Lattice Reduction for Modular Knapsack

Thomas Plantard
Willy Susilo
Zhenfei Zhang

Centre for Computer and Information Security Research
Universiy of Wollongong

http://www.uow.edu.au/~thomaspl
thomaspl@uow.edu.au

Outline

Cryptography concerned by Lattice Reduction

Problem

- Shortest Vector Problem (SVP): Ajtai-Dwork, Regev, ...
- Closet Vector Problem (CVP): GGH, NTRU, ...
- Knapsack Problem
- Coding based cryptosystem
- RSA, Factorization.
- Short Integer Solution (SIS): SWIFFT, SWIFFTX, ...
- Learning With Error (LWE).
- Approximate-GCD Problem.

Lattice Reduction: Heuristic BUT successful

- Weeks, Month of Computation: Good Estimation.
- 2^{80}, 2^{100}: Unknown.

The 2010 FHE Gentry-Halevi implementation

Challenge

- Find a short vector in a modular knapsack type lattice.
- Dimension, $d = 2048$
- Length of digits, $\beta = 720,000$.

Security based on impossibility to run LLL

- Perform a LLL reduction is enough to break challenge.
- However, $d^3\beta^2 = (2^{11})^3(2^{19.5})^2 = 2^{72}$.

Lattice Theory

Lattice

Definition of a Lattice

- All the integral combinations of $d \leq n$ linearly independent vectors over $\mathbb{R}$

$$\mathcal{L} = \mathbb{Z}\,\mathbf{b}_1 + \cdots + \mathbb{Z}\,\mathbf{b}_d = \{\lambda_1 \mathbf{b}_1 + \cdots + \lambda_d \mathbf{b}_d \;:\; \lambda_i \in \mathbb{Z}\}$$

- d dimension.
- $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a *basis*.

An Example

$$\mathbf{B} = \begin{pmatrix} 5 & \frac{1}{2} & \sqrt{3} \\ \frac{3}{5} & \sqrt{2} & 1 \end{pmatrix}$$

$d = 2 \leq n = 3$

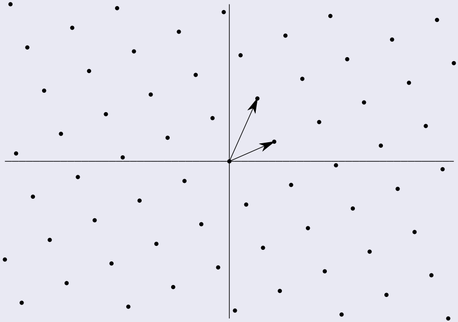
In this work, integer Basis: $B \in \mathbb{Z}^{d,n}$.

Example

A lattice $\mathcal{L}$

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix}$$

An infinity of basis

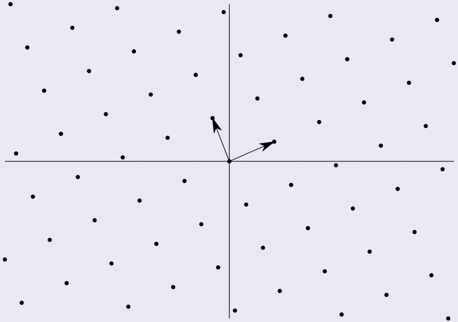


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix}$$

An infinity of basis

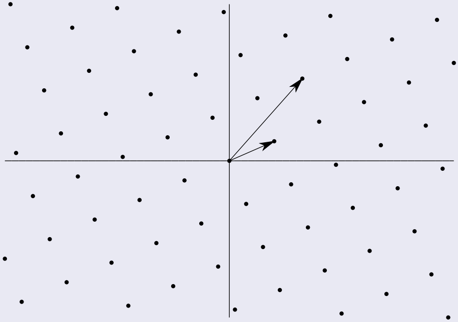


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ 13 & 21 \end{pmatrix}$$

An infinity of basis

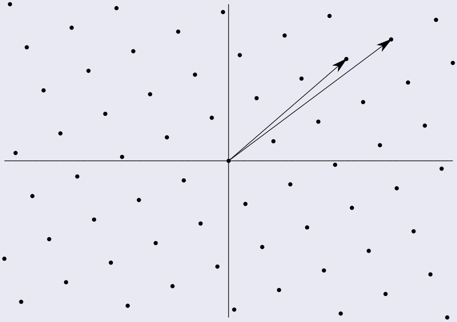


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 29 & 31 \\ 21 & 26 \end{pmatrix}$$

An infinity of basis

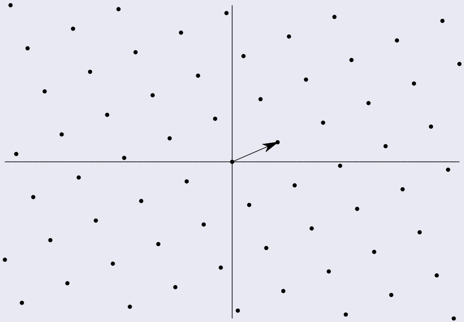


Example

The Shortest Vector and The First Minima

$$\mathbf{v} = \begin{pmatrix} 8 & 5 \end{pmatrix}, \text{ with } \lambda_1 = \sqrt{8^2 + 5^2} = 9.434$$

The Shortest Vector

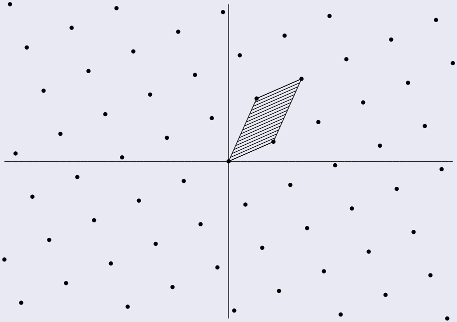


Example

The Determinant

$$\det \mathcal{L} = \sqrt{\det\left(\mathbf{B}\mathbf{B}^T\right)} = 103$$

The Determinant



Lattice Reduction Algorithm

Find $v \in \mathcal{L}$ smallest

- SVP is NP-Hard under randomized reduction.
- Deterministic $O(d^{\frac{d}{2e}})$: Kannan 1986, Hanrot and Sthele 2007.
- Probabilistic $O(2^d)$: AKS 2001.

Find $v \in \mathcal{L}$ small

- LLL: Lenstra, Lenstra and Lovasz (Poly in d).
- $DEEP_k$: LLL with Deep Insertion (Exponential in k, Poly in d).
- BKZ_k: Block Korkine Zolotaref (Exponential in k, Poly in d).
- ...

LLL

LLL

- Input: a matrix $A \in [-2^{\beta}, 2^{\beta}]^{d,n}$.
- Output: a matrix $B \in \mathbb{Z}^{d,n}$ with $\|b_i\| \sim 2^{\frac{d}{2}} det^{\frac{1}{d}}$
- Shortest Basis: $\|b_i\| \sim \sqrt{\frac{d}{2\pi e}} det^{\frac{1}{d}}$

Comparison of time complexity

Algorithms	Time Complexity
LLL	$O(d^{5+\varepsilon}\beta^{2+\varepsilon})$
L^2	$O(d^{4+\varepsilon}\beta^2 + d^{5+\varepsilon}\beta)$
L^1	$O(d^{4+\varepsilon}\beta^{1+\varepsilon} + d^{5+\varepsilon}\beta)$

LLL for Modular Knapsack Lattice

Modular Knapsack Basis

A modular knapsack basis

$$\mathbf{A} = \begin{pmatrix} A_0 & 0 & 0 & 0 & 0 \\ A_1 & 1 & 0 & 0 & 0 \\ A_2 & 0 & 1 & 0 & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ A_{d-1} & 0 & 0 & 0 & 1 \end{pmatrix} \text{ with } |A_i| < 2^\beta.$$

A classic format

- Natural format of lattice attack on knapsack problem.
- Use as public key as most of lattice based cryptosystem.
- Easy to compute from a random basis, using Hermite Normal Form.

LLL for modular knapsack lattice

Comparison of time complexity

Algorithms	Time Complexity
LLL for knapsack	$O(d^{4+\varepsilon}\beta^{2+\varepsilon})$
L^2 for knapsack	$O(d^{3+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$
L^1	$O(d^{4+\varepsilon}\beta^{1+\varepsilon} + d^{5+\varepsilon}\beta)$

Why faster than random basis: an intuition

- To reduce $i+1$ vectors, LLL requires the first i vectors to be reduced.
- For modular knapsack basis, each i first vectors are a triangular matrix.

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} 86670401 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 38009011 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
86670401 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
38009011 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} -3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\ -14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$
\left(\begin{array}{ccccccccc}
-24 & 153 & -215 & 0 & 0 & 0 & 0 & 0 \\
183 & 242 & 76 & 0 & 0 & 0 & 0 & 0 \\
-920 & 440 & 343 & 0 & 0 & 0 & 0 & 0 \\
\hline
38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc} -24 & 153 & -215 & 0 & 0 & 0 & 0 & 0 \\ 183 & 242 & 76 & 0 & 0 & 0 & 0 & 0 \\ -920 & 440 & 343 & 0 & 0 & 0 & 0 & 0 \\ 38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} 8 & -27 & -66 & 42 & 0 & 0 & 0 & 0 \\ -40 & -45 & -47 & -38 & 0 & 0 & 0 & 0 \\ 0 & 126 & -18 & -23 & 0 & 0 & 0 & 0 \\ 103 & 26 & 0 & -53 & 0 & 0 & 0 & 0 \\ \hline 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
8 & -27 & -66 & 42 & 0 & 0 & 0 & 0 \\
-40 & -45 & -47 & -38 & 0 & 0 & 0 & 0 \\
0 & 126 & -18 & -23 & 0 & 0 & 0 & 0 \\
103 & 26 & 0 & -53 & 0 & 0 & 0 & 0 \\
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
-17 & -31 & -5 & 6 & 1 & 0 & 0 & 0 \\
24 & -20 & -6 & 4 & 7 & 0 & 0 & 0 \\
-3 & -7 & -45 & 3 & 17 & 0 & 0 & 0 \\
8 & 4 & -13 & -14 & -36 & 0 & 0 & 0 \\
13 & 0 & 15 & -35 & 24 & 0 & 0 & 0 \\
\hline
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} -17 & -31 & -5 & 6 & 1 & 0 & 0 & 0 \\ 24 & -20 & -6 & 4 & 7 & 0 & 0 & 0 \\ -3 & -7 & -45 & 3 & 17 & 0 & 0 & 0 \\ 8 & 4 & -13 & -14 & -36 & 0 & 0 & 0 \\ 13 & 0 & 15 & -35 & 24 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
-7 & -6 & -14 & 11 & 4 & -7 & 0 & 0 \\
-14 & -9 & -3 & -1 & -15 & -6 & 0 & 0 \\
-2 & 15 & 14 & 10 & -6 & 4 & 0 & 0 \\
8 & -14 & 5 & 13 & -14 & -2 & 0 & 0 \\
-5 & 11 & -6 & -10 & -12 & 12 & 0 & 0 \\
4 & -16 & 12 & -4 & 12 & 13 & 0 & 0 \\
\hline
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
-7 & -6 & -14 & 11 & 4 & -7 & 0 & 0 \\
-14 & -9 & -3 & -1 & -15 & -6 & 0 & 0 \\
-2 & 15 & 14 & 10 & -6 & 4 & 0 & 0 \\
8 & -14 & 5 & 13 & -14 & -2 & 0 & 0 \\
-5 & 11 & -6 & -10 & -12 & 12 & 0 & 0 \\
4 & -16 & 12 & -4 & 12 & 13 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\hline
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\left(\begin{array}{cccccccc}
5 & -4 & -8 & 0 & 1 & 10 & -1 & 0 \\
9 & -1 & 4 & -6 & -7 & -8 & 2 & 0 \\
1 & -4 & 0 & 6 & -12 & -1 & 4 & 0 \\
4 & 8 & -4 & 9 & 4 & 0 & -3 & 0 \\
3 & -2 & -11 & -4 & -5 & -3 & -6 & 0 \\
4 & -9 & -7 & 9 & 3 & -2 & 7 & 0 \\
7 & -10 & 5 & 7 & -2 & -1 & -4 & 0 \\
\hline
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} 5 & -4 & -8 & 0 & 1 & 10 & -1 & 0 \\ 9 & -1 & 4 & -6 & -7 & -8 & 2 & 0 \\ 1 & -4 & 0 & 6 & -12 & -1 & 4 & 0 \\ 4 & 8 & -4 & 9 & 4 & 0 & -3 & 0 \\ 3 & -2 & -11 & -4 & -5 & -3 & -6 & 0 \\ 4 & -9 & -7 & 9 & 3 & -2 & 7 & 0 \\ 7 & -10 & 5 & 7 & -2 & -1 & -4 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of LLL reduction for Modular Knapsack

$$\begin{pmatrix} -2 & 6 & -1 & -8 & 0 & 1 & -3 & 1 \\ 2 & -3 & -8 & 1 & 3 & -1 & 4 & 1 \\ 3 & -3 & 6 & 2 & -6 & 2 & 4 & 3 \\ -2 & -1 & -6 & 4 & -6 & -3 & 0 & -3 \\ 5 & -4 & 4 & -1 & -2 & 0 & -7 & 1 \\ 4 & 2 & 3 & -1 & -4 & 1 & -1 & -7 \\ -2 & 3 & -4 & 0 & 0 & 11 & 2 & -2 \\ 5 & 11 & 1 & 3 & -2 & 3 & -2 & 4 \end{pmatrix}$$

A Recursive LLL

Example Recursive LLL

$$\begin{pmatrix} 86670401 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 38009011 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example Recursive LLL

$$\begin{pmatrix} 86670401 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 38009011 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
10117311 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
38269415 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
\hline
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example Recursive LLL

$$
\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
\hline
45874978 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
33538152 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
\hline
1348 & 0 & 0 & 0 & 2830 & -3871 & 0 & 0 \\
10894 & 0 & 0 & 0 & -2009 & 2748 & 0 & 0 \\
\hline
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
1348 & 0 & 0 & 0 & 2830 & -3871 & 0 & 0 \\
10894 & 0 & 0 & 0 & -2009 & 2748 & 0 & 0 \\
\hline
61611560 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
66174289 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example Recursive LLL

$$
\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
1348 & 0 & 0 & 0 & 2830 & -3871 & 0 & 0 \\
10894 & 0 & 0 & 0 & -2009 & 2748 & 0 & 0 \\
\hline
3 & 0 & 0 & 0 & 0 & 0 & 2248 & -2093 \\
29437 & 0 & 0 & 0 & 0 & 0 & 29 & -27
\end{array}\right)
$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
-3227 & -3165 & 0 & 0 & 0 & 0 & 0 & 0 \\
-14111 & 13018 & 0 & 0 & 0 & 0 & 0 & 0 \\
1391 & 0 & 4036 & -1067 & 0 & 0 & 0 & 0 \\
-8121 & 0 & 3949 & -1044 & 0 & 0 & 0 & 0 \\
\hline
1348 & 0 & 0 & 0 & 2830 & -3871 & 0 & 0 \\
10894 & 0 & 0 & 0 & -2009 & 2748 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 2248 & -2093 \\
29437 & 0 & 0 & 0 & 0 & 0 & 29 & -27
\end{array}\right)$$

Example Recursive LLL

$$\left(\begin{array}{cccccccc}
8 & -27 & -66 & 42 & 0 & 0 & 0 & 0 \\
-40 & -45 & -47 & -38 & 0 & 0 & 0 & 0 \\
0 & 126 & -18 & -23 & 0 & 0 & 0 & 0 \\
103 & 26 & 0 & -53 & 0 & 0 & 0 & 0 \\
\hline
1348 & 0 & 0 & 0 & 2830 & -3871 & 0 & 0 \\
10894 & 0 & 0 & 0 & -2009 & 2748 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 2248 & -2093 \\
29437 & 0 & 0 & 0 & 0 & 0 & 29 & -27
\end{array}\right)$$

Example Recursive LLL

$$
\left(\begin{array}{cccccccc}
8 & -27 & -66 & 42 & 0 & 0 & 0 & 0 \\
-40 & -45 & -47 & -38 & 0 & 0 & 0 & 0 \\
0 & 126 & -18 & -23 & 0 & 0 & 0 & 0 \\
103 & 26 & 0 & -53 & 0 & 0 & 0 & 0 \\
\hline
-22 & 0 & 0 & 0 & -7 & -19 & -36 & 48 \\
93 & 0 & 0 & 0 & -25 & -2 & -5 & 23 \\
-32 & 0 & 0 & 0 & -97 & 13 & 63 & 2 \\
1 & 0 & 0 & 0 & -25 & -111 & 93 & -13
\end{array}\right)
$$

Example Recursive LLL

$$\begin{pmatrix} 8 & -27 & -66 & 42 & 0 & 0 & 0 & 0 \\ -40 & -45 & -47 & -38 & 0 & 0 & 0 & 0 \\ 0 & 126 & -18 & -23 & 0 & 0 & 0 & 0 \\ 103 & 26 & 0 & -53 & 0 & 0 & 0 & 0 \\ -22 & 0 & 0 & 0 & -7 & -19 & -36 & 48 \\ 93 & 0 & 0 & 0 & -25 & -2 & -5 & 23 \\ -32 & 0 & 0 & 0 & -97 & 13 & 63 & 2 \\ 1 & 0 & 0 & 0 & -25 & -111 & 93 & -13 \end{pmatrix}$$

Example Recursive LLL

$$\begin{pmatrix}
-2 & 6 & -1 & -8 & 0 & 1 & -3 & 1 \\
2 & -3 & -8 & 1 & 3 & -1 & 4 & 1 \\
3 & -3 & 6 & 2 & -6 & 2 & 4 & 3 \\
-2 & -1 & -6 & 4 & -6 & -3 & 0 & -3 \\
5 & -4 & 4 & -1 & -2 & 0 & -7 & 1 \\
4 & 2 & 3 & -1 & -4 & 1 & -1 & -7 \\
-2 & 3 & -4 & 0 & 0 & 11 & 2 & -2 \\
5 & 11 & 1 & 3 & -2 & 3 & -2 & 4
\end{pmatrix}$$

Recursive LLL

RLLL

- If $d = 2$, Return $LLL(A)$;
- If $d > 2$,
  1. Cut $A = \begin{pmatrix} A_0 \\ A_1 \end{pmatrix}$
  2. $A'_0 = RLLL(A_0)$.
  3. $A'_1 = RLLL(A_1)$.
  4. Reconstruct $A' = \begin{pmatrix} A'_0 \\ A'_1 \end{pmatrix}$.
  5. Return $LLL(A')$

Analysis

Why better?

- LLL (L^2) complexity is in $O(d^4\beta^2 + d^5\beta)$.
- If $d' = (d/2)$ and $\beta = 2\beta'$ therefore $d'^4\beta'^2 + d'^5\beta' < d^4\beta^2 + d^5\beta$.
- All preprocessing are negligible compare to last LLL.

Complexity of the last LLL

- Assuming uniform distribution, $\beta' = \frac{2\beta}{d}$.
- $O\left(d^4\beta'^2 + d^5\beta'\right)$
- $O\left(d^4\left(\frac{2\beta}{d}\right)^2 + d^5\frac{2\beta}{d}\right)$
- $O\left(d^2\beta^2 + d^4\beta\right)$

Conclusion

Conclusion

Improvement

- Previous complexity of LLL for knapsack lattice: $O(d^{3+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$.
- New recursive techniques: $O(d^{2+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$.

Future Work

- Specificity of Ideal Lattice.
- For given input and a given quality, estimate 2^x.