}_{\mathcal{O}, t}$**

- A split prime ideal $\mathfrak{a}$ of norm $l$ acts via an isogeny of degree $l$.
- If $l$ is large, the action is hard to evaluate.
Group action on elliptic curves

- Let $\mathcal{O}$ be a quadratic order, $\mathbb{F}_q$ a finite field and a prime $l \nmid q$.
- Isomorphism classes are represented by $j$-invariants.

$$\text{Ell}_{\mathcal{O},t} := \{\text{Isomorphism classes of } E(\mathbb{F}_q) \mid \text{End}(E) \simeq \mathcal{O} \text{ and trace}(E) = t\}.$$ 

Group action of $\text{Cl} (\mathcal{O})$ on $\text{Ell}_{\mathcal{O},t}$

- A split prime ideal $\alpha$ of norm $l$ acts via an isogeny of degree $l$.
- If $l$ is large, the action is hard to evaluate.

If $\alpha \sim \prod p_i$ with small $\mathcal{N}(p_i)$, it boils down to evaluating that of the $p_i$.
- Transports the discrete logarithm problem to another curve.
- Allows endomorphism ring computation.
1 Motivation
2 Class group and unit group computation
3 Complexity aspects
4 Relations in the polarized class group
Input and output of the algorithm

**Input**
- A number field $K$.
- Its $r_1$ real embeddings, its $r_2$ pairs of complex embeddings.
- Its ring of integers $\mathcal{O}_K = \sum_i \mathbb{Z} \alpha_i$.

**Output**
- $\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$.
- $U = \mu \times \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_r \rangle$

where $r := r_1 + r_2 - 1$ and $\mu$ is the set of roots of unity.
Input and output of the algorithm

**Input**
- A number field $K$.
- Its $r_1$ real embeddings, its $r_2$ pairs of complex embeddings.
- Its ring of integers $\mathcal{O}_K = \sum_i \mathbb{Z}\alpha_i$.

**Output**
- $\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$.
- $U = \mu \times \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_r \rangle$

where $r := r_1 + r_2 - 1$ and $\mu$ is the set of roots of unity.

The $\gamma_i$ are given in compact representation.
Class group computation

Factor base

Let \( \mathcal{B} = \{p_1, \ldots, p_N\} \) be a set of ideals whose classes generate \( \text{Cl}(\mathcal{O}_K) \).

We consider the surjective morphism

\[
\begin{align*}
\mathbb{Z}^N & \xrightarrow{\varphi} \mathcal{I} \xrightarrow{\pi} \text{Cl}(\mathcal{O}_K) \\
(e_1, \ldots, e_N) & \mapsto \prod_i p_i^{e_i} \mapsto \prod_i [p_i]^{e_i}
\end{align*}
\]
Class group computation

Factor base

Let $\mathcal{B} = \{p_1, \cdots, p_N\}$ be a set of ideals whose classes generate $\text{Cl}(\mathcal{O}_K)$.

We consider the surjective morphism

\[
\mathbb{Z}^N \xrightarrow{\varphi} \mathcal{I} \xrightarrow{\pi} \text{Cl}(\mathcal{O}_K)
\]

\[
(e_1, \ldots, e_N) \quad \xrightarrow{\quad \quad \quad \quad } \quad \prod_i p_i^{e_i} \quad \rightarrow \quad \prod_i [p_i]^{e_i}
\]

Property

The class group satisfies $\text{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}^N / \ker(\pi \circ \varphi)$.

We deduce $\text{Cl}(\mathcal{O}_K)$ from the lattice of all the $(e_1, \cdots, e_N)$ such that

\[
p_1^{e_1} \cdots p_N^{e_N} = (\alpha) = 1 \in \text{Cl}(\mathcal{O}_K) \text{ for some } \alpha \in \mathcal{O}_K.
\]
From relations to the ideal class group

The rows \((e_1, \cdots, e_N)\) of the relation matrix \(M\) satisfy

\[ p_1^{e_1} \cdots p_N^{e_N} = (\alpha) \]
From relations to the ideal class group

The rows \((e_1, \cdots, e_N)\) of the relation matrix \(M\) satisfy

\[
p_1^{e_1} \cdots p_N^{e_N} = (\alpha)
\]

There are unimodular matrices \(U, V\) and integers \(d_i\) such that \(d_{i+1} \mid d_i\) and

\[
U \cdot M \cdot V = \\
\begin{pmatrix}
d_1 & 0 & \cdots & 0 \\
0 & d_2 & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & d_N \\
(0) & \end{pmatrix}
\]
From relations to the ideal class group

The rows \((e_1, \cdots, e_N)\) of the relation matrix \(M\) satisfy

\[
p_{e_1} \cdots p_{e_N}^N = (\alpha)
\]

There are unimodular matrices \(U, V\) and integers \(d_i\) such that \(d_{i+1} \mid d_i\) and

\[
U \cdot M \cdot V = \begin{pmatrix}
d_1 & 0 & \cdots & 0 \\
0 & d_2 & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & d_N \\
(0) & \end{pmatrix},
\]

If the rows of \(M\) generate all the possible relations then

\[
\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_N\mathbb{Z}.
\]
From relations to the unit group

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, p_{1}^{m_{i,1}} \cdots p_{N}^{m_{i,N}} = (\alpha_{i}) = 1 \in \text{Cl}(\mathcal{O}_{K}).$$

**Property**

Let $X = (x_{1}, \cdots, x'_{N})$ be such that $XM = 0$. Then,

$$\beta_{X} := \alpha_{1}^{x_{1}} \cdots \alpha_{N}^{x'_{N}} \text{ is a unit}$$
From relations to the unit group

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, p_{\frac{m_i}{1}}^{m_i,1} \cdots p_{\frac{m_i}{N}}^{m_i,N} = (\alpha_i) = 1 \in \text{Cl}(\mathcal{O}_K).$$

**Property**

Let $X = (x_1, \cdots, x_N)$ be such that $XM = 0$. Then,

$$\beta_X := \alpha_1^{x_1} \cdots \alpha_N^{x'_N} \text{ is a unit}$$

We use the following strategy

- We derive units in compact representation from elements in $\ker(M)$.
- We construct a minimal generating set for $U$ by induction.
The principal ideal problem (PIP)

Let $a \subseteq \mathcal{O}_K$. We wish to
- Decide if $a$ is principal.
- If so, find $\alpha \in \mathcal{O}_K$ such that $a = (\alpha)$. 
Connexion with the principal ideal problem

The principal ideal problem (PIP)

Let $\alpha \subseteq \mathcal{O}_K$. We wish to

- Decide if $\alpha$ is principal.
- If so, find $\alpha \in \mathcal{O}_K$ such that $\alpha = (\alpha)$.

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, p_1^{m_{i,1}} \cdots p_N^{m_{i,N}} = (\alpha_i) = 1 \in \text{Cl}(\mathcal{O}_K).$$
Connexion with the principal ideal problem

The principal ideal problem (PIP)

Let $\alpha \subseteq \mathcal{O}_K$. We wish to

- Decide if $\alpha$ is principal.
- If so, find $\alpha \in \mathcal{O}_K$ such that $\alpha = (\alpha)$.

Let $M \in \mathbb{Z}^{N \times N'}$ be a relation matrix. That is,

$$\forall i, p_1^{m_i,1} \cdots p_N^{m_i,N} = (\alpha_i) = 1 \in \text{Cl}(\mathcal{O}_K).$$

Algorithm for solving the PIP

- Decompose $\alpha = (\alpha)p_1^{y_1} \cdots p_N^{y_N}$.
- If $XA = Y$ has no solution, $\alpha$ is not principal.
- Otherwise, $\alpha = (\beta)$ with $\beta = \alpha \cdot \alpha_1^{x_1} \cdots \alpha_N^{x_N}$. 
1 Motivation

2 Class group and unit group computation

3 Complexity aspects

4 Relations in the polarized class group
Choice of a factor base

The algorithm starts by choosing prime ideals generating $\text{Cl}(\mathcal{O})$

$$\mathcal{B} := \{ p \text{ prime} \mid N(p) \leq B \} = \{ p_1, \cdots, p_N \}$$
Choice of a factor base

The algorithm starts by choosing prime ideals generating $\text{Cl}(\mathcal{O})$

$$
\mathcal{B} := \{ p \text{ prime } | N(p) \leq B \} = \{ p_1, \cdots, p_N \}
$$

Asymptotic bounds with respect to $\Delta = \text{disc}(\mathcal{O})$

The most commonly used bounds for the asymptotic analysis are

- **Minkowski bound** : $B = O(\sqrt{|\Delta|})$ (unconditional).
- **Bach bound** : $B = O(\log^2 |\Delta|)$ (under GRH).
Choice of a factor base

The algorithm starts by choosing prime ideals generating $\text{Cl}(\mathcal{O})$

$$\mathcal{B} := \{p \text{ prime } | \mathcal{N}(p) \leq B\} = \{p_1, \cdots, p_N\}$$

Asymptotic bounds with respect to $\Delta = \text{disc}(\mathcal{O})$

The most commonly used bounds for the asymptotic analysis are

- Minkowski bound: $B = O(\sqrt{|\Delta|})$ (unconditional).
- Bach bound: $B = O(\log^2 |\Delta|)$ (under GRH).

Another bound, asymptotically larger, is used in practice (Belabas et al.)

$$\sum_{(m,p):\mathcal{N}(p^m) \leq B'} \frac{\log \mathcal{N}(p)}{\mathcal{N}(p^{m/2})} \left(1 - \frac{\log \mathcal{N}(p^m)}{\log(B')}\right) > \frac{1}{2} \log |\Delta| - 1.9n - 0.785r_1$$

$$+ \frac{2.468n + 1.832r_1}{\log(B')}.$$
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

\[ \prod_{i} p_i^{e_i} = (\alpha)a, \]

where \( \alpha \in K \) and \( a \neq \prod_{i} p_i^{e_i} \).
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

$$\prod_i p_i^{e_i} = (\alpha)a,$$

where $\alpha \in K$ and $a \neq \prod_i p_i^{e_i}$.

In particular, if $N(a)$ is small, $a$ has a better chance to be $B$-smooth.
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

$$
\prod_{i} p_{i}^{e_i} = (\alpha)a,
$$

where $\alpha \in K$ and $a \neq \prod_{i} p_{i}^{e_i}$.

In particular, if $\mathcal{N}(a)$ is small, $a$ has a better chance to be $B$-smooth.

LLL-reduction of an ideal

Let $a \subseteq \mathcal{O}_K$. We use LLL to find $a' = a \in \text{Cl}(\mathcal{O})$ with small norm.
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

\[ \prod_i p_i^{e_i} = (\alpha) a, \]

where \( \alpha \in K \) and \( a \neq \prod_i p_i^{e_i} \).

In particular, if \( N(a) \) is small, \( a \) has a better chance to be \( B \)-smooth.

LLL-reduction of an ideal

Let \( a \subseteq \mathcal{O}_K \). We use LLL to find \( a' = a \in \text{Cl}(\mathcal{O}) \) with small norm.

- \( b \leftarrow k a^{-1} \) where \( k \) is the denominator of \( a^{-1} \).
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

\[
\prod_{i} p_i^{e_i} = (\alpha) a,
\]

where \( \alpha \in K \) and \( a \neq \prod_i p_i^{e_i} \).

In particular, if \( \mathcal{N}(a) \) is small, \( a \) has a better chance to be \( B \)-smooth.

LLL-reduction of an ideal

Let \( a \subseteq \mathcal{O}_K \). We use LLL to find \( a' = a \in \text{Cl}(\mathcal{O}) \) with small norm.

- \( b \leftarrow ka^{-1} \) where \( k \) is the denominator of \( a^{-1} \).
- Let \( \beta \) be the first element of an LLL-reduced basis of \( b \).
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

$$\prod_i p_i^{e_i} = (\alpha)a,$$

where $\alpha \in K$ and $a \neq \prod_i p_i^{e_i}$.

In particular, if $N(a)$ is small, $a$ has a better chance to be $B$-smooth.

LLL-reduction of an ideal

Let $a \subseteq \mathcal{O}_K$. We use LLL to find $a' = a \in \text{Cl}(\mathcal{O})$ with small norm.

- $b \leftarrow ka^{-1}$ where $k$ is the denominator of $a^{-1}$.
- Let $\beta$ be the first element of an LLL-reduced basis of $b$.
- $a' \leftarrow \left(\frac{\beta}{k}\right) a$
Reduction of an ideal

Ideals have unique factorization, but it is possible to have

\[ \prod_{i} p_{i}^{e_{i}} = (\alpha)a, \]

where \( \alpha \in K \) and \( a \neq \prod_{i} p_{i}^{e_{i}}. \)

In particular, if \( N(a) \) is small, \( a \) has a better chance to be \( B \)-smooth.

LLL-reduction of an ideal

Let \( a \subseteq \mathcal{O}_{K} \). We use LLL to find \( a' = a \in \text{Cl}(\mathcal{O}) \) with small norm.

- \( b \leftarrow ka^{-1} \) where \( k \) is the denominator of \( a^{-1} \).
- Let \( \beta \) be the first element of an LLL-reduced basis of \( b \).
- \( a' \leftarrow \left( \frac{\beta}{k} \right) a \)

Then we have \( a' \subseteq \mathcal{O}_{K} \) and \( N(a') \leq 2^{O(n^{2})} \sqrt{|\Delta|} \).
The subexponential function

To measure the complexity of the operations, we use the subexponential function

\[ L_\Delta(\alpha, \beta) := e^{\beta (\log |\Delta|)^\alpha (\log \log |\Delta|)^{1-\alpha}}. \]
The subexponential function

To measure the complexity of the operations, we use the subexponential function

\[ L_\Delta(\alpha, \beta) := e^{\beta (\log |\Delta|)^\alpha (\log \log |\Delta|)^{1-\alpha}}. \]

Property

For \( \alpha \in [0, 1] \), \( L_\Delta(\alpha, \beta) \) is between polynomial and exponential in \( \log |\Delta| \).

\[ L_\Delta(0, \beta) = (\log |\Delta|)^\beta \]
\[ L_\Delta(1, \beta) = (|\Delta|)^\beta \]
The subexponential function

To measure the complexity of the operations, we use the subexponential function

\[ L_\Delta(\alpha, \beta) := e^{\beta (\log |\Delta|)^\alpha (\log \log |\Delta|)^{1-\alpha}}. \]

**Property**

For \( \alpha \in [0, 1] \), \( L_\Delta(\alpha, \beta) \) is between polynomial and exponential in \( \log |\Delta| \).

\[
L_\Delta(0, \beta) = (\log |\Delta|)^\beta \\
L_\Delta(1, \beta) = (|\Delta|)^\beta
\]

Some interesting rules of calculation:

\[
L_\Delta(\alpha, \beta_1) \times L_\Delta(\alpha, \beta_2) = L_\Delta(\alpha, \beta_1 + \beta_2) \\
L_\Delta(\alpha, \beta)^k = L_\Delta(\alpha, k\beta).
\]
Smoothness probability

Let $\Psi(x, y)$ be the number of $y$-smooth ideals of norm bounded by $x$. Subexponential methods consist of falling in the range where

$$\frac{\Psi(x, y)}{x} = u^{-u(1+o(1))}, \quad u = \frac{\log x}{\log y} \quad (1).$$
Smoothness probability

Let $\Psi(x, y)$ be the number of $y$-smooth ideals of norm bounded by $x$. Subexponential methods consist of falling in the range where

$$\frac{\Psi(x, y)}{x} = u^{-u(1+o(1))}, \quad u = \frac{\log x}{\log y} \quad (1).$$

Known estimates (for which (1) holds)

- Over $\mathbb{Z}$: Hildebrand 84
- Over ideals of a number field: Sourfield 04 (GRH).
- Over principal ideals: conjectural.
Smoothness probability

Let $\Psi(x, y)$ be the number of $y$-smooth ideals of norm bounded by $x$. Subexponential methods consist of falling in the range where

$$\frac{\Psi(x, y)}{x} = u^{-u(1+o(1))}, \quad u = \frac{\log x}{\log y} \quad (1).$$

Known estimates (for which (1) holds)

- Over $\mathbb{Z}$ : Hildebrand 84
- Over ideals of a number field : Sourfield 04 (GRH).
- Over principal ideals : conjectural.

If $x = L_\Delta(a, b)$ and $y = L_\Delta(c, d)$, then

$$\frac{\Psi(x, y)}{x} = L_\Delta \left( a - c, -\frac{c}{d}(b - d) + o(1) \right).$$
Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$. 
Fixed degree number fields

Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

Creation of relations in $\text{Cl}(\mathcal{O})$

We choose $\mathcal{B} = \{p \mid \mathcal{N}(p) \leq B\}$ where $B = L_\Delta(1/2, c)$. 
Fixed degree number fields

Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

### Creation of relations in $\text{Cl}(\mathcal{O})$

We choose $\mathcal{B} = \{p \mid \mathcal{N}(p) \leq B\}$ where $B = L_\Delta(1/2, c)$.

- Draw $\alpha := \prod_i p_i^{e_i}$ at random where $p_i \in \mathcal{B}$. 

\[ \text{Biasse (U of C)} \]

large degree fields

October 2013 14 / 30
Fixed degree number fields

Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

**Creation of relations in $\text{Cl}(\mathcal{O})$**

We choose $\mathcal{B} = \{\mathfrak{p} \mid N(\mathfrak{p}) \leq B\}$ where $B = L_\Delta(1/2, c)$.

- Draw $\alpha := \prod_i p_i^{e_i}$ at random where $p_i \in \mathcal{B}$.
- Let $b = (\alpha)\alpha$ with $N(b) \leq 2^{O(n^2)} \sqrt{|\Delta|}$. 

Fixed degree number fields

Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

Creation of relations in $\text{Cl}(\mathcal{O})$

We choose $\mathcal{B} = \{p | N(p) \leq B\}$ where $B = L_\Delta(1/2, c)$.

- Draw $\alpha := \prod_i p_i^{e_i}$ at random where $p_i \in \mathcal{B}$.
- Let $b = (\alpha)\alpha$ with $N(b) \leq 2^{O(n^2)} \sqrt{|\Delta|}$.
- If $b = \prod_j q_j$ is $B$-smooth, keep the relation $\prod_i p_i^{e_i} \cdot \prod_j q_j^{-1} = 1$. 
Fixed degree number fields

Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

**Creation of relations in $\text{Cl}(\mathcal{O})$**

We choose $\mathcal{B} = \{p \mid \mathcal{N}(p) \leq B\}$ where $B = L_\Delta(1/2, c)$.

- Draw $\alpha := \prod_i p_i^{e_i}$ at random where $p_i \in \mathcal{B}$.
- Let $b = (\alpha)\alpha$ with $\mathcal{N}(b) \leq 2^{O(n^2)} \sqrt{|\Delta|}$.
- If $b = \prod_j q_j$ is $\mathcal{B}$-smooth, keep the relation $\prod_i p_i^{e_i} \cdot \prod_j q_j^{-1} = 1$.

- If $n$ is fixed, we derive $|\mathcal{B}| = L_\Delta(1/2, c)$ relations in $L_\Delta(1/2, d)$. 
Hafner-McCurley and Buchmann computed the class group and unit group for fixed $n = [K : \mathbb{Q}]$ in time $L_\Delta(1/2, c)$.

### Creation of relations in $\text{Cl}(\mathcal{O})$

We choose $\mathcal{B} = \{p \mid \mathcal{N}(p) \leq B\}$ where $B = L_\Delta(1/2, c)$.

- Draw $a := \prod_i p_i^{e_i}$ at random where $p_i \in \mathcal{B}$.
- Let $b = (\alpha)a$ with $\mathcal{N}(b) \leq 2^{O(n^2)} \sqrt{|\Delta|}$.
- If $b = \prod_j q_j$ is $\mathcal{B}$-smooth, keep the relation $\prod_i p_i^{e_i} \cdot \prod_j q_j^{-1} = 1$.

- If $n$ is fixed, we derive $|\mathcal{B}| = L_\Delta(1/2, c)$ relations in $L_\Delta(1/2, d)$.
- Then $\text{Cl}(\mathcal{O})$ and $U(\mathcal{O})$ are found in time $|\mathcal{B}|^k = L_\Delta(1/2, kd)$. 
When \( n \to \infty \): changing the reduction algorithm

If LLL-reduce \( a := \prod_i p_i \), we get \( b \sim a \) with \( \mathcal{N}(b) \leq 2^{O(n^2)} \sqrt{|\Delta|} \).

- We have \( \mathcal{N}(b) \geq L_\Delta(2, c) \) for some \( c > 0 \).
- With \( B = L_\Delta(\alpha, d) \) for some \( \alpha < 1 \) and \( d > 0 \),

\[
E(\text{time to find } b \text{ } B \text{ – smooth}) \geq L_\Delta(2 - \alpha, e) \geq |\Delta|^e \text{ for some } e > 0.
\]
When $n \to \infty$: changing the reduction algorithm

If LLL-reduce $a := \prod_i p_i$, we get $b \sim a$ with $\mathcal{N}(b) \leq 2^{O(n^2)} \sqrt{\Delta}$.

- We have $\mathcal{N}(b) \geq L_\Delta(2, c)$ for some $c > 0$.
- With $B = L_\Delta(\alpha, d)$ for some $\alpha < 1$ and $d > 0$,

$$E(\text{time to find } b \text{ } B - \text{smooth}) \geq L_\Delta(2 - \alpha, e) \geq |\Delta|^e$$

for some $e > 0$.

**BKZ reduction**

Let $k > 0$, the BKZ$_k$ reduction allows to find $b = (\alpha)a$ with

$$\mathcal{N}(b) \leq 2^{O\left(\frac{n^2}{k}\right)} \sqrt{\Delta}$$

in time $O(2^k)$. 

We replace LLL-reduction by BKZ$_k$ reduction with $k = \frac{2}{3}$. It runs in time $L_\Delta(\frac{2}{3} + \varepsilon, d)$ for $d > 0$ and arbitrary small $\varepsilon > 0$. 

Biasse (U of C) 
large degree fields
October 2013
When \( n \to \infty \): changing the reduction algorithm

If LLL-reduce \( a := \prod_i p_i \), we get \( b \sim a \) with \( \mathcal{N}(b) \leq 2^{O(n^2)} \sqrt{|\Delta|} \).

- We have \( \mathcal{N}(b) \geq L_\Delta(2, c) \) for some \( c > 0 \).
- With \( B = L_\Delta(\alpha, d) \) for some \( \alpha < 1 \) and \( d > 0 \),

\[
E(\text{time to find } b \text{ } B \text{-smooth}) \geq L_\Delta(2 - \alpha, e) \geq |\Delta|^e \text{ for some } e > 0.
\]

**BKZ reduction**

Let \( k > 0 \), the BKZ\(_k\) reduction allows to find \( b = (\alpha)a \) with

\[
\mathcal{N}(b) \leq 2^{O \left( \frac{n^2}{k} \right)} \sqrt{|\Delta|} \text{ in time } O(2^k).
\]

- We replace LLL-reduction by BKZ\(_k\) reduction with \( k = 2/3 \).
- It runs in time \( L_\Delta(2/3 + \varepsilon, d) \) for \( d > 0 \) and arbitrary small \( \varepsilon > 0 \).
Let $K/\mathbb{Q}$ defined by $P \in \mathbb{Z}[X]$ with $n = \deg(P)$ and $d = \log(H(P))$.

- We draw $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$ with $k = \deg(A)$ and $a = \log(H(A))$.
- We have $\mathcal{N}(\phi) \leq na + dk + n \log k + k \log n$. 
Let $K/\mathbb{Q}$ defined by $P \in \mathbb{Z}[X]$ with $n = \deg(P)$ and $d = \log(H(P))$.

- We draw $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$ with $k = \deg(A)$ and $a = \log(H(A))$.
- We have $N(\phi) \leq na + dk + n \log k + k \log n$.

**Property**

When $n = \log(|\Delta|)^\alpha$ and $d = \log(|\Delta|)^{1-\alpha}$ for $\alpha \in \left] \frac{1}{3}, \frac{2}{3} \right]$
Class group and unit group of $\mathbb{Z}[[\theta]]$ in $L_\Delta(1/3)$

Let $K/\mathbb{Q}$ defined by $P \in \mathbb{Z}[X]$ with $n = \text{deg}(P)$ and $d = \log(H(P))$.

- We draw $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$ with $k = \text{deg}(A)$ and $a = \log(H(A))$.
- We have $\mathcal{N}(\phi) \leq na + dk + n \log k + k \log n$.

**Property**

When $n = \log(|\Delta|)^\alpha$ and $d = \log(|\Delta|)^{1-\alpha}$ for $\alpha \in ]\frac{1}{3}, \frac{2}{3}[$

- We can choose $A \in \mathbb{Z}[X]$ such that $\mathcal{N}(\phi) \leq L_\Delta \left(\frac{2}{3}, c\right)$ for $c > 0$. 
Class group and unit group of $\mathbb{Z}[\theta]$ in $L_\Delta(1/3)$

Let $K/\mathbb{Q}$ defined by $P \in \mathbb{Z}[X]$ with $n = \deg(P)$ and $d = \log(H(P))$.

- We draw $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$ with $k = \deg(A)$ and $a = \log(H(A))$.
- We have $N(\phi) \leq na + dk + n \log k + k \log n$.

**Property**

When $n = \log(|\Delta|)^\alpha$ and $d = \log(|\Delta|)^{1-\alpha}$ for $\alpha \in ]\frac{1}{3}, \frac{2}{3}[$

- We can choose $A \in \mathbb{Z}[X]$ such that $N(\phi) \leq L_\Delta \left(\frac{2}{3}, c\right)$ for $c > 0$.
- It takes $L_\Delta \left(\frac{1}{3}, e\right)$ to find an $L_\Delta \left(\frac{1}{3}, d\right)$-smooth $\phi$. 
Class group and unit group of $\mathbb{Z}[\theta]$ in $L_\Delta(1/3)$

Let $K/\mathbb{Q}$ defined by $P \in \mathbb{Z}[X]$ with $n = \text{deg}(P)$ and $d = \log(H(P))$.

- We draw $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$ with $k = \text{deg}(A)$ and $a = \log(H(A))$.
- We have $N(\phi) \leq na + dk + n \log k + k \log n$.

**Property**

When $n = \log(|\Delta|)^\alpha$ and $d = \log(|\Delta|)^{1-\alpha}$ for $\alpha \in ]\frac{1}{3}, \frac{2}{3}[$,

- We can choose $A \in \mathbb{Z}[X]$ such that $N(\phi) \leq L_\Delta \left(\frac{2}{3}, c\right)$ for $c > 0$.
- It takes $L_\Delta \left(\frac{1}{3}, e\right)$ to find an $L_\Delta \left(\frac{1}{3}, d\right)$-smooth $\phi$.

- We can compute $\text{Cl}(\mathbb{Z}[\theta])$ and $U(\mathbb{Z}[\theta])$ in $L_\Delta(1/3, f)$ for some $f > 0$.
- This does not extend to $\mathbb{Z}[\theta] \not\subset \mathcal{O}$.
Cyclotomic fields

We want to calculate $\text{Cl}(\mathbb{Z}[\theta])$ and $U(\mathbb{Z}[\theta])$ for $K = \mathbb{Q}[X]/X^N + 1$.

- $H(X^N + 1) = 1$.
- $\log |\text{Disc}(X^N + 1)| := \log |\Delta| = N \log(N)$. 

Relation search

We draw $\phi \in \mathbb{Z}[\theta]$ of the form $A(\theta)$ with $k := \deg(A) = N$.

$a := \log(H(A)) = \log(N)$

$\log|\phi| \leq O(a \cdot N + k + N \log(k) + k \log(N)) \leq O(\log |\Delta|)$

This way, we can perform the relation search in time $L^\Delta(\frac{1}{2}, c)$ for some $c > 0$. 
Cyclotomic fields

We want to calculate $\text{Cl}(\mathbb{Z}[\theta])$ and $U(\mathbb{Z}[\theta])$ for $K = \mathbb{Q}[X]/X^N + 1$.

- $H(X^N + 1) = 1$.
- $\log |\text{Disc}(X^N + 1)| := \log |\Delta| = N \log(N)$.

Relation search

We draw $\phi \in \mathbb{Z}[\theta]$ of the form $A(\theta)$ with

- $k := \deg(A) = N$.
- $a := \log(H(A)) = \log(N)$

$$\log \mathcal{N}(\phi) \leq O(a \cdot N + k + N \log(k) + k \log(N)) \leq O(\log |\Delta|)$$
Cyclotomic fields

We want to calculate $\text{Cl}(\mathbb{Z}[\theta])$ and $U(\mathbb{Z}[\theta])$ for $K = \mathbb{Q}[X]/X^N + 1$.

- $H(X^N + 1) = 1$.
- $\log |\text{Disc}(X^N + 1)| := \log |\Delta| = N \log(N)$.

**Relation search**

We draw $\phi \in \mathbb{Z}[\theta]$ of the form $A(\theta)$ with

- $k := \deg(A) = N$.
- $a := \log(H(A)) = \log(N)$

\[
\log \mathcal{N}(\phi) \leq O(a \cdot N + k + N \log(k) + k \log(N)) \leq O(\log |\Delta|)
\]

This way, we can perform the relation search in time $L_\Delta \left( \frac{1}{2}, c \right)$ for some $c > 0$. 
Short generators of ideals

Let $\mathfrak{a} \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for $U$ and a generator of $\mathfrak{a}$.
- We want a small generator of $\mathfrak{a}$.

Assume we find $\alpha \in \mathcal{O}$ such that $\mathfrak{a} = (\alpha)$, then

$$\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r, \mathfrak{a} = (\varepsilon^{e_1}, \cdots, \varepsilon^{e_r} \alpha).$$

When $r = 1$, then we find $e \in \mathbb{Z}$ such that $\log |\alpha| - e \log |\varepsilon|$ has the desired size.

Let $\vec{v}_x = (\log |x_1|, \cdots, \log |x_r|) \in \mathbb{R}^r$. We want $\|\vec{\alpha} + \sum_i e_i \vec{\varepsilon}_i\|_2$ small.

In arbitrary dimension, we want to solve the closest vector problem.
Short generators of ideals

Let \( \alpha \subseteq \mathcal{O} \) a principal ideal and \( U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle \) the unit group.

- We know how to compute generators for \( U \) and a generator of \( \alpha \).
- We want a small generator of \( \alpha \).

Assume we find \( \alpha \in \mathcal{O} \) such that \( \alpha = (\alpha) \), then

\[
\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r, \quad \alpha = (\varepsilon_1^{e_1}, \cdots, \varepsilon_r^{e_r} \alpha).
\]
Short generators of ideals

Let $\alpha \subseteq \mathcal{O}$ a principal ideal and $U = \mu \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_r \rangle$ the unit group.

- We know how to compute generators for $U$ and a generator of $\alpha$.
- We want a small generator of $\alpha$.

Assume we find $\alpha \in \mathcal{O}$ such that $\alpha = (\alpha)$, then

$$
\forall (e_1, \cdots, e_r) \in \mathbb{Z}^r, \ a = (\varepsilon_1^{e_1}, \cdots, \varepsilon_r^{e_r} \alpha).
$$

When $r = 1$, then we find $e \in \mathbb{Z}$ such that $\log |\alpha| - e \log |\varepsilon|$ has the desired size.

- Let $\vec{v}_x = (\log |x|_1, \cdots, \log |x|_r) \in \mathbb{R}^r$.
- We want $||\vec{\alpha} + \sum_i e_i \vec{\varepsilon_i}||_2$ small.

In arbitrary dimension, we want to solve the closest vector problem.
The $q$-descent

**Goal**

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order in $K$, and a $|\Delta|$-smooth $\alpha \subseteq \mathcal{O}$.

- We find a $L_\Delta(1/3, b)$-smooth decomposition of $\alpha$ in time $L_\Delta(1/3, c)$.
- This allows an $L_\Delta(1/3)$ algorithm to compute $\text{Cl}(\mathcal{O})$ and $U(\mathcal{O})$. 
The $q$-descent

**Goal**

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order in $K$, and a $|\Delta|$-smooth $\alpha \subseteq \mathcal{O}$.
- We find a $L_\Delta(1/3, b)$-smooth decomposition of $\alpha$ in time $L_\Delta(1/3, c)$.
- This allows an $L_\Delta(1/3)$ algorithm to compute $\text{Cl}(\mathcal{O})$ and $U(\mathcal{O})$.

Let $q \subseteq \mathcal{O}$ and $v_q$ such that $q = q\mathcal{O} + (\theta - v_q)\mathcal{O}$. Then

$$L_q := \mathbb{Z}v_0 + \mathbb{Z}(v_1 - \theta) + \cdots + \mathbb{Z}(v_k - \theta^k) \subseteq q,$$

where $v_i = v_p^i \mod q$. 
The $q$-descent

**Goal**

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order in $K$, and a $\mid \Delta \mid$-smooth $a \subseteq \mathcal{O}$.

- We find a $L_\Delta(1/3, b)$-smooth decomposition of $a$ in time $L_\Delta(1/3, c)$.
- This allows an $L_\Delta(1/3)$ algorithm to compute $\text{Cl}(\mathcal{O})$ and $\text{U}(\mathcal{O})$.

Let $q \subseteq \mathcal{O}$ and $\nu_q$ such that $q = q\mathcal{O} + (\theta - \nu_q)\mathcal{O}$. Then

$$\mathcal{L}_q := \mathbb{Z}\nu_0 + \mathbb{Z}(\nu_1 - \theta) + \cdots + \mathbb{Z}(\nu_k - \theta^k) \subseteq q,$$

where $\nu_i = \nu_p^i \mod q$.

- The $\phi \in \mathcal{L}_q$ are of the form $\phi = A(\theta)$ for $A \in \mathbb{Z}[X]$.
- We look for small elements $\phi \in \mathcal{L}_q$. 
The $q$-descent

$$a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k$$

$$\mathcal{N}(q_j) \in L_\Delta \left( \frac{1}{3} + \tau, 1 \right)$$
The $q$-descent

$$a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k$$

$N(q_j) \in L_\Delta \left( \frac{1}{3} + \tau, 1 \right)$

find $\alpha_i \in q_i$ with $\langle \alpha_i \rangle / q_i \ L_\Delta(1/3 + \tau/2, c)$-smooth
The $q$-descent

\[ a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k \]

\[ \mathcal{N}(q_j) \in L_\Delta \left( \frac{1}{3} + \tau, 1 \right) \]

Find $\alpha_i \in q_i$ with $(\alpha_i)/q_i \in L_\Delta(1/3 + \tau/2, c)$-smooth

\[ q_i = (\alpha_i)q_1^{-1} \cdots q_i^{-1} \cdots q_k^{-1} \]

\[ \mathcal{N}(q_i') \in L_\Delta \left( \frac{1}{3} + \frac{\tau}{2}, 1 \right) \]
The \( q \)-descent

\[
a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k
\]

\[
\mathcal{N}(q_j) \in L_\Delta \left( \frac{1}{3} + \tau, 1 \right)
\]

\[\text{find } \alpha_i \in q_i \text{ with } (\alpha_i)/q_i \text{ } L_\Delta(1/3 + \tau/2, c)\text{-smooth}\]

\[
q_i = (\alpha_i)q_i^{-1} \cdots q_i^{-1} \cdots q_i^{-1}
\]

\[
\mathcal{N}(q_j') \in L_\Delta \left( \frac{1}{3} + \frac{\tau}{2}, 1 \right)
\]

Repeat until \( \tau \) is small enough
The $q$-descent

\[
a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k
\]

find $\alpha_i \in q_i$ with $(\alpha_i)/q_i \in L_{\Delta}(1/3 + \tau/2, c)$-smooth

\[
q_i = (\alpha_i)q_i^{-1} \cdots q_i^{-1} \cdots q_i^{-1}
\]

Repeat until $\tau$ is small enough

Find $\alpha_i \in q'_i$ with $\mathcal{N}(\alpha_i) \in L_{\Delta}(1/3, c_\infty)$

\[
\mathcal{N}(q_j) \in L_{\Delta} \left( \frac{1}{3} + \tau, 1 \right)
\]

\[
\mathcal{N}(q'_j) \in L_{\Delta} \left( \frac{1}{3} + \frac{\tau}{2}, 1 \right)
\]
The $q$-descent

\[ a = (\alpha) \cdot q_1 \cdots q_i \cdots q_k \]

\[ \mathcal{N}(q_j) \in L_{\Delta} \left( \frac{1}{3} + \tau, 1 \right) \]

find $\alpha_i \in q_i$ with $(\alpha_i)/q_i \in L_\Delta(1/3 + \tau/2, c)$-smooth

\[ q_i = (\alpha_i)q'_1^{-1} \cdots q'_i^{-1} \cdots q'_{k'}^{-1} \]

\[ \mathcal{N}(q'_j) \in L_{\Delta} \left( \frac{1}{3} + \frac{\tau}{2}, 1 \right) \]

Repeat until $\tau$ is small enough

Find $\alpha_i \in q'_i$ with $\mathcal{N}(\alpha_i) \in L_\Delta(1/3, c_\infty)$

\[ a = (\alpha) \cdot q''^e_1 \cdots q''^e_l \]

\[ \mathcal{N}(q''_j) \in L_{\Delta} \left( \frac{1}{3}, c_\infty \right) \]
1 Motivation

2 Class group and unit group computation

3 Complexity aspects

4 Relations in the polarized class group
The polarized class group

Let $K$ be a CM field, $K_+$ be the maximal totally real subfield of $K$ and $\mathcal{O}$ an order in $K$.

An ideal $a \subseteq \mathcal{O}$ is polarized if

$$\exists \alpha \in K_+ \text{ totally real such that } a\bar{a} = (\alpha).$$
The polarized class group

Let $K$ be a CM field, $K_+$ be the maximal totally real subfield of $K$ and $\mathcal{O}$ an order in $K$.

An ideal $a \subseteq \mathcal{O}$ is polarized if

$$\exists \alpha \in K_+ \text{ totally real such that } a\bar{a} = (\alpha).$$

The polarized class group

$$\mathcal{C}(\mathcal{O}) = \{\text{Polarized ideals of } \mathcal{O}\}/\{\text{Principal polarized ideals}\}$$
The polarized class group

Let $K$ be a CM field, $K_+$ be the maximal totally real subfield of $K$ and $\mathcal{O}$ an order in $K$.

An ideal $\alpha \subseteq \mathcal{O}$ is polarized if

$$\exists \alpha \in K_+ \text{ totally real such that } \alpha \bar{\alpha} = (\alpha).$$

The polarized class group

$$\mathcal{C}(\mathcal{O}) = \{ \text{Polarized ideals of } \mathcal{O} \}/\{ \text{Principal polarized ideals} \}$$

$\mathcal{C}(\mathcal{O})$ acts on isomorphism classes of principally polarized Abelian varieties with complex multiplication by $\mathcal{O}$.

- The class of $\alpha$ acts via an isogeny of degree $N(\alpha)$.
- This action preserves the polarization.
Relations in the polarized class group

The cost of evaluating the action of the class of $\alpha \subseteq \mathcal{O}$ grows with $\mathcal{N}(\alpha)$.
- The action of $\alpha$ is deduced from the action of ideals of smaller norm.
- This boils down to decomposing $\alpha$ in $\mathcal{C}(\mathcal{O})$. 

Using smooth ideals

Let $\alpha$ be a polarized ideal of $\mathcal{O}$ and $B > 0$. We rewrite the class of $\alpha$ as $\alpha = p_1 \cdots p_k$ in $\mathcal{C}(\mathcal{O})$, where $\mathcal{N}(p_i) \leq B$. Evaluating the action of $\alpha$ boils down to evaluating that of the $p_i \leq k$. 

Ideals in $\mathcal{O}$ are unlikely to be polarized. We need to produce relations between polarized ideals.
Relations in the polarized class group

The cost of evaluating the action of the class of $a \subseteq \mathcal{O}$ grows with $N(a)$.
- The action of $a$ is deduced from the action of ideals of smaller norm.
- This boils down to decomposing $a$ in $\mathcal{C}(\mathcal{O})$.

Using smooth ideals

Let $a$ be a polarized ideal of $\mathcal{O}$ and $B > 0$. We rewrite the class of $a$ as

$$a = p_1 \cdots p_k \text{ in } \mathcal{C}(\mathcal{O}), \text{ where } N(p_i) \leq B.$$ 

Evaluating the action of $a$ boils down to evaluating that of the $(p_i)_{i \leq k}$. 

Relations in the polarized class group

The cost of evaluating the action of the class of \( a \subseteq \mathcal{O} \) grows with \( \mathcal{N}(a) \).
- The action of \( a \) is deduced from the action of ideals of smaller norm.
- This boils down to decomposing \( a \) in \( \mathcal{C}(\mathcal{O}) \).

Using smooth ideals

Let \( a \) be a polarized ideal of \( \mathcal{O} \) and \( B > 0 \). We rewrite the class of \( a \) as

\[
a = p_1 \cdots p_k \text{ in } \mathcal{C}(\mathcal{O}), \text{ where } \mathcal{N}(p_i) \leq B.
\]

Evaluating the action of \( a \) boils down to evaluating that of the \((p_i)_{i \leq k}\).

- Ideals in \( \mathcal{O} \) are unlikely to be polarized.
- We need to produce relations between polarized ideals.
From relations in $\text{Cl}(\mathcal{O})$ to relations in $\mathcal{C}(\mathcal{O})$ Bisson-11

Let $K$ a CM field with type $\Phi$ and reflex field $K^r$ with type $\Phi^r$. We have maps between $K$ and $K^r$.

- Type norm : $\mathcal{N}_\Phi : x \in K \rightarrow \prod_{\phi \in \Phi} \phi(x) \in K^r$.
- Reflex type norm : $\mathcal{N}_{\Phi^r} : x \in K^r \rightarrow \prod_{\phi \in \Phi^r} \phi(x) \in K$. 
From relations in $\text{Cl}(O)$ to relations in $\mathcal{C}(O)$ Bisson-11

Let $K$ a CM field with type $\Phi$ and reflex field $K^r$ with type $\Phi^r$. We have maps between $K$ and $K^r$.

- **Type norm**: $N_\Phi : x \in K \rightarrow \prod_{\phi \in \Phi} \phi(x) \in K^r$.
- **Reflex type norm**: $N_{\Phi^r} : x \in K^r \rightarrow \prod_{\phi \in \Phi^r} \phi(x) \in K$.

**Property**

Let $\mathfrak{a} \subseteq O$ be an ideal of $O$ and $\mathfrak{a}^r \subseteq O_{K^r}$ be an ideal of $O_{K^r}$.

- $N_\Phi(\mathfrak{a})$ is an ideal of $O_{K^r}$ and $N(\mathfrak{a}^r)$ is an ideal of $O_K$.
- $N_{\Phi^r}(\mathfrak{a}^r)$ is a polarized ideal of $O_K$. 

Biasse (U of C) large degree fields October 2013 23 / 30
From relations in \( \text{Cl}(\mathcal{O}) \) to relations in \( \mathcal{C}(\mathcal{O}) \) Bisson-11

Let \( K \) a CM field with type \( \Phi \) and reflex field \( K^r \) with type \( \Phi^r \). We have maps between \( K \) and \( K^r \).

- Type norm: \( N_{\Phi} : x \in K \to \prod_{\phi \in \Phi} \phi(x) \in K^r \).
- Reflex type norm: \( N_{\Phi^r} : x \in K^r \to \prod_{\phi \in \Phi^r} \phi(x) \in K \).

Property

Let \( \mathfrak{a} \subseteq \mathcal{O} \) be an ideal of \( \mathcal{O} \) and \( \mathfrak{a}^r \subseteq \mathcal{O}_{Kr} \) be an ideal of \( \mathcal{O}_{Kr} \).

- \( N_{\Phi}(\mathfrak{a}) \) is an ideal of \( \mathcal{O}_{Kr} \) and \( N(\mathfrak{a}^r) \) is an ideal of \( \mathcal{O}_K \).
- \( N_{\Phi^r}(\mathfrak{a}^r) \) is a polarized ideal of \( \mathcal{O}_K \).

We draw a relation \( p_1 \cdots p_k = 1 \) in \( \text{Cl}(\mathcal{O}) \) and deduce the relation

\[
N_{\Phi^r}(N_{\Phi}(p_1)) \cdots N_{\Phi^r}(N_{\Phi}(p_k)) = 1 \in \mathcal{C}(\mathcal{O}).
\]
Relations in $\mathcal{C}(\mathcal{O})$

\[ \begin{align*}
K_{\mathcal{C}} & \quad \mid \quad K = p_1 \cdots p_k \quad \mid \quad K^r = p'_1 \cdots p'_k \\
K_{\mathcal{C}} & \quad \mid \quad K = (\alpha_1, \Omega_1) \cdots (\alpha_k, \Omega_k) \quad \mid \quad K^r = (\beta_1, \Omega_1) \cdots (\beta_k, \Omega_k) \\
\end{align*} \]
Relations in $\mathcal{C}(\mathcal{O})$

\[ (\alpha) = p_1 \cdots p_k \]
Relations in $\mathcal{C}(\mathcal{O})$

$\Phi$.

$K^c$.

$K_r$

$N_\Phi$

$\Phi(p_i) = p'_i$

$(\alpha) = p_1 \cdots p_k$

$(\alpha') = p'_1 \cdots p'_k$
Relations in $\mathcal{C}(\mathcal{O})$

\[ (\alpha) = p_1 \cdots p_k \]
\[ (\beta) = (q_1, \beta_1) \cdots (q_k, \beta_k) \]
\[ N_\Phi(p_i) = p'_i \]
\[ N_{\Phi r}(p'_j) = q_j \]
\[ (\alpha') = p'_1 \cdots p'_k \]
The case of $g \to \infty$

Let $V/F_q$ be a dimension $g$ Abelian variety defined over $\mathbb{F}_q$ with CM by an order $\mathcal{O}$ in $K$.

- We want to derive relations in $\mathcal{C}(\mathcal{O})$.
- We want to establish conditions on $K$ to use the $q$-descent.
The case of $g \to \infty$

Let $V/F_q$ be a dimension $g$ Abelian variety defined over $F_q$ with CM by an order $\mathcal{O}$ in $K$.

- We want to derive relations in $\mathcal{C}(\mathcal{O})$.
- We want to establish conditions on $K$ to use the $q$-descent.

$K = \mathbb{Q}[X]/\chi(X)$ is defined by a $q$-Weil polynomial of the form

$$
\chi(X) = \prod_{j \leq 2g} (X - \sqrt{q} e^{i\theta_j}).
$$
The case of $g \to \infty$

Let $V/\mathbb{F}_q$ be a dimension $g$ Abelian variety defined over $\mathbb{F}_q$ with CM by an order $\mathcal{O}$ in $K$.

- We want to derive relations in $\mathcal{C}(\mathcal{O})$.
- We want to establish conditions on $K$ to use the $q$-descent.

$K = \mathbb{Q}[X]/\chi(X)$ is defined by a $q$-Weil polynomial of the form

$$\chi(X) = \prod_{j \leq 2g} (X - \sqrt{q}e^{i\theta_j}).$$

Let $\Delta = \text{disc}(\chi)$, do $n = \deg(\chi)$ and $d = \log(H(\chi))$ satisfy

$$n = n_0(\log |\Delta|)^\alpha(1 + o(1))$$

$$d = d_0(\log |\Delta|)^{1-\alpha}(1 + o(1)),$$

for $\alpha \in ]0, 1[$ and $n_0, d_0 > 0$, allowing a subexponential $q$-descent?
The case of $g \to \infty$

Let $\log |\Delta'| := g^2 \log(q)$, and $g = \log(q)^\delta$ for some $\delta > 0$, then

- $n = n_0 \log |\Delta'|^\alpha (1 + o(1))$.
- $d = d_0 \log |\Delta'|^{1-\alpha} (1 + o(1))$. 

We can have subexponential time with respect to $\log |\Delta'|$. Do we have $\log |\Delta'| \sim \log |\text{Disc}(\chi)|$?

The discriminant of $\chi$ is given by $\text{Disc}(\chi) = (\sqrt{q} \Delta^{\delta}) \prod_{j \neq k} (e^{i \theta_j} - e^{i \theta_k})$.

We have the upper bound $\log |\text{Disc}(\chi)| \leq O(g^2 \log(q)) (1 + o(1))$. But we might have $\log |\text{Disc}(\chi)| \ll g^2 \log(q)$.

If $|e^{i \theta_j} - e^{i \theta_k}| \geq \frac{1}{p^\epsilon}$ for some $\epsilon < 1/2$, then $\log |\text{Disc}(\chi)| \gtrsim O(g^2 \log(q))$. 

Biasse (U of C) large degree fields October 2013 26 / 30
The case of $g \to \infty$

Let $\log |\Delta'| := g^2 \log(q)$, and $g = \log(q)\delta$ for some $\delta > 0$, then

- $n = n_0 \log |\Delta'|^\alpha (1 + o(1))$.
- $d = d_0 \log |\Delta'|^{1-\alpha} (1 + o(1))$.

We can have subexponential time with respect to $\log |\Delta'|$. Do we have $\log |\Delta'| \sim \log |\text{Disc}(\chi)|$?
The case of $g \rightarrow \infty$

Let $\log |\Delta'| := g^2 \log(q)$, and $g = \log(q)^\delta$ for some $\delta > 0$, then

- $n = n_0 \log |\Delta'|^\alpha (1 + o(1))$.
- $d = d_0 \log |\Delta'|^{1-\alpha} (1 + o(1))$.

We can have subexponential time with respect to $\log |\Delta'|$. Do we have $\log |\Delta'| \sim \log |\text{Disc}(\chi)|$?

The discriminant of $\chi$ is given by

$$\text{Disc}(\chi) = (\sqrt{q})^{(2g \choose g)} \prod_{j \neq k} \left( e^{i\theta_j} - e^{i\theta_k} \right).$$
The case of $g \to \infty$

Let $\log |\Delta'| := g^2 \log(q)$, and $g = \log(q)^\delta$ for some $\delta > 0$, then

- $n = n_0 \log |\Delta'|^\alpha (1 + o(1))$.
- $d = d_0 \log |\Delta'|^{1-\alpha} (1 + o(1))$.

We can have subexponential time with respect to $\log |\Delta'|$. Do we have $\log |\Delta'| \sim \log |\text{Disc}(\chi)|$?

The discriminant of $\chi$ is given by

$$\text{Disc}(\chi) = (\sqrt{q})^{2g \choose g} \prod_{j \neq k} \left( e^{i\theta_j} - e^{i\theta_k} \right).$$

- We have the upper bound $\log |\text{Disc}(\chi)| \leq O(g^2 \log(q))(1 + o(1))$.
- But we might have $\log |\text{Disc}(\chi)| \ll g^2 \log(q)$. 
The case of $g \to \infty$

Let $\log |\Delta'| := g^2 \log(q)$, and $g = \log(q)^\delta$ for some $\delta > 0$, then

- $n = n_0 \log |\Delta'|^\alpha (1 + o(1))$.
- $d = d_0 \log |\Delta'|^{1-\alpha} (1 + o(1))$.

We can have subexponential time with respect to $\log |\Delta'|$. Do we have $\log |\Delta'| \sim \log |\text{Disc}(\chi)|$?

The discriminant of $\chi$ is given by

$$\text{Disc}(\chi) = (\sqrt{q})^{\binom{2g}{g}} \prod_{j \neq k} \left( e^{i\theta_j} - e^{i\theta_k} \right).$$

- We have the upper bound $\log |\text{Disc}(\chi)| \leq O(g^2 \log(q))(1 + o(1))$.
- But we might have $\log |\text{Disc}(\chi)| \ll g^2 \log(q)$.

If $|e^{i\theta_j} - e^{i\theta_k}| \geq \frac{1}{p^\varepsilon}$ for some $\varepsilon < 1/2$, then $\log |\text{Disc}(\chi)| \gtrsim O(g^2 \log(q))$. 
Choosing roots of $\chi(X)$

$$d = \sin(\theta_2 - \theta_1) \sim \theta_2 - \theta_1$$
Choosing roots of $\chi(X)$

$$d = \sin(\theta_2 - \theta_1) \sim \theta_2 - \theta_1$$
Choosing roots of $\chi(X)$

$$d = \sin(\theta_2 - \theta_1) \sim \theta_2 - \theta_1$$
Distribution of eigenangles

We study the case where $g \sim (\log(q))^\delta$ for some $\delta > 0$.

- $|e^{i\theta_j} - e^{i\theta_k}| < \frac{1}{p^\varepsilon}$ implies $\theta_j - \theta_k \to 0$.
- In this case, $|e^{i\theta_j} - e^{i\theta_k}| \sim |\theta_j - \theta_k| := \Theta < \frac{1}{p^\varepsilon}$. 
Distribution of eigenangles

We study the case where $g \sim (\log(q))^\delta$ for some $\delta > 0$.

- $|e^{i\theta_j} - e^{i\theta_k}| < \frac{1}{p^\epsilon}$ implies $\theta_j - \theta_k \to 0$.
- In this case, $|e^{i\theta_j} - e^{i\theta_k}| \sim |\theta_j - \theta_k| := \Theta < \frac{1}{p^\epsilon}$.

If the $(\theta_j)_{j \leq 2g}$ were equidistributed then we would have

$$P \left( \forall j, k, |e^{i\theta_j} - e^{i\theta_k}| \geq \frac{1}{p^\epsilon} \right) = \prod_{l \leq 2g} (1 - l \cdot \Theta) \to 1.$$
Distribution of eigenangles

We study the case where $g \sim (\log(q))^\delta$ for some $\delta > 0$.

- $|e^{i\theta_j} - e^{i\theta_k}| < \frac{1}{p^\epsilon}$ implies $\theta_j - \theta_k \to 0$.
- In this case, $|e^{i\theta_j} - e^{i\theta_k}| \sim |\theta_j - \theta_k| := \Theta < \frac{1}{p^\epsilon}$.

If the $(\theta_j)_{j \leq 2g}$ were equidistributed then we would have

$$P\left(\forall j, k, |e^{i\theta_j} - e^{i\theta_k}| \geq \frac{1}{p^\epsilon}\right) = \prod_{l \leq 2g} (1 - l \cdot \Theta) \to 1.$$ 

Katz-Sarnak

The distribution of the eigenangles is “close” to uniform

$$\lim_{g \to \infty} \lim_{q \to \infty} \left(\frac{1}{|\mathcal{M}_g(\mathbb{F}_q)|}\right) \sum_{C \in \mathcal{M}_g(\mathbb{F}_q)} \text{discrep}(\mu(\text{univ}), \mu(C/\mathbb{F}_q)) = 0.$$
Computing the action of $\mathfrak{C}(\mathcal{O})$

Let $V/\mathbb{F}_q$ of dimension $g$ and a polarized ideal $(\alpha, l)$ with $\mathcal{N}(\alpha) = lg$.

- We represent $V$ by a theta structure of level $n$.
- We want to evaluate the action of $\alpha$ on the isomorphism class of $V$.

Let $H$ be an isotropic subgroup of $V$ isomorphic to $(\mathbb{Z}/l\mathbb{Z})^g$.

Evaluating $\phi$ with $\ker(\phi) = H$ takes $O(l^{3g} + o(1))$ operations in $\mathbb{F}_q$.

Computing $H$ boils down to computing the $l$-torsion.

1. Compute the zeta function $Z_A(T)$ of $A/\mathbb{F}_q$. Set $L \leftarrow \emptyset$.
2. Write $#A(\mathbb{F}_q^{lg-1})$ as $ml^k$ where $l \nmid m$.
3. Let $P = mO$ where $O$ is a random point of $A(\mathbb{F}_q^{lg-1})$.
4. If $P/\mathbb{F}_q \in \langle L \rangle \subseteq A[1/l]$, then $L \leftarrow L \cup P$.
Computing the action of $\mathfrak{C}(\mathcal{O})$

Let $V/\mathbb{F}_q$ of dimension $g$ and a polarized ideal $(\alpha, l)$ with $N(\alpha) = l^g$.
- We represent $V$ by a theta structure of level $n$.
- We want to evaluate the action of $\alpha$ on the isomorphism class of $V$.

Computation of an $(\mathbb{Z}/l\mathbb{Z})^g$-isogeny

- Let $\mathcal{H}$ be an isotropic subgroup of $V$ isomorphic to $(\mathbb{Z}/l\mathbb{Z})^g$.
- Evaluating $\phi$ with $\ker(\phi) = \mathcal{H}$ takes $O(l^{3g}+o(1))$ operations in $\mathbb{F}_q$. 
Computing the action of $\mathfrak{C}(\mathcal{O})$

Let $V/F_q$ of dimension $g$ and a polarized ideal $(\alpha, l)$ with $\mathcal{N}(\alpha) = l^g$.

- We represent $V$ by a theta structure of level $n$.
- We want to evaluate the action of $\alpha$ on the isomorphism class of $V$.

Computation of an $(\mathbb{Z}/l\mathbb{Z})^g$-isogeny

- Let $\mathcal{H}$ be an isotropic subgroup of $V$ isomorphic to $(\mathbb{Z}/l\mathbb{Z})^g$.
- Evaluating $\phi$ with $\ker(\phi) = \mathcal{H}$ takes $O(l^{3g+o(1)})$ operations in $F_q$.

Computing $\mathcal{H}$ boils down to computing the $l$-torsion.

1. Compute the zeta function $Z_A(T)$ of $A/F_q$. Set $L \leftarrow \{\}$
2. Write $\#A(F_{q^{lg-1-1}})$ as $ml^k$ where $l \nmid m$.
3. Let $P = mO$ where $O$ is a random point of $A(F_{q^{lg-1-1}})$.
4. If $P \notin \langle L \rangle \subseteq A[l]$ then $L \leftarrow L \cup P$. 
**Subexponential relations in $\mathfrak{C}(\mathcal{O})$**

We have $g \sim \log(q)^\delta$. Our goal is to find $\alpha, \beta < 1$ such that

- The factor base is $\mathcal{B} = \{p \mid N(p) \leq L_\Delta(\alpha, c + o(1))\}$.
- We can find and evaluate $\mathcal{B}$-smooth relations in time $L_\Delta(\beta, d + o(1))$.  

were $c, d > o$ and $\log |\Delta| = g^2 \log(q)$. 

\[ 
\]
Subexponential relations in $\mathfrak{C}(\mathcal{O})$

We have $g \sim \log(q)^\delta$. Our goal is to find $\alpha, \beta < 1$ such that

- The factor base is $\mathcal{B} = \{p \mid N(p) \leq L_\Delta(\alpha, c + o(1))\}$.
- We can find and evaluate $\mathcal{B}$-smooth relations in time $L_\Delta(\beta, d + o(1))$. were $c, d > o$ and $\log |\Delta| = g^2 \log(q)$.

**Cost of the evaluation**

- For $N(p) = 1$, the evaluation of the action of $p$ takes $l^{O(g)}$.
- We want to adjust the trade-off between $|\mathcal{B}|$ and the expected time.
Subexponential relations in $\mathcal{O}(\mathcal{O})$

We have $g \sim \log(q)^{\delta}$. Our goal is to find $\alpha, \beta < 1$ such that

- The factor base is $B = \{p \mid \mathcal{N}(p) \leq L_\Delta(\alpha, c + o(1))\}$.
- We can find and evaluate $B$-smooth relations in time $L_\Delta(\beta, d + o(1))$.

were $c, d > o$ and $\log \mid \Delta \mid = g^2 \log(q)$.

Cost of the evaluation

- For $\mathcal{N}(p) = 1$, the evaluation of the action of $p$ takes $1^{O(g)}$.
- We want to adjust the trade-off between $|B|$ and the expected time.

We have subexponential time when the conditions are satisfied

- $1 - \beta \geq \delta \geq 1 - \alpha - \beta$.
- $\beta + 2\alpha \geq 1$ and $2\beta + \alpha \geq 1$.
- $\beta > \delta$ or $2\beta + \alpha = 1$.

For example: $\alpha = \beta = 1/3$ works for $\frac{1}{3} \leq \delta \leq \frac{2}{3}$. 
Thank you for your attention.