An Investigation on Integer Factorization applied to Public Key Cryptography

Giordano Santilli

Università degli Studi di Trento

17 July 2020

Outline

1. The problem of Factorization
2. An elementary approach
3. GNFS
4. First-degree prime ideals in biquadratic fields

The problem of Factorization

Integer Factorization Problem (IFP)

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer N greater than 1 can be represented in a unique way as a product of prime powers:

$$N = p_1^{e_1} \cdots p_k^{e_k},$$

where $k \in \mathbb{N}^+$, $p_1, \ldots, p_k$ prime numbers and $e_1, \ldots, e_k \in \mathbb{N}$.

$$p_1^{e_1} \cdots p_k^{e_k} \xrightarrow{\text{easy}} N$$

$$N \xrightarrow{\text{hard}} p_1^{e_1} \cdots p_k^{e_k}$$

Integer Factorization Problem (IFP)

Integer Factorization Problem (IFP)

Given a semiprime $N \in \mathbb{Z}$, find its prime factors p and q.

Remark

Usually, we call p the smaller factor and q the bigger one.

Cryptography based on IFP

- RSA
- Rabin Cryptosystem
- Schmidt-Samoa Cryptosystem
- Goldwasser-Micali Cryptosystem
- Cayley-Purser algorithm
- Paillier Cryptosystem

Factorization Methods

First-Category Algorithms

These methods returns the smaller prime divisor p of N.
They are effective if $p \approx 7 - 40$ digits.

Factorization Methods

First Category Algorithms	
Factorization Method	**Execution Time**
Trial Division	$O\left(N^{\frac{1}{2}}\right)$
Pollard's $p-1$ Algorithm	$O\left(N^{\frac{1}{2}}\right)$
Pollard's ρ	$O\left(N^{\frac{1}{4}}\right)$
Shanks' Class Group Method	$O\left(N^{\frac{1}{4}}\right)$
Lenstra's Elliptic Curves Method (ECM)	$O\left(e^{\sqrt{2\log N \log\log N}}\right)$

Table: Recap of some first category factorization methods for $N = p \cdot q$.

Factorization Methods

Second-Category Algorithms

These methods do not take into account the size of the factors of N and only depend on its size.
They are effective if N has more than ≈ 100 digits and no small factors.
They are based on Fermat's idea.

Factorization Methods

Fermat's approach

IFP can be solved finding $x, y \in \mathbb{Z}_N$ such that

$$x^2 \equiv y^2 \bmod N \qquad \text{and} \qquad x \not\equiv \pm y \bmod N,$$

meaning that

$$N = pq | (x^2 - y^2) = (x-y)(x+y) \Longrightarrow p | (x-y)(x+y) \text{ and } q | (x+y)(x-y).$$

But since p and q are primes:

$$\begin{cases} p | (x-y) \vee p | (x+y) \\ q | (x-y) \vee q | (x+y) \end{cases}$$

Factorization Methods

The possible cases are the following:

$p \mid (x-y)$	$p \mid (x+y)$	$q \mid (x-y)$	$q \mid (x+y)$	gcd$(x-y,N)$	gcd$(x+y,N)$	Factorization
✓	✓	✓	✓	N	N	✗
✓	✓	✓	✗	N	p	✓
✓	✓	✗	✓	p	N	✓
✓	✗	✓	✓	N	q	✓
✓	✗	✓	✗	N	1	✗
✓	✗	✗	✓	p	q	✓
✗	✓	✓	✗	q	p	✓
✗	✓	✗	✓	1	N	✗
✗	✓	✓	✓	q	N	✓

Table: Output for $x^2 \equiv y^2 \bmod N$.

It is possible to recover a successful factorization in 6 cases over $9 \approx 66\%$.

Factorization Methods

Second Category Algorithms	
Factorization Method	**Execution Time**
Lehman's method	$O\left(N^{\frac{1}{3}}\right)$
Shanks' Square Forms Factorization (SQUFOF)	$O\left(N^{\frac{1}{4}}\right)$
Dixon's Factorization Method	$O\left(e^{2\sqrt{2\log N \log\log N}}\right)$
Continued Fractions Method (CFRAC)	$O\left(e^{\sqrt{2\log N \log\log N}}\right)$
Multiple Polynomial Quadratic Sieve (MPQS)	$O\left(e^{\sqrt{\log N \log\log N}}\right)$
General Number Field Sieve (GNFS)	$O\left(e^{\sqrt[3]{\frac{64}{9}\log N (\log\log N)^2}}\right)$

Table: Recap of some second category factorization methods for $N = p \cdot q$.

Factorization Records

RSA-Number	Binary Digits	Date of Factorization	Method used
RSA-100	330	1 April 1991	MPQS
RSA-110	364	14 April 1992	MPQS
RSA-120	397	9 July 1993	MPQS
RSA-129	426	26 April 1994	MPQS
RSA-130	430	10 April 1996	GNFS
RSA-140	463	2 February 1999	GNFS
RSA-150	496	16 April 2004	GNFS
RSA-155	512	22 August 1999	GNFS
RSA-160	530	1 April 2003	GNFS
RSA-170	563	29 December 2009	GNFS
RSA-576	576	3 December 2003	GNFS
RSA-180	596	8 May 2010	GNFS
RSA-190	629	8 November 2010	GNFS
RSA-640	640	2 November 2005	GNFS
RSA-200	663	9 May 2005	GNFS
RSA-210	696	26 September 2013	GNFS
RSA-704	704	2 July 2012	GNFS
RSA-220	729	13 May 2016	GNFS
RSA-230	762	15 August 2018	GNFS
RSA-232	768	17 February 2020	GNFS
RSA-768	768	12 December 2009	GNFS
RSA-240	795	2 December 2019	GNFS
RSA-250	829	28 February 2020	GNFS

Table: Known factorizations of RSA moduli.

An elementary approach

Successive moduli

Let m be $\left\lfloor\sqrt{\frac{N}{2}}\right\rfloor \leq m \leq \left\lfloor\sqrt{N}\right\rfloor$ and let

$$\begin{cases} N \equiv a_0 \bmod m \\ N \equiv a_1 \bmod (m+1) \\ N \equiv a_2 \bmod (m+2), \end{cases}$$

where a_0, a_1, a_2 are $a_0 \leq a_1 \leq a_2$ or $a_0 \geq a_1 \geq a_2$.
We define $k := a_1 - a_0$ and

$$w := \begin{cases} a_2 - 2a_1 + a_0 & \text{if } a_2 - 2a_1 + a_0 \geq 0, \\ a_2 - 2a_1 + a_0 + m + 2 & \text{if } a_2 - 2a_1 + a_0 < 0. \end{cases}$$

Successive moduli

Proposition

Let N be such that $N \geq 50$ and let $m \in \mathbb{N}^+$ with $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$, then

$$w = \begin{cases} 2, \\ 4, \\ 6. \end{cases}$$

Corollary

If we have also that $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$, then $w = 4$.

Successive moduli

Example

$N = 925363$ and $m = 680$:

$$\begin{aligned} N &\equiv a_0 = 563 && \bmod m \\ N &\equiv a_1 = 565 && \bmod (m+1) \\ N &\equiv a_2 = 571 && \bmod (m+2) \\ N &\equiv 581 && \bmod (m+3) \\ N &\equiv 595 && \bmod (m+4) \\ N &\equiv 613 && \bmod (m+5) \\ N &\equiv 635 && \bmod (m+6) \\ N &\equiv 661 && \bmod (m+7) \\ N &\equiv 3 && \bmod (m+8) \end{aligned}$$

Successive moduli

Example

$N = 925363$ and $m = 680$:

$$\begin{aligned}
N &\equiv a_0 = 563 && \bmod m \\
N &\equiv a_1 = 565 = a_0 + k = 563 + 2 && \bmod (m+1) \\
N &\equiv a_2 = 571 = a_1 + k + w = 565 + 2 + 4 && \bmod (m+2) \\
N &\equiv 581 = 571 + 2 + 2 \cdot 4 && \bmod (m+3) \\
N &\equiv 595 = 581 + 2 + 3 \cdot 4 && \bmod (m+4) \\
N &\equiv 613 = 595 + 2 + 4 \cdot 4 && \bmod (m+5) \\
N &\equiv 635 = 613 + 2 + 5 \cdot 4 && \bmod (m+6) \\
N &\equiv 661 = 635 + 2 + 6 \cdot 4 && \bmod (m+7) \\
N &\equiv 3 = 661 + 2 + 7 \cdot 4 = 691 && \bmod (m+8)
\end{aligned}$$

A formula for successive moduli

Proposition

Let $N \geq 50$ *and such that* $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor \leq m \leq \left\lfloor \sqrt{N} \right\rfloor$, *then for every* $i \in \mathbb{N}$,

$$N \equiv \left(a_0 + ik + w \sum_{j=1}^{i-1} j \right) \bmod (m+i).$$

Corollary

If $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$, *then for every* $i \in \mathbb{N}$,

$$N \equiv \left(a_0 + ik + 2i^2 - 2i \right) \bmod (m+i).$$

A formula for successive moduli

Example

$N = 925363$ and $m = 680$:

$$N \equiv 563 \bmod m$$
$$N \equiv 565 \bmod (m+1)$$
$$N \equiv 571 \bmod (m+2).$$

If we want to compute the remainder of $N \bmod 759$, then $i = 79$ and using the formula we obtain

$$N \equiv 563 + 2i^2 \bmod (m+i) \equiv 13045 \equiv 142 \bmod 759.$$

Interpolating polynomial

Consider the polynomial $f \in \mathbb{Q}[x]$ of degree 2, such that

$$\begin{cases} f(0) = a_0, \\ f(1) = a_1, \\ f(2) = a_2. \end{cases}$$

Proposition

Let $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1$*. Then, the interpolating polynomial* $f \in \mathbb{Q}(x)$ *is such that, for every* $i \in \mathbb{Z}$*,*

$$N \equiv f(i) \bmod (m + i).$$

Successive moduli in factorization

In order to find a factor of N, we would like to solve the following equation for some $x \in \mathbb{Z}$:

$$a_0 + ik + 2i^2 - 2i = x(m + i).$$

Successive moduli in factorization

In order to find a factor of N, we would like to solve the following equation for some $x \in \mathbb{Z}$:

$$a_0 + ik + 2i^2 - 2i = x(m + i).$$

Proposition

Let N be a semiprime and m such that $\left\lfloor \sqrt{\frac{N}{2}} \right\rfloor + 1 \leq m \leq \left\lfloor \sqrt{N} \right\rfloor - 1.$ Then producing the factorization of N is equivalent to finding an integer $i \in \mathbb{N}^+$ for which

$$N \equiv \left(a_0 + ik + 2i^2 - 2i\right) \equiv 0 \bmod (m + i).$$

Successive moduli in factorization

If we consider the interpolating polynomial f, then if m is close to one of the factor of N, then the roots of f are exactly the $i \in \mathbb{Z}$ such that

$$f(i) \equiv 0 \bmod (m+i).$$

However to achieve this result, we need to choose the first remainder a_0 in the monotonic descending sequence that leads to 0.

Successive moduli in factorization

Example

$N = 925363$ and $m = 943$, then

$$\begin{cases} N \equiv 280 \bmod 943, \\ N \equiv 243 \bmod 944, \\ N \equiv 208 \bmod 945. \end{cases}$$

The interpolating polynomial is

$$f(i) = i^2 - 38i + 280,$$

which has two roots: $i_1 = 10$ and $i_2 = 28$. Therefore the two factors of N are:

$$m + i_1 = 953 \qquad m + i_2 = 971.$$

GNFS

Algebraic Preliminaries

Definition

An element $\alpha \in \mathbb{C}$ *is called algebraic integer if there exists a monic polynomial* $f \in \mathbb{Z}[x]$ *such that* $f(\alpha) = 0$*.*
We define also the set of all algebraic integers as

$$\mathcal{B} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic integer}\}.$$

Definition

Fon any number field K*, we define the ring of integers of* K*, as the set*

$$\mathfrak{O}_K = K \cap \mathcal{B},$$

namely all the algebraic integers contained in K*.*

Algebraic Preliminaries

Remark

If we consider the number field $\mathbb{Q}(\theta)$*, the element* θ *is an algebraic integer, meaning that* $\theta \in \mathfrak{O}_{\mathbb{Q}(\theta)}$*, then* $\mathbb{Z}[\theta] \subseteq \mathfrak{O}_{\mathbb{Q}(\theta)}$*. However, usually* $\mathbb{Z}[\theta] \neq \mathfrak{O}_{\mathbb{Q}(\theta)}$*!*

Example

The element $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}) \setminus \mathbb{Z}[\sqrt{5}]$, but it is a root of the polynomial $f(x) = x^2 - x - 1 \in \mathbb{Z}[x]$, so

$$\mathbb{Z}[\sqrt{5}] \subsetneq \mathfrak{O}_{\mathbb{Q}(\sqrt{5})} \subsetneq \mathbb{Q}(\sqrt{5}).$$

Algebraic Preliminaries

Definition

Given $\alpha \in \mathbb{Q}(\theta)$ with $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, we define the norm of α as the product of all its conjugates: $N(\alpha)_{\mathbb{Q}(\theta)/\mathbb{Q}} = N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

Theorem

The ring of integers $\mathfrak{O}_K$ of a number field K is a Dedekind Domain, i.e. every non-zero ideal of $\mathfrak{O}_K$ can be written as a product of powers of prime ideals, uniquely up to the order of the factors.

Definition

Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a non-zero ideal, then the finite quantity

$$\mathscr{N}(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$$

is called the norm of the ideal $\mathfrak{a}$.

Algebraic Preliminaries

Proposition

Let K be a number field of degree n.

1. *For every $\mathfrak{a} \subseteq \mathfrak{O}_K$ non-zero ideal, then $\mathscr{N}(\mathfrak{a}) \in \mathbb{N}^+$ and $\mathscr{N}(\mathfrak{a}) \in \mathfrak{a}$.*
2. *For every $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{O}_K$ non-zero ideals, then $\mathscr{N}(\mathfrak{a}\mathfrak{b}) = \mathscr{N}(\mathfrak{a})\mathscr{N}(\mathfrak{b})$.*
3. *If $\mathfrak{a} = \langle a \rangle$ is a principal ideal in $\mathfrak{O}_K$, then $\mathscr{N}(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|$.*
4. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{O}_K$, then if $\mathscr{N}(\mathfrak{a})$ is prime, then $\mathfrak{a}$ is a prime ideal.*
5. *Conversely, if $\mathfrak{p}$ is a prime ideal, then there exist $p \in \mathbb{N}^+$ prime number and $m \in \mathbb{N}^+$ such that $\mathscr{N}(\mathfrak{p}) = p^m$, where $m \leq n$. The number m is called the degree of the ideal $\mathfrak{p}$.*

First Degree Prime Ideals

Definition

A first-degree prime ideal is a prime ideal $\mathfrak{p}$, such that $\mathscr{N}(\mathfrak{p}) = p$.

First Degree Prime Ideals

Definition

A first-degree prime ideal is a prime ideal $\mathfrak{p}$*, such that* $\mathscr{N}(\mathfrak{p}) = p$*.*

Theorem

Let $f \in \mathbb{Z}[x]$ *be an irreducible monic polynomial and* $\theta \in \mathbb{C}$*, one of its roots. Then, for every positive prime* p *there exists a bijection between*

$$\{(r, p) : r \in \mathbb{Z}_p \mid f(r) \equiv 0 \bmod p\}$$

and

$$\{\mathfrak{p} : \mathfrak{p} \text{ is a first-degree prime ideal in } \mathbb{Z}[\theta] \mid \mathscr{N}(\mathfrak{p}) = p\}.$$

Choice of the Polynomial

We want to find a monic irreducible polynomial $f \in \mathbb{Z}[x]$ such that there exists $m \in \mathbb{Z}$, which verifies $f(m) \equiv 0 \bmod N$.

Choice of the Polynomial

We want to find a monic irreducible polynomial $f \in \mathbb{Z}[x]$ such that there exists $m \in \mathbb{Z}$, which verifies $f(m) \equiv 0 \bmod N$.

Proposition

Given $f \in \mathbb{Z}[x]$ an irreducible monic polynomial, let $\theta \in \mathbb{C}$ be one of its roots and $m \in \mathbb{Z}$ a root of f modulo N. Then, the function ϕ

$$\begin{aligned} \phi :& \mathbb{Z}[\theta] \to \mathbb{Z}_N \\ & a + b\theta \mapsto a + bm \bmod N \end{aligned}$$

is a surjective ring homomorphism.

Choice of the Polynomial

In GNFS, to provide two squares we search for a set $U \subset \mathbb{Z} \times \mathbb{Z}$ such that

$$\prod_{(a,b)\in U} (a + b\theta) = \beta^2 \in \mathbb{Z}[\theta] \qquad \text{and} \qquad \prod_{(a,b)\in U} (a + bm) = y^2 \in \mathbb{Z}.$$

So if we define $x = \phi(\beta) \bmod N$, we obtain that

$$\begin{aligned} x^2 &\equiv \phi\left(\beta\right)^2 = \phi\left(\beta^2\right) = \\ &= \phi\left(\prod_{(a,b)\in U} (a + b\theta)\right) = \prod_{(a,b)\in U} \phi\left(a + b\theta\right) \equiv \\ &\equiv \prod_{(a,b)\in U} (a + bm) = y^2 \bmod N. \end{aligned}$$

Choice of the Polynomial

Actually U is a subset of S

$$S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \gcd(a, b) = 1, |a| \leq \mu, 0 < b \leq \eta\},$$

where μ, η are parameters decided at the beginning of the algorithm.

Choice of the Polynomial

Actually U is a subset of S

$$S = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : \gcd(a,b) = 1, |a| \leq \mu, 0 < b \leq \eta\},$$

where μ, η are parameters decided at the beginning of the algorithm.

To extract from S the elements that belongs to U, GNFS employs three particular sets, called *bases*:

- The *Rational Factor Base*
- The *Algebraic Factor Base*
- The *Quadratic Characters Base*

First Degree Prime Ideals in GNFS

If $\alpha \in \mathbb{Z}[\theta]$ and $\mathfrak{a} = \langle \alpha \rangle$, then

$$p_1^{m_1} \cdots p_h^{m_h} = |N(\alpha)| = \mathscr{N}(\mathfrak{a}) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right),$$

where p_i are prime numbers, $\mathfrak{p}_j$ are prime ideals and $m_i, e_j \in \mathbb{N}^+$ are exponents.

First Degree Prime Ideals in GNFS

If $\alpha \in \mathbb{Z}[\theta]$ and $\mathfrak{a} = \langle \alpha \rangle$, then

$$p_1^{m_1} \cdots p_h^{m_h} = |N(\alpha)| = \mathscr{N}(\mathfrak{a}) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right),$$

where p_i are prime numbers, $\mathfrak{p}_j$ are prime ideals and $m_i, e_j \in \mathbb{N}^+$ are exponents.

If $\mathfrak{a}$ is a square, then $m_1, \ldots, m_h, e_1, \ldots, e_k$ are even.

If $m_1, \ldots, m_h$ are even, then is $\mathfrak{a}$ a square?

First Degree Prime Ideals in GNFS

If $\alpha \in \mathbb{Z}[\theta]$ and $\mathfrak{a} = \langle \alpha \rangle$, then

$$p_1^{m_1} \cdots p_h^{m_h} = |N(\alpha)| = \mathscr{N}(\mathfrak{a}) = \mathscr{N}\left(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}\right),$$

where p_i are prime numbers, $\mathfrak{p}_j$ are prime ideals and $m_i, e_j \in \mathbb{N}^+$ are exponents.
If $\mathfrak{a}$ is a square, then $m_1, \dots, m_h, e_1, \dots, e_k$ are even.
If $m_1, \dots, m_h$ are even, then is $\mathfrak{a}$ a square?

Two problems in finding the squares

- There can be an ideal (e.g. $\mathfrak{p}_1$) for which there exists $u \in \mathbb{N}^+$ such that

$$\mathscr{N}({\mathfrak{p}_1}^{e_1}) = p_1^{e_1 \cdot u} \qquad \text{and} \qquad e_1 \cdot u = m_1$$

- There can be two (or more) ideals (e.g. $\mathfrak{p}_1$, $\mathfrak{p}_2$) such that

$$\mathscr{N}({\mathfrak{p}_1}^{e_1}) = {p_1}^{e_1} \quad \text{and} \quad \mathscr{N}({\mathfrak{p}_2}^{e_2}) = {p_1}^{e_2} \quad \text{and} \quad e_1 + e_2 = m_1$$

First Degree Prime Ideals in GNFS

Proposition

Let $a, b \in \mathbb{Z}$ be coprime. Then every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$ that divides $\langle a + b\theta \rangle$ is a first-degree prime ideal.

First Degree Prime Ideals in GNFS

Proposition

Let $a, b \in \mathbb{Z}$ *be coprime. Then every prime ideal* $\mathfrak{p}$ *of* $\mathbb{Z}[\theta]$ *that divides* $\langle a + b\theta \rangle$ *is a first-degree prime ideal.*

Proposition

Let $a, b \in \mathbb{Z}$ *such that* $\gcd(a, b) = 1$*. Let* $f \in \mathbb{Z}[x]$ *be a monic irreducible polynomial and call* $\theta \in \mathbb{C}$ *on of its roots. Then, the first-degree prime ideal* $\mathfrak{p}$ *of* $\mathbb{Z}[\theta]$ *(corresponding to the pair* (r, p)*) divides* $\langle a + b\theta \rangle$ *with exponent equal to*

$$e_{p,r}(a + b\theta) = \begin{cases} \mathrm{ord}_p \left(|N(a + b\theta)| \right) & \textit{if } a + br \equiv 0 \bmod p \\ 0 & \textit{otherwise,} \end{cases}$$

where $\mathrm{ord}_p(k)$ *is the maximum exponent of* p *in the factorization of* k*.*

Algebraic Factor Base

Definition

Given $N \in \mathbb{N}^+$, $f \in \mathbb{Z}[x]$ an irreducible monic polynomial and $\theta \in \mathbb{C}$ one of its roots, we fix a threshold value $C \in \mathbb{N}^+$ and define the Algebraic Factor Base $\mathcal{A}$ as

$$\mathcal{A} = \{\mathfrak{p} : \mathfrak{p} \textit{ is a first-degree prime ideal of } \mathbb{Z}[\theta] \textit{ with } \mathscr{N}(\mathfrak{p}) \leq C\}\,.$$

Equivalently,

$$\mathcal{A} = \{(r,p) : p \in \{2,\ldots,C\} \textit{ is a prime number and } f(r) \equiv 0 \bmod p\}\,.$$

Algebraic Factor Base

Definition

Given $N \in \mathbb{N}^+$, $f \in \mathbb{Z}[x]$ an irreducible monic polynomial and $\theta \in \mathbb{C}$ one of its roots, we fix a threshold value $C \in \mathbb{N}^+$ and define the Algebraic Factor Base $\mathcal{A}$ as

$$\mathcal{A} = \{\mathfrak{p} : \mathfrak{p} \text{ is a first-degree prime ideal of } \mathbb{Z}[\theta] \text{ with } \mathscr{N}(\mathfrak{p}) \leq C\}.$$

Equivalently,

$$\mathcal{A} = \{(r, p) : p \in \{2, \ldots, C\} \text{ is a prime number and } f(r) \equiv 0 \bmod p\}.$$

Definition

An element $(a, b) \in S$ is called smooth in $\mathcal{A}$ if the ideal $\langle a + b\theta \rangle$ has as factors only elements in $\mathcal{A}$, meaning that $|N(a + b\theta)|$ is C-smooth.

First-degree prime ideals in biquadratic fields

joint work with Ph.D. Daniele Taufer

A new setting

Consider the following irreducible polynomials in $\mathbb{Z}[x]$

$$f_a(x) = x^2 - a \qquad \text{and} \qquad f_b(x) = x^2 - b$$

and call α and β respectively one of their roots.

A new setting

Consider the following irreducible polynomials in $\mathbb{Z}[x]$

$$f_a(x) = x^2 - a \qquad \text{and} \qquad f_b(x) = x^2 - b$$

and call α and β respectively one of their roots.

Build the following field extensions:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\theta) = \mathbb{Q}(\alpha + \beta) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\beta) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

It is well-known that θ can be chosen as $\alpha + \beta$ and the minimal polynomial of θ is

$$f_c(x) = x^4 - 2(a+b)x^2 + (a-b)^2.$$

First-degree Prime Ideals of Biquadratic Extensions

Our question

Is there a link between first-degree prime ideals in $\mathbb{Z}[\theta]$ and those in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$?

First-degree Prime Ideals of Biquadratic Extensions

Theorem

Let (r, p) be a first-degree prime ideal of $\mathbb{Z}[\alpha]$ and (s, p) a first-degree prime ideal of $\mathbb{Z}[\beta]$. Then $(r + s, p)$ is a first-degree prime ideal of $\mathbb{Z}[\theta]$.

$$
\begin{tikzcd}
 & \begin{matrix} \mathbb{Z}[\theta] \\ (r+s, p) \end{matrix} & \\
\begin{matrix} \mathbb{Z}[\alpha] \\ (r, p) \end{matrix} \arrow[ur] & & \begin{matrix} \mathbb{Z}[\beta] \\ (s, p) \end{matrix} \arrow[ul]
\end{tikzcd}
$$

Definition

We will refer to $(r + s, p) \subseteq \mathbb{Z}[\theta]$ as the combination of the ideals $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$.

First-degree Prime Ideals of Biquadratic Extensions

Theorem

Let (t, p) be a first-degree prime ideal of $\mathbb{Z}[\theta]$. If either $p = 2$ or $t \not\equiv 0 \bmod p$ then there exists a unique pair $r, s \in \mathbb{Z}_p$ such that $t \equiv r + s \bmod p$ and $(r, p), (s, p)$ are first-degree prime ideals of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, respectively.

$$
\begin{array}{ccc}
 & \begin{array}{c}\mathbb{Z}[\theta] \\ (t = r + s, p) \\ t \not\equiv 0 \bmod p\end{array} & \\
\swarrow & & \searrow \\
\begin{array}{c}\mathbb{Z}[\alpha] \\ (r, p)\end{array} & & \begin{array}{c}\mathbb{Z}[\beta] \\ (s, p)\end{array}
\end{array}
$$

First-degree Prime Ideals of Biquadratic Extensions

The only exception

What about ideals in $\mathbb{Z}[\theta]$ of the form $(0, p)$ with $p \neq 2$?

One of the following situations takes place, depending on the number ν of roots of f_a modulo p:

- $\nu = 0$: $(0, p) \subseteq \mathbb{Z}[\theta]$ cannot be found as a combination of first-degree prime ideals of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.
- $\nu = 1$: $(0, p) \subseteq \mathbb{Z}[\theta]$ is the combination of $(0, p) \subseteq \mathbb{Z}[\alpha]$ and $(0, p) \subseteq \mathbb{Z}[\beta]$.
- $\nu = 2$: $(0, p) \subseteq \mathbb{Z}[\theta]$ is determined by two different combinations of first-degree prime ideals of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

First-degree Prime Ideals of Biquadratic Extensions

An example

Let $f_a = x^2 - 50$ and $f_b = x^2 - 155$ generate the quadratic fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, so that the composite biquadratic field $\mathbb{Q}(\theta)$ is generated by the polynomial $f_c = x^4 - 410x^2 + 11025$.

- $(0,3) \in \mathbb{Z}[\theta] \longrightarrow$ no ideals with norm equal to 3 in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.
- $(0,5) \in \mathbb{Z}[\theta] \longrightarrow$ combination of $\{(0,5),(0,5)\}$.
- $(0,7) \in \mathbb{Z}[\theta] \longrightarrow$ combination of $\{(1,7),(6,7)\}$ and $\{(6,7),(1,7)\}$.

Division of Principal Ideals

Proposition

Let n *and* $m \neq 0$ *be coprime integers and let* $I = \langle n + m\theta \rangle \subseteq \mathbb{Z}[\theta]$. *Then* $I \cap \mathbb{Z}[\alpha]$ *is a principal ideal of* $\mathbb{Z}[\alpha]$ *generated by*

$$I \cap \mathbb{Z}[\alpha] = \langle (n + m\alpha + m\beta)(n + m\alpha - m\beta) \rangle \, .$$

Division of Principal Ideals

Theorem

Let n and $m \neq 0$ be coprime integers and $I = \langle n + m\theta \rangle$ be a principal ideal of $\mathbb{Z}[\theta]$. Let us assume that there are (r, p) first-degree prime ideal of $\mathbb{Z}[\alpha]$ dividing $I_a = I \cap \mathbb{Z}[\alpha]$ and (s, p) first-degree prime ideal of $\mathbb{Z}[\beta]$ dividing $I_b = I \cap \mathbb{Z}[\beta]$. Then $(r + s, p)$ is a first-degree prime ideal of $\mathbb{Z}[\theta]$ dividing I unless the following conditions simultaneously hold:

$$p \neq 2, \quad n \equiv 0 \bmod p, \quad r + s \not\equiv 0 \bmod p.$$

$$\begin{tikzcd}
 & \begin{array}{c}\mathbb{Z}[\theta] \\ (r+s,p) \mid I\end{array} & \\
\begin{array}{c}\mathbb{Z}[\alpha] \\ (r,p) \mid I_a\end{array} \arrow[ur] & & \begin{array}{c}\mathbb{Z}[\beta] \\ (s,p) \mid I_b\end{array} \arrow[ul]
\end{tikzcd}$$

Division of Principal Ideals

Example

Let $f_a = x^2 + 4$ and $f_b = x^2 - 6$ generate the quadratic fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, so that the composite biquadratic field $\mathbb{Q}(\theta)$ is generated by the polynomial $f_c = x^4 - 4x^2 + 100$.
The first-degree prime ideals of $\mathbb{Z}[\theta]$ with norm $p = 5$ are $(0, 5), (2, 5)$ and $(3, 5)$, while those of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are $(1, 5)$ and $(4, 5)$.
Let I be the principal ideal $\langle 5 + \theta \rangle \subseteq \mathbb{Z}[\theta]$. By the previous proposition we have

$$I_a = \langle 15 + 10\alpha \rangle \subseteq \mathbb{Z}[\alpha], \quad I_b = \langle 35 + 10\beta \rangle \subseteq \mathbb{Z}[\beta].$$

It is easy to see that both $(1, 5)$ and $(4, 5)$ divide I_a and I_b.

Division of Principal Ideals

Example

- $$\begin{cases}(1,5) \mid I_a \\ (4,5) \mid I_b\end{cases} \quad \text{or} \quad \begin{cases}(4,5) \mid I_a \\ (1,5) \mid I_b\end{cases} \implies (0,5) \mid I$$
- $$\begin{cases}(1,5) \mid I_a \\ (1,5) \mid I_b\end{cases} \implies (2,5) \nmid I$$
- $$\begin{cases}(4,5) \mid I_a \\ (4,5) \mid I_b\end{cases} \implies (3,5) \nmid I$$

Division of Principal Ideals

Theorem

Let n and $m \neq 0$ be integers, $I = \langle n + m\theta \rangle \subseteq \mathbb{Z}[\theta]$ and let (t, p) be a first-degree prime ideal dividing I. If there exist first-degree prime ideals $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ such that $r + s \equiv t \bmod p$, then (r, p) divides $I_a = I \cap \mathbb{Z}[\alpha]$ and (s, p) divides $I_b = I \cap \mathbb{Z}[\beta]$.

$$\begin{tikzcd}
 & \begin{array}{c} \mathbb{Z}[\theta] \\ (r+s,p)|I \end{array} \arrow[dl] \arrow[dr] & \\
\begin{array}{c} \mathbb{Z}[\alpha] \\ (r,p)|I_a \end{array} & & \begin{array}{c} \mathbb{Z}[\beta] \\ (s,p)|I_b \end{array}
\end{tikzcd}$$

Division of Principal Ideals

Corollary

Let n and $m \neq 0$ be coprime integers, $I = \langle n + m\theta \rangle \subseteq \mathbb{Z}[\theta]$ and let (t, p) be a first-degree prime ideal dividing I, with $t \neq 0$ if $p \neq 2$. Then there exist two unique first-degree prime ideals $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ such that (r, p) divides $I \cap \mathbb{Z}[\alpha]$, (s, p) divides $I \cap \mathbb{Z}[\beta]$ and $r + s \equiv t \bmod p$.

$$
\begin{tikzcd}
 & \begin{array}{c} \mathbb{Z}[\theta] \\ (t = r + s, p) | I \\ t \not\equiv 0 \bmod p \end{array} \arrow[dl] \arrow[dr] & \\
\begin{array}{c} \mathbb{Z}[\alpha] \\ (r, p) | I_a \end{array} & & \begin{array}{c} \mathbb{Z}[\beta] \\ (s, p) | I_b \end{array}
\end{tikzcd}
$$

Division of Principal Ideals

Summarizing,

$$\begin{tikzcd}[column sep=small]
& \begin{array}{c}\mathbb{Z}[\theta] \\ (r+s,p)|I\end{array} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] & \\
\begin{array}{c}\mathbb{Z}[\alpha] \\ (r,p)|I_a\end{array} & & \begin{array}{c}\mathbb{Z}[\beta] \\ (s,p)|I_b\end{array}
\end{tikzcd}$$

except for some ecceptional cases completely analysed.

A new Algebraic Factor Base

We need to study the exponents of the first-degree prime ideals that divides the principal ideals. In order to do so, we need to analyse the norm:

Proposition

Let $I = \langle n + m\theta \rangle$ *be a principal ideal in* $\mathbb{Z}[\theta]$, *with* $\gcd(n, m) = 1$. *Let* $I_a = I \cap \mathbb{Z}[\alpha]$ *and* $I_b = I \cap \mathbb{Z}[\beta]$. *Then,*

$$\begin{aligned} N_{\mathbb{Q}(\theta)/\mathbb{Q}}(n + m\theta) &= N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(n^2 + m^2(a - b) + 2nm\alpha) \\ &= N_{\mathbb{Q}(\beta)/\mathbb{Q}}(n^2 + m^2(b - a) + 2nm\beta). \end{aligned}$$

Limits and Future Works

In this way we only consider biquadratic polynomials for GNFS of degree 4. However, such polynomial are not suitable for the use in the algorithm, because they would not lead to enough sieving pairs.

Limits and Future Works

In this way we only consider biquadratic polynomials for GNFS of degree 4. However, such polynomial are not suitable for the use in the algorithm, because they would not lead to enough sieving pairs.

We are currently working on a generalization of this approach to enlarge the result to any two field extensions. In this way we hope to increase the performance of GNFS.

THANK YOU
FOR THE ATTENTION!