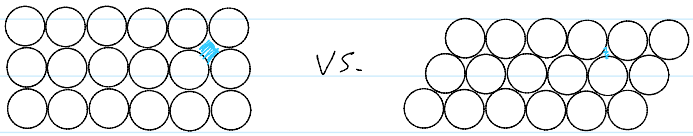
Lattices

Sunday, November 5, 2023 5:24 PM

Post-Quantum Cryptography

What are lattices?

e.g. stack of oranges



vs.

"Sphare packing"

more dense

1] Def^{n}. a lattice is a discrete additive subgroup Λ of $\mathbb{R}^m$

i.e.

① subgroup $\begin{cases} \Lambda \subseteq \mathbb{R} \\ \Lambda \text{ is closed under addition} \\ \text{there is } \vec{v}_0 \in \Lambda \text{ is the identity.} \\ \forall \vec{v} \in \Lambda, \exists \vec{v}^{-1} \in \Lambda, \ \vec{v} + \vec{v}^{-1} = \vec{v}_0 \end{cases}$

② discrete:

$\exists \varepsilon > 0$, for any two distinct points $x, y \in \Lambda$, the distance $\| x - y \| \geq \varepsilon$

2] e.g. ① $\mathbb{Q}^m \subseteq \mathbb{R}^m$, but $\mathbb{Q}^m$ is not discrete $\Rightarrow$ not lattice

② $\mathbb{Z}^m \subseteq \mathbb{R}^m$ is a lattice because it is subgroup of $\mathbb{R}^m$ and discrete for $\varepsilon = 0.2$

3] Applications:

① Sphere packing:

for $m = 3$ (3D), 74.05%

for $m \geq 4$, it is an open problem

② Number Theory. Lattices are discrete subgroups of $\mathbb{R}^m$

③ Cryptography:

- lattices have been used to break cryptosystems.
- lattice-based cryptosystems can resist known quantum attacks for post-quantum cryptography.

4] Def^n. Given n linearly independent vectors $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ the lattice generated by them is:

$$\mathcal{L}(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\}$$

$$= \{ \underbrace{x_1 b_1 + x_2 b_2 + \dots + x_n b_n}_{P_1}, \underbrace{x_1' b_1, x_2' b_2 + \dots}_{P_2} \}$$

Here, $b_1, b_2, \dots, b_n$ are called the basis of $\mathcal{L}$

n is the rank of the lattice $\mathcal{L}$

m is the dimension of the lattice, $n \leq m$

if $n = m$ then we have a full-rank lattice.

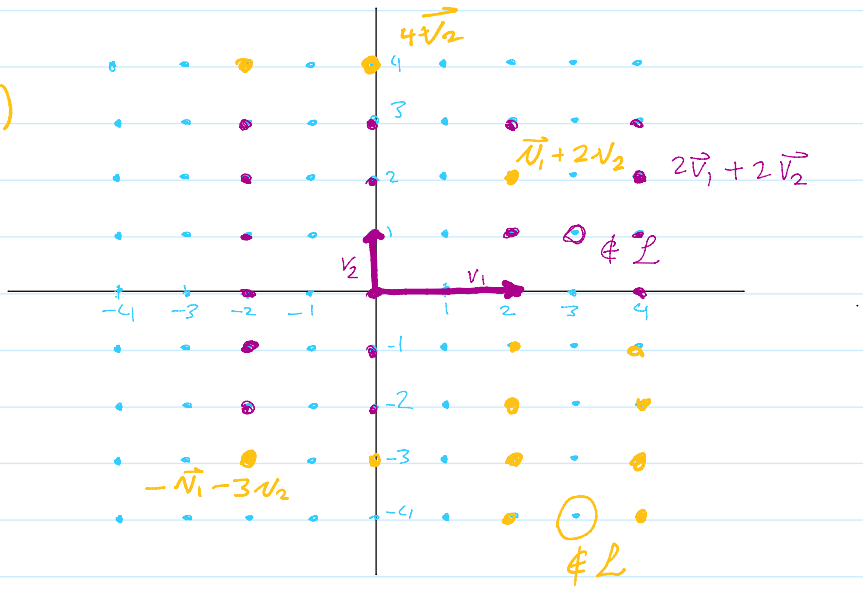
5] Examples:

$$v = \begin{bmatrix} x \\ y \end{bmatrix} = (x, y)$$

① $\vec{v_1} = \begin{bmatrix} 2 \\ 0 \end{bmatrix} = b_1$

$\vec{v_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = b_2$

$x_1 \vec{v_1} + x_2 \vec{v_2} \in \mathcal{L}$

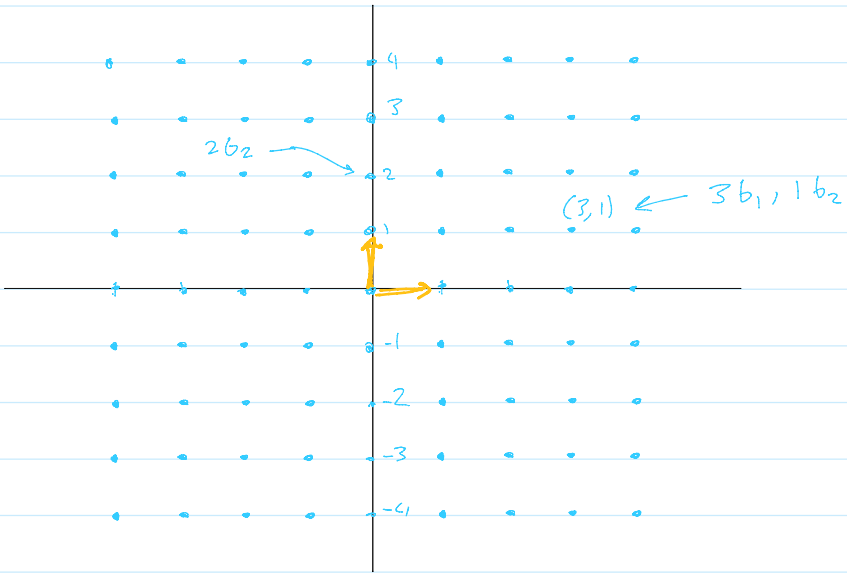


(2)

$b_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$b_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

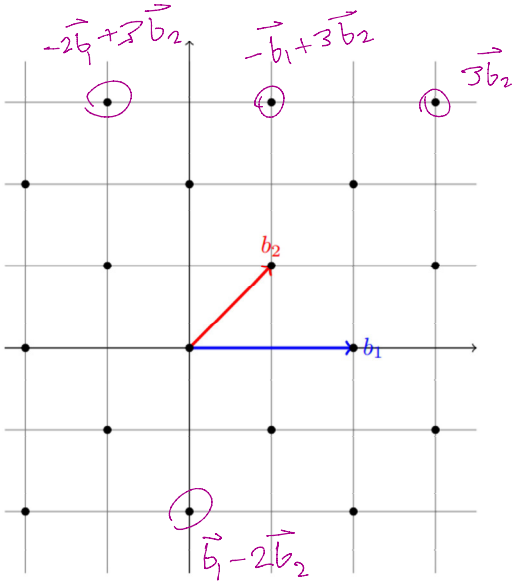
$\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$



(3)

$b_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix} = (2,0)$

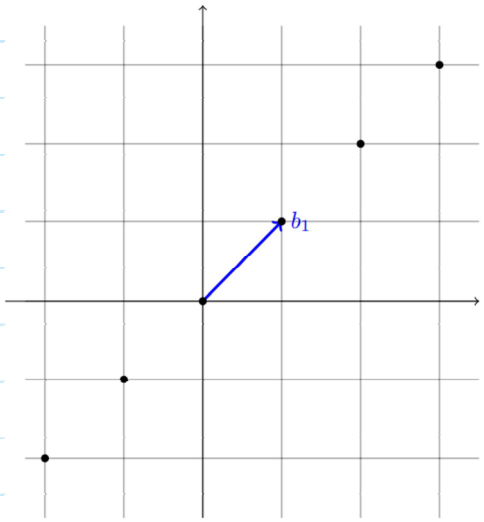
$b_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = (1,1)$



(c) A full-rank lattice generated by the basis vectors $(1,1)$ and $(2,0)$. Note that this is a sub-lattice of $\mathbb{Z}^2$.

(4)

$b_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$



(d) A *non full-rank* lattice with basis vector $(1,1)$

6] Notation

$$\mathcal{L}(b_1, b_2, \ldots, b_n)$$

let $B = \begin{bmatrix} | & | & & | \\ b_1 & b_2 & \cdots & b_n \\ | & | & & | \end{bmatrix}$ $\Big\}$ m

Then $\mathcal{L}(B) = \{ Bx \mid x \in \mathbb{Z}^n \}$

$$\mathcal{L} = \underset{m \times n}{[B]} \times \underset{n \times 1}{[x]} = \underset{m \times 1}{[v]}$$

Q4. a) $12.28 = 336$

26^k

$26^{(6\times 6)}$

31.26^3

$C = P \cdot K$

$4\times 6 - 6 \times 6$

b)

DES		16
3DES		48
AES		12
		14

c) adv. large key 168 bit.

cons. triple round $\longrightarrow$ slow

64 bit blocks

d) $\geq$ 3DES security

faster

128 / 192 / 256 keys

64 or 128 block

Q5.

order	$\mathbb{Z}_{64}$	$\mathbb{Z}_{64}^*$	
	64	$\phi(64) = 32$	
	32	none	$p = 2, 4, 2p^k, p^k$
	none	none	
	32	$-1 \equiv 63$	

Q6. a)

$\langle 7 \rangle = \{ 7, 23, 5, 9, 11, 25,$ 93/95

$\langle 7 \rangle = \{ 7, 23, 5, 9, 11, 25, 19, 3, 21, 17, 15, 1 \}$

b) $\{23, 9, 25, 3, 17, 1\}$

c) 5, 21

d) $\frac{ord(7)}{gcd(7, 12)} = \frac{ord(7)}{1} = 12$

e) $\mathbb{Z}_{12} \cong \mathbb{Z}_{26}^{*}$

a	1	2	3	4	5	6	7	8	9	10	11	0
$\theta(a)$	7,	23,	5,	9,	11,	25	19,	3,	21,	17,	15,	1