Recovering Short Generators of Principal Ideals in Cyclotomic Fields of Conductor $p^\alpha q^\beta$

Patrick Holzer, Thomas Wunderer, Johannes Buchmann

TECHNISCHE UNIVERSITÄT DARMSTADT

Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Introduction
Lattice-based cryptography

- Lattice-based crypto is assumed to be post-quantum secure.
- Based on well known lattice problems such as the shortest vector problem (SVP).
- To boost efficiency special lattices such as ideal lattices are used.
- Ideal lattices correspond to fractional ideals in algebraic number fields.
- Some schemes (e.g., [SV10] and [GGH13]) use principal ideals with short generators.
- To break those schemes, one needs to solve the short generator principal ideal problem (SG-PIP).

Introduction
The SG-PIP

Let K be an algebraic number field. The SG-PIP is defined as follows:

- **Given:** A $\mathbb{Z}$-basis of some principal fractional ideal $\mathfrak{a} \subseteq K$ that has some "short" generator g.
- **Task:** Recover some shortest generator of $\mathfrak{a}$.

The folklore approach is to solve the SG-PIP in two steps:

1.
   - Recover some arbitrary generator of the ideal, which is known as the *principal ideal problem (PIP)*.
   - Solvable in polynomial time on quantum computers for any number field due to Biasse and Song.
2.
   - Transform this generator into some shortest generator.
   - Solvable in polynomial time for cyclotomic fields $\mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha$ due to Cramer, Ducas, Peikert, and Regev [CDPR16].

→ **Our work:** task 2 for cyclotomic fields $\mathbb{Q}(\zeta_m)$ of conductor $m = p^\alpha q^\beta$.

Contents

Preliminaries
Cyclotomic Fields

Let $\zeta_m = \exp(^{2\pi i}/_m) \in \mathbb{C}$ be a primitive m-th root of unity, i.e., $\zeta_m^m = 1$.

- The m-th **cyclotomic field** $K_m = \mathbb{Q}(\zeta_m) \subseteq \mathbb{C}$.
  Example:
  $$\frac{3 \cdot \zeta_3^2 + 1}{2 \cdot \zeta_3^2 + \zeta_3 - 8} \in K_3.$$
- The **ring of integers** $\mathcal{O}_m$ of K_m is given by $\mathcal{O}_m = \mathbb{Z}[\zeta_m]$.
  Example:
  $$\zeta_7^5 + 6\zeta_7^3 + 2\zeta_7 + 5 \in \mathbb{Z}[\zeta_7].$$
- The set of all units of $\mathcal{O}_m$ is denoted by $\mathcal{O}_m^\times$.

- A principal fractional ideal of K_m:

$$\langle g \rangle = g \cdot \mathcal{O}_m = \{g \cdot z \mid z \in \mathcal{O}_m\}$$

  for some $g \in K_m$.

- Fact: If $\langle g \rangle = \langle g' \rangle$, then $g = g' \cdot u$ for some $u \in \mathcal{O}_m^\times$

TECHNISCHE UNIVERSITÄT DARMSTADT

Let $n = \varphi(m) = 2s$ and $m \geq 3$.

Complex embeddings of K_m:

$$\sigma_1, \overline{\sigma_1}, ..., \sigma_s, \overline{\sigma_s} : K_m \to \mathbb{C}, \text{ where}$$

$$\sigma_i(\zeta_m) = \zeta_m^j \text{ for some } j \in \mathbb{Z}_m^\times.$$

The **logarithmic embedding** as

$$\begin{aligned} \text{Log} : \; K_m^\times &\to \mathbb{R}^s \\ \alpha &\mapsto \big((\log(|\sigma_1(\alpha)|), ..., \log(|\sigma_s(\alpha)|)\big), \end{aligned}$$

$\to$ $\text{Log}(\mathcal{O}_m^\times)$ is a lattice in $\mathbb{R}^s$ of rank $s-1$!

Logarithmic Embedding
Short Generator

TECHNISCHE UNIVERSITÄT DARMSTADT

Let $\mathfrak{a} = \langle g \rangle \subset K_m$.

$g' \in K_m$ is called a **shortest generator** of $\mathfrak{a}$, if

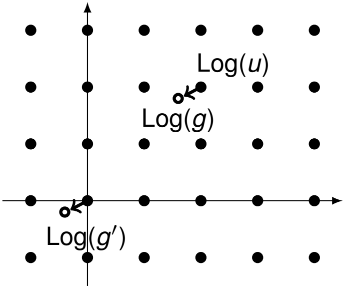
- $\langle g' \rangle = \mathfrak{a}$ and
- $||\mathrm{Log}(g')||_2 = \min_{f \in K_m, \langle f \rangle = \mathfrak{a}} ||\mathrm{Log}(f)||_2 = \min_{u \in \mathcal{O}_m^\times} ||\mathrm{Log}(g \cdot u)||_2$.

Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Algorithmic Approach
Idea

- Let $g' = gu$ be a shortest generator of $\langle g \rangle = \mathfrak{a} \subset K_m$ for some $u \in \mathcal{O}_m^\times$.
- Hence $\mathrm{Log}(g') = \mathrm{Log}(g) + \mathrm{Log}(u)$ and $\mathrm{Log}(g) \in \mathrm{Log}(\mathcal{O}_m^\times) + \mathrm{Log}(g')$.
- Since $\mathrm{Log}(g')$ is short, this is a CVP problem.
- **Solve CVP in the lattice Log**$(\mathcal{O}_m^\times)$ (or in some **small-index subgroup**).



Algorithmic Approach
CVP

TECHNISCHE UNIVERSITÄT DARMSTADT

Algorithm: Round-off Algorithm

Input: $\mathbf{B}, \mathbf{t}$.
Output: Close(st) vector $\mathbf{v} \in \mathcal{L}$ to t.
$\mathbf{a} \leftarrow \lfloor (\mathbf{B}^*)^T \cdot \mathbf{t} \rceil$
$\mathbf{v} \leftarrow \mathbf{B} \cdot \mathbf{a}$
return $(\mathbf{v}, \mathbf{a})$

Where $\mathbf{B}$ is a basis of the lattice Γ and $\mathbf{B}^*$ denotes its dual basis.

On input $\mathbf{t} := \mathbf{v} + \mathbf{e} \in \mathbb{R}^n$ for $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ and (small) error $\mathbf{e} \in \mathbb{R}^n$ the algorithm outputs $\mathbf{v}$ if $\langle \mathbf{b}_j^*, \mathbf{e} \rangle \in [-\frac{1}{2}, \frac{1}{2})$.

$\rightarrow$ Needs a sufficiently good basis (short dual vectors).

Algorithmic Approach
CVP

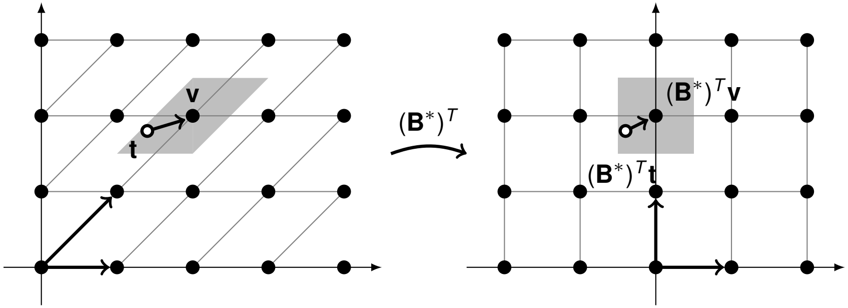


Figure: Round-off Algorithm

Algorithmic Approach
Recovering Shortest Generator

What is left:

1. Construct a basis $\mathbf{B}$ of a sublattice $L \subset \Gamma = \mathrm{Log}(\mathcal{O}_m^\times)$.
2. Show that the index $[\Gamma : L]$ is small.
3. Show that $||\mathbf{b}_j^*||_2$ is small enough to guarantee $\langle \mathbf{b}_j^*, \mathrm{Log}(g') \rangle \in [-\frac{1}{2}, \frac{1}{2})$.

Algorithmic Approach
Subgroups of $\mathcal{O}_m^\times$

We consider the following subgroups of $\mathcal{O}_m^\times$.

For $j \in \mathbb{Z}_m^\times \setminus \{\pm 1\}$ let

$$b_j := \frac{\zeta_m^j - 1}{\zeta_m - 1} \in \mathcal{O}_m^\times$$

- For $m = p^\alpha$: Consider the subgroup $\mathcal{C}_m$ generated by the b_j's.
- For $m = p^\alpha q^\beta$: Consider the subgroup $\mathcal{S}_m$ generated by the b_j's and $\pm\zeta_m$.

Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Index
The case $m = p^\alpha$ as in [CDPR16]

TECHNISCHE UNIVERSITÄT DARMSTADT

Let $m = p^\alpha$.
Fact: the index of $\mathcal{C}_m \subset \mathcal{O}_m^\times$ is given by

$$h_m^+ = \left[\mathcal{O}_m^\times : \mathcal{C}_m\right],$$

where h_m^+ is the class number of $K_m^+ = \mathbb{Q}(\zeta_m + \overline{\zeta_m})$.

1. We need h_m^+ to be small.
2. **Weber's class number problem**: conjectured that $h_{2^l}^+ = 1$ for all $l \in \mathbb{N}$.
3. Conjectured: for every prime p exists a constant c_p such that $h_{p^l}^+ \leq c_p$ for all $l \in \mathbb{N}$.

$\rightarrow$ In the prime-power case, the index is small enough.

Index
The case $m = p^\alpha q^\beta$

TECHNISCHE UNIVERSITÄT DARMSTADT

- More complicated for $m = p^\alpha q^\beta$.
- Let $G_m = \mathbb{Z}_m^\times / \{\pm 1\}$ and set

$$\beta_m := \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \not\equiv 1}} \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} (1 - \chi(p)) .$$

- If m is not a prime-power:

$$[\mathcal{O}_m^\times : \mathcal{S}_m] = \begin{cases} 2h_m^+ \beta_m & \text{if } 2h_m^+ \beta_m \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

- Cohen-Lenstra heuristics and computations suggest h_m^+ is polynomial in m. Evaluating β_m leads to the new notion of **generator prime pairs**.

Index if $m = p^\alpha q^\beta$
Generator Prime Pairs

TECHNISCHE UNIVERSITÄT DARMSTADT

Definition 1

Let $\alpha, \beta \in \mathbb{N}$ and $p, q \in \mathbb{P} \setminus \{2\}$ be distinct. Then (p, q) is called an (α, β)-**generator prime pair (GPP)** if:

i)
- If $q - 1 \equiv 0 \mod 4$: $\langle p \rangle = \mathbb{Z}_{q^\beta}^\times$.
- If $q - 1 \not\equiv 0 \mod 4$: $\langle p \rangle = \mathbb{Z}_{q^\beta}^\times$ or $[\mathbb{Z}_{q^\beta}^\times : \langle p \rangle] = 2$.

And

ii)
- If $p - 1 \equiv 0 \mod 4$: $\langle q \rangle = \mathbb{Z}_{p^\beta}^\times$.
- If $p - 1 \not\equiv 0 \mod 4$: $\langle q \rangle = \mathbb{Z}_{p^\beta}^\times$ or $[\mathbb{Z}_{p^\beta}^\times : \langle q \rangle] = 2$.

If (p, q) is an (α, β)-GPP for every $\alpha, \beta \in \mathbb{N}$, we call (p, q) a **generator prime pair** (**GPP**).

Index if $m = p^\alpha q^\beta$
Generator Prime Pairs

Some facts about GPPs:

- If (p, q) is an (α, β)-GPP and $\beta \geq 2$, then (p, q) is an (α, l)-GPP for all $l \in \mathbb{N}$.
- In particular, (p, q) is a GPP iff it is a $(2, 2)$-GPP.
- Experiments suggest that $\approx$ 36% of all odd prime pairs are GPPs.

p	q	p	q	p	q	p	q	p	q	p	q	p	q
3	5	5	17	7	11	11	13	13	37	17	23	19	23
3	7	5	23	7	17	11	17	13	41	17	31	19	29
3	23	5	37	7	23	11	29	13	59	17	37	19	41
3	29	5	47	7	47	11	31	13	67	17	41	19	47

Figure: Generator prime pairs

Index if $m = p^{\alpha} q^{\beta}$
Generator Prime Pairs

TECHNISCHE UNIVERSITÄT DARMSTADT

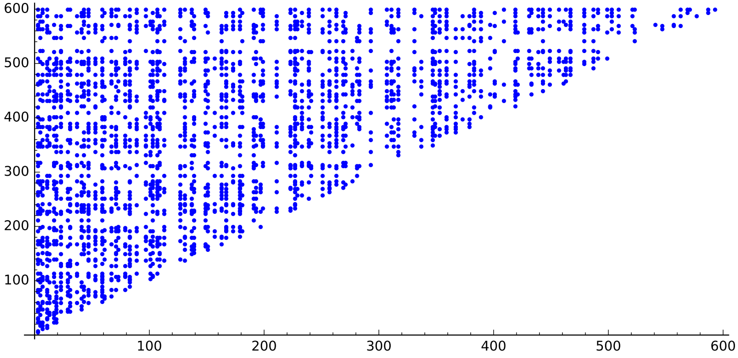


Figure: Generator prime pairs

Index if $m = p^\alpha q^\beta$
The factor β_m

TECHNISCHE UNIVERSITÄT DARMSTADT

Theorem 2

Let p, q be two distinct odd primes and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$. Then

$$\beta_m = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t \mid m \\ t \in \mathbb{P}}} (1 - \chi(t)) \neq 0 \text{ iff } (p, q) \text{ is an } (\alpha, \beta)\text{-generator prime pair.}$$

Theorem 3

If (p, q) is an (α, β)-generator prime pair and $m = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{N}$, then

$$\beta_m = \prod_{\substack{\chi \in \widehat{G_m} \\ \chi \neq 1}} \prod_{\substack{t \mid m \\ t \in \mathbb{P}}} (1 - \chi(t)) = \frac{\varphi(m)}{4}.$$

Index if $m = p^\alpha q^\beta$
The factor β_m

TECHNISCHE UNIVERSITÄT DARMSTADT

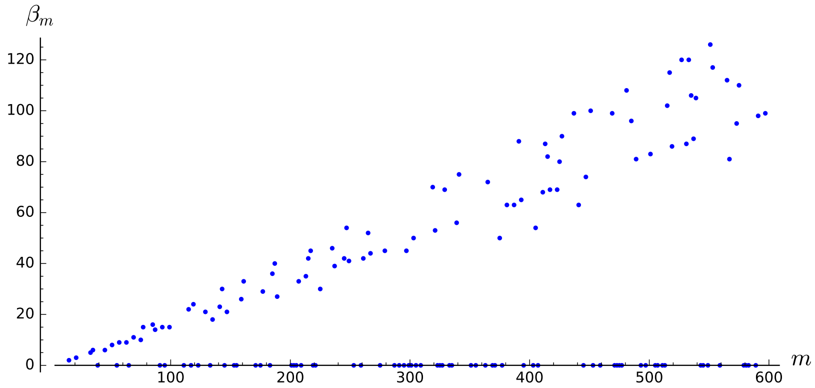


Figure: The factor β_m for $m = p^\alpha q^\beta$ with two **odd** primes p, q

Contents

Norm Bound
$m = p^\alpha$ as in [CDPR16]

Prime-power case studied by Cramer, Ducas, Peikert and Regev:

Theorem 4

If $m = p^\alpha$, then

$$||Log(b_j)^*||_2^2 \in O\left(\frac{\log^3 m}{m}\right).$$

$\rightarrow$ **sufficiently short to solve CVP**

Norm Bound
$m = p^\alpha q^\beta$

More complicated for $m = p^\alpha q^\beta$.

We derived the following result:

Theorem 5

Let (p, q) be an (α, β)-generator prime pair, and $m := p^\alpha q^\beta$. Then

$$||\boldsymbol{b}_j^*||_2^2 \leq \frac{15C}{m} + C^2 \log^2(m) \cdot \left(\frac{15\alpha\beta}{2m} + \frac{55(\alpha+\beta)}{8m} + \frac{5\beta}{12p^\alpha} + \frac{5\alpha}{12q^\beta} \right)$$

holds for some universal constant $C > 0$ (i.e., C is independent of m).

$\rightarrow$ **Sufficiently short under some conditions on α, β.**

Contents

Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

- We extended the results of [CDPR16] to cyclotomic fields $\mathbb{Q}(\zeta_m)$ of conductor $m = p^\alpha q^\beta$.
- We introduced a new notion called generator prime pairs.
- We showed how to efficiently solve the SG-PIP on quantum computers for cyclotomic fields of conductor $m = p^\alpha q^\beta$, if (p, q) is an (α, β)-GPP.
- Full version on eprint (2017/513).

Thank you!

Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 559–585. Springer, 2016.

Sanjam Garg, Craig Gentry, and Shai Halevi.
Candidate multilinear maps from ideal lattices.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–17. Springer, 2013.

Nigel P Smart and Frederik Vercauteren.
Fully homomorphic encryption with relatively small key and ciphertext sizes.
In *International Workshop on Public Key Cryptography*, pages 420–443. Springer, 2010.