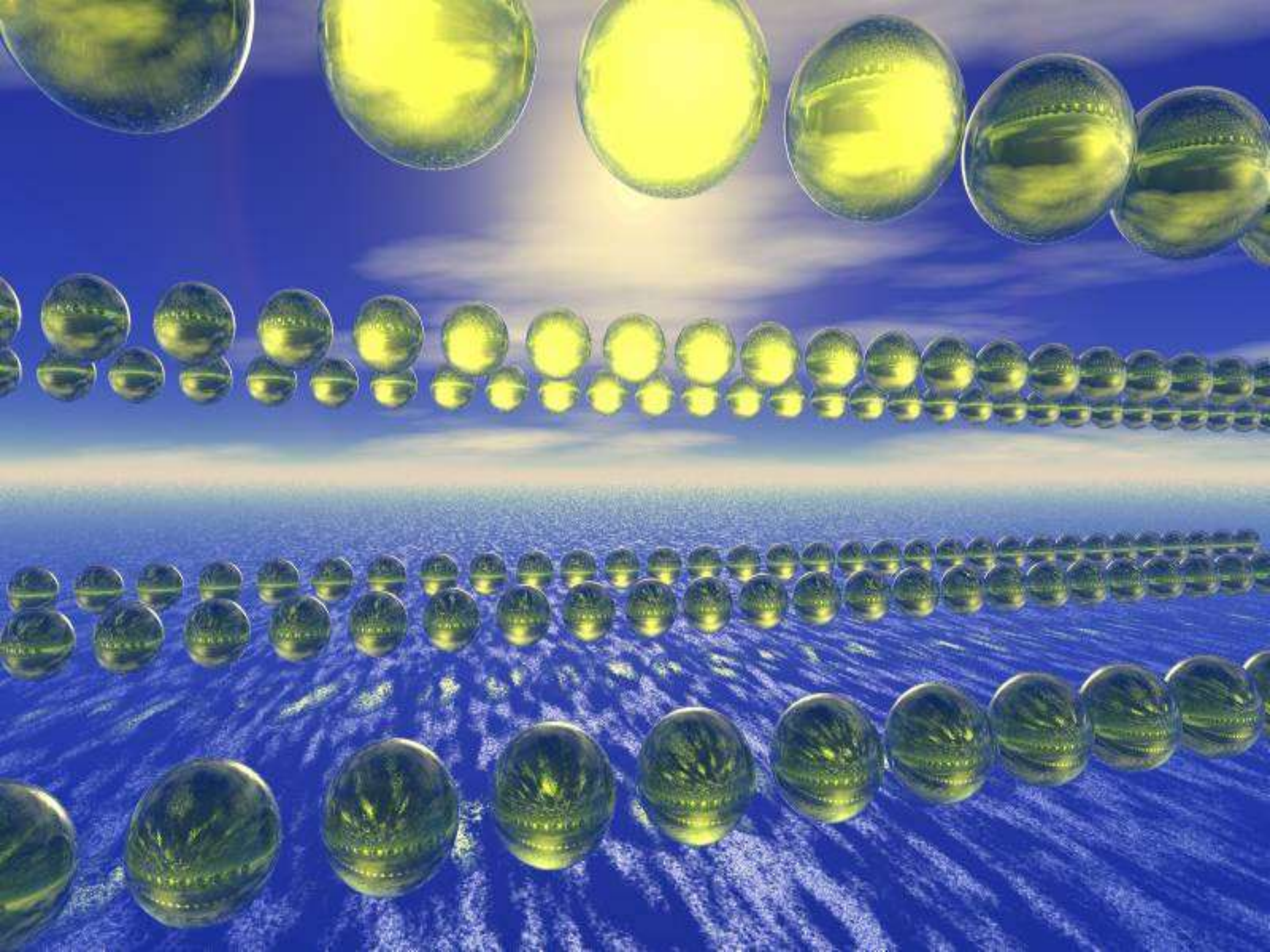
Winter School on Lattice-Based Cryptography and Applications
Bar-Ilan University, Israel 19/2/2012

# Introduction to Lattices

Oded Regev
(Tel Aviv University and CNRS, ENS-Paris)

Bar-Ilan University
Dept. of Computer Science



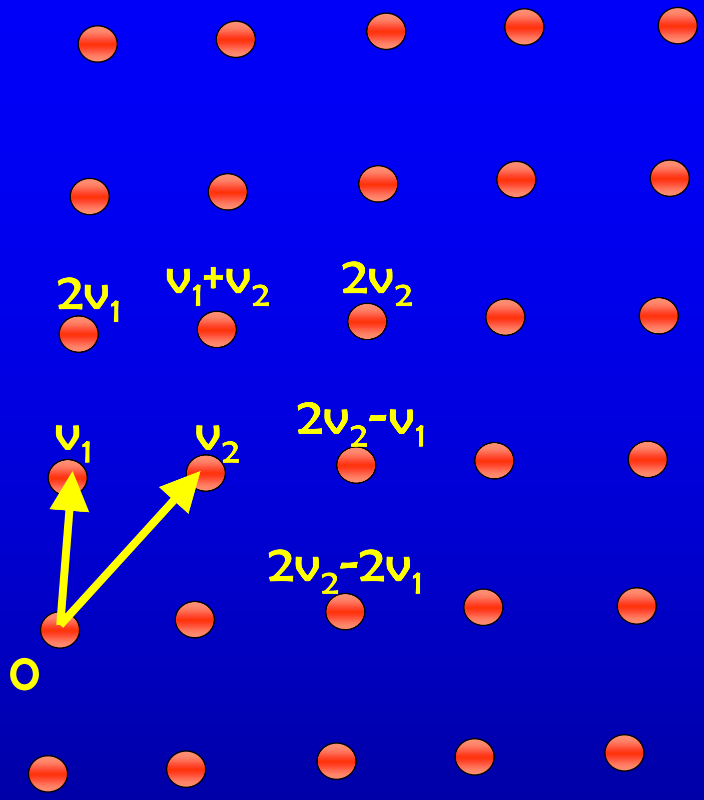
# Lattices

- A lattice is a set of points

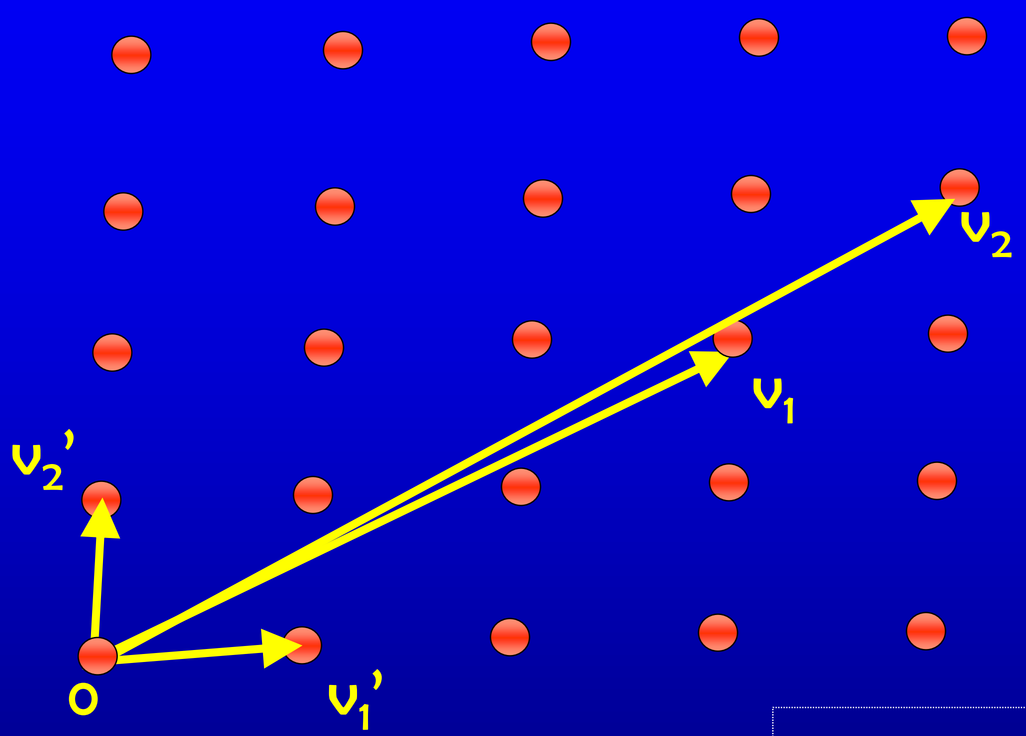
  $L=\{a_1v_1+\ldots+a_nv_n \mid a_i \text{ integers}\}$

  for some linearly independent vectors $v_1,\ldots,v_n$ in $R^n$

- We call $v_1,\ldots,v_n$ a basis of L



# Basis is not Unique



# History

- Geometric objects with rich mathematical structure
- Considerable mathematical interest, starting from early work by Gauss 1801, Hermite 1850, and Minkowski 1896.

# History

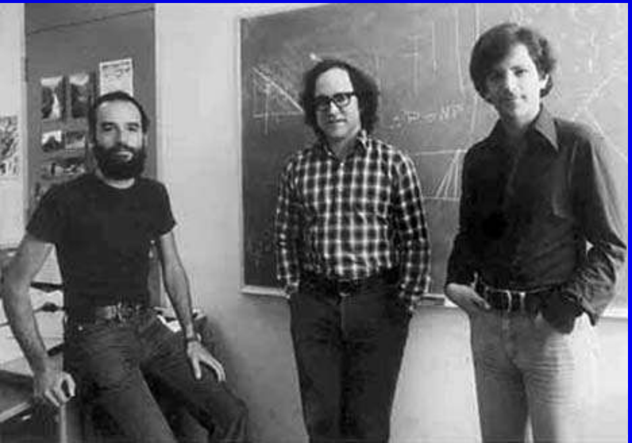
- Recently, many interesting applications in computer science:
  - LLL algorithm - approximates the shortest vector in a lattice [LenstraLenstraLovàsz82]. Used for:
    - Factoring polynomials over rationals,
    - Solving integer programs in a fixed dimension,
    - Finding integer relations:

$$6.73205080756887\ldots \overset{?}{=} \sqrt{3} + 5$$

# Cryptography

- Modern economy is based on cryptography
- Cryptography is everywhere:
  - In credit cards, passports, mobile phones, Internet,…
- Most systems are based on the RSA cryptosystem, developed by Rivest, Shamir, and Adleman in 1977

RSA SECURITY

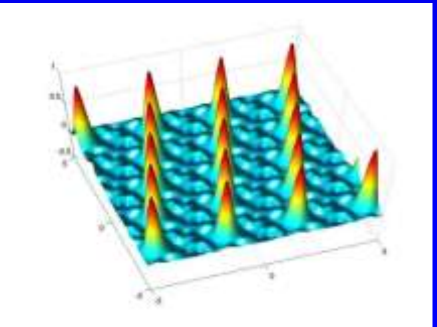


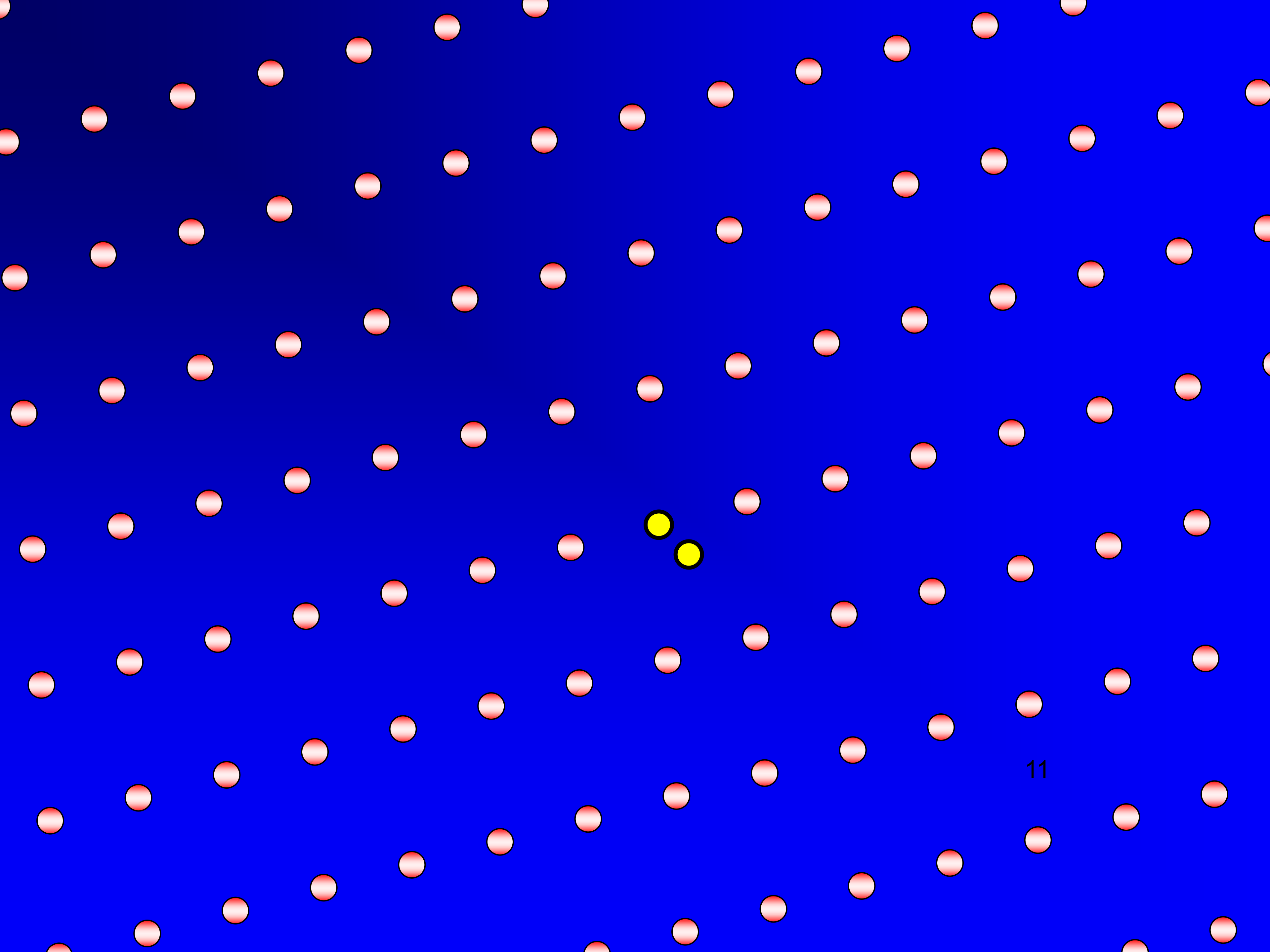
# Lattices and Cryptography (1)

- LLL can be used as a cryptanalysis tool (i.e., to break cryptography):
  - Knapsack-based cryptosystem [LagariasOdlyzko'85]
  - Variants of RSA [Håstad'85, Coppersmith'01]

# Lattices and Cryptography (2)

- Lattices can also be used to create cryptography
- This started with a breakthrough of Ajtai in 1996
- Cryptography based on lattices has many advantages compared with ‘traditional’ cryptography like RSA:
  - It has strong, mathematically proven, security
  - It is resistant to quantum computers
  - In some cases, it is much faster





# Why use lattice-based cryptography

| Lattice-based crypto | 'Standard' cryptography |
| --- | --- |
| ☺ Provably secure | 😐 Not always provable… |
| ☺ Security based on a worst-case problem | 😐 Security based on an average-case problem |
| ☺ Based on hardness of lattice problems | 😐 Based on hardness of factoring, discrete log, etc. |
| ☺ (Still) Not broken by quantum algorithms | 😐 Broken by quantum algs |
| ☺ Very simple computations | 😐 Require modular exponentiation etc. |
| ☺ Can do more things | |

# Provable Security

- Security proof: a reduction from solving a hard problem to breaking the cryptographic function
- A security proof gives a strong evidence that our cryptographic function has no fundamental flaws
- Can also give hints as to choice of parameters

- Example: One-wayness of modular squaring
  - Somehow choose $N=pq$ for two large primes $p,q$
  - $f(x)=x^2 \bmod N$
  - If we can compute square roots mod N

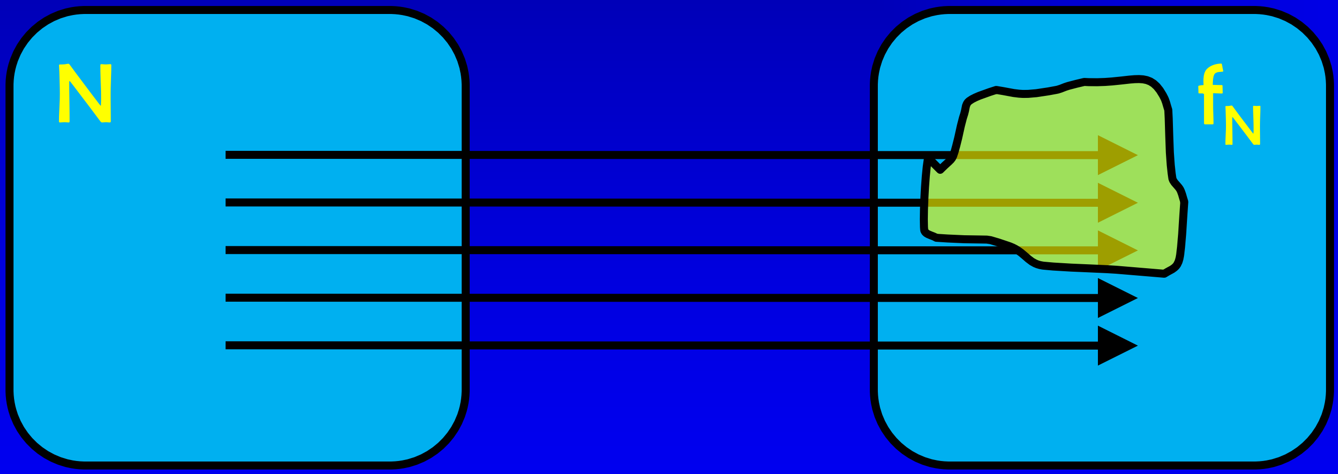
    then we can factor N

# Average-case hardness is not so nice…

- How do you pick a "good" N in RSA?
- Just pick p,q as random large primes and set N=pq?
  - (1978) Largest prime factors of p-1,q-1 should be large
  - (1981) p+1 and q+1 should have a large prime factor
  - (1982) If the largest prime factor of p-1 and q-1 is p' and q', then p'-1 and q'-1 should have large prime factors
  - (1984) If the largest prime factor of p+1 and q+1 is p' and q', then p'-1 and q'-1 should have large prime factors
- Bottom line: currently, none of this is relevant

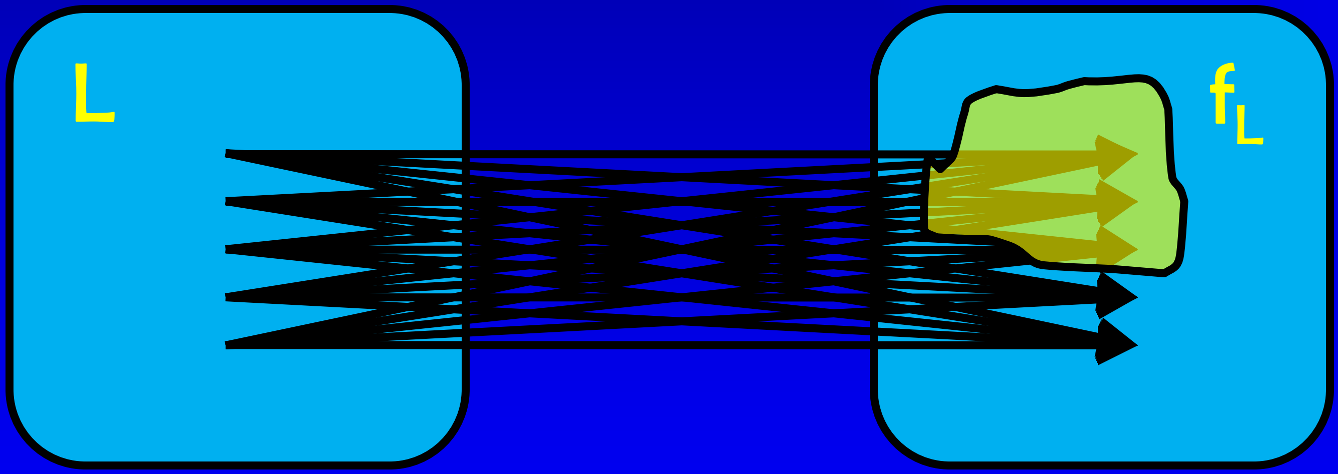
# Provable security based on average-case hardness

- The cryptographic function is hard provided almost all N are hard to factor



# Provable security based on worst-case hardness

- The cryptographic function is hard provided the lattice problem is hard in the worst-case
- This is a much stronger security guarantee
- It assures us that our distribution is correct



# Modern Lattice-based Crypto

- The seminal work of Ajtai and Ajtai-Dwork in 1996 showed the power of lattice-based crypto, but the resulting systems were extremely inefficient (keys require gigabytes, slow,…), cumbersome to use, and nearly impossible to extend
- Recent work [MicciancioR03,R05,…] identified two key problems called Short Integer Solution (SIS) and Learning With Errors (LWE) that lead to very efficient constructions and are extremely versatile
- Another line of work [Micciancio02, PeikertRosen06, LyubashevskyMicciancio06,…] gives extremely efficient constructions from ideal lattices (Ring-LWE and Ring-SIS)

# Introduction to Lattices

# Lattices

Basis:

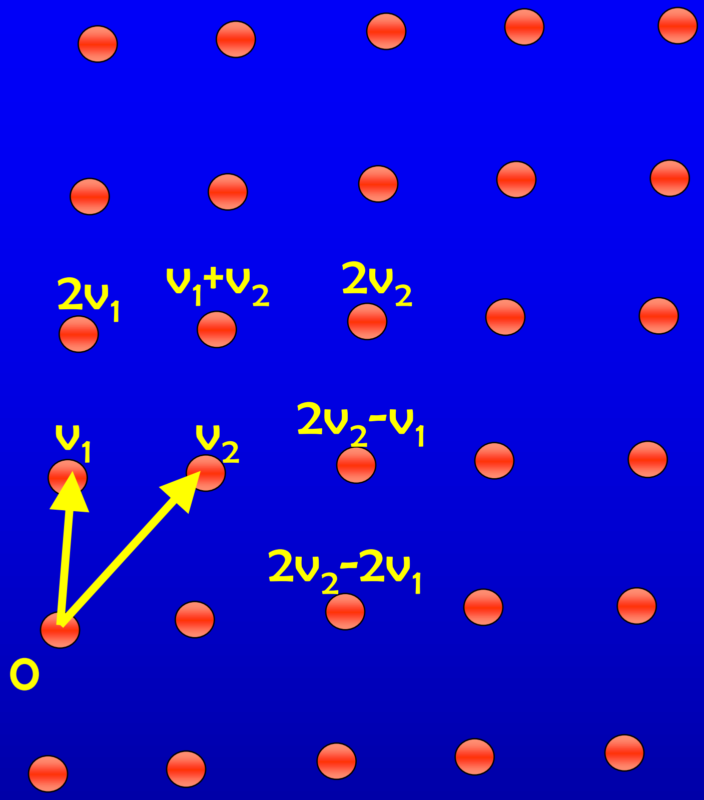
$v_1,\dots,v_n$ linearly independent vectors in $R^n$

The lattice L is

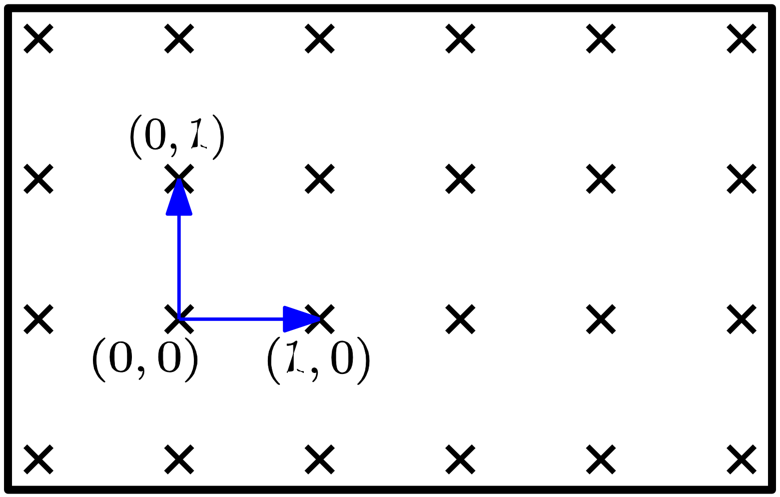
$L=\{a_1v_1+\dots+a_nv_n \mid a_i \text{ integers}\}$

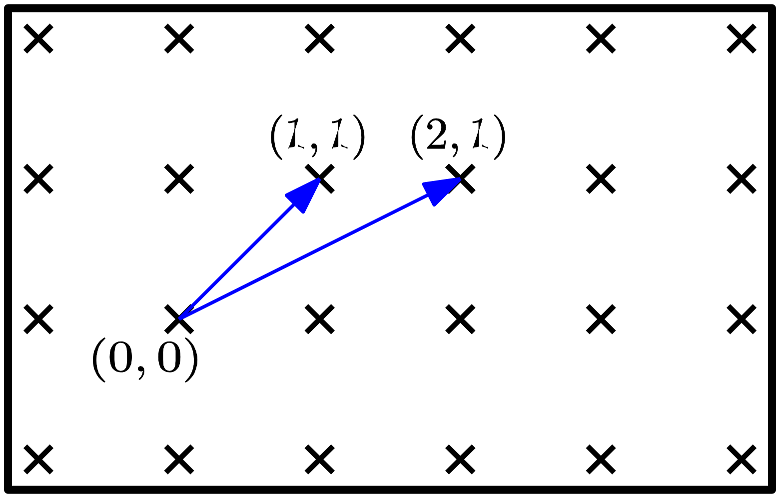
Also denoted L(B) where B is an n*n matrix with columns $v_1,\dots,v_n$.

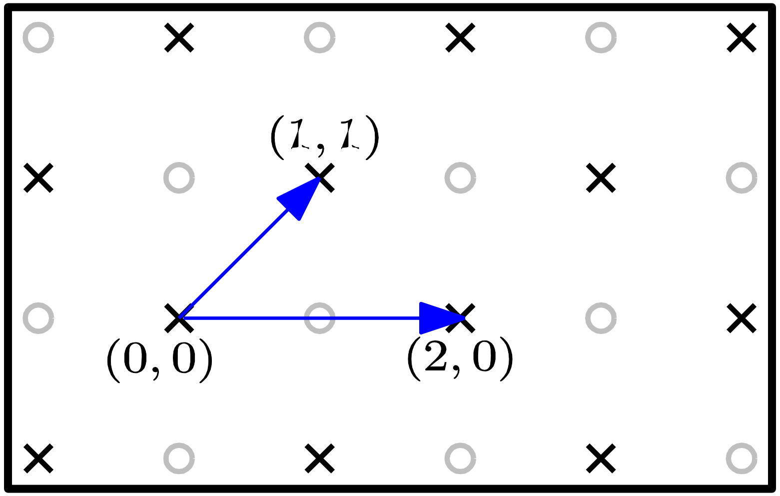
Equivalently, one can define a lattice as a discrete additive subgroup of $R^n$



# Lattice Bases



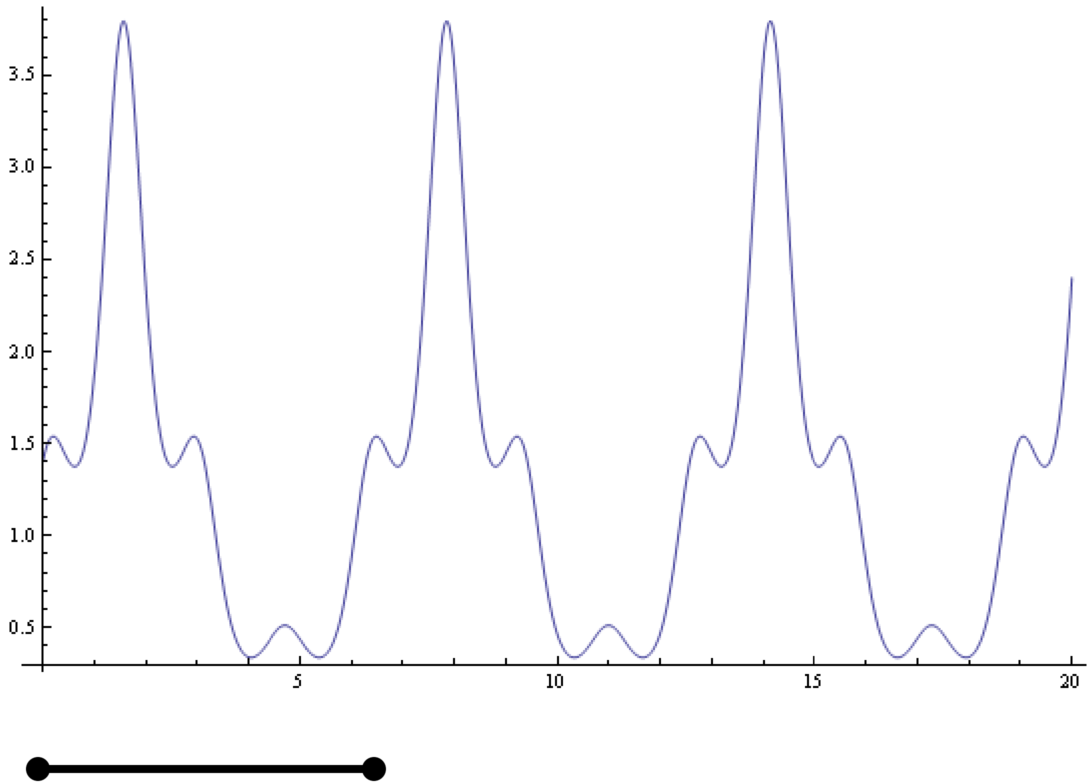
# Equivalent Bases

- When do two bases generate the same lattice?
  - We can clearly permute the vectors $v_i \leftrightarrow v_j$
  - We can negate a vector $v_i \leftarrow -v_i$
  - We can add an integer multiple of one vector to another, $v_i \leftarrow v_i + kv_j$ for some $k \in \mathbb{Z}$
- More succinctly, we can multiply B from the right by any *unimodular* matrix U (i.e., an integer matrix of determinant $\pm 1$)
- Thm: Two bases $B_1, B_2$ are equivalent

  iff $B_2 = B_1 U$ for a unimodular U

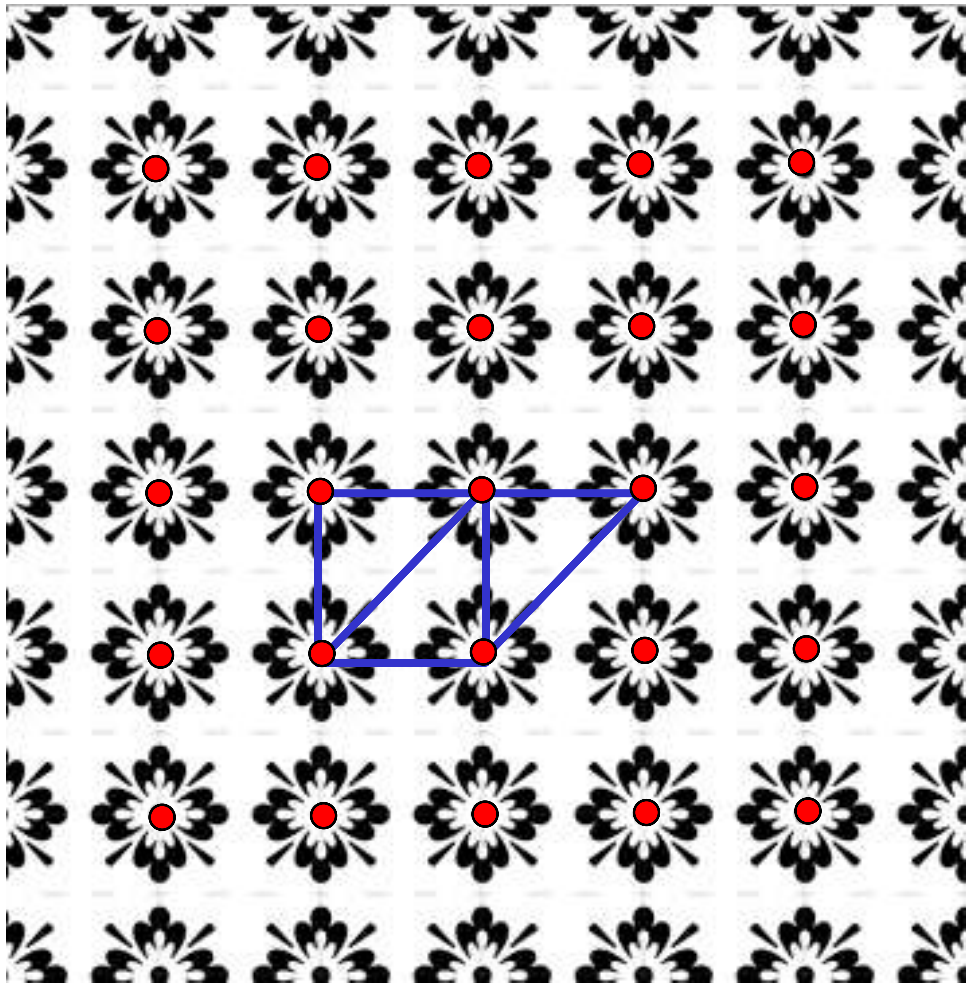
# Periodic Function on R

- f:$\mathbb{R} \to \mathbb{R}$ with period $2\pi$ (equivalently f:$\mathbb{R}/(2\pi\mathbb{Z}) \to \mathbb{R}$)
- Enough to store values on $[0,2\pi)$ and read x at x mod $2\pi$

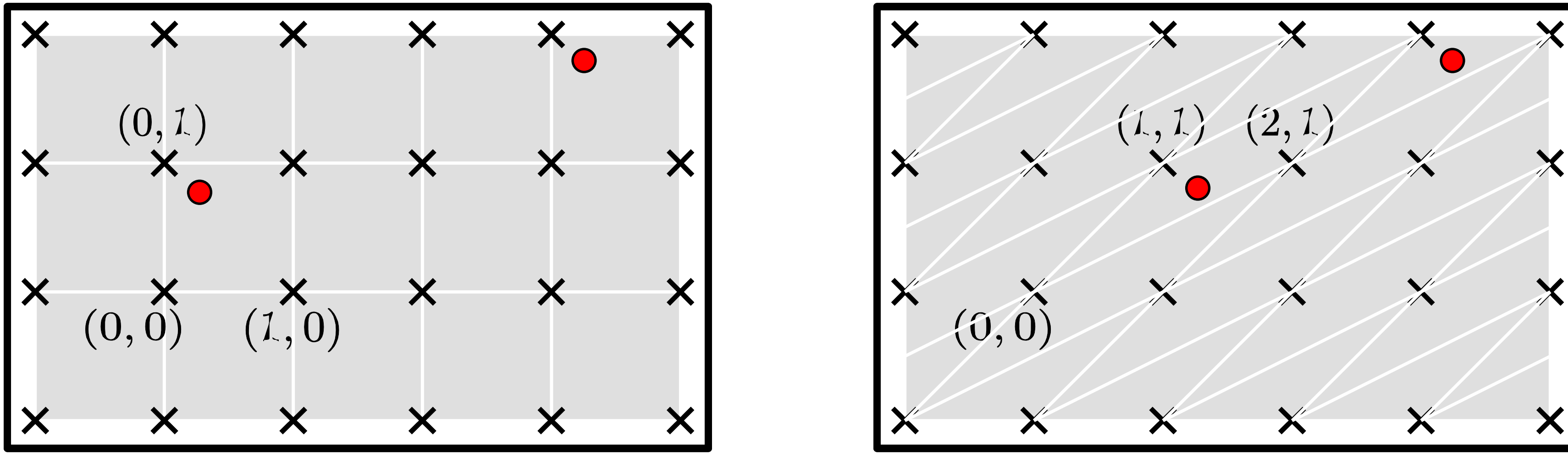


# Periodic Function on $R^2$

- $f:\mathbb{R}^n \rightarrow \mathbb{R}$ with period L (equivalently, $f:\mathbb{R}^n/L \rightarrow \mathbb{R}$)



# The Fundamental Parallelepiped



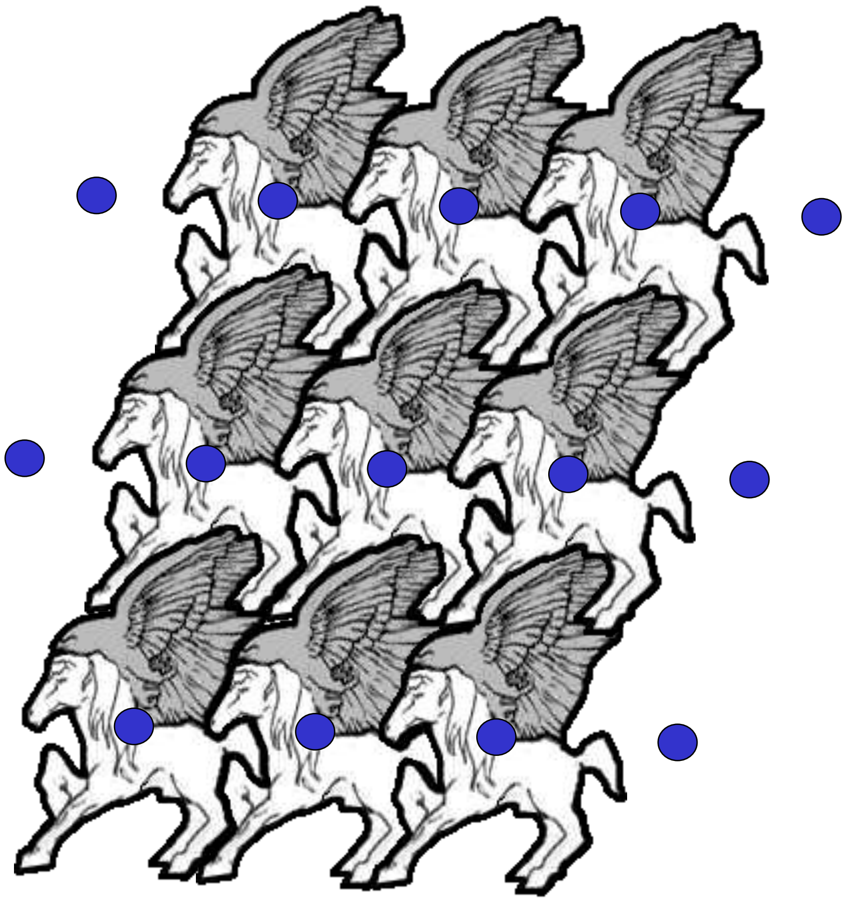

$P(B)=\{a_1b_1+\ldots+a_nb_n \mid a_i \text{ in } [0,1)\}$

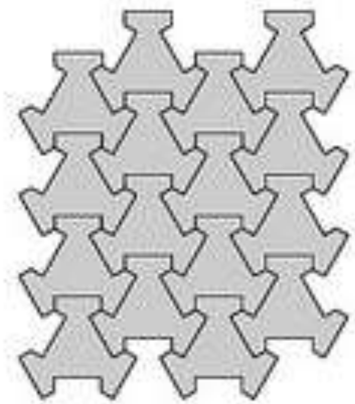
If $x=a_1b_1+\ldots+a_nb_n$ then

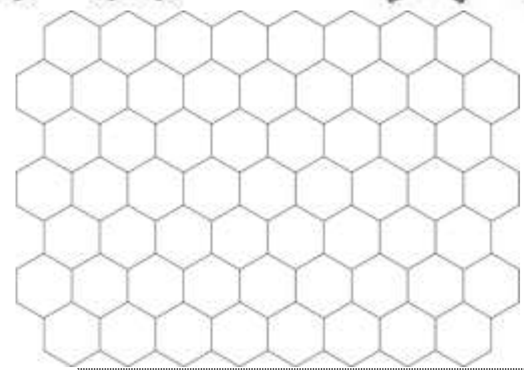
$x \bmod P(B) :=$

$(a_1 \bmod 1)b_1+\ldots+(a_n \bmod 1)b_n$

# Other Fundamental Regions







# Determinant

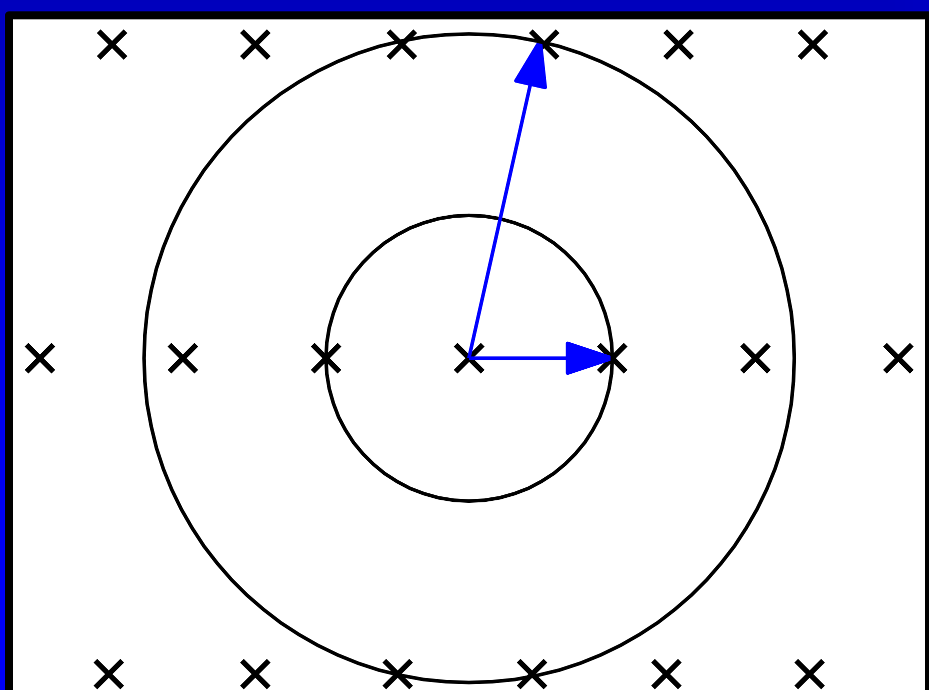
- Def: The determinant of a lattice $L(B)$ is $\det(L) := |\det(B)|$
- Notice that this is well defined since

  $$|\det(BU)| = |\det(B)\det(U)| = |\det(B)|$$
- The determinant is the volume of the fundamental parallelepiped, and hence is the reciprocal of the density

# Successive Minima

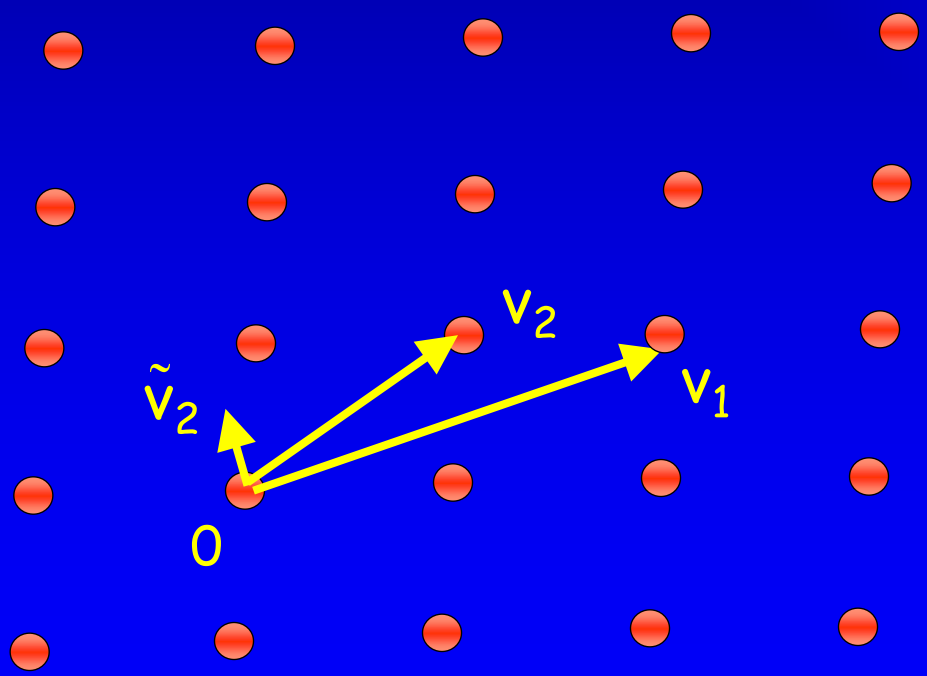
$\ell_2$ nonzero

- $\lambda_1(L)$ denotes the length of the shortest vector in L
- More generally, $\lambda_k(L)$ denotes the smallest radius of a ball containing k linearly independent vectors

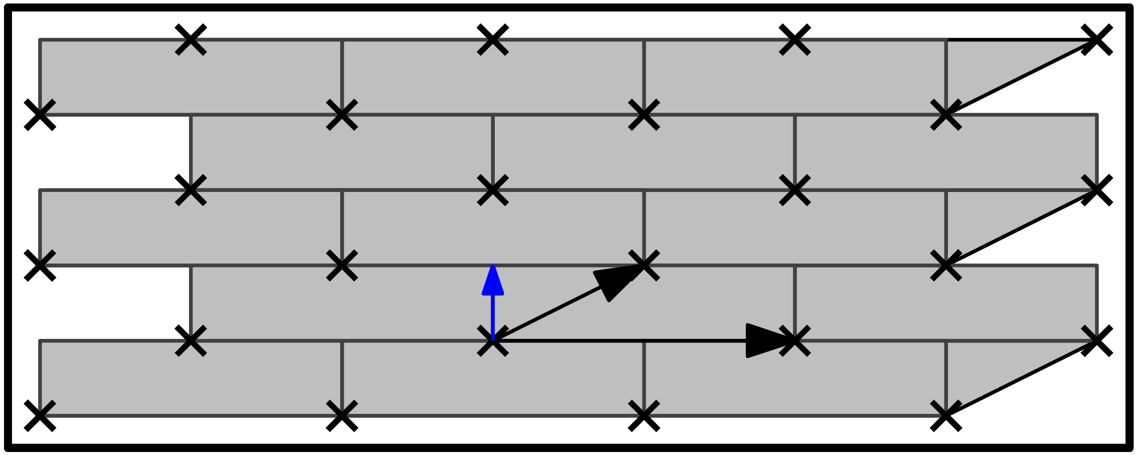


# Gram-Schmidt Orthogonalization

- Given a sequence of vectors $v_1,\ldots,v_n$ their GSO $\tilde{v}_1,\ldots,\tilde{v}_n$ is defined by projecting each vector on the orthogonal complement of the previous vectors
- So $\tilde{v}_1=v_1$, $\tilde{v}_2=v_2-\langle v_2,\tilde{v}_1\rangle\tilde{v}_1/||\tilde{v}_1||^2$, etc.



# The GS Fundamental Region



# Gram-Schmidt Orthogonalization

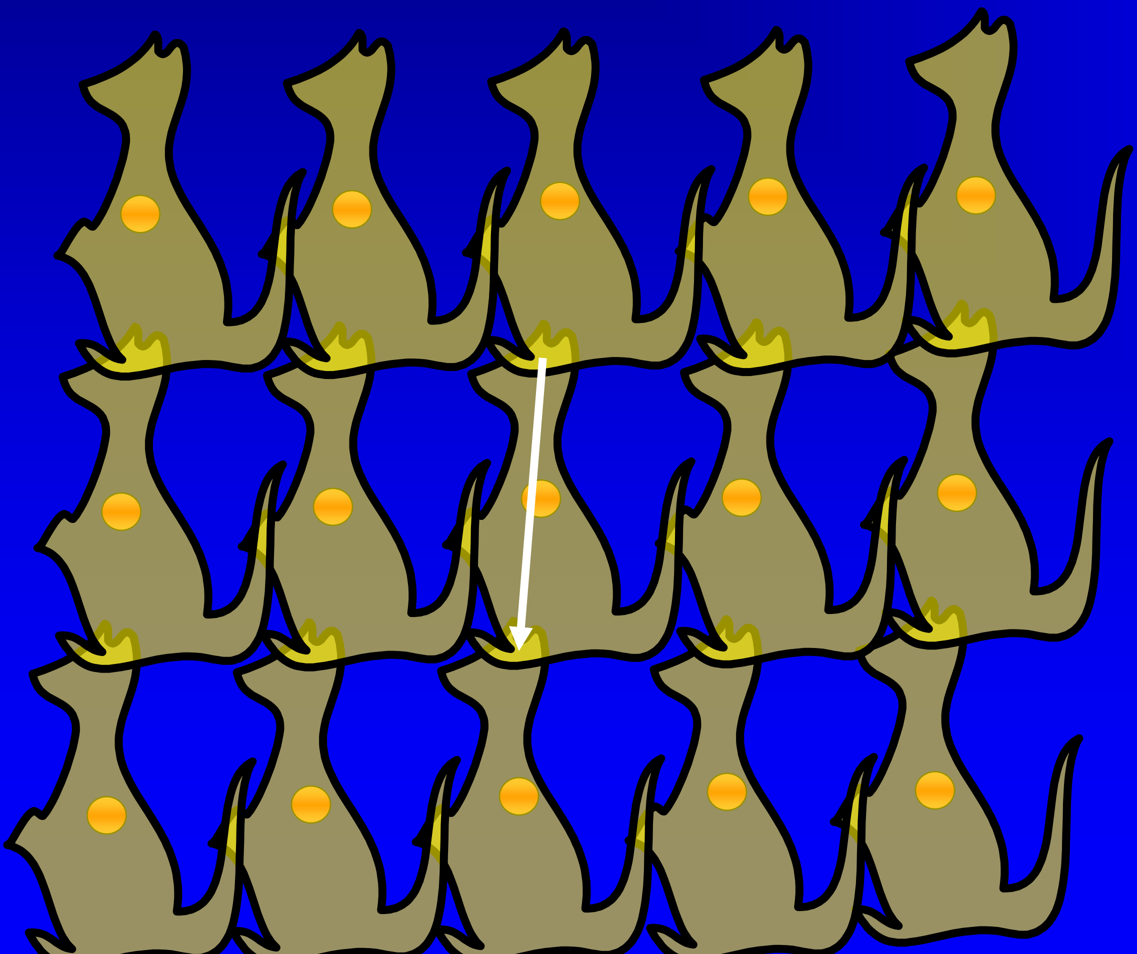
- Since $\tilde{v}_1,\ldots,\tilde{v}_n$ are orthogonal, we can normalize them to get an *orthonormal* basis $\tilde{v}_1/||\tilde{v}_1||,\ldots,\tilde{v}_n/||\tilde{v}_n||$
- Written in this basis, the vectors $v_1,\ldots,v_n$ are

$$\begin{pmatrix} ||\tilde{v}_1|| & * & \cdots & * \\ 0 & ||\tilde{v}_2|| & & * \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & ||\tilde{v}_n|| \end{pmatrix}$$

- (This is known as the QR decomposition)
- Lemma 1: The lattice generated by $v_1,\ldots,v_n$ has determinant $\prod ||\tilde{v}_i||$
- Lemma 2: $\lambda_1$ is at least $\min ||\tilde{v}_i||$

# Minkowski's Theorem

- <u>Thm (Blichfeld)</u>: For any lattice $\Lambda$ and set S of volume $>\det(\Lambda)$ there exist $z_1, z_2 \in S, z_1 \neq z_2$ such that $z_1 - z_2 \in \Lambda$

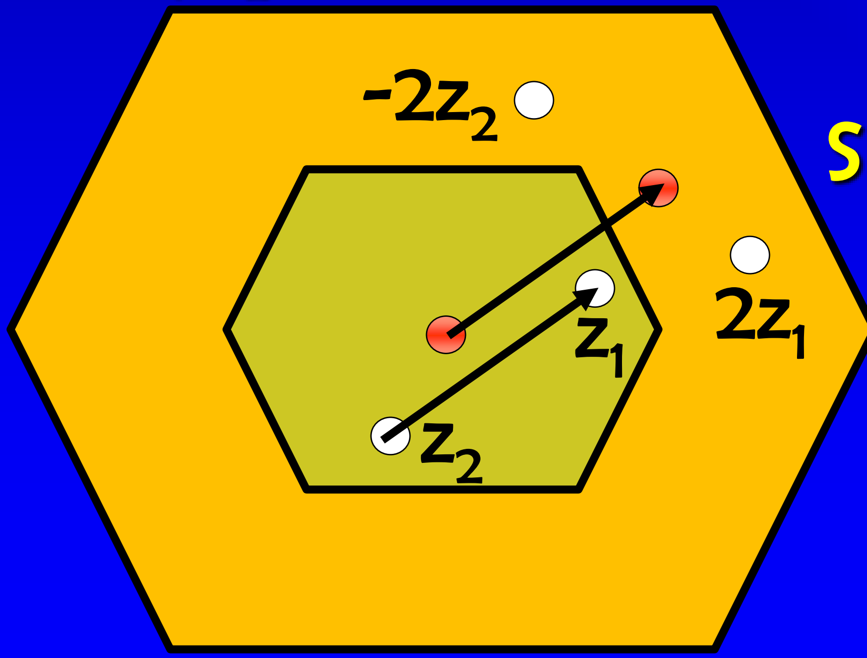


# Minkowski's Theorem

- <u>Thm (Minkowski)</u>: For any lattice $\Lambda$ and convex zero-symmetric set S of volume $>2^n\det(\Lambda)$, there exists a lattice point in S
- Proof: Let $z_1,z_2 \in S/2$ such that $z_1-z_2 \in \Lambda$.

  Therefore $2z_1 \in S$ and also $-2z_2 \in S$.

  So we get $z_1-z_2 \in S$

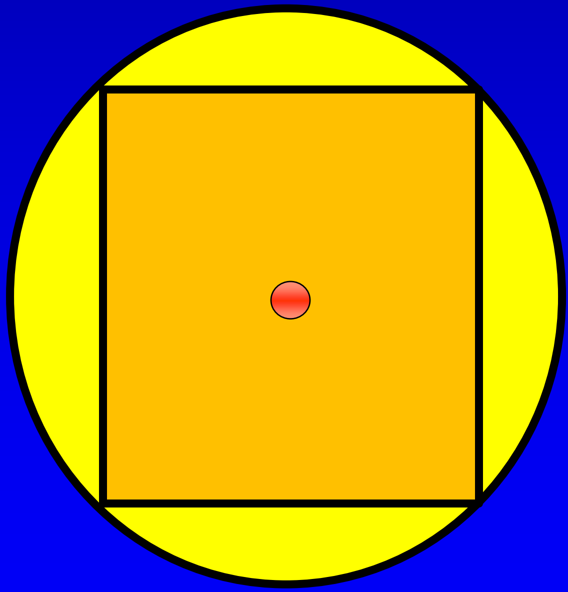


# Minkowski's Theorem

- Cor (Minkowski): For any lattice $\Lambda$,

$$\lambda_1(\Lambda) \leq \sqrt{n} \cdot \det(\Lambda)^{\frac{1}{n}}$$

- Proof: Use fact that volume of ball of radius $\sqrt{n}$ is greater than $2^n$. (This is true because it contains $[-1,1]^n$)

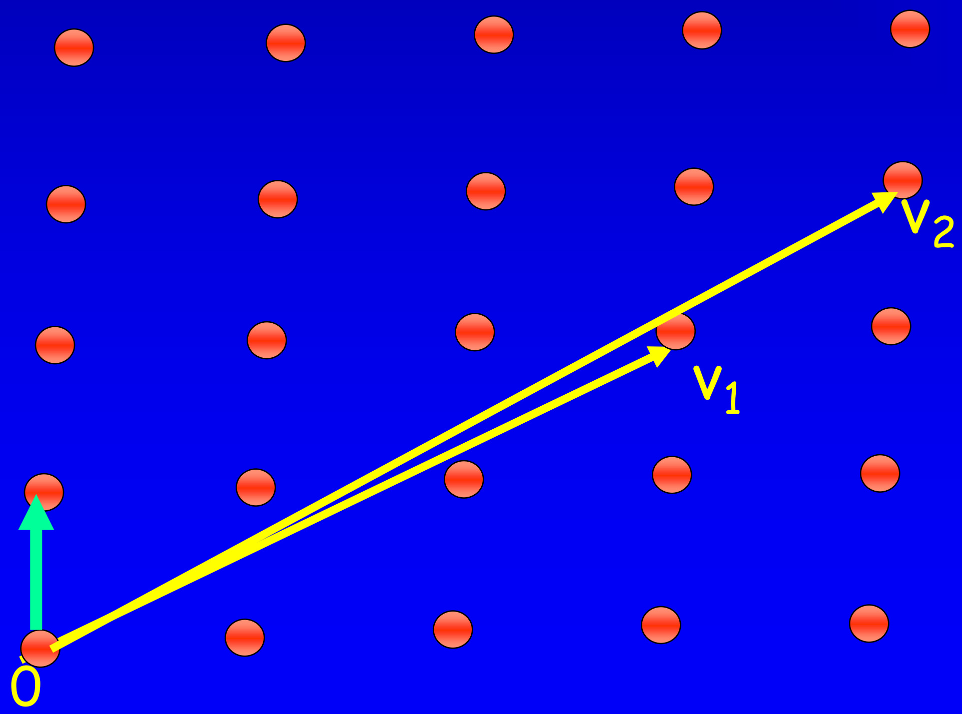


# Computational Problems

- Given a basis B and a vector v, it is easy to decide if v is in L(B)
- Similarly, given two bases $B_1$ and $B_2$, it is easy to decide if $L(B_1)=L(B_2)$
- Contrary to these *algebraic* problems, *geometric* problems seem much harder!

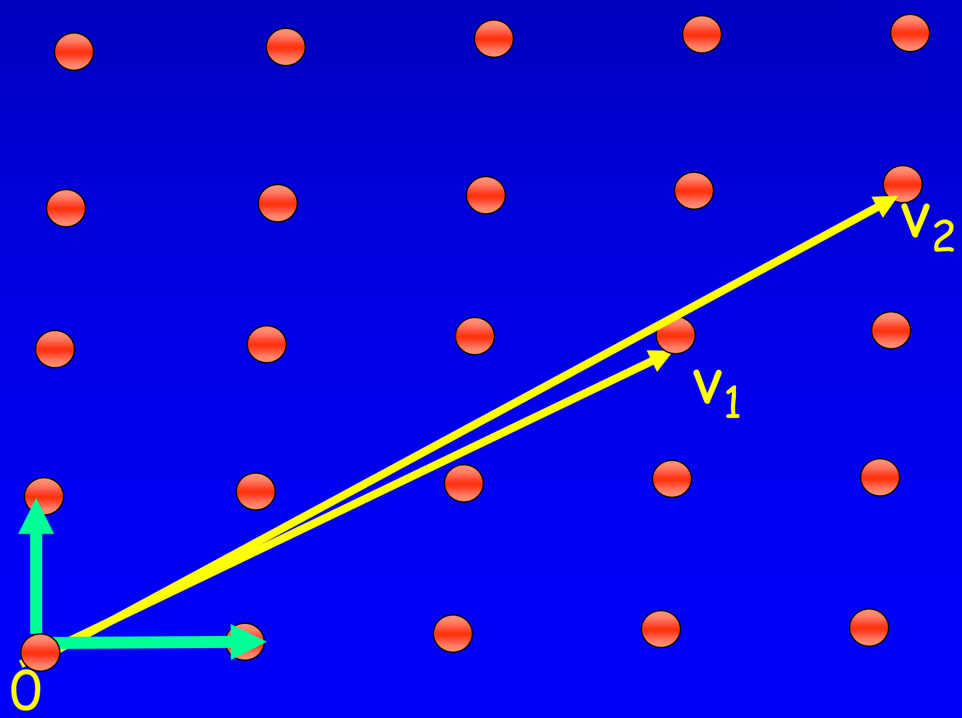
# Shortest Vector Problem (SVP)

- $SVP_\gamma$: Given B, find a vector in L(B) of length $\leq \gamma\lambda_1(L(B))$
- $GapSVP_\gamma$: Given a lattice, decide if $\lambda_1$ (i.e., the length of the shortest nonzero vector) is:
  - YES: less than 1
  - NO: more than $\gamma$



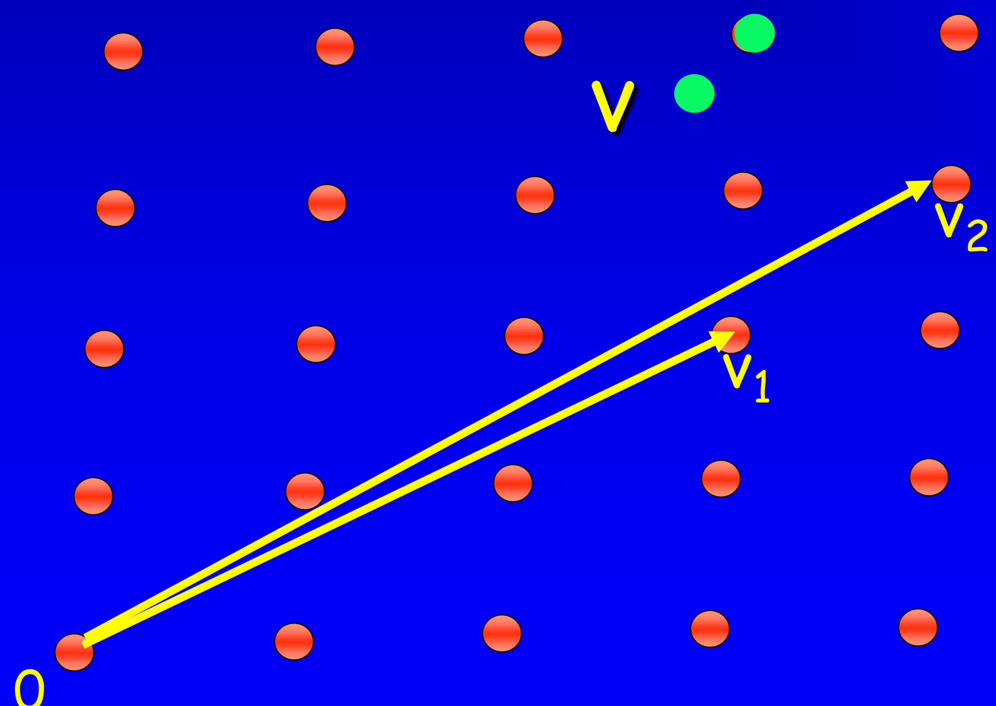
# Shortest Independent Vectors Problem (SIVP)

- SIVP$_\gamma$: Given B, find n linearly independent vectors in L(B) of length $\leq \gamma\lambda_n(L(B))$

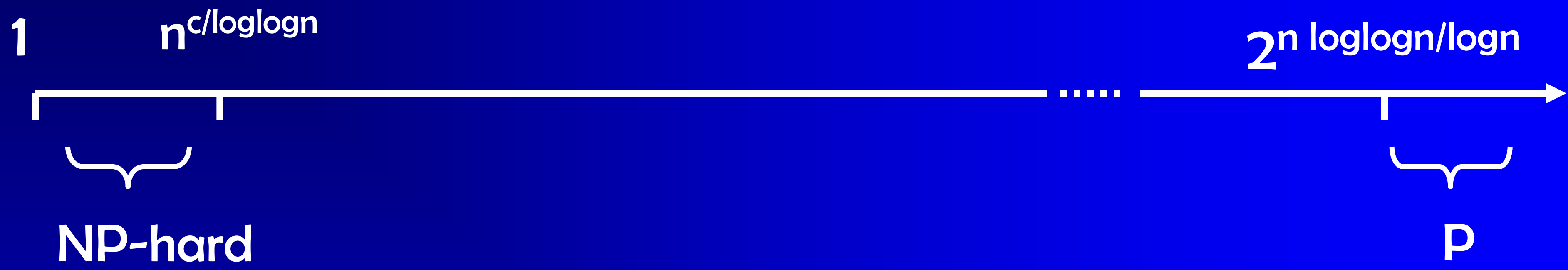


# Closest Vector Problem (CVP)

- $CVP_\gamma$: Given B and a point v, find a lattice point that is at most $\gamma$ times farther than the closest lattice point
- $SVP_\gamma$ is not harder than $CVP_\gamma$ [GoldreichMicciancioSafraSeifert99]
- BDD: find closest lattice point, given that v is already "pretty close"



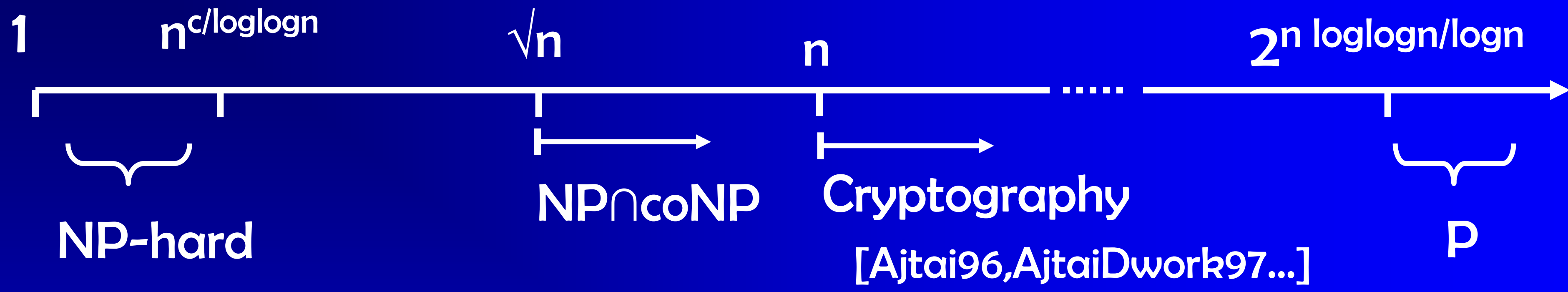
# Summary of Known Results




- Algorithms:
  - Exact algorithm in time $2^n$ [AjtaiKumarSivakumar02,MicciancioVoulgaris10,...]
  - Polytime algorithms for gap $2^{n \log\log n/\log n}$ [LLL82,Schnorr87,AjtaiKumarSivakumar02]
  - No better quantum algorithm known
- NP-hardness:
  - GapCVP: $n^{c/\log\log n}$ [...,DinurKindlerRazSafra03]
  - GapSVP: $n^{c/\log\log n}$

    [Ajtai97,Micciancio01,Khot04,HavivR07]

# Summary of Known Results




- **Cryptography:**
  - One-way functions based on $\mathrm{GapSVP}_n$ [Ajtai96,…,MicciancioR05,…]
  - Public key cryptosystems [AjtaiDwork97,R04,R05,…]
- **Limits on inapproximability:**
  - $\mathrm{GapCVP}_{\sqrt{(n/\log n)}} \in \mathrm{NP} \cap \mathrm{coAM}$ [GoldreichGoldwasser98]
  - $\mathrm{GapCVP}_{\sqrt{n}} \in \mathrm{NP} \cap \mathrm{coNP}$ [AharonovR05]

# Summary of Computational Aspects

- Approximating lattice problems (SVP, SIVP,…) to within poly(n) factors is believed to be hard:
  - Best known algorithm runs in time $2^n$ [AjtaiKumarSivakumar02]
  - No better quantum algorithm known!
  - On the other hand, not believed to be NP-hard (for approximation factors beyond $\sqrt{n}$) [GoldreichGoldwasser00, AharonovR04]

# Thanks !!