$f: A \to B$ "function signature"

name domain codomain

Ever element of A is mapped to <u>exactly</u> one element of B.

The range of f is the set of elements actually mapped to

$f: \mathbb{Z} \to \mathbb{Z}$ Domain = $\mathbb{Z}$ = $\{\ldots -2, -1, 0, 1, 2, \ldots\}$

$f(x) = x^2$ Codomain = $\mathbb{Z}$

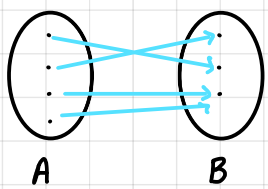
Range = $\{0, 1, 4, 9, 16, \ldots\}$

Note: When the elements of a function's domain can be listed, the function is "discrete"

In cryptography, all functions will be discrete functions with discrete domains.

Properties:

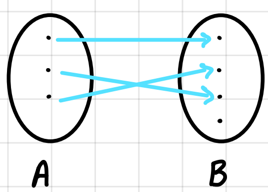
A function is onto (surjective) iff every codomain element is mapped to ≥ 1



onto b/c ≥ 1 arrowhead

Note: This is not an invertible function

One-to-One (injective) iff every codomain element is mapped to ≤ 1



one-to-one b/c ≤ 1 arrowhead

Note: This is not an invertible function

Invertible (bijective) iff every codomain element is mapped to $= 1$

A function is invertible iff it is onto and one-to-one

The domain and codomain must be the same size in an invertible function.

Table-based Mappings

def: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$f: \mathbb{Z}_4 \to \mathbb{Z}$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

x	$f(x)$
0	0
1	1
2	4
3	9

domain in-order ea. once

Range

each from codomain

Onto if $f(x)$ columns list each codomain element ≥ 1

One-to-One if $f(x)$ column lists each codomain element ≤ 1

Invertible iff every codomain element is listed $= 1$ in the $f(x)$ codomain

* Not invertible Missing elements 2, 3, 5, 6, 7, 8

Random Function:

$f: \mathbb{Z}_4 \to \{0, 1\}$

x	$f(x)$
0	0
1	1
2	0
3	0

fill each $f(x)$ with uniform value from codomain

Note: Randomness is only when the function is defined.

Fill each $f(x)$ with uniform value from codomain.

Random invertible function:

$f: \mathbb{Z}_6 \to \text{Die}$

x	$f(x)$
0	⚃
1	⚀
2	⚅
3	⚄
4	⚂
5	⚁

Fill each $f(x)$ with uniform unselected codomain value.

A function is a permutation if it is invertible and the domain and codomain are equal

$f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$

x	$f(x)$
0	1
1	3
2	0
3	2

permutation of each other

Reasoning with Tables:

Let $f: \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{20}$ be a random function

$P: \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ be a random permutation

$Pr[f(0) = 0] = 1/20$

$Pr[P(0) = 0] = 1/10$

$Pr[f(1) = 1 \mid f(0) = 0] = 1/20$

$Pr[A \mid B]$

* Each row is independent of each other

$Pr[P(1) = 1 \mid P(0) = 0] = 1/9$

* In a permutation, each element must occur only 1 time

$Pr[f(1) = 0 \mid f(0) = 0] = 1/20$

$Pr[P(1) = 0 \mid P(0) = 0] = 0/10 = 0$

* In a permutation, no repeats

x	$f(x)$
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

x	$P(x)$
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	