The principal ideal problem in quaternion algebras

Aurel Page
IMB, Université de Bordeaux

11 August 2014
ANTS XI - GyeongJu, Korea

The principal ideal problem

Let F be a number field with ring of integers $\mathbb{Z}_F$.

Problem

Given an ideal I in $\mathbb{Z}_F$, decide whether it is principal and find a generator.

Applications:

- Selmer group computations and descent (Cremona–Fisher–O'Neil–Simon–Stoll 2011)
- class field theory (Cohen–Diaz y Diaz–Olivier 2000)
- norm and Thue equations (Tzanakis–de Weger 1989, Bilu–Hanrot 1996)

Buchmann's algorithm

Hafner and McCurley 1989 (quadratic case), Buchmann 1990.

Precomputation:

- Choose a set of primes in F that generates $\mathrm{Cl}(F)$: the factor base $\mathcal{B}$.
- Look for random smooth elements in $\mathbb{Z}_F$: the relations $\mathcal{R}$.
- Stop when $\langle \mathcal{B} \rangle / \langle \mathcal{R} \rangle \cong \mathrm{Cl}(F)$.

Buchmann's algorithm

Hafner and McCurley 1989 (quadratic case), Buchmann 1990.

Precomputation:

- Choose a set of primes in F that generates $\mathrm{Cl}(F)$: the factor base $\mathcal{B}$.
- Look for random smooth elements in $\mathbb{Z}_F$: the relations $\mathcal{R}$.
- Stop when $\langle\mathcal{B}\rangle/\langle\mathcal{R}\rangle \cong \mathrm{Cl}(F)$.

Given a fractional ideal I:

- Look for a random element $x \in I^{-1}$ such that xI is smooth.
- Do linear algebra.

Smooth numbers

Theorem (Canfield–Erdös–Pomerance 1983)

Let $\psi(x, y) = |\{n \leq x, n \text{ is } y\text{-smooth}\}|$*. If we set*

$$L(x) = \exp(\sqrt{\ln x \ln \ln x}),$$

then

$$\psi(x, L(x)^a) = x \cdot L(x)^{-1/(2a)+o(1)}.$$

The principal ideal problem in quaternion algebras

Let A be a quaternion algebra over a number field F.

Problem

Given a right ideal I in A, decide whether it is principal and find a generator.

Applications:

- CM points on Shimura curves (Voight 2006).
- Hilbert modular forms (Dembélé–Donnelly 2008, Greenberg–Voight 2011, Voight 2010).
- More generally automorphic forms for GL_2 over number fields.

Quaternion algebras

Quaternion algebra over F = central simple algebra A of dimension 4.

Equivalently, $A = \left(\frac{a,b}{F}\right) = F + Fi + Fj + Fij$ where $i^2 = a$, $j^2 = b$ and $ij = -ji$ $(a, b \in F^\times)$.

Example: $\left(\frac{1,1}{F}\right) \cong \mathcal{M}_2(F)$.

Quaternion algebras

Quaternion algebra over F = central simple algebra A of dimension 4.

Equivalently, $A = \left(\frac{a,b}{F}\right) = F + Fi + Fj + Fij$ where $i^2 = a$, $j^2 = b$ and $ij = -ji$ ($a, b \in F^\times$).

Example: $\left(\frac{1,1}{F}\right) \cong \mathcal{M}_2(F)$.

The **reduced norm** is
$\mathrm{nrd}(x + yi + zj + tij) = x^2 - ay^2 - bz^2 + abt^2$.

Example: $\mathrm{nrd} = \det$.

Orders and ideals

Order $\mathcal{O} \subset A$ = finitely generated $\mathbb{Z}_F$-submodule s.t. $F\mathcal{O} = A$, that is also a subring with unit.

Examples: $\mathbb{Z}_F + \mathbb{Z}_F i + \mathbb{Z}_F j + \mathbb{Z}_F ij$, $\mathcal{M}_2(\mathbb{Z}_F)$.

From now on, assume that $\mathcal{O}$ is a **maximal order**.

Orders and ideals

Order $\mathcal{O} \subset A$ = finitely generated $\mathbb{Z}_F$-submodule s.t. $F\mathcal{O} = A$, that is also a subring with unit.

Examples: $\mathbb{Z}_F + \mathbb{Z}_F i + \mathbb{Z}_F j + \mathbb{Z}_F ij$, $\mathcal{M}_2(\mathbb{Z}_F)$.

From now on, assume that $\mathcal{O}$ is a **maximal order**.

Right ideals: $I = x\mathcal{O}$ (**principal** right ideal) and sums of such.

- Multiplication of right ideals does not form a group.
- nrd is not multiplicative on right ideals.

Orders and ideals

Order $\mathcal{O} \subset A$ = finitely generated $\mathbb{Z}_F$-submodule s.t. $F\mathcal{O} = A$, that is also a subring with unit.

Examples: $\mathbb{Z}_F + \mathbb{Z}_F i + \mathbb{Z}_F j + \mathbb{Z}_F ij$, $\mathcal{M}_2(\mathbb{Z}_F)$.

From now on, assume that $\mathcal{O}$ is a **maximal order**.

Right ideals: $I = x\mathcal{O}$ (**principal** right ideal) and sums of such.

- Multiplication of right ideals does not form a group.
- nrd is not multiplicative on right ideals.

Two-sided ideals: abelian group generated by

- $\mathfrak{P}$ where $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}$: $\mathfrak{p} \subset \mathbb{Z}_F$ is **ramified** in A.
- $\mathfrak{P} = \mathfrak{p}\mathcal{O}$ otherwise: $\mathfrak{p} \subset \mathbb{Z}_F$ is **split** in A.

Definite case

Two natural cases:

1. A is **definite** if $\mathrm{Tr}(\mathrm{nrd})$ is positive definite. Donnelly–Dembélé 2008: algorithm using lattice enumeration.

Theorem (Kirschmer–Voight 2010)

*The Dembélé–Donnelly algorithm runs in **polynomial time** in the size of the input when the **base field is fixed**.*

Indefinite case

2. A is **indefinite** otherwise.
   $\mathrm{Cl}_A(F)$: ray class group with modulus the product of the real places where nrd is positive definite.

Theorem (Eichler)

If A is indefinite and $\mathcal{O}$ a maximal order in A, then a right ideal I is principal iff $\mathrm{nrd}(I)$ is trivial in $\mathrm{Cl}_A(F)$.

Decision problem $\rightsquigarrow$ same problem over the base field.

Indefinite case

2. A is **indefinite** otherwise.
   $\mathrm{Cl}_A(F)$: ray class group with modulus the product of the real places where nrd is positive definite.

Theorem (Eichler)

If A is indefinite and $\mathcal{O}$ a maximal order in A, then a right ideal I is principal iff $\mathrm{nrd}(I)$ is trivial in $\mathrm{Cl}_A(F)$.

Decision problem $\rightsquigarrow$ same problem over the base field.

Problem

Given a principal right $\mathcal{O}$-ideal I in A, find a generator.

Indefinite case

Problem

Given a principal right $\mathcal{O}$-ideal I in A, find a generator.

Kirschmer–Voight 2010: algorithm based on lattice enumeration, complexity is unknown.

Indefinite case

Problem

Given a principal right $\mathcal{O}$-ideal I in A, find a generator.

Kirschmer–Voight 2010: algorithm based on lattice enumeration, complexity is unknown.

Theorem (P. 2014)

There exists an explicit algorithm that, given a generator of $\mathrm{nrd}(I)$*, finds a generator of* I *in time*

$$\exp(O(\log \Delta_A) + O_N(\log \log \Delta_A)),$$

where $N = \dim_{\mathbb{Q}} A$ *and* Δ_A *is the discriminant of* $A/\mathbb{Q}$*.*

Goal

The previous algorithm has proved complexity, but it is not efficient in practice.

Goal

Describe an analogue of Buchmann's algorithm for indefinite quaternion algebras:

- precomputed structure + principalization algorithm
- factor base, **heuristically** subexponential complexity

Trying to adapt Buchmann's algorithm

1. smoothness: choose $\mathcal{B}$ a set of primes of $\mathbb{Z}_F$.
   Integral right ideal is **smooth** if its reduced norm is.
2. linear algebra: no group structure!

Trying to adapt Buchmann's algorithm

1. smoothness: choose $\mathcal{B}$ a set of primes of $\mathbb{Z}_F$.
   Integral right ideal is **smooth** if its reduced norm is.
2. linear algebra: no group structure!
   but works on
   - the norm: given smooth I, can find x such that $\mathrm{nrd}(xI) = (1)$
   - two-sided ideals

Trying to adapt Buchmann's algorithm

1. smoothness: choose $\mathcal{B}$ a set of primes of $\mathbb{Z}_F$.
   Integral right ideal is **smooth** if its reduced norm is.
2. linear algebra: no group structure!
   but works on
   - the norm: given smooth I, can find x such that $\mathrm{nrd}(xI) = (1)$
   - two-sided ideals

Solution: from $\mathrm{nrd}(I) = (1)$, make I two-sided by working prime by prime: multiply on the left by $\mathfrak{p}$-units.

Local problem

F_v completion at a finite place v that is split in A: $A_v \cong \mathcal{M}_2(F_v)$.
$\mathbb{Z}_v$ integers of F_v, residue field $\mathbb{F}_v$.

- Maximal order $\mathcal{O} = \mathcal{M}_2(\mathbb{Z}_v)$.
- Every right ideal I is principal, generator $g \in \mathrm{GL}_2(F_v)$.
- $I = g\mathcal{O}$ two-sided $\Leftrightarrow g \in F_v^\times \mathrm{GL}_2(\mathbb{Z}_v)$.

$\rightsquigarrow$ need to understand $\mathrm{GL}_2(F_v)/F_v^\times \mathrm{GL}_2(\mathbb{Z}_v)$.

Local problem

F_v completion at a finite place v that is split in A: $A_v \cong \mathcal{M}_2(F_v)$.
$\mathbb{Z}_v$ integers of F_v, residue field $\mathbb{F}_v$.

- Maximal order $\mathcal{O} = \mathcal{M}_2(\mathbb{Z}_v)$.
- Every right ideal I is principal, generator $g \in \mathrm{GL}_2(F_v)$.
- $I = g\mathcal{O}$ two-sided $\Leftrightarrow g \in F_v^\times \mathrm{GL}_2(\mathbb{Z}_v)$.

$\rightsquigarrow$ need to understand $\mathrm{GL}_2(F_v)/F_v^\times \mathrm{GL}_2(\mathbb{Z}_v)$.

Geometric interpretation: Bruhat–Tits tree

- transitive action of $\mathrm{GL}_2(F_v)$
- stabilizer of vertex $F_v^\times \mathrm{GL}_2(\mathbb{Z}_v)$
- vertices at distance 1 $\leftrightarrow \mathbb{P}^1(\mathbb{F}_v)$

Example

$A = \left(\frac{3,-1}{\mathbb{Q}}\right)$, $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$ where $\omega = (1 + i + j + ij)/2$,
$I = x\mathcal{O} + 19\mathcal{O}$ where $x = -3 - 4i + j \in A$.

Example

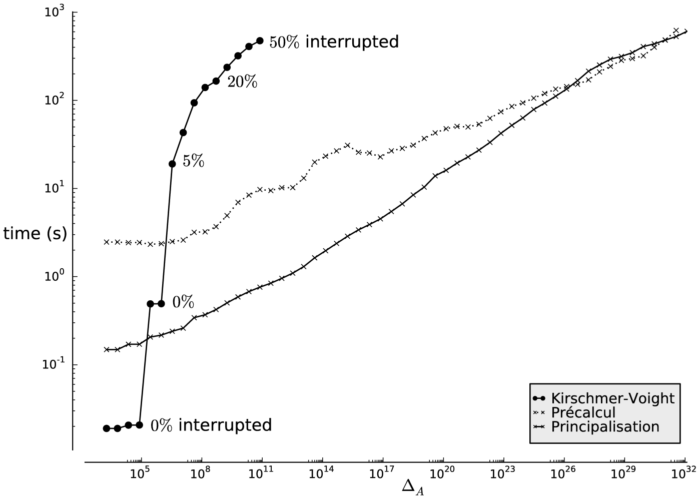
$A = \left(\frac{3,-1}{\mathbb{Q}}\right)$, $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega$ where $\omega = (1 + i + j + ij)/2$,
$I = x\mathcal{O} + 19\mathcal{O}$ where $x = -3 - 4i + j \in A$.

Factor base $\mathcal{B} = \{2, 3, 5, 7, 11, 13, 17\}$.

1. $\mathrm{Cl}(\mathbb{Q}) = 1$, so I is principal.
2. Find $x = (7 + i - 9j - 3\omega)/19 \in I^{-1}$ such that $\mathrm{nrd}(xI) = 7\mathbb{Z}$: xI is smooth.
3. Linear algebra: $c = -1 - 2i - j + \omega$, $cxI/7 = J/7$ where $J = 49\mathcal{O} + w\mathcal{O}$ with $w = -17 - 8i + j$.
4. Local reduction at 7: $h = (-9 - 5i - 7j - 3\omega)/7$.

Multiply out everything: $3 + 4i - 3j - 11\omega$ has norm -19, generator of the ideal I.

Running time



Let F be imaginary quadratic, $\mathfrak{p}, \mathfrak{q}$ primes in $\mathbb{Z}_F$.
Let A be ramified at $\mathfrak{p}, \mathfrak{q}$ and $\mathcal{O} \subset A$ a maximal order.
Let $\Gamma_0(\mathfrak{p}\mathfrak{q})$ be the subgroup of $\mathrm{PGL}_2(\mathbb{Z}_F)$ of elements that are upper triangular modulo $\mathfrak{p}\mathfrak{q}$.

Theorem (Jacquet–Langlands 1970)

There is an injection of Hecke-modules

$$H_1(\mathcal{O}^\times/\mathbb{Z}_F^\times, \mathbb{C}) \longrightarrow H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{C}).$$

Let F be imaginary quadratic, $\mathfrak{p}, \mathfrak{q}$ primes in $\mathbb{Z}_F$.
Let A be ramified at $\mathfrak{p}, \mathfrak{q}$ and $\mathcal{O} \subset A$ a maximal order.
Let $\Gamma_0(\mathfrak{p}\mathfrak{q})$ be the subgroup of $\mathrm{PGL}_2(\mathbb{Z}_F)$ of elements that are upper triangular modulo $\mathfrak{p}\mathfrak{q}$.

Theorem (Jacquet–Langlands 1970)

There is an injection of Hecke-modules

$$H_1(\mathcal{O}^\times/\mathbb{Z}_F^\times, \mathbb{C}) \longrightarrow H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{C}).$$

What happens if we replace $\mathbb{C}$ with another ring, say $\mathbb{F}_p$?

Modulo p cohomology of arithmetic groups

Theorem (Calegari–Venkatesh 2012)

$$H_1(\mathcal{O}^\times/\mathbb{Z}_F^\times, \mathbb{Z})_{tors} \approx H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{Z})_{tors}.$$

Modulo p cohomology of arithmetic groups

Theorem (Calegari–Venkatesh 2012)

$H_1(\mathcal{O}^\times/\mathbb{Z}_F^\times, \mathbb{Z})_{tors} \approx H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{Z})_{tors}$.

Theorem (Scholze 2013)

For any system of eigenvalues in $H_1(\Gamma_0(\mathfrak{N}), \mathbb{F}_p)$, there is a continuous semisimple representation $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ such that Frobenius and Hecke eigenvalues match up.

A modulo p Jacquet-Langlands correspondence ?

Joint work with M. H. Şengün (in progress).

Let $F = \mathbb{Q}(\zeta_3)$, $\mathfrak{p} = (7, 2 + \zeta_3)$, $\mathfrak{q} = (31, 25 + \zeta_3)$.
Let A be the quaternion algebra ramified exactly at $\mathfrak{p}, \mathfrak{q}$.
Let $\mathcal{O}$ be a maximal order in A, and $\Gamma = \mathcal{O}^\times / \mathbb{Z}_F^\times$.

A modulo p Jacquet-Langlands correspondence ?

Joint work with M. H. Şengün (in progress).

Let $F = \mathbb{Q}(\zeta_3)$, $\mathfrak{p} = (7, 2 + \zeta_3)$, $\mathfrak{q} = (31, 25 + \zeta_3)$.
Let A be the quaternion algebra ramified exactly at $\mathfrak{p}, \mathfrak{q}$.
Let $\mathcal{O}$ be a maximal order in A, and $\Gamma = \mathcal{O}^\times / \mathbb{Z}_F^\times$.

We have

$$H_1(\Gamma, \mathbb{C}) = 0, \text{ and } H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{C}) = 0.$$

A modulo p Jacquet-Langlands correspondence ?

Joint work with M. H. Şengün (in progress).

Let $F = \mathbb{Q}(\zeta_3)$, $\mathfrak{p} = (7, 2 + \zeta_3)$, $\mathfrak{q} = (31, 25 + \zeta_3)$.
Let A be the quaternion algebra ramified exactly at $\mathfrak{p}, \mathfrak{q}$.
Let $\mathcal{O}$ be a maximal order in A, and $\Gamma = \mathcal{O}^\times / \mathbb{Z}_F^\times$.

We have

$$H_1(\Gamma, \mathbb{C}) = 0, \text{ and } H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{C}) = 0.$$

Let $p = 5$. Then

$$H_1(\Gamma, \mathbb{F}_p) = \mathbb{F}_p c_1, \text{ and } H_1(\Gamma_0(\mathfrak{p}\mathfrak{q}), \mathbb{F}_p) = \mathbb{F}_p c_2 + \mathbb{F}_p c_3.$$

Eigenvalues of Hecke operators

$N(\mathfrak{l})$	$\lambda_\mathfrak{l}(c_1)$	$\lambda_\mathfrak{l}(c_2)$	$\lambda_\mathfrak{l}(c_3)$
3	2	2	4
4	0	0	0
7	0	0	3
13	1	1	4
13	2	2	4
19	4	4	0
19	1	1	0
25	3	3	1
31	2	2	2
37	4	4	3
37	1	1	3
43	3	3	4
43	0	0	4

The end

Thank you!