IMACC 2017

December 12–14, 2017

Lattice Reductions over Euclidean Rings with Applications to Cryptanalysis

Taechan Kim and Changmin Lee

NTT Secure Platform Laboratories, Japan and Seoul National University, Korea

Backgrounds

Lattice-based cryptography

- post-quantum cryptography
- fully homomorphic encryption
- many other applications

Lattices (classical)

- M: a free $\mathbb{Z}$-module, i.e. closed under addition/multiplication by $\mathbb{Z}$
- A free $\mathbb{Z}$-module has a $\mathbb{Z}$-basis $(b_1, \ldots, b_n) \subset M^n$ s.t.

$$M = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$$

- M has "infinitely" many number of basis
- n, the size of the basis, is "invariant" under the choice of the basis.
- n: the rank (or dimension) of M, written as $n := \mathrm{rk}(M)$

Backgrounds

Lattice reduction

- Some basis of lattices are good, but some are not.
- Many lattice problems (SVP/CVP) are easier to solve, if a "good" basis is given.
- Informally, a good basis consists of "reasonably small" and "almost orthogonal" components.
- "Lattice reduction" is to find such a "good" basis from an arbitrary basis.
- LLL-algorithm is one of the most popular algorithms for lattice reduction.
- A key tool not only for lattice-based crypto, but also for various cryptanalysis (e.g. RSA attack)

LLL-algorithm

LLL-algorithm (classical)

- Given a $\mathbb{Z}$-basis of a lattice M, find an LLL-reduced basis.
- (Gram-Schmidt orthogonalization) Given a basis $(b_1, \ldots, b_n) \subset \mathbb{Q}^n$, $(b_1^*, \ldots, b_n^*) \subset \mathbb{R}^m$ is GS orthogonalization, if $b_1^* = b_1$ and

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \text{ for } \mu_{i,j} = \langle b_i, b_j^* \rangle / \langle b_j^*, b_j^* \rangle.$$

- (LLL-reduced basis) A basis $(b_1, \ldots, b_n)$ is LLL-reduced w.r.t $\delta > 0$ if

$$|\mu_{i,j}| \leq 1/2 \text{ for } 1 \leq j < i \leq n \text{ (size reduced)} ,$$

$$||b_i^*||^2 \geq (\delta - \mu_{i,i-1}^2)||b_{i-1}^*|| \text{ for } 1 < i \leq n \text{ (Lovasz conditions)}$$

Note

- LLL algorithm outputs a small vector of lattices
  - If $(b_1, \ldots, b_n)$ is LLL-reduced w.r.t. $\delta = 3/4$, then $||b_1|| \leq 2^{(n-1)/4} \det(M)^{1/n}$.
- Its running time depends on the size of the dimension, n.

Notations

Number fields

- $h \in \mathbb{Z}[t]$: an irreducible polynomial of degree n.
- $L := \mathbb{Q}[t]/h(t)$: a number field of degree n.
- $\mathbb{Z}_L$: a ring of integers of L (e.g. $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$)

Ideal lattices

- An ideal $\mathcal{I} \subset L$ is a $\mathbb{Z}_L$-submodule of L, thus trivially a $\mathbb{Z}$-module.
- $\mathcal{I}$ is free, since $\mathbb{Z}$ is a PID (Principal Ideal Domain).
- Thus, it is a $\mathbb{Z}$-lattice and called as "ideal-lattice".
- Typically, $\mathrm{rk}(\mathcal{I}) = n = [L : \mathbb{Q}]$.

Motivations

In cryptography,

- L typically has a proper subfield $K \neq \mathbb{Q}$.
- E.g. ℓ-th cyclotomic field $L = \mathbb{Q}[t]/(t^\ell + 1)$ has a subfield $K = \mathbb{Q}[t]/(t^k + 1)$, where $\ell = 2^l$ for some $l > 0$ and $k \mid \ell$.

Ideal lattice as a $\mathbb{Z}_K$-module

- An ideal $\mathcal{I} \subset L$ is also a $\mathbb{Z}_K$-module for a subfield $K \subset L$.
- If $\mathbb{Z}_K$ is a PID, then $\mathcal{I}$ is a free $\mathbb{Z}_K$-module ($\mathbb{Z}_K$-lattice), thus

$$\mathcal{I} = \mathbb{Z}_K\beta_1 \oplus \cdots \oplus \mathbb{Z}_K\beta_d$$

for a basis $(\beta_1, \ldots, \beta_d) \in L^d$ and $d = [L : K]$.

Matrices of Lattices

- We consider a $\mathbb{Z}_K$-lattice as a $d \times d$ matrix $M_\mathcal{I} = [\beta_1 | \ldots | \beta_d] \in K^{d\times d}$, instead of $[b_1 | \ldots | b_n] \in \mathbb{Q}^{n\times n}$, where $n = [L : \mathbb{Q}]$ and $d = [L : K]$.

Our goal

Motivation

- If a $\mathbb{Z}$-lattice $M \subset L$ can also be considered as a free $\mathbb{Z}_K$-module, $rk_{\mathbb{Z}_K}(M) = [L : K] = d$ is smaller than $rk_{\mathbb{Z}}(M) = [L : \mathbb{Q}] = n$.
- Smaller dimension, faster LLL-algorithm?

LLL algorithm over $\mathbb{Z}_K$

- We restrict our concern to "norm-Euclidean domain" $\mathbb{Z}_K$ (that is, Euclidean domain w.r.t. algebraic norm $N_{K/\mathbb{Q}}$).
- We propose two heuristic LLL algorithms running over $\mathbb{Z}_K$-lattices.

Technical hurdles

- For "GS orthogonalization", one needs to define "inner product" over $K^d \times K^d$.
- What would be analogous notions for "size reduced" and "Lovasz conditions"?

Related works

Related works

- (Napias '96) over Gaussian integers, more generally, quadratic norm-Euclidean domain
  - use "Hermitian product";
  - Euclidean norm (induced by Hermitian product) and algebraic norm coincides, i.e. $N_{K/\mathbb{Q}}(a + b\iota) = a^2 + b^2 = ||(a, b)||^2$.
- (Fieker-Phost '96) over arbitrary Dedekind domain, using pseudo-basis
  - inner product induced by Hermitian product;
  - in a size-reduction step, given $a \in K$, tried to find $q \in \mathbb{Z}_K$ s.t. $Tr_{K/\mathbb{Q}}((a - q)\overline{(a - q)})$ is minimal (in general, not easy to do so).
- (Gan-Ling-Mow '09) over complex fields
  - basically the same as Napias's;
  - does not consider the number field structures.
- (Fieker-Stehlé '10) over arbitrary Dedekind domain, using pseudo-basis
  - convert $\mathbb{Z}_K$-lattice into $\mathbb{Z}$-lattice of a higher dimension;
  - LLL-algorithm is carried over $\mathbb{Z}$-lattice.

Mathematical Background

Euclidean domain

- A ring R is Euclidean if $\exists \phi : R \to \mathbb{N}$ s.t. $\phi(a) \leq \phi(ab)$ for $0 \neq a, b \in R$ and there exists q and $r \in R$ s.t.

$$a = bq + r \text{ with } r = 0 \text{ or } \phi(r) < \phi(b).$$

- E.g. $\mathbb{Z}$ with $\phi(a) = |a|$ and division algorithm

Norm-Euclidean domain

- If $\mathbb{Z}_K$ in K is Euclidean w.r.t. $\phi(a) = |N_{K/\mathbb{Q}}(a)|$, then $\mathbb{Z}_K$ is called norm-Euclidean.
- (Example 1.) $\mathbb{Z}_K$ for $K = \mathbb{Q}(\zeta_k)$, the k-th cyclotomic field, is norm-Euclidean iff

$$k \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 16, 20, 24\}^a$$

- (Example 2.) $\mathbb{Z}_K$ for $K = \mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta})$ is norm-Euclidean iff

$$\begin{aligned} &\alpha = 1, \quad \beta = 2, 3, 5, 7; \\ &\alpha = 2, \quad \beta = -3, 5; \\ &\alpha = 3, \quad \beta = 2, 5, -7, -11, 17, -19; \\ &\alpha = 7, \quad \beta = 5.^b \end{aligned}$$

[a] [Lenstra '75, Masley '75, Ojala '79]

[b] [Lemmermeyer '11]

Mathematical Background

Euclidean minimum

- "norm-Euclideanity" leads us to consider Euclidean minimum of K, $\mathfrak{M}(K)$.
- For any $\xi \in K$, $\exists q \in \mathbb{Z}_K$ s.t. $|N_{K/\mathbb{Q}}(\xi - q)| < \mathfrak{M}(K) < 1$.
- E.g. $\mathfrak{M}(\mathbb{Q}) = 1/2$

Euclidean minimum of $K = \mathbb{Q}(\zeta_k)$

k	1	3	4	5	7	8	9	12	15	16	20	24
$\mathfrak{M}(\mathbb{Q}(\zeta_k))$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{2}$	$\frac{1}{5}$	$\frac{1}{4}$

Table: Euclidean minimum of k-th cyclotomic fields [Lezowski '14]

Euclidean minimum of $K = \mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta})$

(α, β)	(1,2)	(1,3)	(1,5)	(1,7)	(2,-3)	(2,5)	(3,2)
$\mathfrak{M}(\mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta}))$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{5}{16}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{11}{16}$	$\geq \frac{1}{4}$
(α, β)	(3,5)	(3,-7)	(3,-11)	(3,17)	(3,-19)	(7,5)	
$\mathfrak{M}(\mathbb{Q}(\sqrt{-\alpha}, \sqrt{\beta}))$	$\frac{1}{4}$	$\frac{4}{9}$	≤ 0.46	$\frac{13}{16}$	< 0.95	$\frac{9}{16}$	

Table: Euclidean minimum of biquadratic fields [Lemmermeyer '11]

Size reduction over norm-Euclidean ring

Size reduction (classical)

- Size reduction is actually the same as "for any given $\mu \in \mathbb{Q}$, find $q \in \mathbb{Z}$ s.t. $|\mu - q| < 1/2$".
- This can be done by a simple rounding, i.e. $q = \lfloor \mu \rceil$.
- Note that $\mathfrak{M}(\mathbb{Q}) = 1/2$ and $|\cdot|$ is the Euclidean function for $\mathbb{Z}$.
- Recall, in size reduction step, b_i is set to be $b_i - q_j b_j$, where $q_j = \lfloor \mu_{i,j} \rceil$ for $\mu_{i,j} \in \mathbb{Q}$.

Rounding function in norm-Euclidean ring

- For size reduction in K, we need an algorithm, for any $\xi \in K$, to find $q \in \mathbb{Z}_K$ s.t. $|N_{K/\mathbb{Q}}(\xi - q)| \leq \mathfrak{M}(K)$
- (Rounding function) For $a \in K$, we write $a = \sum_{i=0}^{n-1} a_i \zeta^i$ where $a_i \in \mathbb{Q}$. Define

$$\lfloor a \rceil := \sum_i \lfloor a_i \rceil \zeta^i.$$

- However, $|N_{K/\mathbb{Q}}(a - \lfloor a \rceil)| < \mathfrak{M}(K)$ does not hold in general.

Rounding algorithm for norm-Euclidean ring

Algorithm 1 Rounding algorithm for norm-Euclidean rings

Input A norm-Euclidean number field K, its Euclidean minimum $\mathfrak{M}(K)$, the unit group $K^\times$ of K, and an element $a \in K$

Output $q \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(a - q) \leq \mathfrak{M}(K)$

1: Compute $r := a - \lfloor a \rceil$
2: **if** $N_{K/\mathbb{Q}}(r) \leq \mathfrak{M}(K)$ **then**
3: **return** $q := \lfloor a \rceil$
4: **else**
5: **repeat**
6: $u \leftarrow_\$ K^\times$
7: **until** $N_{K/\mathbb{Q}}(ur - \lfloor ur \rceil) \leq \mathfrak{M}(K)$
8: **end if**
9: **return** $q := \lfloor a \rceil + u^{-1} \lfloor ur \rceil$

Notes

Notes on the rounding algorithm

- The algorithm may not terminate, but it is unlikely to happen.
- In our experiments, the unit u is chosen from a power of a fundamental unit, e.g. $u \leftarrow v^i$ for a fundamental unit v.
- In the case of $K = \mathbb{Q}(\zeta_{16})$,
  - For 97% of 200,000 uniformly chosen random elements, it suffices to run the simple rounding (i.e. $q = \lfloor a \rceil$ is the desired output).
  - For the rests, it was enough to work with only a few units of the form v^i for $1 \leq i \leq 3$, where $v = (\zeta_{16}^6 + \zeta_{16}^4 + \zeta_{16}^2)$ is a fundamental unit.

LLL-algorithm over norm-Euclidean rings

Hermitian product

- Define a blinear map $H : K^d \times K^d \to K$ by

$$(\mathbf{v}, \mathbf{w}) \mapsto \sum_{i=1}^{d} v_i \overline{w}_i,$$

  where $\bar{\cdot}$ denotes the complex conjugation.
- GS-orthogonalization is analogously defined w.r.t. H.

LLL-reduced condition

- A basis $(\beta_1, \ldots, \beta_d) \subset K^d$ is called $\mathbb{Z}_K$-LLL-reduced w.r.t $\delta > 0$ if
  - $N_{K/\mathbb{Q}}(\mu_{i,j}) \leq \mathfrak{M}(K)$ for $1 \leq j < i \leq n$ (size reduced)
  - $N_{K/\mathbb{Q}}\big(B_i + \mu_{i,i-1}\overline{\mu_{i,i-1}} B_{i-1}\big) \geq \delta \cdot N_{K/\mathbb{Q}}(B_{i-1})$ for $1 < i \leq n$ (Lovasz condition), where $B_i = H(\beta_i^*, \beta_i^*)$.

Cautions

- Unlike the classical case, the Lovasz condition cannot be replaced with $N_{K/\mathbb{Q}}(B_i) \geq \big(\delta - \mu_{i,i-1}\overline{\mu_{i,i-1}}\big) \cdot N_{K/\mathbb{Q}}(B_{i-1})$.
- This is because the triangle inequality does not hold w.r.t. $N_{K/\mathbb{Q}}$.

LLL-algorithm over norm-Euclidean rings

Input a basis $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\} \subset K^d$, $\mathfrak{M}(K)$, the unit group $K^\times$, and $\delta > 0$.
Output LLL-reduced basis $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$.

Compute the Gram-Schmidt basis $\{\mathbf{b}_1^*, \cdots, \mathbf{b}_d^*\}$ with respect to the bilinear map $H(\cdot, \cdot)$
Compute the coefficients $\mu_{i,j} = H(\mathbf{b}_i, \mathbf{b}_j^*)/H(\mathbf{b}_j^*, \mathbf{b}_j^*)$ for $1 \leq j < i \leq d$ and $B_i = H(\mathbf{b}_i^*, \mathbf{b}_i^*)$ for $1 \leq i \leq d$.
Set $k = 2$
while $k \leq d$ **do**
    for $j = k - 1$ **to** 1 **do**
        Compute $q_j \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(\mu_{k,j} - q_j) \leq \mathfrak{M}(K)$ using Algorithm 1
        Set $\mathbf{b}_k = \mathbf{b}_k - q_j \cdot \mathbf{b}_j$
        Update $\mu_{k,j} = H(\mathbf{b}_k, \mathbf{b}_j^*)/H(\mathbf{b}_j^*, \mathbf{b}_j^*)$ and B_k for $1 \leq j \leq k$
    end for
    if $N_{K/\mathbb{Q}}\big(B_k + \mu_{k,k-1}\overline{\mu_{k,k-1}}B_{k-1}\big) \geq \delta \cdot N_{K/\mathbb{Q}}(B_{k-1})$ **then**
        $k = k + 1$
    else
        Swap $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$
        Update $\mathbf{b}_k^*, \mathbf{b}_{k-1}^*, B_k, B_{k-1}$, and $\mu_{i,j}$ for $1 \leq i, j \leq s$
        $k = \min\{2, k - 1\}$
    end if
end while

Experimental Results

Lattices

- The lattice $\mathcal{L}$ is generated by rows of the matrix in $K^{d\times d}$,

$$\begin{pmatrix} q & 0 & \cdots & \cdots & 0 \\ \gamma_1 & 1 & \cdots & \cdots & 0 \\ \gamma_2 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_{d-1} & 0 & \cdots & \cdots & 1 \end{pmatrix},$$

  where q and $\gamma_i \in \mathbb{Z}_K$.
- This shape of the lattice basis appears in several cryptanalysis.

Parameter choices

- We carried out the reduction of lattices over $K = \mathbb{Q}(\zeta_k)$ for $k = 5, 8, 16$ of dimension $10 \leq d \leq 50$.
- If the lattices are considered as $\mathbb{Z}$-lattices, the dimension 50 over $\mathbb{Z}_K$ corresponds to the dimension 200 over $\mathbb{Z}$ when $k = 5$ or 8, or 400 when $k = 16$.
- $\delta = 3/4$

Experimental Results

Output quality

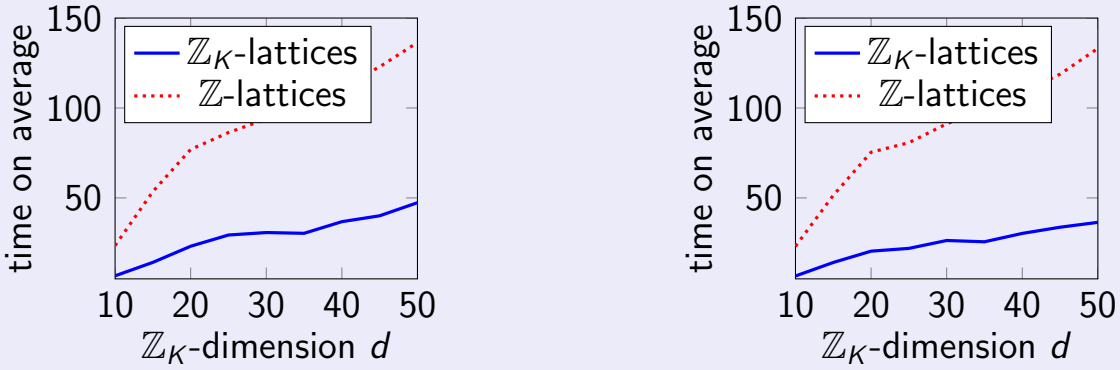
- Theoretically, we have no guarantee on the output quality.
- In biquadratic case, it is possible to guarantee output quality using a different type of inner product, but its practical performance is worse than general case that uses Hermitian product (see our paper).
- Let $n = d \cdot [K : \mathbb{Q}]$, a dimension of $\mathcal{L}$ over $\mathbb{Z}$
- For $\mathbf{v} := (v_1, \ldots, v_d) \in K^d$, define $||\mathbf{v}||_\infty = \max_i ||v_i||_\infty$.
- As a measure of output quality, we use

$$C := \frac{||\mathbf{b}_1||_\infty}{N_{K/\mathbb{Q}}(\det(\mathcal{L}))^{1/n}},$$

  where the volume of $\mathcal{L}$ over $\mathbb{Z}$ is the same as $N_{K/\mathbb{Q}}(\det(\mathcal{L})) = N_{K/\mathbb{Q}}(q)$.
- The classical Hermite factor is defined with $||\cdot||_2$ norm.
- Heuristically, we observe that $C \approx 1.02^n$.
- Taking $||\mathbf{v}||_2 \leq \sqrt{n}||\mathbf{v}||_\infty$ into account, the Hermite constant of our reduction is $\lesssim 1.02 n^{1/2n}$.
- As n grows, Hermite constant becomes close to the average Hermite factor 1.02.

Experimental Results

Timing results



(a) $\mathbb{Z}_K = \mathbb{Z}[\zeta_5]$

(b) $\mathbb{Z}_K = \mathbb{Z}[\zeta_8]$

Figure: Time comparison of running time

Note

- Our $\mathbb{Z}_K$-lattice reduction is about 3 times faster than the classical reduction done over $\mathbb{Z}$.
- We did not attempt to compare our naive implementation with already well-optimized LLL implementation.
- For the consistency of the comparison, we used our own implementation for both $\mathbb{Z}$ and $\mathbb{Z}_K$-reduction (see our SAGE codes in Appendix).

Applications

Sieving in exTNFS (by K.-Barbulescu)

- exTNFS is a best known algorithm to solve the DLP over $\mathbb{F}_{p^n}$ (n: composite, p: not small).
- In a step called special-q method in exTNFS method, we need to consider: find a small basis of the lattice

$$M_{\mathfrak{Q}} := \left\{ (a_0, \ldots, a_{\tau-1}) \in \mathbb{Z}[\iota]^{\tau} : \left(\sum_{i=0}^{\tau-1} a_i \alpha_f \right) \equiv 0 \mod \mathfrak{Q} \right\},$$

  where $\mathfrak{Q}$ is a prime ideal in $\mathbb{Z}_L$ for $L = K[\alpha] = K[x]/f(x)$ and $K = \mathbb{Q}[\iota] = \mathbb{Q}[t]/h(t)$.
- $M_{\mathfrak{Q}}$ is the τ-dimensional $\mathbb{Z}_K$-lattice.
- A classical approach is to consider the lattice as $\mathbb{Z}$-lattice.

Parameters for BN curves

- Set $h(t) = \Phi_5(t) = t^4 + t^3 + t^2 + t + 1$ so that $K = \mathbb{Q}(\zeta_5)$ and $\mathbb{Z}_K = \mathbb{Z}[\zeta_5]$.
- Set $f(x) = x^3 - x^2 - u$, where $p = P(u)$ and $P(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ and $u = 2^{158} - 2^{128} - 2^{68} + 1$
- Set $L = K[x]/f(x)$.

Special-$\mathfrak{q}$ in BN curve parameters

Example (cont.)

- Take a prime ideal $\mathfrak{Q} = \langle \mathfrak{q}, \alpha_f - \gamma \rangle \subset L$ and $\tau = 2$.
- where,

$$\mathfrak{q} = (q) = \big(-461479\zeta_5^3 - 383970\zeta_5^2 - 265505\zeta_5 - 303923 \big);$$

$$\gamma = 169465786435052577 63313.$$

- Then $M_{\mathfrak{Q}} = \begin{pmatrix} q & 0 \\ -\gamma & 1 \end{pmatrix}$.
- We obtained

$$\mathrm{LLL}\,(M_{\mathfrak{Q}}) = \begin{pmatrix} 532\zeta_5^3 + 850\zeta_5^2 + 179\zeta_5 - 464 & 224\zeta_5^3 + 132\zeta_5^2 - 13\zeta_5 + 367 \\ -649\zeta_5^3 + 186\zeta_5^2 + 661\zeta_5 + 73 & 11\zeta_5^3 - 264\zeta_5^2 + 35\zeta_5 - 71 \end{pmatrix}.$$

- Note that $\log_2(850) \approx 9.73$ and $\log_2\left(N_{K/\mathbb{Q}}(q)^{\frac{1}{\tau m}}\right) \approx 9.29$.

Future works

Open questions

- Apply to cryptanalysis of lattice-based cryptography
- BKZ, lattice enumeration over Euclidean ring?
- Prove the output quality

Thanks for your attention!