$$(3x+2) \bmod 7 = 4 \quad | \cdot 5$$

$$\Rightarrow x = \frac{1}{3}\cdot(4-2)$$

$$\Rightarrow 3x \bmod 7 = 2$$

To find $\frac{1}{3} \bmod 7$:

$$3 \cdot 2 = 6 \equiv -1 \bmod 7$$

$$3\cdot(-2) \bmod 7 = 3\cdot 5 \bmod 7 = 1$$

$$\Rightarrow \frac{1}{3} \bmod 7 = 5$$

$$x \bmod 7 = 2\cdot 5 \bmod 7 = 3$$

$$x - y \bmod 7 = 3 \quad -3$$

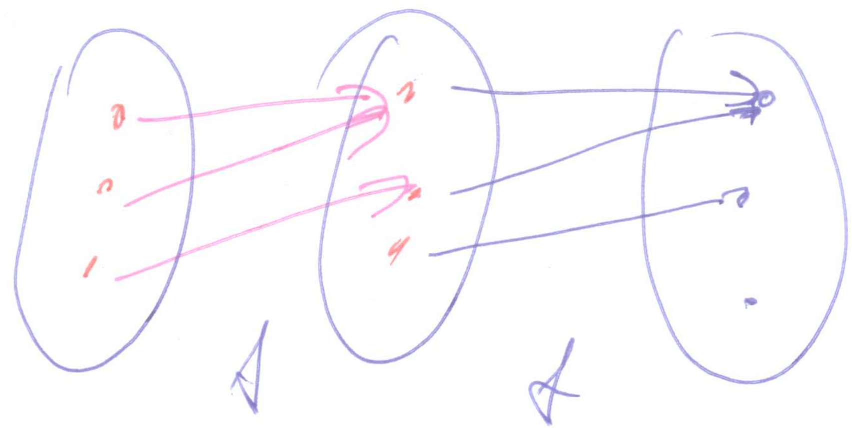
$$3x + 5y \bmod 7 = 4$$

$$-3x + 3y$$

$$8y = 1y \bmod 7$$

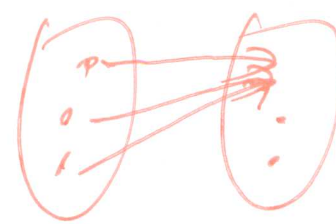
$$1y \bmod 7 = 2$$

$$-5 \bmod 7 = 2$$

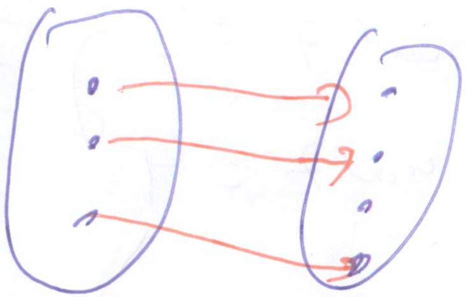


Calculate: $\frac{1}{3}\cdot\underbrace{(4-2)}_{2} \bmod 7$

$f\circ f\circ f = f\circ f$:

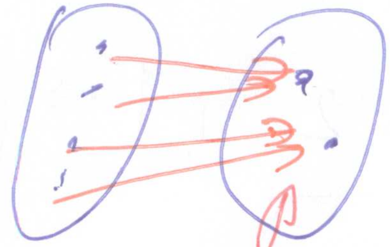


One-to-one



No two arrows to same image

Onto

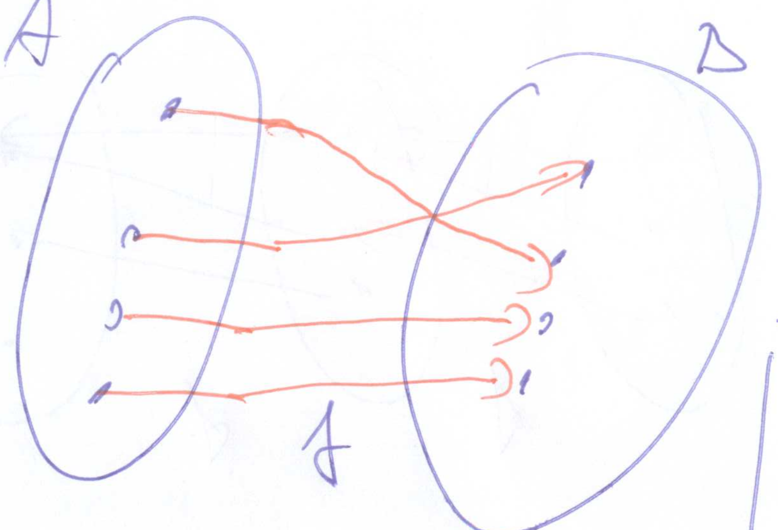


At least one arrow to every image

Onto and One-to-One: Bijective

f is

Then:



Every set has exactly one partner $f(x)$ in B

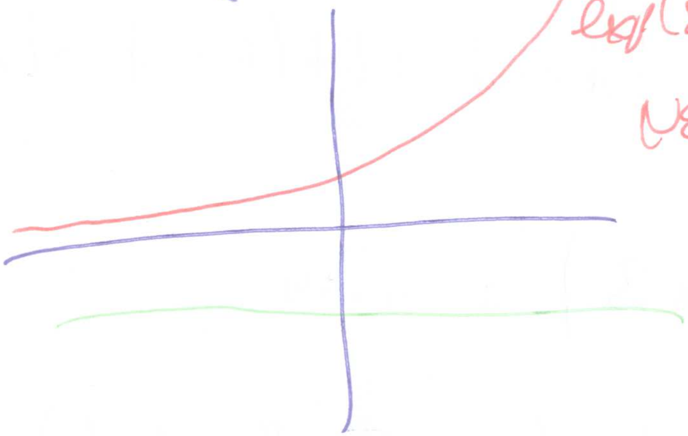
Formally: The size (cardinality) of a set A is n if there a bijective function

$f : A \to \{1, 2, 3, 4, \ldots, n\}$

Note: If $|A| = |B|$ finite

Then $f: A \to B$ is onto if and only if it is one-to-one

False if set is infinite



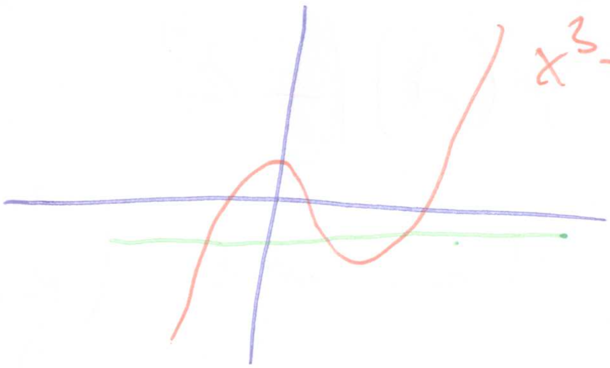
If $f: A \to B$ is ~~on~~ bijective,

then the converse relation f^{-1}

Not $\frac{1}{f}$

$\{(f(a), a) \mid a \in A\}$

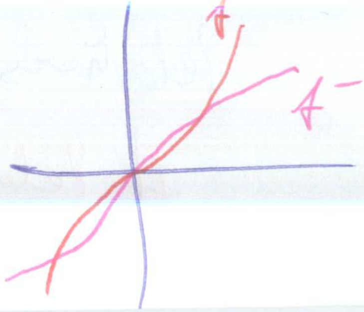
is a function. (and is also bijective)



Finding a formula for inverse fct. can be hard.

ex: $f(x) = x^3 + x \; : \mathbb{R} \to \mathbb{R}$

(One can show: onto and one-to-one



Counting formulas for sets of objects.

Assume A, B sets. $|A| = n$, $|B| = m$

Then: $|A \cup B| = |A| + |B| - |A \cap B|$

$|A \times B| = n \cdot m$

Power set (set of all subsets)

$$|\mathcal{P}(A)| = 2^n$$

$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$

Note: There are $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ subsets of size k

n choose k, Binomial Coefficient

[illegible]tions Between A and B:

Relations is $|\mathcal{P}(A \times B)| = 2^{n \cdot m}$

Functions from A to B

Imagine a function as an n-tuple of elements of B

List of images $(f(a_1), f(a_2), \dots, f(a_n))$ where $A = \{a_1, a_2, \dots, a_n\}$

$\Rightarrow m^n = \underbrace{m \cdot m \cdot \ldots \cdot m}_{n \text{ factors}}$

function from A to B.

Multiplication Table mod 7

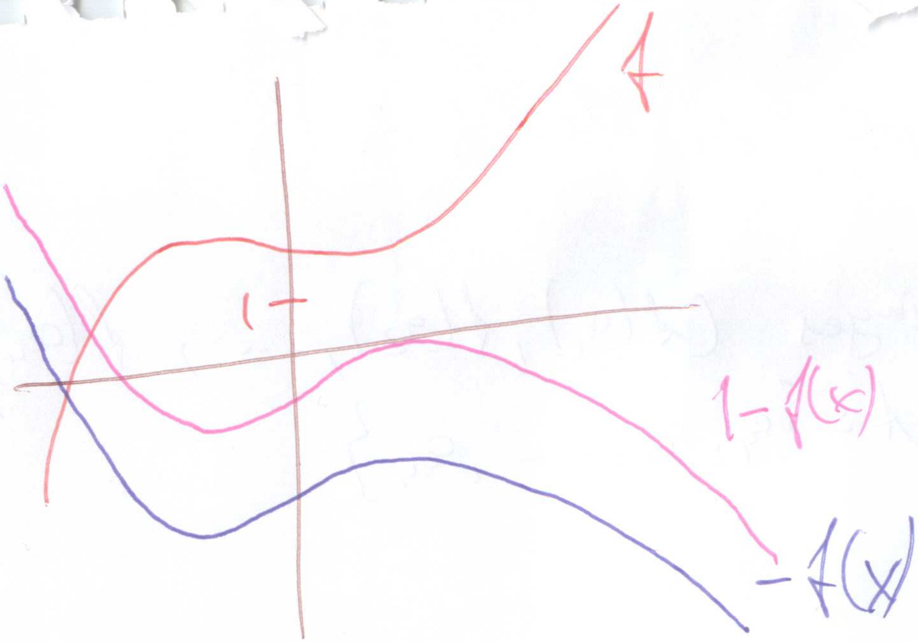
	0	1	2	3	4	5	6
3	0	3	6	2	5	1	4

$\Rightarrow \frac{1}{3} \bmod 7 = 5$

c)

$x^3 - 4x + 3 \bmod 7$

x	0	1	2	 7
	3	0	3	



$1 - f(x)$

$1 + (-f(x))$