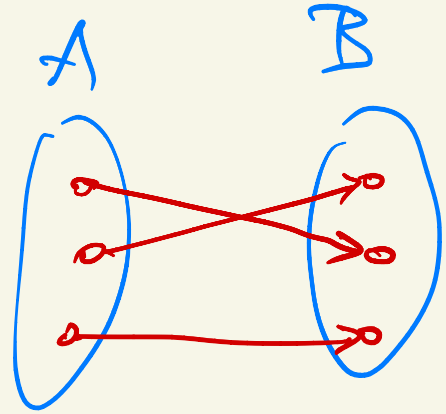
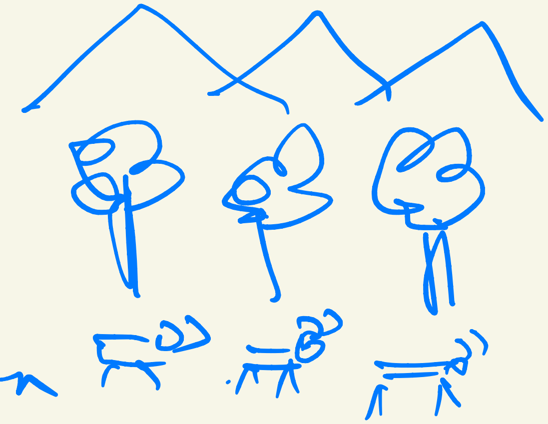
23-10-05 | 1





bijection: $f : A \to B$

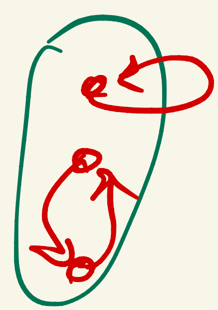
injection and surjection

1-1 correspondence

FACT $A \to B$ bijection exits $\iff |A| = |B|$

DEF Permutation of a set A:

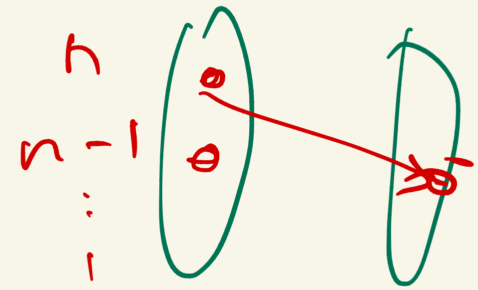
$A \to A$ bijection



$|A| = |B| = n$

\# bijections $A \to B$

$n!$ n-factorial



$\therefore$ A set A of size n has $n!$ permutations

DEF POWERSET of A $\mathcal{P}(A) = \{B \mid B \subseteq A\}$

set of all subsets

$|A| = n$

$|\mathcal{P}(A)| =$

a a b a b a a b b b

0 0 1 0 1 0 0 1 1 1

Bijection $\{a,b\}^n \longrightarrow \mathcal{P}(A)$

Strings of length n over alphabet $\{a,b\}$

$$\therefore \quad \underbrace{|\{a,b\}^n|}_{2^n} = |\mathcal{P}(A)|$$

$$\therefore \quad \boxed{\mathcal{P}(A) = 2^{|A|}}$$

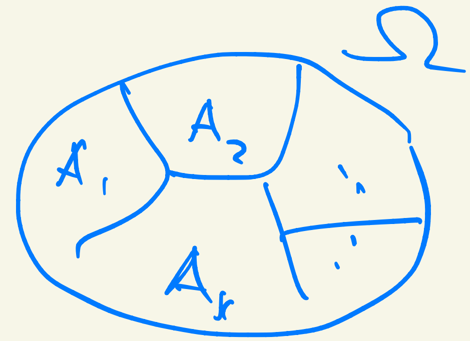
PARTITION of a set Ω: $\Pi = \{A_1, \dots, A_k\}$

$$\Omega = A_1 \,\dot\cup\, A_2 \,\dot\cup \dots \dot\cup\, A_k$$

$$A_i \neq \phi$$

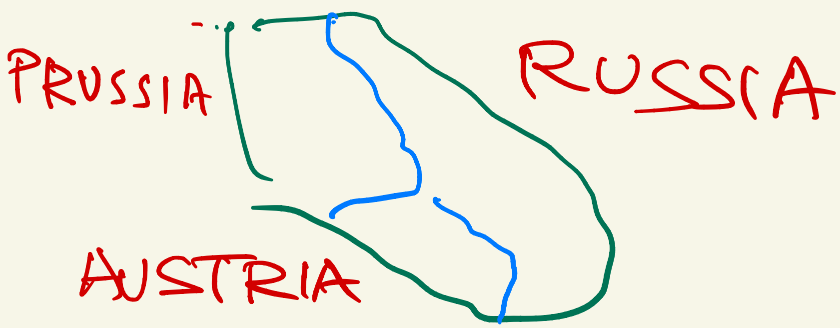
$$i \neq j \Rightarrow A_i \cap A_j = \phi \quad \text{disjoint}$$

$$\bigcup_{i=1}^{k} A_i = \Omega$$



A_i blocks

parts



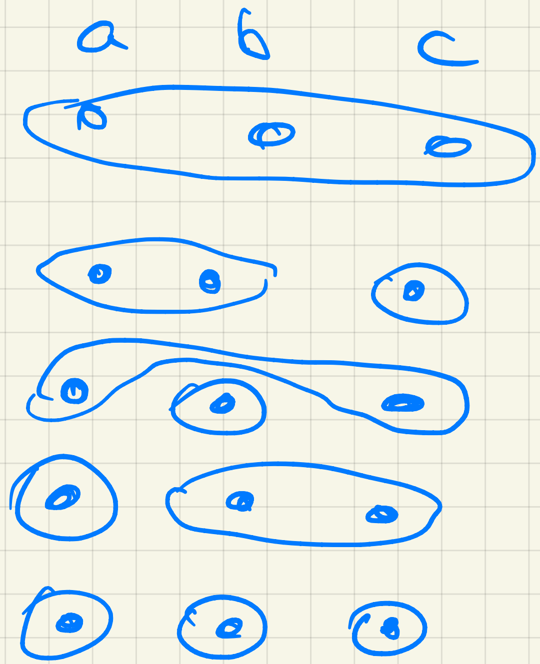
$B(n) = \#$ partitions of an n-set

$|\Omega| = n$

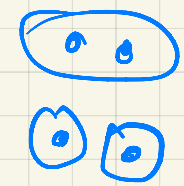
n^{th} Bell number

$n = 3$

$B(3) = 5$



$B(2) = 2$



$B(1) = 1$

$B(0) = 1$

HW $B(n) \le n!$ injective proof

6

Number theory $\mathbb{Z}$

Divisibility $a \mid b$ if $(\exists x)(ax = b)$

"a is a divisor of b"

Ex $37 \mid 999$

proof: $x = 27$

b/c $37 \cdot 27 = 999$

$0 \mid 0$

proof: $x = 72$

Additivity of divibility

7

<u>EX</u> $a \mid x \wedge a \mid y \Rightarrow a \mid x+y$

$x-y$

ASSUMPTIONS: $(\exists s,t)(x=as \wedge y=at)$

DESIRED CONCLUSION: $(\underline{\exists r})(x+y=a\cdot r)$

<u>Proof</u> (Let $r = s+t$

pick s,t

s.t. $x=as$

$y=at$

$x+y=as+at = a(s+t)$ ✓

DISTRIBUTIVITY

TRANSITIVITY OF DIVISIBILITY

$\forall a b c$

thm $(a \mid b \wedge b \mid c) \Rightarrow (a \mid c)$

$\boxed{\text{DO}}$

EX $5 \mid 15$

$15 \mid 75$

$5 \mid 75$

$\mathrm{Div}(a) = \{b : b \mid a\}$ $b \in \mathbb{Z}$

$\{b \mid b \mid a\}$

$\mathrm{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$\mathrm{Div}(1) = \{1, -1\} = \{\pm 1\}$

$(\forall x)(1 \mid x)$

$-1 \mid x$

$\mathrm{Div}(0) = \mathbb{Z}$

$\boxed{\text{DO}}$ $(\forall x)(a \mid x) \Leftrightarrow (a = \pm 1)$

$\boxed{\text{Do}}$ $(\forall x)(x \mid a) \iff \underline{\underline{a = 0}}$

<u>DEF</u> $a \equiv b \pmod{m}$ if $m \mid a - b$

<u>a</u> is congruent to <u>b</u> modulo <u>m</u>

3^{rd} is Tuesday $\Longrightarrow$ 24^{th} is Tuesday

b/c $3 \equiv 24 \mod 7$

"CALENDAR ARITHMETIC"

Fix m Congruence modulo m is

$a \equiv a \pmod{m}$ reflexive b/c $m \mid 0$ $\quad$ $[10]$

$a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ b/c $m \mid x \implies m \mid -x$

symmetric

HW $\left.\begin{array}{l} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{array}\right\} \implies a \equiv c \pmod{m}$

transitive

HW If x is odd then $x^2 \equiv 1 \pmod{8}$

HW If p is a prime number and $p \geq 5$ then $p \equiv \pm 1 \pmod{6}$

DEF p is a prime number if $p \geq 1$ and $|\mathrm{Div}(p)| = 4$

$\mathrm{Div}(5) = \{\pm 1, \pm 5\}$

$\mathrm{Div}(1) = \{\pm 1\}$

$\mathrm{Div}^+(a) = \{b \geq 0 \mid b \mid a\}$

THEOREM

"prime property"

If p is a prime and $p \mid ab$ then $p \mid a \vee p \mid b$

$\boxed{\text{DO}}$ 6 does not have the prime property

DEF x has the prime property

if $(\forall a b)(x \mid ab \Rightarrow x \mid a \vee x \mid b)$

XC Find all numbers in $\mathbb{Z}$ that have the prime property

0010100 ✓

0011001 ✗

XC If p is prime and $x^2 \equiv 1 \bmod p$

then $x \equiv \pm 1 \bmod p$