Recovering short generators of principal ideals in some cyclotomic fields of pq-order

Jaroslav Šeděnka
PhD Student at Masaryk University, CZ

Work in progress with Efthymios Sofos

February 6th, 2016
AAA91 Brno

Outline

- Cyclotomic field $k = \mathbb{Q}(\zeta)$
  - Representation of ideals in $\mathcal{O}_k$
  - Log-embedding of k^*
- Lattices
  - Closest vector problem
  - Babai's rounding algorithm
- Short Generator of Principal Ideal
  - Solution for $k = \mathbb{Q}(\zeta_{p^k})$
  - Obstacles for $k = \mathbb{Q}(\zeta_{pq})$
- Preliminary results

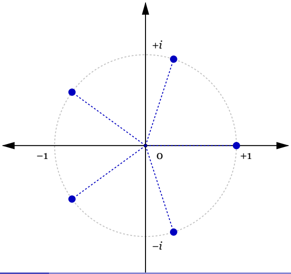
Cyclotomic field $k = \mathbb{Q}(\zeta)$

Let $\zeta_m = e^{2\pi i/m}$

$k = \mathbb{Q}(\zeta_m)$ is a cyclotomic number field of order m and degree $\varphi(m)$

$\mathcal{O}_k = \mathbb{Z}[\zeta_m]$ the ring of integers in k.

There are exactly $\varphi(m)$ different complex embeddings $\sigma_j : k \to \mathbb{C}$, defined for each $j \in \{1, \dots, m-1\}$ satisfying $(j, m) = 1$. These embeddings can be defined by setting $\sigma_j(\zeta_m) = \zeta_m^j$.



Log-embedding of $k^* = \mathbb{Q}(\zeta_m)^*$

We can set $n = \varphi(m)/2$ and define the log-embedding

$$\text{Log} : k^* \to \mathbb{R}^n$$

$$\alpha \longmapsto (\log|\sigma_{j_1}(\alpha)|, \cdots, \log|\sigma_{j_n}(\alpha)|)$$

Important remark

$\Lambda = \text{Log}(\mathcal{O}_k^\times)$ is a full-rank (n-1) lattice in $H = (1, \dots, 1)^\perp \subset \mathbb{R}^n$.

Principal ideals of $\mathcal{O}_k$ with short generators

Proposed by several lattice cryptosystems

- Homomorphic encryption Smart and Vercauteren [2010]
- Soliloquy Campbell et al. [2014]

Cryptoanalyzed later

- Soliloquy Campbell et al. [2014]
- Dan Bernstein's blog post
- Cramer et al. [2015]

Principal ideals of $\mathcal{O}_k$ with short generators

Let $g \in \mathcal{O}_k$ be a "short" element, and let $I = (g) = g\mathcal{O}_k$ be a principal ideal.
We will consider retrieving g (or other short element) from a arbitrary element h such as $I = (h)$.

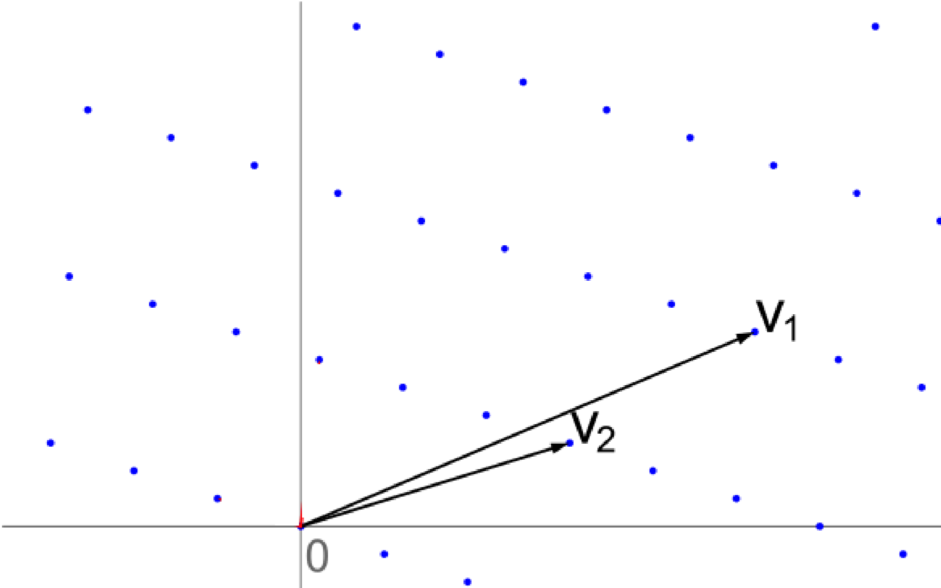
Reduction modulo Λ

We have $g = hu$ for some $u \in \mathcal{O}_k^\times$, so

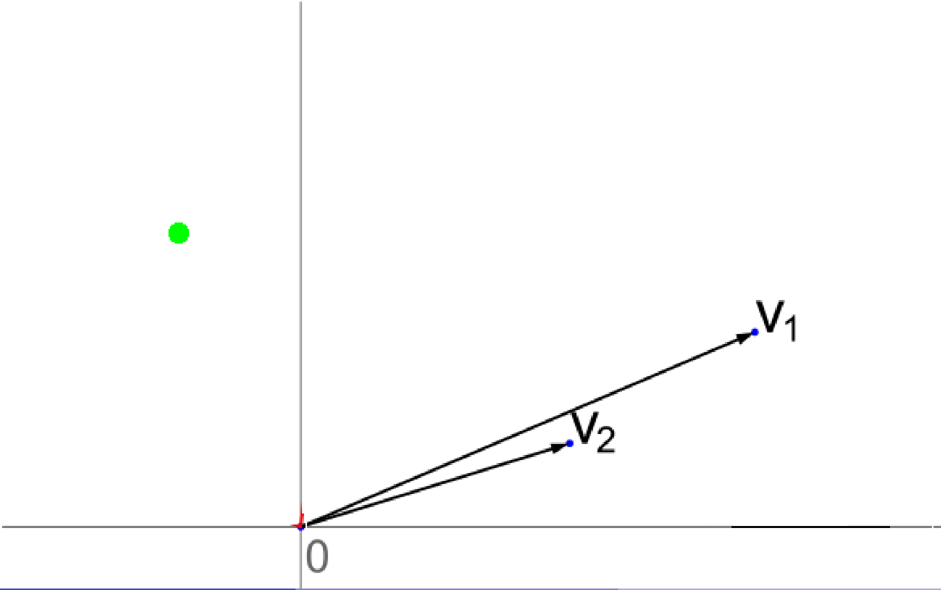
$$\mathrm{Log}(g) \in \mathrm{Log}(h) + \Lambda$$

To minimize the right side is equivalent to solving the Closest Vector Problem for $\mathrm{Log}(h)$ in Λ.

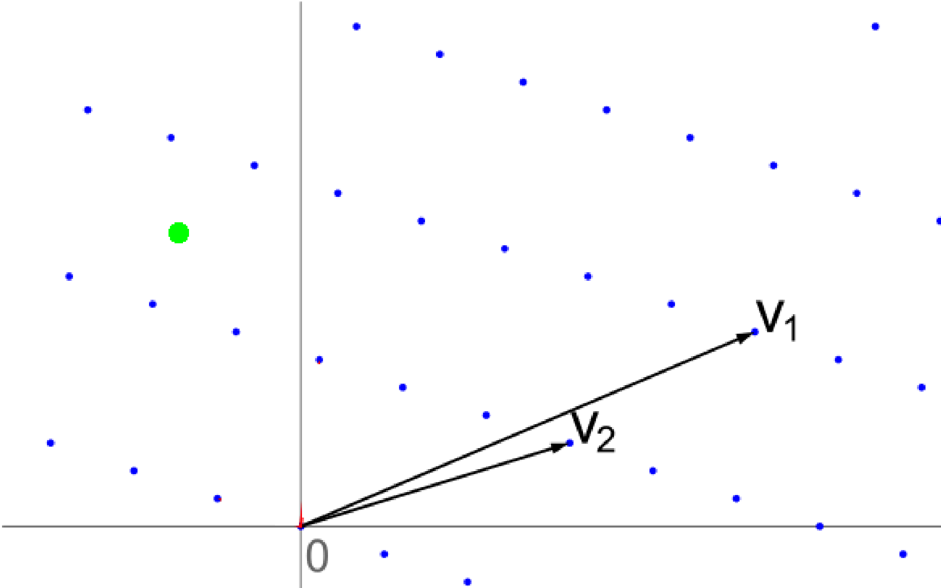
Lattice L generated by $\{v_1, v_2\}$



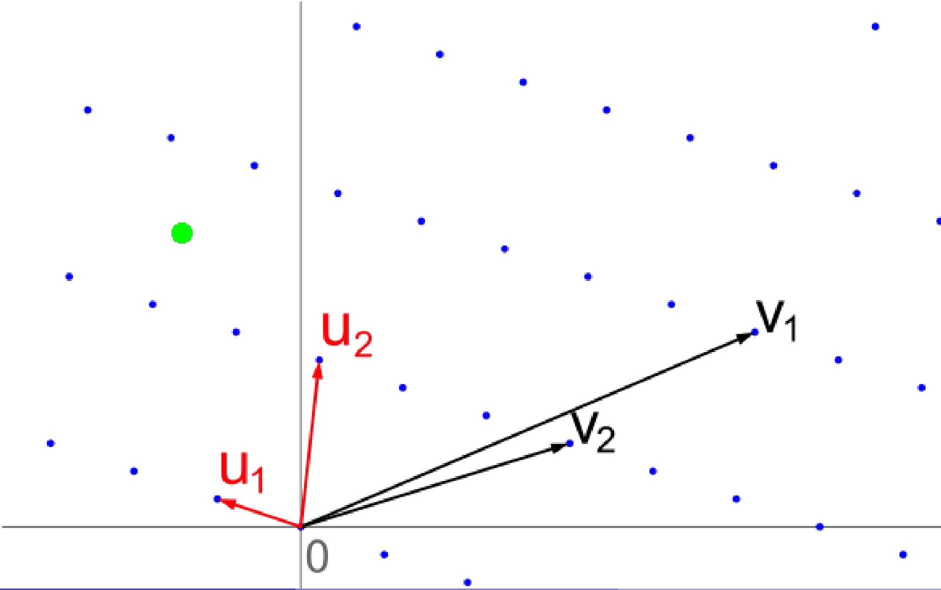
Closest vector problem (CVP)



Closest vector problem (CVP)



Solving CVP using U



Babai's rounding algorithm

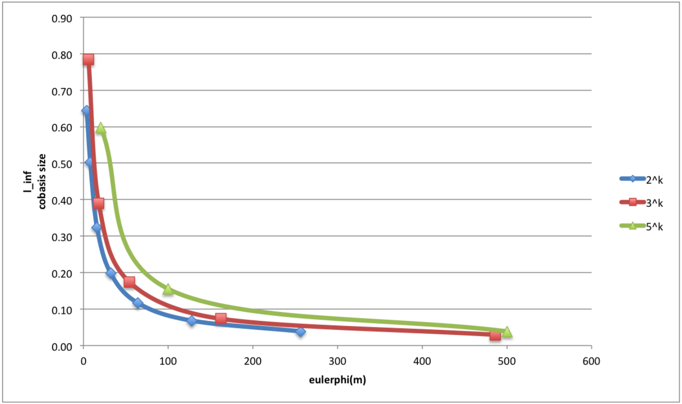
Goal: Given basis B of lattice L and a vector $v \in span(B)$, compute a vector $w \in L$ close to v

- Let $\mathbb{R}^n = span(B)$, compute the dual basis $B^\dagger = (B^{-1})^T$
- Express v in dual basis as $v^\dagger = (B^\dagger)^T a$
- Round coefficient-wise $w^\dagger = round((B^\dagger)^T a)$
- Transform $w^\dagger$ back to standard basis as $w = Bw^\dagger$

Finding short generator in $\mathbb{Q}(\zeta_{p^r})$

As has been shown in Cramer et al. [2015], the canonical basis of cyclotomic units $C \subset \mathcal{O}_k^\times$, defined as $b_i = \frac{\zeta^i - 1}{\zeta - 1}$ for $i \neq 1, (i, m) = 1$ is suitable for Babai's rounding algorithm.

All $||b_i^\dagger||$ are the same and $||b_i^\dagger||^2 = O(m^{-1} \log^3 m)$.



Generalizing the result for $k = \mathbb{Q}(\zeta_m)$

Recovering g from $\mathrm{Log}(g)$: double exponential in number of distinct primes

Babai's algorithm recovers $\mathrm{Log}(g) = \mathrm{Log}(h) + \mathrm{Log}(u)$, so we know u up to $\mathrm{Ker}\,\mathrm{Log} = \langle \zeta_m, -1 \rangle$ and $[\mathcal{O}_k^\times : C] = 2^k h^+(m)$ (showed by Sinnott [1978]). Here $k = 2^{s-2} + 1 - s$ where $s \geq 2$ is the number of distinct primes dividing m.

We need some small-index subgroup of $\mathcal{O}_k^\times$ with a nice basis. So we do not want too many distinct primes dividing m.

b_i is not a basis for units

In general, b_i for $(i, m) = 1$ do not suffice as generators for C. Adding b_{jp} and b_{lq} would help (in some sense), but these elements are not units.

Focus on $k = \mathbb{Q}(\zeta_{pq})$

$[\mathcal{O}_k^\times : C] = h^+(pq)$.

Do we have a simple basis of C?

Yes, under a technical condition: we need p, q to be mutual *semi-primitive roots*, that is, $\langle p, -1 \rangle = \mathbb{F}_q^*$ and $\langle q, -1 \rangle = \mathbb{F}_p^*$.
Then $\{z_i = \zeta_{pq}^i - 1; s.t.(i, pq) = 1\}$ is a full set of generators of C.

From now on, we will use $m = pq$ such that p, q satisfy the above condition.

Caveat!

There are $\varphi(pq)/2$ generators of $\mathrm{Log}(C)$, but $rank(\Lambda) = \varphi(pq)/2 - 1$, so we have one too many elements to get a basis.

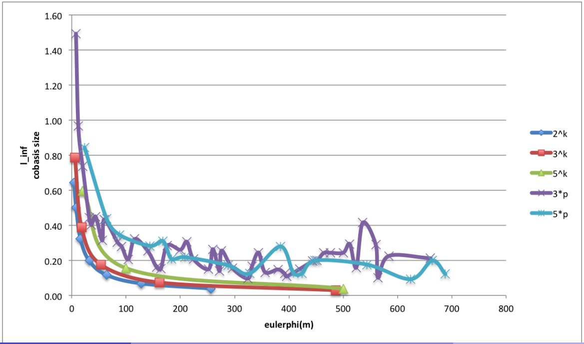
First possible solution

Set $n = \varphi(pq)/2$.

1. Lift generators to $\mathbb{R}^n$

By using $z_i' = z_i + t.(1, \ldots, 1)$ as a basis of $L \subset \mathbb{R}^n$, we can compute a dual basis and project it back to H to get a dual basis of $\mathrm{Log}(C)$.

- Prone to numerical instability (how do you pick the right t)?
- Rather unsatisfactory results

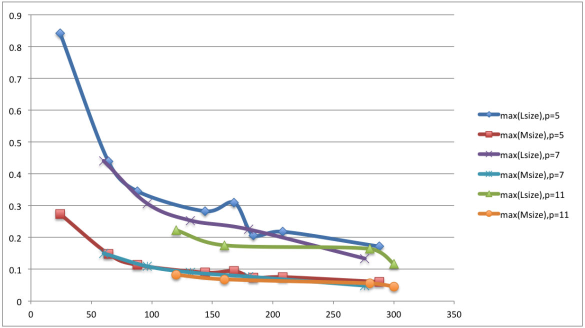


Second possibility

Sacrifice n in index

We can repeat the work of Cramer et al. [2015] and use $\mathrm{Log}(b_i) = \mathrm{Log}(z_i) - \mathrm{Log}(z_1)$ as basis of some C'.

- We get a symmetric basis
- However, $[C : C'] = n$.



Precisely and full-index

Remember, the problem was to find a lattice basis in $(1, \ldots, 1)^{\perp} = H \subset \mathbb{R}^n$ from a set of n (one too many!) generators.

There is $\mathrm{Gal}(k/Q) \cong (\mathbb{Z}/(pq\mathbb{Z}))^{\times}$-action on k, which corresponds to $(\mathbb{Z}/(pq\mathbb{Z}))^{\times}/\{\pm 1\} \cong G$-action on $\mathrm{Log}(k^*)$

$$0 \longrightarrow I_G \xrightarrow{\iota} \mathbb{R}[G] \xrightarrow{\epsilon} \mathbb{R} \longrightarrow 0$$

Decompose $R[G] \cong e\mathbb{R} \times (1-e)\mathbb{R}$ using ring idempotent $e = \frac{1}{n}\sum_{\sigma \in G} \sigma$

Thank you for your attention.

References

Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale. In *ETSI 2nd Quantum-Safe Crypto Workshop*, 2014.

Ronald Cramer, Leo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. Cryptology ePrint Archive, Report 2015/313, 2015.

Warren Sinnott. On the stickelberger ideal and the circular units of a cyclotomic field. *Annals of Mathematics*, pages 107–134, 1978.

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