# CIS 700 Lecture 23: Lattice reduction and cryptanalysis



Recall:

Finding $v \in L \setminus \{0\}$ with $\|v\| = \lambda(L)$ is NP-hard (SVP)

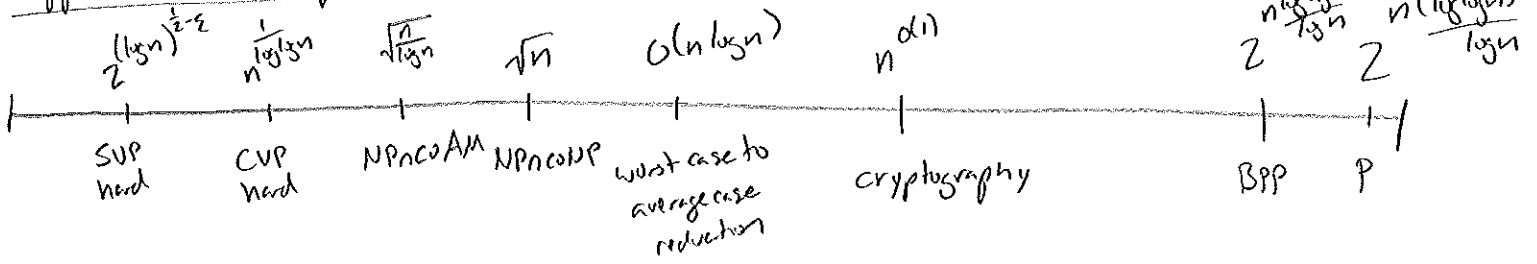
Finding a basis $b_1, \dots, b_n$ of $L$ with $\|b_i\|$ minimal is NP-hard.

CVP is NP-hard

Approximation versions

| SVP | CVP |
|---|---|
| find $\|v\| \le \gamma \lambda(L(B))$ | find $v \in L$ with $\|v-t\| \le \gamma \cdot dist(t, L(B))$ |

## Approximation Complexity of Lattice Problems




## Lenstra Lenstra Lovasz Lattice Basis Reduction

**Thm** Let $(b_1, \dots, b_n)$ be an LLL-reduced basis for $L$. Then:

1. $\|b_1\| \le 2^{\frac{(n-1)}{2}} \lambda(L)$
2. $\|b_1\| \le 2^{\frac{(n-1)}{4}} (\det L)^{\frac{1}{n}}$
3. $\|b_1\| \cdots \|b_n\| \le 2^{\frac{1}{2}\binom{n}{2}} \det L$

**Def** A basis $B = (b_1, \dots, b_n)$ is LLL-reduced if: $(\frac{1}{4} < \delta < 1)$

1. $|\mu_{i,j}| \le \frac{1}{2}$ for $1 \le j < i \le n$ ("size-reduced" or "weakly reduced")

   Gram-Schmidt:
   $$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \qquad \mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \qquad \Rightarrow b_i = \sum_{j=1}^{i} \mu_{ij} b_j^*$$

2. $\delta \|b_i^*\|^2 \le \|\mu_{i+1,i} b_i^* + b_{i+1}^*\|^2$ for $1 \le i < n$

   Alternatively:
   Define $\pi_i(x) = \sum_{j=i}^{n} \frac{\langle x, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$ projection onto $\sum_{j \ge i} b_j^*$
   (Component of $x$ orthogonal to $b_1^*, \dots, b_{i-1}^*$)
   $\pi_i(b_i) = b_i^*$

   $\Rightarrow \delta \|\pi_i(b_i)\|^2 \le \|\pi_i(b_{i+1})\|^2$

$\|b_{i+1}^*\|^2 \ge (\delta - \mu_{i+1,i}^2) \|b_i^*\|^2 \ge (\delta - \frac{1}{4}) \|b_i^*\|^2$ ("$b_{i+1}^*$ is not too much shorter than $b_i^*$")

LLL algorithm:

Input basis $b_1, \dots, b_n$ of $L$

Until done:

1. Size-reduce:

   Compute $b_1^*, \dots, b_n^*$

   For $i = 2$ to $n$

   For $j = i-1$ to $1$

   set $b_i = b_i - m b_j$ $\quad m = \left\lceil \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \right\rfloor = \lceil \mu_{i,j} \rfloor$

2. Swap:

   If $\exists i$ s.t. $\delta \|b_i^*\|^2 > \|\mu_{i+1,i} b_i^* + b_{i+1}^*\|^2$

   swap $b_i, b_{i+1}$

Thm The LLL algorithm terminates in polynomial time.

Babai's Nearest Plane Algorithm for CVP

Algorithm:

Input basis $B$, target vector $t$.

1. Run LLL on $B$

   Set $b = t$.

2. For $j$ from $n$ to $1$:

   $b = b - m_j b_j \qquad m_j = \left\lceil \frac{\langle x, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \right\rfloor$

3. Output $t - b = x \in L(B)$

Thm $\|x - t\| \le 2^{\frac{n}{2}} \operatorname{dist}(t, L)$

Lemma: $x$ satisfies $x - t = \sum_{i=1}^{n} r_i b_i^*$ with $|r_i| < \frac{1}{2}$ $\Rightarrow \|x-t\|^2 \le (\frac{1}{2})^2 \sum_{i=1}^{n} \|b_i^*\|^2$

Lemma $\|x - t\| \le \frac{1}{2} 2^{\frac{n}{2}} \|b_n^*\|$

$B$ is LLL-reduced, so $\|b_i^*\| \le 2^{\frac{n-i}{2}} \|b_n^*\|$

$$\|x-t\|^2 \le \frac{1}{4} \sum_{i=1}^{n} \|b_i^*\|^2 \le \frac{1}{4} \sum_{i=1}^{n} 2^{n-i} \|b_n^*\|^2 \le \frac{1}{4} 2^n \|b_n^*\|^2$$

$\Rightarrow$ if $\operatorname{dist}(t, L) \ge \frac{1}{2} \|b_n^*\|$, $x$ is $2^{n/2}$-approx for CVP.

# Cryptanalysis

## Knapsacks

Input $a_i$ find $\sum x_i a_i = t \quad x_i \in \{0,1\}$

Knapsack Lattices:

$$\begin{bmatrix} 1 & & & & & a_1 \\ & 1 & & & & a_2 \\ & & 1 & & & \vdots \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & -t \end{bmatrix}$$

solution corresponds to vector $v = [x_1, x_2 \ldots 0]$

$\|v\| \approx \sqrt{\frac{n}{2}}$

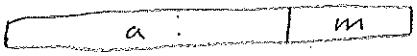
LLL might find $v$ if $\sqrt{\frac{n}{2}} < 2^{\frac{n}{4}} t^{\frac{1}{n+1}}$

and no other vectors that short

## Coppersmith's Theorem

Problem: Fixed-pattern RSA padding

public key $(e, N)$ $\quad c = (m+a)^3 \bmod N$




Problem: assume $a$ known, can we find $m$?

$c, e, N$ public, $e = 3$

**Thm** $f(x)$ monic univariate polynomial of degree $d$, $N$ integer

Can find solutions $f(r) \equiv 0 \bmod N$ when

$|r| < N^{\frac{1}{d}}$

in time polynomial in $\log N, d$.

Intuition: fix polynomial $f(x) = (x+a)^3 - c \quad f(m) \equiv 0 \bmod N$

$a, c$ big so $f(m) \neq 0$ over $\mathbb{Z}$.

Search for new poly $Q(x)$ s.t. $Q(m) = 0$ over $\mathbb{Z}$.

$f(x) = x^3 + f_2 x^2 + f_1 x + f_0 \quad f(m) \equiv 0 \bmod N$

$N \quad N \equiv 0 \bmod N$

$Nx \quad Nm \equiv 0 \bmod N$

$Nx^2 \quad Nm^2 \equiv 0 \bmod N$

If $Q(x) = c_3 f(x) + c_2 N x^2 + c_2 N x + c_1 N \quad c_i \in \mathbb{Z} \quad Q(m) \equiv 0 \bmod N$

If also $Q(x) = q_3 x^3 + q_2 x^2 + q_1 x + q_0$ and $|Q(m)| = \left|\sum q_i m^i\right| \leq \sum |q_i| |m|^i < N$

$\Rightarrow Q(m) = 0$ over $\mathbb{Z}$

## Algorithm

Let $|m| < M$

1. Generate lattice $\begin{bmatrix} M^3 & f_2M^2 & f_1M & f_0 \\ & NM^2 & & \\ & & NM & \\ & & & N \end{bmatrix}$ ← coeff. vector of $f(Mx)$

$v \in L = (v_3M^3, v_2M^2, v_1M, v_0) \Rightarrow$ polynomial $v(x) = v_3x^3 + v_2x^2 + v_1x + v_0$

$|v|_1 = \sum_i |v_i| M^i$ satisfies $|v(m)| \le \sum_i |v_i| m^i \le \sum_i |v_i| M^i = |v|_1$

2. Use LLL to find $v$ satisfying $|v|_2 \le 2^{\frac{n-1}{4}} \det L^{\frac{1}{n}}$

$n = 4 \quad \det L = M^6N^3 \quad \det L^{\frac{1}{n}} = (M^6N^3)^{\frac{1}{4}}$

Condition for success:

$|v|_1 \le \sqrt{4}\,|v|_2 \le 2^{\frac{n-1}{4}} \det L^{\frac{1}{n}} = 2^{\frac{3}{4}} (M^6N^3)^{\frac{1}{4}} < N$

$2^3 M^6 N^3 < N^4$

$M < \frac{N^{\frac{1}{6}}}{2^{\frac{1}{2}}} \Rightarrow$ Break fixed-pattern RSA padding if $|m| < N^{\frac{1}{6}}$!

**Pf** (of Coppersmith's Theorem)

Generate lattice from $N^k, xN^k \dots, fN^{k-1}, \dots, f^k, \dots, x^t f^k$

Wiener Small $d$:

$e \cdot d \equiv 1 \bmod (p-1)(q-1)$

$e \cdot d = 1 + k(N - (p+q) + 1)$

$e \cdot d + k(p+q+1) - 1 = kN$

$f(x,y) = ex + y \equiv 0 \bmod N$

$k < d, \quad p+q \sim N^{\frac{1}{2}}$

$\begin{bmatrix} y & eX \\ 0 & NX \end{bmatrix}$ $\quad a\, f(x,y) + bNx$

$\det L = NXY \qquad (NXY)^{\frac{1}{2}} < N$

$\dim L = 2 \qquad XY < N$

$d \cdot d \cdot N^{\frac{1}{2}} < N$

$d < N^{\frac{1}{4}}$