THE MATHEMATICS OF LATTICE-BASED CRYPTOGRAPHY

2. Short Integer Solutions (SIS) Problem

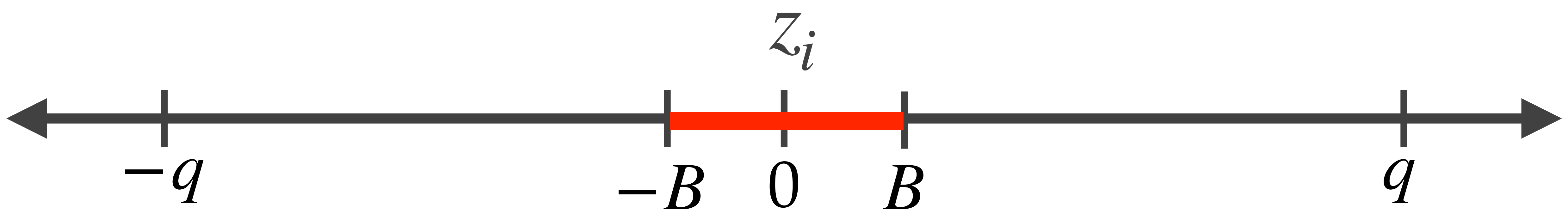
Alfred Menezes
cryptography101.ca

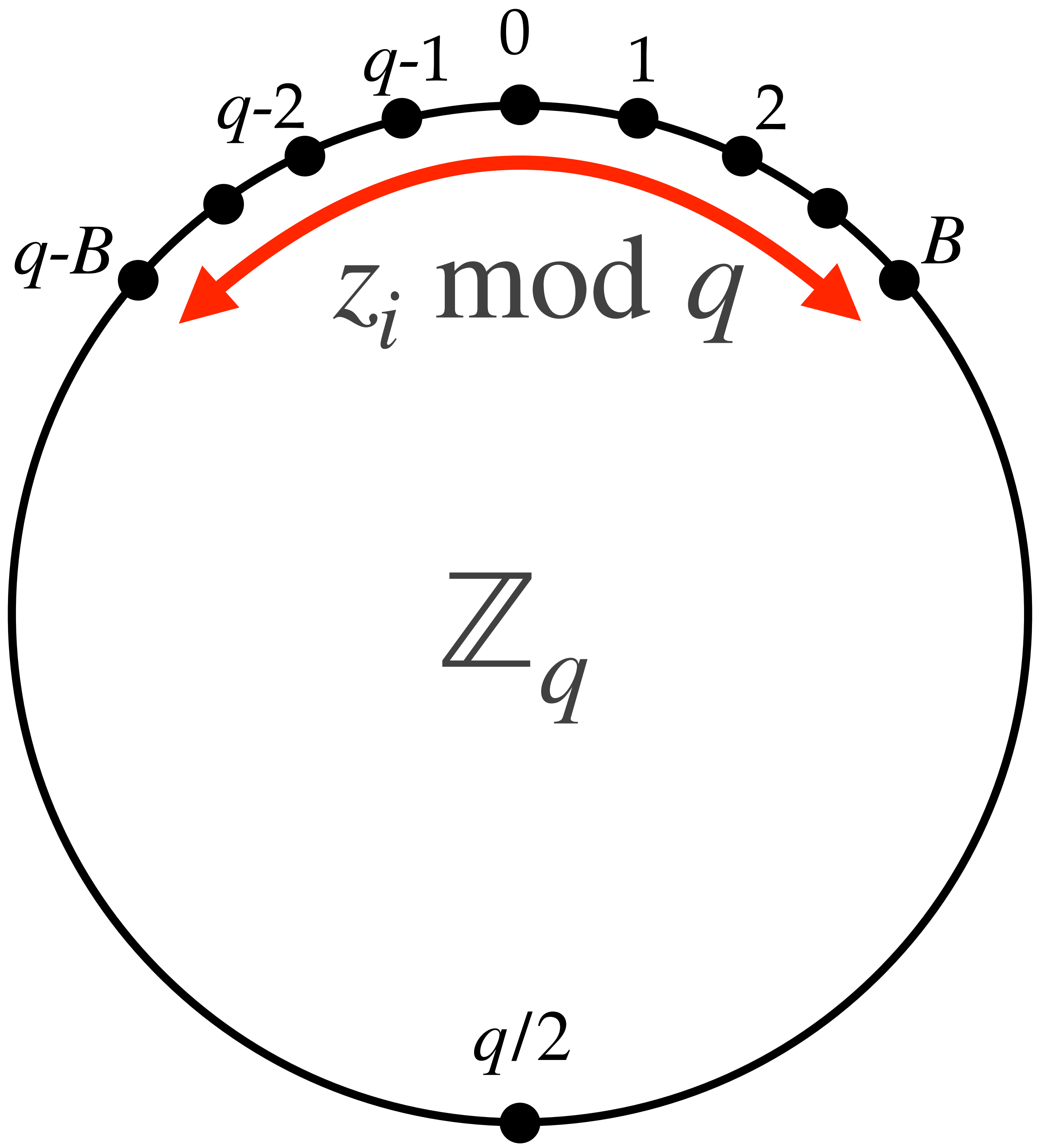
Outline

1. SIS definition
2. Collision-resistant hash function
3. ISIS definition
4. SIS and ISIS are equivalent
5. Normal-form ISIS

SIS definition

- SIS was introduced by Ajtai in 1996.
- **Definition**. (*Homogeneous*) *Short Integer Solutions problem*: SIS(n, m, q, B)
Given $A \in_R \mathbb{Z}_q^{n \times m}$, find $z \in \mathbb{Z}^m$ such that $Az = 0 \pmod{q}$, where $z \neq 0$ and $z \in [-B, B]^m$ (and $B \ll q/2$).





- **Notation**:
  1. $\mathbb{Z}_q = \{0,1,2,\ldots, q-1\}$.
  2. $x \in_R S$ means that x is selected uniformly (and independently) at random from S.
  3. All vectors are column vectors.

Existence of an SIS solution

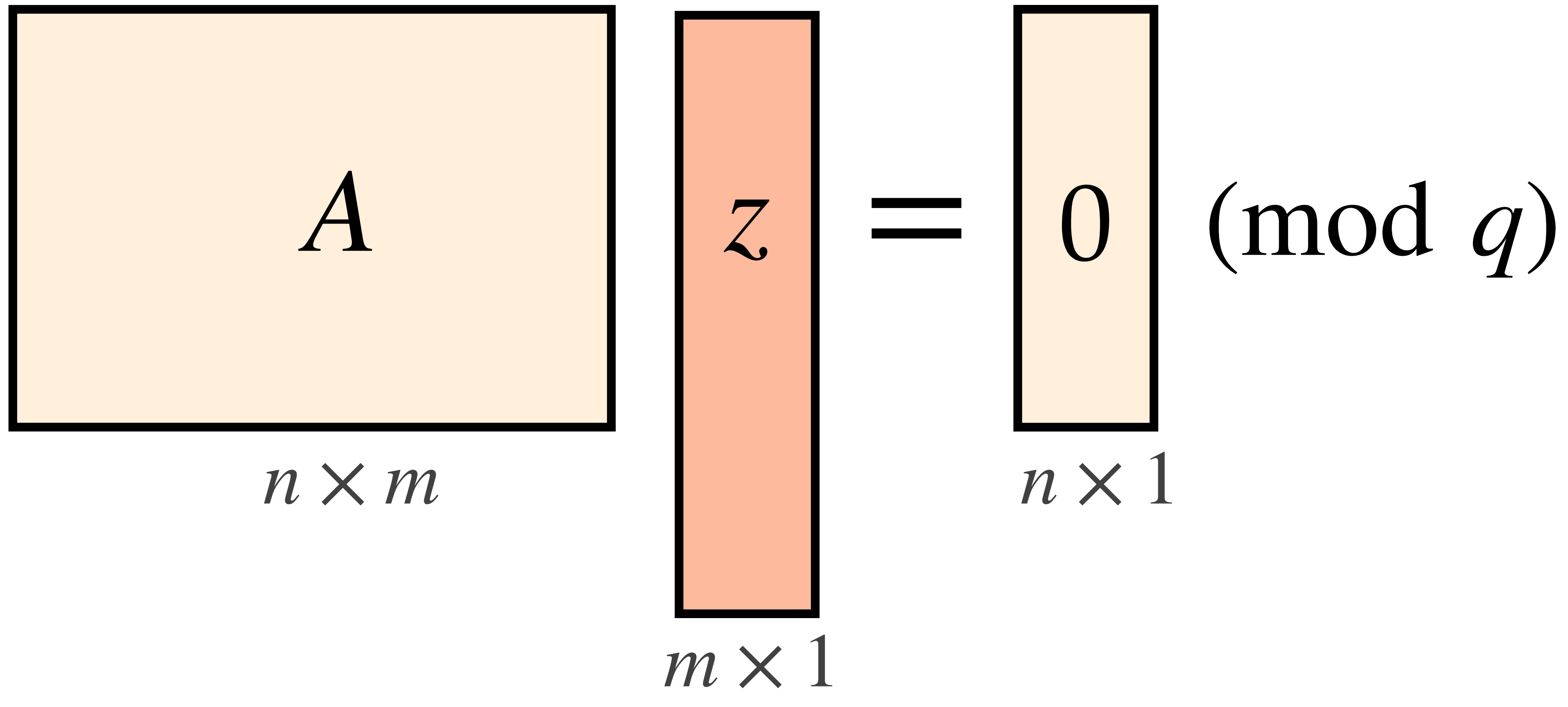
1. If $n \geq m$, then one expects that $Az = 0 \pmod{q}$ has a unique solution $z = 0$, so no SIS solution exists.
Henceforth, we'll assume that $n < m$.

2. If $(B+1)^m > q^n$, then by the pigeonhole principle there must exist $z_1, z_2 \in [-B/2, B/2]^m$ such that $z_1 \neq z_2$ and $Az_1 = Az_2 \pmod{q}$.
Then $z = z_1 - z_2$ is an SIS solution.

3. So, we'll henceforth assume that $(B+1)^m > q^n$, i.e., $m > (n \log q)/\log(B+1)$, whereby an SIS solution is guaranteed to exist.

4. The SIS solution is not unique.
Indeed, if z is an SIS solution, then so is $-z \bmod q$.

SIS: Given $A \in_R \mathbb{Z}_q^{n \times m}$, find $z \in \mathbb{Z}^m$ such that $Az = 0 \pmod{q}$, where $z \neq 0$ and $z \in [-B, B]^m$ (and $B \ll q/2$).



SIS example

- Let $n = 3$, $m = 5$, $q = 13$, and $B = 3$.
- **SIS instance:**
$$A = \begin{bmatrix} 1 & 0 & 7 & 12 & 4 \\ 2 & 11 & 3 & 6 & 12 \\ 9 & 8 & 10 & 5 & 1 \end{bmatrix}.$$
- We need to find nonzero $z = (z_1, z_2, z_3, z_4, z_5) \in [-3,3]^5$ with $Az = 0 \pmod{13}$.
- Equivalently, we have $z_i \bmod 13 \in \{0,1,2,3,10,11,12\}$.
- Performing Gaussian elimination on A yields the reduced matrix $A' = \begin{bmatrix} 1 & 0 & 0 & 5 & 10 \\ 0 & 1 & 0 & 10 & 12 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$.
- Thus the complete solution to $Az = 0 \pmod{13}$ is $z_1 = 8z_4 + 3z_5$, $z_2 = 3z_4 + z_5$, $z_3 = 12z_4 + 12z_5$, $z_4 \in \mathbb{Z}_{13}$, $z_5 \in \mathbb{Z}_{13}$.
- Among the $13^2 = 169$ solutions $z \in \mathbb{Z}_{13}^5$, are **six SIS solutions:** $z = \pm\,(3,1,\text{-}1,0,1)$, $z = \pm\,(1,0,\text{-}2,\text{-}1,3)$, and $z = \pm\,(2,1,1,1,\text{-}2)$.

SIS application: Collision-resistant hash function

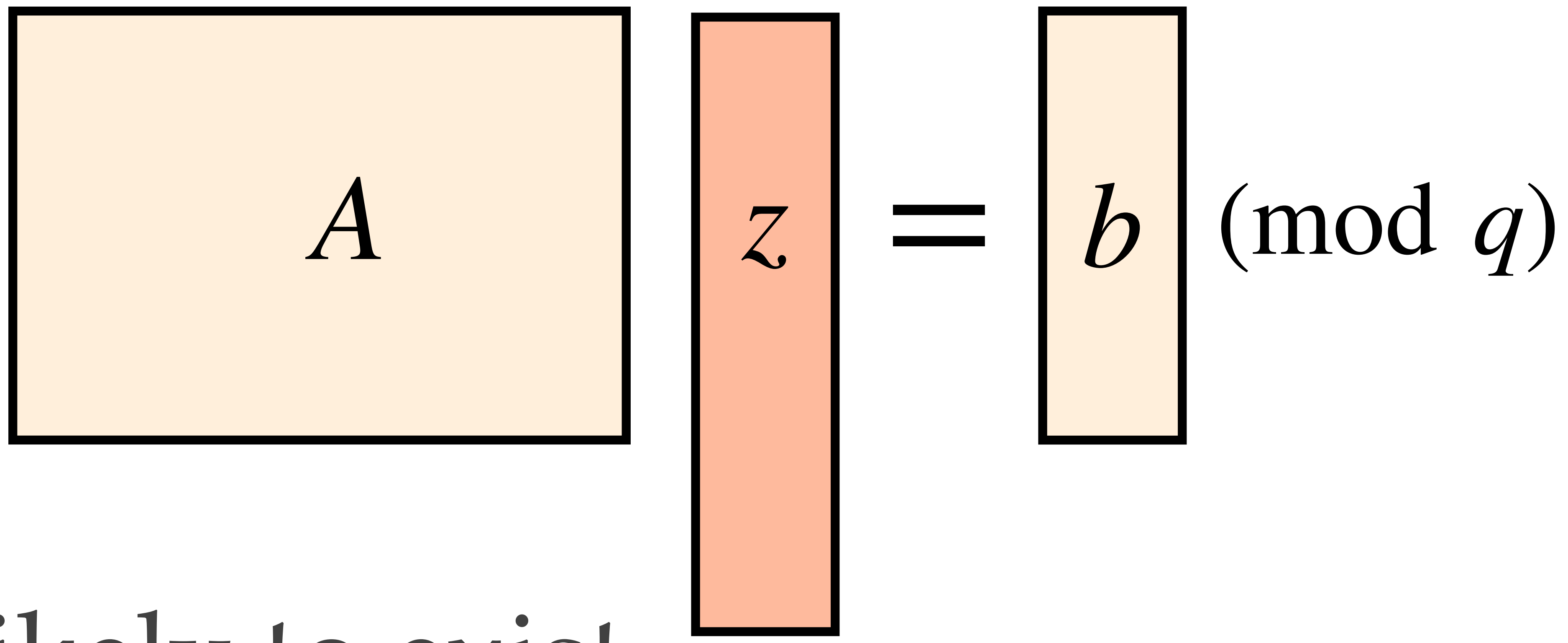
- **Hash function definition**:
  - Select $A \in_R \mathbb{Z}_q^{n \times m}$, where $m > n \log q$.
  - Define $H_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$ by $H_A(z) = Az \pmod{q}$.
- **Notes**

1. **Compression**. Since $m > n \log q$, we have $2^m > q^n$.
   Thus, H_A is indeed a compression function.

2. **Collision resistance**. Suppose that one can efficiently find $z_1, z_2 \in \{0,1\}^m$ with $z_1 \neq z_2$ and $H_A(z_1) = H_A(z_2)$. Then $Az_1 = Az_2 \pmod{q}$, whence $Az = 0 \pmod{q}$ where $z = z_1 - z_2$. Since $z \neq 0$ and $z \in [-1,1]^m$, z is an SIS solution (with $B = 1$) which has been efficiently found. $\square$

Inhomogeneous SIS (ISIS)

- **Definition**. *Inhomogeneous Short Integer Solutions problem*: ISIS(n, m, q, B)
Given $A \in_R \mathbb{Z}_q^{n \times m}$ and $b \in_R \mathbb{Z}_q^n$, find $z \in \mathbb{Z}^m$ such that $Az = b \pmod{q}$ and $z \in [-B, B]^m$.



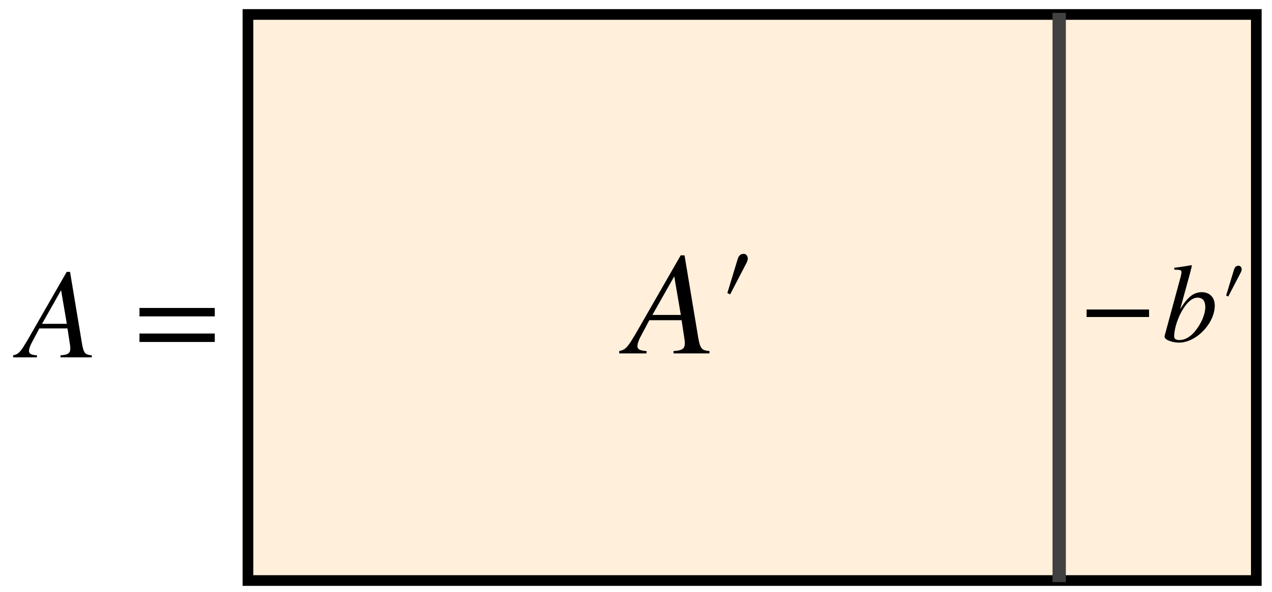
- **Notes**

1. We'll assume that $n < m$.

2. If $(2B+1)^m \gg q^n$, then an ISIS solution is likely to exist.

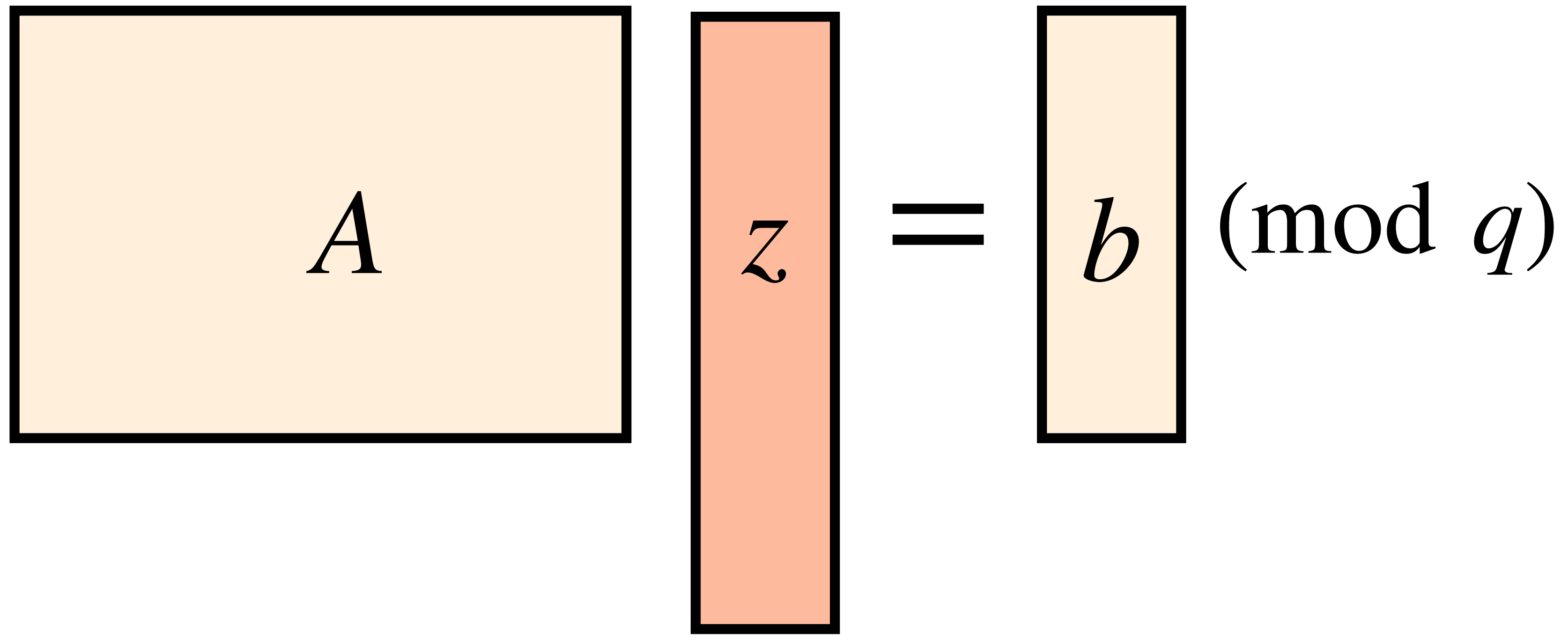
3. So, we'll henceforth assume that $(2B+1)^m \gg q^n$, i.e., $m \gg (n \log q)/\log(2B+1)$.

SIS and ISIS are equivalent (1)



- **Claim 1**. SIS $\leq$ ISIS.
- **Proof**. Let A be an SIS instance.
  Write $A = [A' \mid -b']$ where $A' \in \mathbb{Z}_q^{n\times(m-1)}$ and $b' \in \mathbb{Z}_q^n$.
  Determine an ISIS solution z' to the ISIS instance (A', b'),
  so $A'z' = b' \pmod{q}$ and $z' \in [-B, B]^{m-1}$.
  Then $z = \begin{bmatrix} z' \\ 1 \end{bmatrix} \in \mathbb{Z}^m$ satisfies $Az = 0 \pmod{q}$, $z \neq 0$, and
  $z \in [-B, B]^m$.
  Thus, z is an SIS solution that we have efficiently found. $\square$

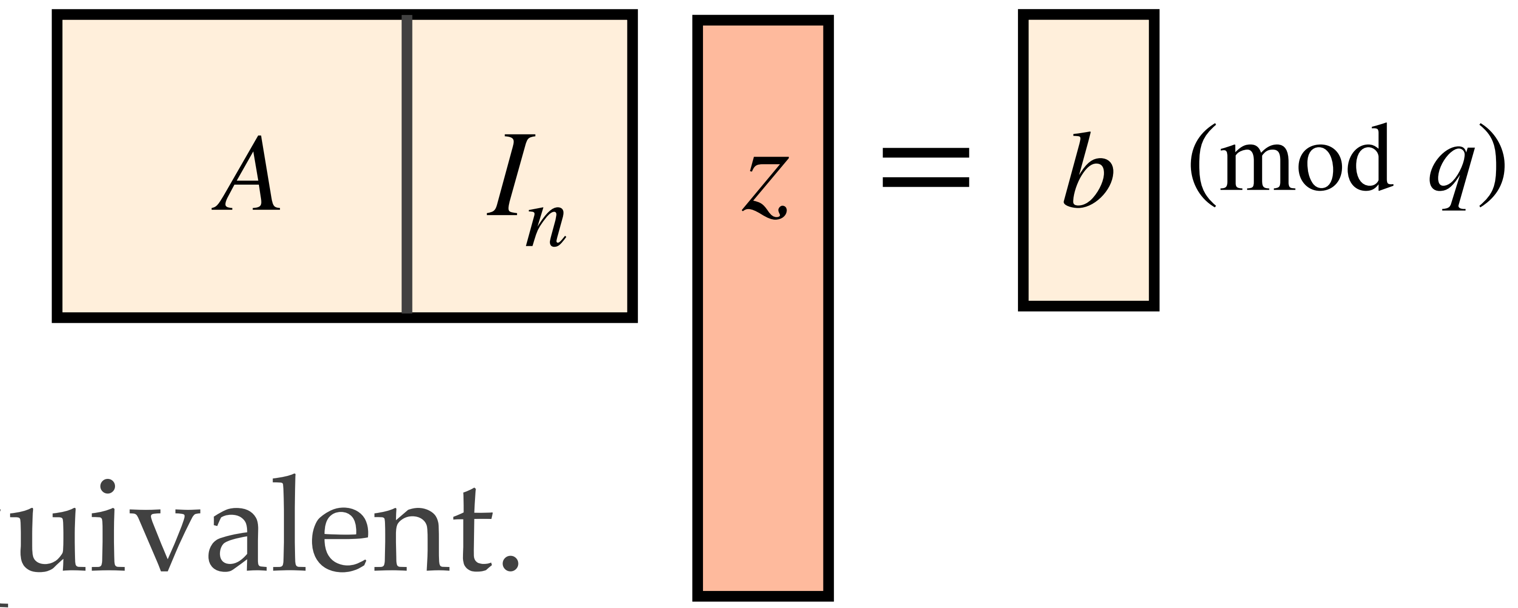
SIS and ISIS are equivalent (2)



- **Claim 2**. ISIS $\leq$ SIS.
- **Proof**. Let (A, b) be an ISIS instance.
  Select $j \in_R [1, m+1]$ and $c \in_R [-B, B]$ with $c \neq 0$.
  Let A' be the $n \times (m+1)$ matrix obtained by inserting $-c^{-1}b \bmod q$ as a new jth column in A.
  Determine an SIS solution $z' \in [-B, B]^{m+1}$ to $A'z' = 0 \pmod{q}$.
  If indeed the jth entry in z' is c, then $Az = b \pmod{q}$, where $z \in [-B, B]^m$ is obtained from z' by deleting its jth entry.
  Thus, z is an ISIS solution that we have efficiently found. $\square$

Normal-form ISIS (nf-ISIS)

- **Definition**. *Normal-form ISIS problem*: nf-ISIS(n, m, q, B)
Given $A \in_R \mathbb{Z}_q^{n\times m}$ and $b \in_R \mathbb{Z}_q^n$, find $z \in \mathbb{Z}^{m+n}$
such that $[A \,|\, I_n]z = b \pmod{q}$ and $z \in [-B, B]^{m+n}$.



- **Claim**. nf-ISIS(n, m, q, B) and ISIS$(n, m+n, q, B)$ are equivalent.

- **Proof**. (nf-ISIS $\leq$ ISIS) Given a nf-ISIS instance (A, b), select $C \in_R \mathbb{Z}_q^{n\times n}$;
C is invertible with probability roughly $(q-1)/q$. Then $([CA \,|\, C], Cb)$ is an ISIS instance with the same solution space as the nf-ISIS instance.

- (ISIS $\leq$ nf-ISIS) Given an ISIS instance (A, b), write $A = [A' \,|\, C]$; note that
C is invertible with probability roughly $(q-1)/q$. Then $([C^{-1}A' \,|\, I_n], C^{-1}b)$ is a nf-ISIS instance with the same solution space as the ISIS instance. $\square$