Review of Prerequisite Topics

- Logic
- Sets, sequences, relations
- Basic combinatorics: counting, summation formulas
- Elementary number theory
- Algebra
- Proofs, proof techniques (mathematical induction)

Logic: propositional and predicate calculus

Propositional calculus:

- Deals with *propositions*, which are statements that can be assigned a boolean value of true or false (1 or 0)
- Establishes rules for:
  - combining propositions into more complex propositions using boolean operations
  - reasoning about validity of propositions

Example:

$$\text{“if } \underbrace{\text{sun is yellow}}_{p} \text{ and } \underbrace{\text{cats bark}}_{q} \text{ then } \underbrace{\text{today is Monday}}_{r}\text{”}$$

$$p \wedge q \Rightarrow r$$

p , q , r are boolean variables (atomic propositions)

Logic: propositional and predicate calculus

Analyzing compound propositions using truth tables:

$p \Rightarrow q$

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

$\neg p \vee q$

p	q	$\neg p \vee q$
0	0	1
0	1	1
1	0	0
1	1	1

These propositions are equivalent!

$$p \Rightarrow q \;\equiv\; \neg p \vee q$$

Tautology: proposition that is true for all combination of values of its variables

$(p \wedge q) \Rightarrow (p \vee q)$

p	q	$p \wedge q$	$p \vee q$	$(p \wedge q) \Rightarrow (p \vee q)$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	1
1	1	1	1	1

Logic: propositional and predicate calculus

Basic laws

de Morgan laws:

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

distributive laws:

$$r \vee (p \wedge q) \equiv (r \vee p) \wedge (r \vee q)$$

$$r \wedge (p \vee q) \equiv (r \wedge p) \vee (r \wedge q)$$

double negation:

$$\neg(\neg p) \equiv p$$

…

Logic: propositional and predicate calculus

Predicate calculus:

- Extension of propositional calculus, where propositions can involve *predicates*, which are properties of elements of some domain that we want to reason about
- We can form propositions from predicates by using quantifiers ∃ and ∀

Example:

"every bird flies"

Use predicates:

$B(x) =$ "x is a bird" $\mathrm{F}(x) =$ "x flies"

Then "every bird flies" can be written as

$$\forall x \;\; B(x) \Rightarrow F(x)$$

Logic: propositional and predicate calculus

de Morgan laws extend to predicate calculus:

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Question: Is the following "distributive law" true?

$$\forall x (P(x) \vee Q(x)) \equiv \forall x P(x) \vee \forall x Q(x)$$

No, only one implication is true

$$\forall x P(x) \vee \forall x Q(x) \longrightarrow \forall x (P(x) \vee Q(x))$$

Logic: propositional and predicate calculus

Puzzle (zoom poll):

Which of the statements below is a negation of statement
"For each *X*, if *X* moos then *X* is a cow" ?

(a) "There is no X that does not moo and is not a cow"

(b) "For each X, X does not moo and X is not a cow"

(c) "For each X, if X does not moo then X is not a cow"

(d) "There exists an X that moos and is not a cow"

(e) None of the above

Logic: propositional and predicate calculus

Puzzle (zoom poll):

Which of the statements below is a negation of statement
"For each *X*, if *X* moos then *X* is a cow" ?

(a) "There is no X that does not moo and is not a cow"

(b) "For each X, X does not moo and X is not a cow"

(c) "For each X, if X does not moo then X is not a cow"

(d) "There exists an X that moos and is not a cow"

(e) None of the above

Solution:

$$\begin{aligned} \neg\forall x\, [M(x) \Rightarrow C(x)] &\equiv \neg\forall x\, [\neg M(x) \vee C(x)] \\ &\equiv \exists x\, \neg[\neg M(x) \vee C(x)] \\ &\equiv \exists x\, M(x) \wedge \neg C(x) \end{aligned}$$

So the answer is (d)

Sets: set notation, operations on sets

- Defining sets

$$
\begin{aligned}
A &= \{a, b, c\} \\
B &= \{1, 2, ..., 10\} \\
C &= \{x \in \mathbb{R} \,:\, x^3 - x^2 + x = 1\} \\
D &= \{p + q \,:\, p, q \in \mathbb{N} \text{ and } p, q \text{ are prime}\}
\end{aligned}
$$

- Relations involving sets

$$
a \in \{a, b, c, d, e\}
$$

$$
\{a, b\} \subseteq \{a, b, c, d, e\}
$$

Question: which of the following relations are true?

$1 \in \{0, \{1,2,3,4\}\}$	False
$\{1,2,3,4\} \subseteq \{0, \{1,2,3,4\}\}$	False
$\{1,2,3,4\} \in \{0, \{1,2,3,4\}\}$	True
$\{\{1,2,3,4\}\} \subseteq \{0, \{1,2,3,4\}\}$	True

Sets: set notation, operations on sets

- Basic operations on sets

$$X \cup Y \qquad X \cap Y \qquad \overline{Y}$$

- Power set of a set X : set of all subsets of X

$$\begin{aligned} X &= \{a, b, c\} \\ \mathcal{P}(X) &= \{\, \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\} \,\} \end{aligned}$$

- Cartesian product of sets X and Y: set of all ordered pairs, one from X and one from Y

$$X = \{a, b\} \qquad Y = \{1, 2, 3\}$$

$$X \times Y = \{\, (a,1), (a,2), (a,3), (b,1), (b,2), (b,3) \,\}$$

- Cardinality of X : number of elements of X

$$\begin{aligned} X &= \{a, b, c, d\} \\ |X| &= 4 \end{aligned} \qquad \begin{aligned} Y &= \{x \in \mathbf{N} : x^2 + 1 \text{ is prime}\} \\ |Y| &= ? \end{aligned}$$

It is an open problem in number theory whether this set is finite

Relations

- Let A be a set. Any subset $R \subseteq A \times A$ is called a *relation*.

in general, relations could be between different sets

Example: Some relations for $A = \mathbb{Z}$ (integers)

$$R = \{(1,3), (7,59), (2,17), (0,10)\}$$
$$Q = \{(a,b) \,:\, b = a^2\}$$
$$S = \{(a,b) \,:\, 3 | a - b\}$$

Notations for a and b being related in R :

$$(a,b) \in R \qquad aRb \qquad R(a,b)$$

Types of relations:

- Functions
- Equivalence relations
- Partial orders
- …

Relations

- An *equivalence relation* is a relation $R \subseteq A \times A$ that satisfies the following properties:
  - Reflexive: $aRa \quad \forall a \in A$
  - Symmetric: $aRb \Rightarrow bRa \quad \forall a,b \in A$
  - Transitive: $aRb \wedge bRc \Rightarrow aRc \quad \forall a,b,c \in A$

Examples:

- Isometry (in geometry)
- $S = \{(x,y) \in \mathbb{R} \times \mathbb{R} : |x| = |y| \}$
- Congruence relation for integers: $a \equiv b \pmod 5$ iff $5 \mid a - b$
- Parallel vectors:

$$D = \{((x,y),(u,v)) \in \mathbb{R}^2 \times \mathbb{R}^2 : xv = yu\}$$

Relations

Equivalence classes: $[a] = \{b \in A : aRb\}$, set of all elements in A related to a.

Theorem: If $R \subseteq A \times A$ is an equivalence relation then its equivalence classes partition A into disjoint subsets.

Example: Congruence relation for integers: $a \equiv b \pmod 5$ iff $5 \mid a - b$.
Equivalence classes:

$$
\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}
$$

Relations

Sample Problem: You are given three relations $P, Q, R \subseteq \{a,b,c,d\} \times \{a,b,c,d\}$

P	a	b	c	d
a	Y	N	Y	N
b	N	Y	N	Y
c	Y	N	Y	N
d	N	Y	N	Y

Q	a	b	c	d
a	Y	Y	N	Y
b	N	Y	N	Y
c	N	N	Y	Y
d	N	N	N	Y

R	a	b	c	d
a	Y	N	N	N
b	N	N	N	Y
c	N	N	N	Y
d	N	N	Y	N

For each relation tell (write Y or N) whether it has the listed properties:

	reflexive	transitive	symmetric	anti-symmetric	equivalence
P					
Q					
R					

Combinatorics: counting and summation formulas

Counting basic combinatorial structures:

- Functions (also sequences, tuples, vectors)
- 1-1 Functions
- k-Permutations
- Permutations
- Subsets
- k-Subsets
- ….

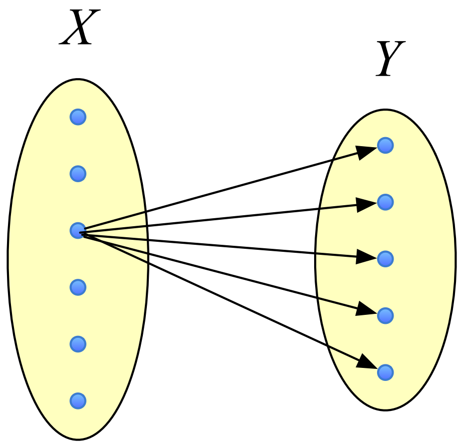
Combinatorics: counting and summation formulas

Principle of independent choices

- Simple form: $|X \times Y| = |X| \cdot |Y|$
- Generalized: If there are p choices to choose x, and for each x there are q choices to choose y, then there are pq choices of pairs (x, y)
- Extends naturally to more sets (or steps)

Combinatorics: counting and summation formulas

- Number of functions
  - $|X| = n$, $|Y| = m$
  - Compute number of functions $f : X \to Y$



Claim: There are m^n such functions

Proof: Use independence principle

- Assign a value to each $x \in X$ one by one
- We have n independent steps
- At each step there are m choices
- So the number of functions is

$$\underbrace{m \cdot m \cdot \ldots \cdot m}_{n \text{ times}} = m^n \qquad \blacksquare$$

Combinatorics: counting and summation formulas

- Number of binary strings of length n
- Number of subsets of $\{1,2, \dots ,n\}$

binary strings of length n ⟷ (1:1) functions from $\{1,2, \dots ,n\}$ to $\{0,1\}$ ⟷ (1:1) subsets of $\{1,2, \dots ,n\}$

So

- there are 2^n binary strings of length n
- there are 2^n subsets of $\{1,2, \dots ,n\}$

Example:

0 1 1 0 1

↕

x	1	2	3	4	5
$f(x)$	0	1	1	0	1

↕

$\{2,3,5\}$

Combinatorics: counting and summation formulas

- Number of 1-1 functions
  - $|X| = n$, $|Y| = m \geq n$
  - Compute number of 1-1 functions $f : X \rightarrow Y$

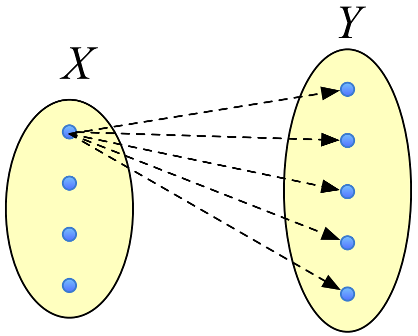
Claim: The number of such 1-1 functions is $m!/(m - n)!$

Proof: Use independence principle

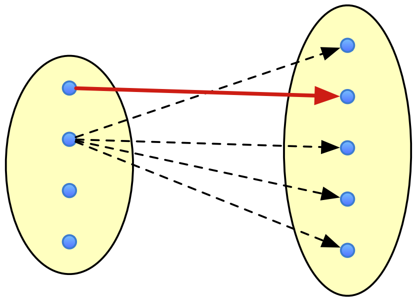
- Assign a value to each $x \in X$ one by one
- We have n steps
- At each step j there are $m - j + 1$ choices (independently of previous choices)
- So the number of 1-1 functions is

$$m \cdot (m-1) \cdot \ldots \cdot (m-n+1) = m!/(m-n)! \quad \blacksquare$$

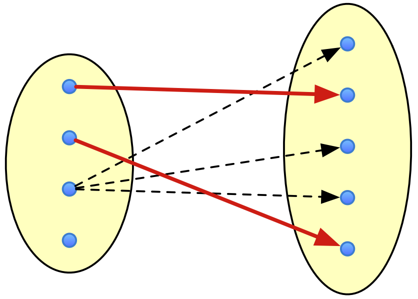
step 1:



step 2:



step 3:



Combinatorics: counting and summation formulas

Let $X = \{1,2, \ldots ,n\}$

A *permutation* of X is an ordering of elements of X

permutations of X ⟷ (1:1) 1-1 functions from X to X

Corollary: The number of permutations of X is $n!$

A k-*permutation* of X is an ordered selection of k elements of X

k-permutations of X ⟷ (1:1) 1-1 functions from $\{1,2, \ldots ,k\}$ to X

Corollary: The number of k-permutations of X is $n!/(n - k)!$

Example:

$X = \{1,2,3,4,5\}$

60 3-permutations:

$1, 2, 3$

$1, 2, 4$

$1, 2, 5$

$1, 3, 2$

$1, 3, 4$

$1, 3, 5$

$1, 4, 2$

$1, 4, 3$

$\ldots$

Combinatorics: counting and summation formulas

Let $X = \{1,2, \ldots ,n\}$

A *k-subset* of X is a subset of cardinality k

Claim: The number of k-subsets of X is $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof:

- The number of k-permutations is $n!/(n - k)!$
- Each k-subset is counted $k!$ times in the list of k-permutations ■

Example: $X = \{1,2,3,4,5\}$

60 3-permutations:

$1, 2, 3$

$1, 2, 4$

$1, 2, 5$

$1, 3, 2$

$1, 3, 4$

$\ldots$

$2, 1, 3$

$\ldots$

$2, 3, 1$

$\ldots$

$3, 1, 2$

$\ldots$

$3, 2, 1$

$\ldots$

$\{1,2,3\}$ appears 6 times

Combinatorics: counting and summation formulas

Puzzle (zoom poll):

What is the number of binary strings of length 7 that have exactly 3 1's?

- 7
- 210
- 343
- 35
- none of the above

Combinatorics: counting and summation formulas

Puzzle (zoom poll):

What is the number of binary strings of length 7 that have exactly 3 1's?

- 7
- 210
- 343
- 35
- none of the above

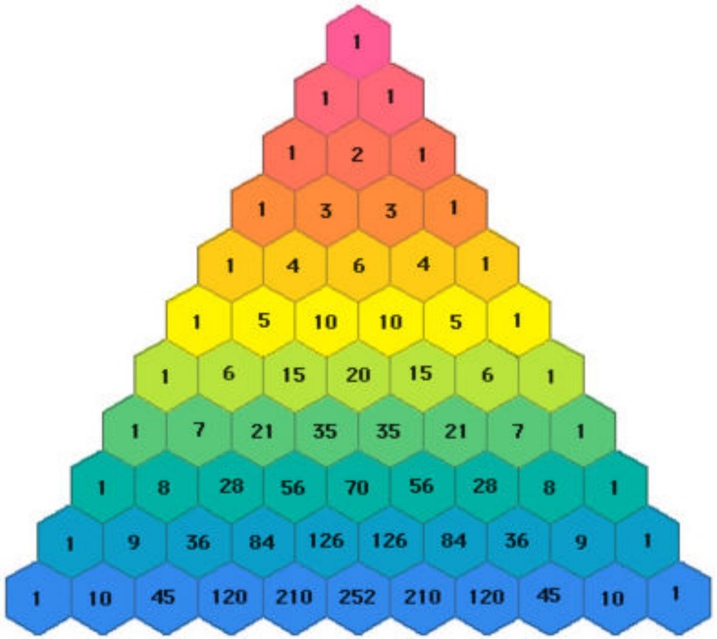
Solution: This is the same as the number of 3-subsets of $\{1,2,3,4,5,6,7\}$.

Answer: $$\binom{7}{3} = \frac{7!}{3! \cdot 4!} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7}{(1 \cdot 2 \cdot 3) \cdot (1 \cdot 2 \cdot 3 \cdot 4)} = 35$$

Combinatorics: counting and summation formulas

Let $1 \le k \le n-1$. Prove the following "Pascal triangle" equality

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

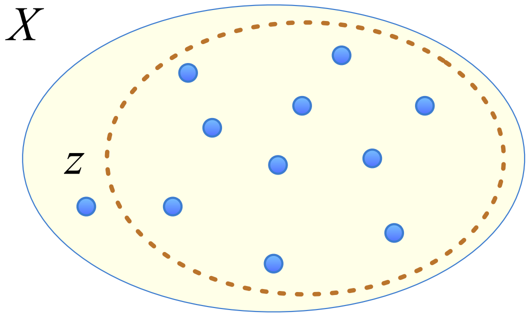


Proof: Let $X = \{1, 2, \ldots, n\}$.

The number of k-subsets of X is

Fix any $z \in X$. Consider two types of k-subsets of X:

- Those that do not contain z ⟷ (1:1) k-subsets of $X \setminus \{z\}$
- Those that contain z ⟷ (1:1) $(k-1)$-subsets of $X \setminus \{z\}$ ■



Combinatorics: counting and summation formulas

- Arithmetic sequence: $a_i = a + b \cdot i$ for $i = 0, 1, 2, \ldots$

Example:

$3, 10, 17, 24, 31, 38, \ldots$

notation for $a_0 + a_1 + \ldots + a_n$

Claim: $\sum_{i=0}^{n} a_i = \frac{1}{2}(n+1)(a_0 + a_n)$

Proof 1: Proof for sequence $0, 1, 2, \ldots, n$. We show that $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$.

1	2	3	. . . .	n-1	n
n	n-2+1	n-2	. . . .	2	1
$n+1$	$n+1$	$n+1$	. . . .	$n+1$	$n+1$

total = $n(n+1)$

We double-count, so we need to divide $n(n+1)$ by 2 ■

Combinatorics: counting and summation formulas

Proof 2: Proof for sequence $0, 1, 2, \ldots, n$. We use induction to show that $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$.

Base case. For $n = 0$, we have $\sum_{i=1}^{0} i = 0 = \frac{1}{2}0(0+1)$

Inductive step. Assume that the claim holds for $n=k$, that is $\sum_{i=1}^{k} i = \frac{1}{2}k(k+1)$.

Then for $n=k+1$, we have

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\ &= \frac{1}{2} \cdot k(k+1) + (k+1) \\ &= (k+1)(\frac{1}{2} \cdot k + 1) \\ &= \frac{1}{2}(k+1)(k+2)\end{aligned}$$

Thus the claim holds for $n=k+1$. From the base case and the inductive step, the claim holds for all n. ■

Combinatorics: counting and summation formulas

- Geometric sequence: $a_i = c \cdot a^i$ for $i = 0, 1, 2, \ldots$ for $a \neq 1$.

for simplicity, assume $c = 1$

Claim: $\sum_{i=0}^{n} a^i = \frac{a^{n+1} - 1}{a - 1}$

Example:

$2, 6, 18, 54, 162, \ldots$

Proof: Proof for sequence $1, 2, 4, \ldots, 2^n$. We show that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

$1 \quad 1 \quad 2 \quad 4 \quad \ldots \quad 2^{i-1} \quad 2^i \quad \ldots \quad 2^n$

extra 1

2

4

8

$\ldots$

2^i

2^{i+1}

$\ldots$

2^{n+1}

■

Combinatorics: counting and summation formulas

Claim: $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}$

Proof 1: We can prove it by direct calculation:

$$
\begin{aligned}
(a-1)\cdot\sum_{i=0}^{n} a^i &= a\cdot\sum_{i=0}^{n} a^i - \sum_{i=0}^{n} a^i \\
&= \sum_{i=0}^{n} a^{i+1} - \sum_{i=0}^{n} a^i \\
&= \sum_{i=1}^{n+1} a^i - \sum_{i=0}^{n} a^i \\
&= a^{n+1} - 1 \qquad \blacksquare
\end{aligned}
$$

Combinatorics: counting and summation formulas

Claim: $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}$

Proof 2: We now prove it using mathematical induction:

Base case. For $n=0$, we have $\text{LHS} = \sum_{i=0}^{0} a^i = a^0 = 1$ and $\text{RHS} = 1$

Inductive step. Assume that the claim holds for $n=k$, that is $\sum_{i=0}^{k} a^i = \frac{a^{k+1}-1}{a-1}$

Then for $n=k+1$, we have

$$\begin{aligned}\sum_{i=0}^{k+1} a^i &= \sum_{i=0}^{k} a^i + a^{k+1} \\ &= \frac{a^{k+1}-1}{a-1} + a^{k+1} \\ &= \frac{a^{k+1}-1+(a-1)a^{k+1}}{a-1} \\ &= \frac{a^{k+2}-1}{a-1}\end{aligned}$$

Thus the claim holds for $n=k+1$. From the base case and the inductive step, the claim holds for all n. ■

Elementary number theory

- prime and composite numbers
- factorization
- greatest common divisor
- basic modular arithmetic

Elementary number theory

Integer numbers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

A natural number $p > 1$ is *prime* iff its only divisors are 1 and p. Otherwise it is called *composite*.

Example: first 15 primes 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 …

Fundamental Theorem of Arithmetic: Every positive natural number has a unique representation as a product of prime numbers.

Example:

prime factors of 84: 2,3,7

factorization of 84

$$84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^1 \cdot 7^1$$

$$16335 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 11 \cdot 11 = 3^3 \cdot 5^1 \cdot 11^2$$

Elementary number theory

Theorem: There are infinitely many prime numbers.

Proof: We give an argument by contradiction. Suppose that there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_t$.

Consider $q = p_1 p_2 \cdots p_t + 1$. We have that $p_1 p_2 \cdots p_t$ is a multiple of each p_i and the next multiple of p_i is $p_1 p_2 \cdots p_t + p_i > q$. So q is not a multiple of any p_i.
This means that the prime factors of q are not not among $p_1, p_2, \ldots, p_t$ — contradiction with the assumption that only $p_1, p_2, \ldots, p_t$ are primes. ∎

This proof was given by Euclid circa 300 BC !!

Elementary number theory

- Greatest common divisor $\gcd(a,b)$: Largest $c \in \mathbb{N}$ such that $c|a$ and $c|b$

Example: $\gcd(15, 27) = 3$ $\gcd(16335, 693) = 99$

Theorem: Let the factorizations of a and b be

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}.$$

Then $\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \ldots p_t^{\min(\alpha_t,\beta_t)}$.

Example: $16335 = 3^3 \cdot 5^1 \cdot 7^0 \cdot 11^2$ and $693 = 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^1$

So $\gcd(16335, 693) = 3^2 \cdot 11^1 = 99$

Numbers a, $b \in \mathbb{N}$ are called *relatively prime (a.k.a. co-prime)* iff $\gcd(a,b) = 1$

Example: $\gcd(15, 22) = 1$ $\gcd(128, 81) = 1$

Elementary number theory

Puzzle (zoom poll): Are numbers 273 and 605 relatively prime? (True/False)

Elementary number theory

Puzzle (zoom poll): Are numbers 273 and 605 relatively prime? (True/False)

Solution: Factor these numbers: $253 = 3 \cdot 7 \cdot 13$ $\quad$ $605 = 5 \cdot 11 \cdot 11$

Answer: Yes

Elementary number theory

- Modular arithmetic

Theorem: For any $a, b \in \mathbb{Z}$ there are $q \in \mathbb{N}$ and $r \in \{0,1,\ldots,q\text{-}1\}$ such that $a = b \cdot q + r$

$q = \lfloor a/b \rfloor$ $r = a$ rem b

remainder of a/b, also denoted $a \bmod b$

Congruence relation: a and b are congruent modulo m, denoted $a \equiv b \pmod{m}$, iff $a \text{ rem } m = b \text{ rem } m$ (or, equivalently $m \mid a - b$).

caution: different meaning of "mod"

Example:

$$68 \equiv 12 \pmod{7}$$
$$57 \not\equiv 23 \pmod{11}$$

Elementary number theory

Theorem: For any fixed m, relation $a \equiv b \pmod{m}$ is an equivalence relation on $\mathbb{Z}$.

Proof: We just need to verify the conditions of equivalence relations:

- Reflexive: $a \equiv a \pmod{m}$ ✓
- Symmetric: $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$ ✓
- Transitive: $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$ ✓

For transitivity, if $m \mid a-b$ and $m \mid b-c$ then $m \mid (a-b) + (b-c)$. So $m \mid a-c$. ■

Theorem: Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

$a+c \equiv b+d \pmod{m}$ and $a \cdot c \equiv b \cdot d \pmod{m}$.

Algebra

- Solving equations: linear, quadratic, polynomial
- Systems of linear equations
- Linear algebra (matrix multiplication)

Algebra

Solve $x^3 - 2x^2 - 2x + 4 = 0$

- If there is an integral root, must be a divisor of 4
- Candidates: $-4\,, -2\,, -1\,, 1\,, 2\,, 4$
- $x = 2$ works
- Factor:

$$x^3 - 2x^2 - 2x + 4 = (x - 2)(x^2 - 2) = 0$$

- So the roots are $2\,, \sqrt{2}\,,\ -\sqrt{2}$

Algebra

Matrix multiplication

what is this value?

$$\overset{A}{\begin{bmatrix} 3 & -1 & 2 \\ 0 & 1 & -2 \\ 1 & 0 & 2 \end{bmatrix}} \times \overset{B}{\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & 3 \\ -1 & 4 & 1 \end{bmatrix}} = \overset{C}{\begin{bmatrix} ? & ? & ? \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix}}$$

Question: What is C_{11} ?

Algebra

Matrix multiplication

$$\overset{A}{\begin{bmatrix} 3 & -1 & 2 \\ 0 & 1 & -2 \\ 1 & 0 & 2 \end{bmatrix}} \times \overset{B}{\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & 3 \\ -1 & 4 & 1 \end{bmatrix}} = \overset{C}{\begin{bmatrix} -1 & 8 & -4 \\ 4 & -8 & 1 \\ -1 & 8 & 1 \end{bmatrix}}$$

Question: What is C_{11} ?

Answer: -1

Proofs

A *proof* is a rigorous argument justifying validity of a mathematical statement, showing that this statement logically follows from the assumptions.

Earlier slides have proofs of

- Formulas for the number of functions, 1-1 functions, permutations, subsets, ….
- Summation formulas for arithmetic and geometric sequences (including two proofs using induction)
- Pascal triangle equality
- That there are infinitely many primes (proof by contradiction)

Proofs

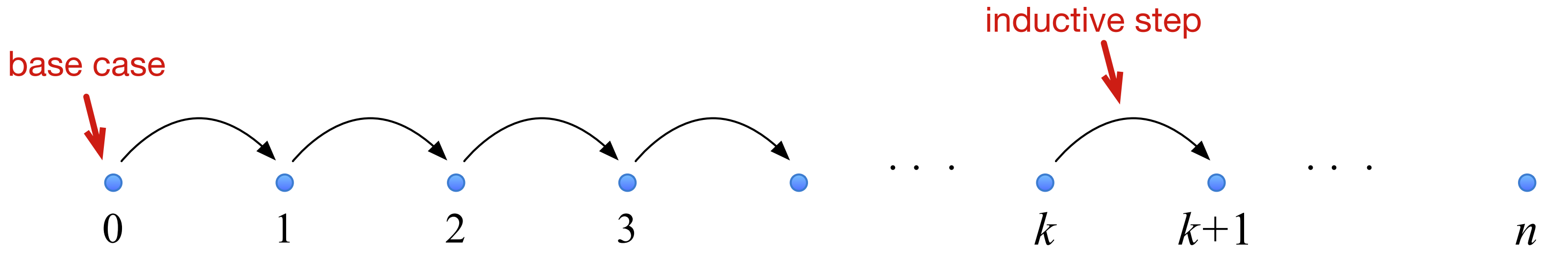
- *Mathematical induction*: technique for proving properties of integers

To prove that $\forall n\ \mathcal{P}(n)$ holds, show the following:

- Base case: $\mathcal{P}(0)$
- Inductive step: $\forall k\ \mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$

← (Note: $\forall n$ is shorthand for $\forall n \in \mathbb{N}$)

Intuition: boostraping property $\mathcal{P}(n)$:



Variants:

- Base case could be $\mathcal{P}(n_0)$, for some n_0. Then the proof shows that $\forall n \geq n_0\ \mathcal{P}(n)$.
- In strong induction, the inductive step is: $\forall k\ [\forall i \leq k\ \mathcal{P}(i)\ ] \Rightarrow \mathcal{P}(k+1)$.

Proofs

Claim: $\forall n \;\; 5 | 7^n - 2^n$

Example:

$$\begin{aligned} 7^3 - 2^3 &= 343 - 8 \\ &= 335 \end{aligned}$$

Proof: We apply mathematical induction.

Base case. For $n = 0$, we have $7^0 - 2^0 = 0 = 5 \cdot 0$.

Inductive step. Consider $k \in \mathbb{N}$. Assume that the claim holds for $n = k$, that is $7^k - 2^k = 5 \cdot b$ for some $b \in \mathbb{N}$.

Then for $n = k+1$, we have

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7 \cdot 7^k - 2 \cdot 2^k \\ &= 5 \cdot 7^k + 2 \cdot (7^k - 2^k) \\ &= 5 \cdot 7^k + 2 \cdot (5b) \\ &= 5 \cdot (7^k + 2b) \end{aligned}$$

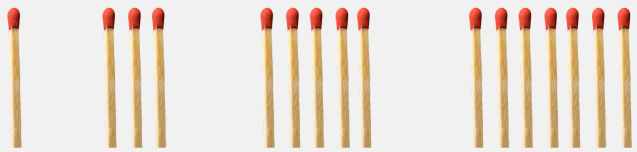
here we use inductive assumption

So $7^{k+1} - 2^{k+1}$ is a multiple of 5, completing the inductive step. ∎

Power of proofs: Game of NIM

Game of NIM:

- In the beginning there are 5 piles of matchsticks:



- Players alternate moves
- At each turn, a player can remove any number of sticks from one pile
- The player that removes the last stick wins

at least one

Power of proofs: Game of NIM

Play:

Power of proofs: Game of NIM

Game of NIM:

- In the beginning there are 5 piles of matchsticks:
- Players alternate moves
- At each turn, a player can remove any number of sticks from one pile
- The player that removes the last stick wins

We will prove the following theorem:

Theorem: The 2nd player has a winning strategy: If she follows this strategy, she is guaranteed to win, no matter how the 1st player moves.

Power of proofs: Game of NIM

Nimsum of numbers: bit-wise xor operation

in our version of NIM, $k = 4$

To compute $y = \text{nimsum}(x_1, x_2, \ldots, x_k)$ do this:

- Convert each $x_1, x_2, \ldots, x_k$ into binary
- For each bit i, xor the i-th bits of all $x_1, x_2, \ldots, x_k$, the result is the i-th bit of y
- Convert these bits into decimal representation of y

parity of number of 1's: 0 if even, 1 if odd

this won't be important, we will only care whether nim-sum is 0 or not

Power of proofs: Game of NIM

Nimsum of numbers: bit-wise xor operation

To compute $y = \text{nimsum}(x_1, x_2, ..., x_k)$ do this:

- Convert each $x_1, x_2, ..., x_k$ into binary
- For each bit i, xor the i-th bits of all $x_1, x_2, ..., x_k$, the result is the i-th bit of y
- Convert these bits into decimal representation of y

Example 1: nimsum$(1,3,5,7)$

$$\begin{aligned} 1 &= 0\,0\,0\,1 \\ 3 &= 0\,0\,1\,1 \\ 5 &= 0\,1\,0\,1 \\ 7 &= 0\,1\,1\,1 \\ \hline \text{nimsum} &= 0\,0\,0\,0 \;=\; 0 \end{aligned}$$

Example 2: nimsum$(11,13,7,5,6)$

$$\begin{aligned} 11 &= 1\,0\,1\,1 \\ 13 &= 1\,1\,0\,1 \\ 7 &= 0\,1\,1\,1 \\ 5 &= 0\,1\,0\,1 \\ 6 &= 0\,1\,1\,0 \\ \hline \text{nimsum} &= 0\,0\,1\,0 \;=\; 2 \end{aligned}$$

Power of proofs: Game of NIM

Nimsum of numbers: bit-wise xor operation

To compute $y = \text{nimsum}(x_1, x_2, \ldots, x_k)$ do this:

- Convert each $x_1, x_2, \ldots, x_k$ into binary
- For each bit i, xor the i-th bits of all $x_1, x_2, \ldots, x_k$, the result is the i-th bit of y
- Convert these bits into decimal representation of y

Zoom poll: what is nimsum$(1,3,9,13)$?

- 3
- 7
- 0
- 6
- 2

Power of proofs: Game of NIM

Nimsum of numbers: bit-wise xor operation

To compute $y = \text{nimsum}(x_1, x_2, \ldots, x_k)$ do this:

- Convert each $x_1, x_2, \ldots, x_k$ into binary
- For each bit i, xor the i-th bits of all $x_1, x_2, \ldots, x_k$, the result is the i-th bit of y
- Convert these bits into decimal representation of y

Zoom poll: what is nimsum$(1,3,9,13)$?

- 3
- 7
- 0
- 6
- 2

Answer: 6

$$
\begin{aligned}
1 &= 0\,0\,0\,1 \\
3 &= 0\,0\,1\,1 \\
9 &= 1\,0\,0\,1 \\
13 &= 1\,1\,0\,1 \\
\hline
\text{nimsum} &= 0\,1\,1\,0 = 6
\end{aligned}
$$

Power of proofs: Game of NIM

Let $x = (x_1, x_2, \ldots, x_k)$ be a configuration.

Lemma 1: If nimsum$(x) = 0$ then all moves from x go to non-0 minsum configurations.

Lemma 2: If nimsum$(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.

$\forall$ moves

$\exists$ move

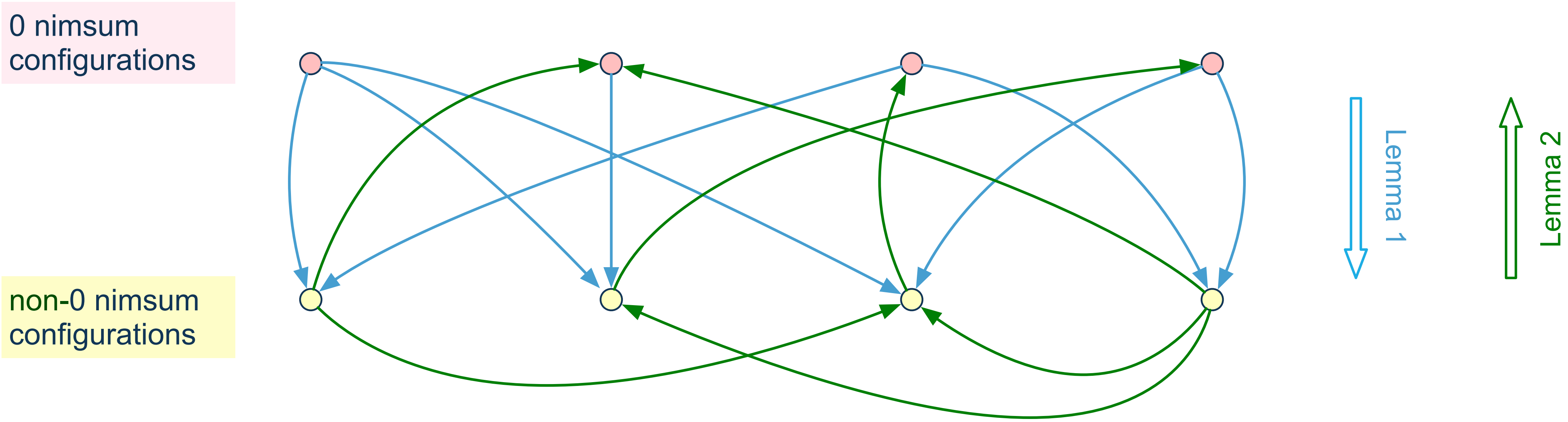
Quantifiers are important !!!

Power of proofs: Game of NIM

Let $x = (x_1, x_2, \ldots, x_k)$ be a configuration.

Lemma 1: If nimsum$(x) = 0$ then all moves from x go to non-0 nimsum configurations.

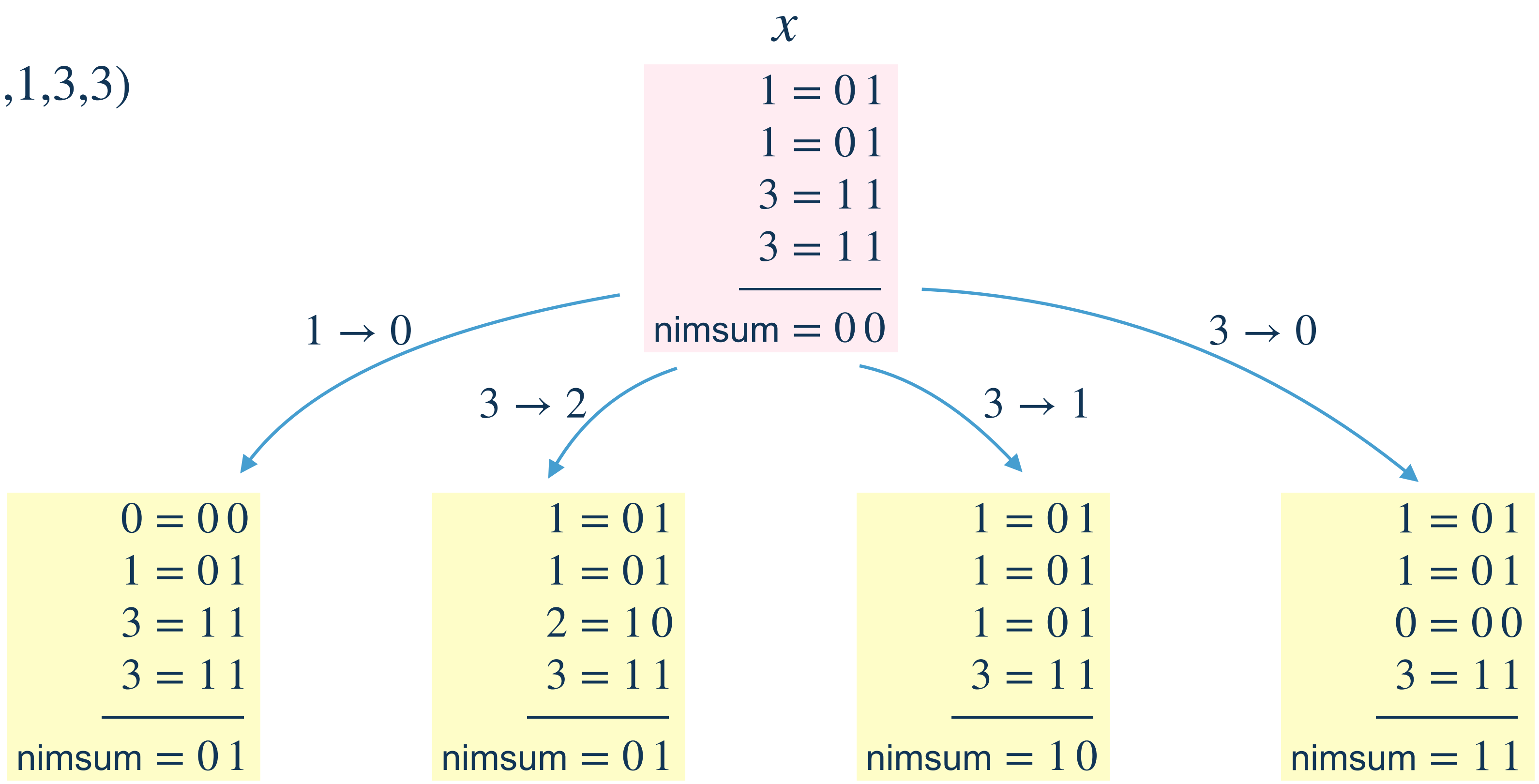
Lemma 2: If nimsum$(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.



Power of proofs: Game of NIM

Lemma 1: If nimsum$(x) = 0$ then all moves from x go to non-0 nimsum configurations.

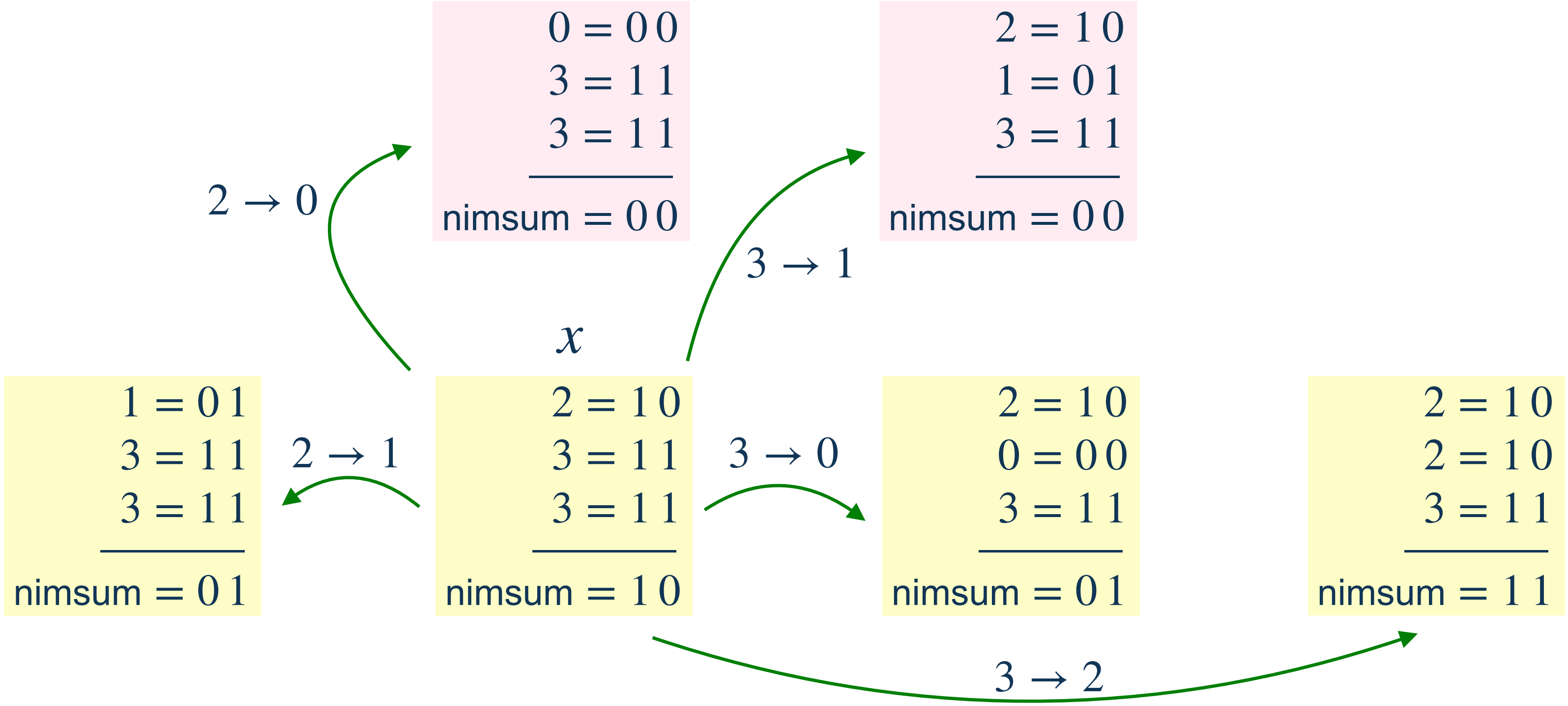
Example: $x = (1,1,3,3)$



Power of proofs: Game of NIM

Lemma 2: If nimsum$(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.

Example: $x = (2,3,3)$



Power of proofs: Game of NIM

Lemma 1: If nimsum$(x) = 0$ then all moves from x go to non-0nimsum configurations.

Lemma 2: If nimsum$(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.

Proof of Theorem: Lemmas 1,2 give the following strategy of Player 2: *At each step move to a configuration with non-0 minsum*.

Then *Player 1 will be always in a 0-nimsum configuration* and *Player 2 will be always in a non-0 nimsum configuration*, because:

- Player 1 starts in a 0-nimsum configuration $(1,3,5,7)$
- If Player 1 is in a 0-nimsum configuration, shen can only go to a non-0 nimsum configuration (by Lemma 1)
- If Player 2 is in a non-0 nimsum configuration, she can move to a 0-nimsum configuration (by Lemma 2)

At each step at least one x_i decreases. So the game must end up in $(0,0,0,0)$, which is a configuration of Player 1 because its nimsum is 0. Thus Player 2 wins !! ■

Power of proofs: Game of NIM

Lemma 1: If $\text{nimsum}(x) = 0$ then all moves from x go to non-0 nimsum configurations.

Proof: Let $y = \text{nimsum}(x)$. If we change some x_i then at least one bit of x_i flips. Then the same bit of y flips, making y non-zero.

$$\begin{array}{rcl} x_1 & = & 0\,1\,1\,1\,0\,0\,1\,1\,0\,0 \\ x_2 & = & 1\,1\,1\,1\,0\,0\,0\,0\,1\,0 \\ & \cdots & \\ x_i & = & 0\,0\,1\,0\,0\,1\,1\,0\,0\,1 \\ & \cdots & \\ x_k & = & 1\,1\,0\,1\,1\,1\,0\,1\,0\,1 \\ \hline y & = & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \end{array} \quad \longrightarrow \quad \begin{array}{rcl} x_1 & = & 0\,1\,1\,1\,0\,0\,1\,1\,0\,0 \\ x_2 & = & 1\,1\,1\,1\,0\,0\,0\,0\,1\,0 \\ & \cdots & \\ x_i & = & 0\,0\,0\,0\,0\,1\,1\,1\,0\,1 \\ & \cdots & \\ x_k & = & 1\,1\,0\,1\,1\,1\,0\,1\,0\,1 \\ \hline y & = & 0\,0\,1\,0\,0\,0\,0\,1\,0\,0 \end{array}$$

∎

Power of proofs: Game of NIM

Lemma 2: If $\text{nimsum}(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.

Proof: Let $y = \text{nimsum}(x)$. Which x_i to change and how?

First attemp: Choose *any* x_i and flip its bits which are 1 in y. This will change y to 0:

$$
\begin{array}{rcl}
x_1 &=& 1\,0\,1\,1\,0\,0\,1\,1\,0\,1\\
x_2 &=& 0\,1\,0\,1\,1\,0\,0\,0\,1\,1\\
&\cdots&\\
x_i &=& 1\,0\,0\,0\,1\,1\,1\,0\,1\,0\\
&\cdots&\\
x_k &=& 1\,1\,0\,1\,1\,1\,0\,1\,0\,1\\
\hline
y &=& 0\,0\,1\,0\,1\,0\,0\,0\,1\,0
\end{array}
\quad \longrightarrow \quad
\begin{array}{rcl}
x_1 &=& 1\,0\,1\,1\,0\,0\,1\,1\,0\,1\\
x_2 &=& 0\,1\,0\,1\,1\,0\,0\,0\,1\,1\\
&\cdots&\\
x_i &=& 1\,0\,1\,0\,0\,1\,1\,0\,0\,0\\
&\cdots&\\
x_k &=& 1\,1\,0\,1\,1\,1\,0\,1\,0\,1\\
\hline
y &=& 0\,0\,0\,0\,0\,0\,0\,0\,0\,0
\end{array}
$$

Problem: If the first bit in x_i we flipped was 0, this increases the value of x_i !

Power of proofs: Game of NIM

Lemma 2: If nimsum$(x) \neq 0$ then some move from x goes to a 0-nimsum configuration.

Proof: Let $y =$ nimsum(x). Which x_i to change and how?
Strategy: Choose x_i that has a 1 on the highest position of 1 in y. (Such x_i must exist because there are odd number of 1's in this position.) Then flip the bits of this x_i.

$$
\begin{aligned}
x_1 &= 1\,0\,1\,1\,0\,0\,1\,1\,0\,1 \\
x_2 &= 0\,1\,0\,1\,1\,0\,0\,0\,1\,1 \\
&\cdots \\
x_i &= 1\,0\,1\,0\,0\,1\,1\,0\,0\,1 \\
&\cdots \\
x_k &= 1\,1\,0\,1\,1\,1\,0\,1\,0\,1 \\
\hline
y &= 0\,0\,1\,0\,1\,0\,0\,0\,1\,0
\end{aligned}
\quad \longrightarrow \quad
\begin{aligned}
x_1 &= 1\,0\,1\,1\,0\,0\,1\,1\,0\,1 \\
x_2 &= 0\,1\,0\,1\,1\,0\,0\,0\,1\,1 \\
&\cdots \\
x_i &= 1\,0\,0\,0\,1\,1\,1\,0\,1\,1 \\
&\cdots \\
x_k &= 1\,1\,0\,1\,1\,1\,0\,1\,0\,1 \\
\hline
y &= 0\,0\,0\,0\,0\,0\,0\,0\,0\,0
\end{aligned}
$$

Then y becomes 0 and x_i decreases. ■

Power of proofs: Game of NIM

Winning Strategy of Player 2: Choose x_i that has a 1 on the highest position of 1 in $y = \text{nimsum}(x_1, x_2, \ldots, x_k)$. Then reduce x_i by fliping its bits which are 1 in y.

Puzzle (zoom poll): If the current configuration is $(1,3,5,5)$, which of the following moves is a winning move:

- $1 \to 0$
- $3 \to 2$
- $3 \to 1$
- $3 \to 0$
- $5 \to 4$
- $5 \to 3$
- $5 \to 2$
- $5 \to 1$
- $5 \to 0$

Proofs

We will now prove that all horses have the same color! Formally:

Claim: $\forall n \geq 1$, if H is a set of n horses, then all horses in H have the same color.

Proof: We apply mathematical induction.

Base case. For $n = 1$, H has just one horse, so the claim is trivially true.

Inductive step. Consider $k \in \mathbb{N}$. Assume that the claim holds for any set of $n = k$ horses.

Let H be a set of $k+1$ horses, say $H = \{ h_1, h_2, \ldots, h_{k+1} \}$.

By the inductive assumption, all horses in these two sets:

$$\{ h_1, h_2, \ldots, h_k \} \qquad \{ h_2, \ldots, h_{k+1} \}.$$

have the same color.

Since these sets overlap, all horses in H also have the same color, completing the inductive step. ■

Question: *Where is the flaw???* These sets do not overlap when $k = 1$.

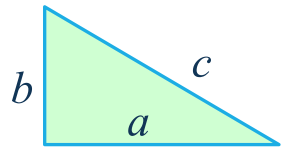
Proofs

Claim: $\forall n \quad \sum_{i=1}^{n} i^2 = \frac{1}{6}(2n+1)(n+1)n$

Proof: Class exercise.

Proofs

Pythagorean Theorem: Let a, b, and c be the width, height, and hypotenuse of a right triangle. Then $a^2 + b^2 = c^2$.



Proof 1: We use simple geometry and some calculation. Consider a $c \times c$ square $A_1A_2A_3A_4$ with four copies of our right triangle attached along its edges, as in the picture.

The angles at each A_i add up to 180 degrees each angle B_i is 90 degrees. So $B_1B_2B_3B_4$ is an $(a+b)\times(a+b)$ square.

Adding the area of four triangles and square $A_1A_2A_3A_4$ we have an equation

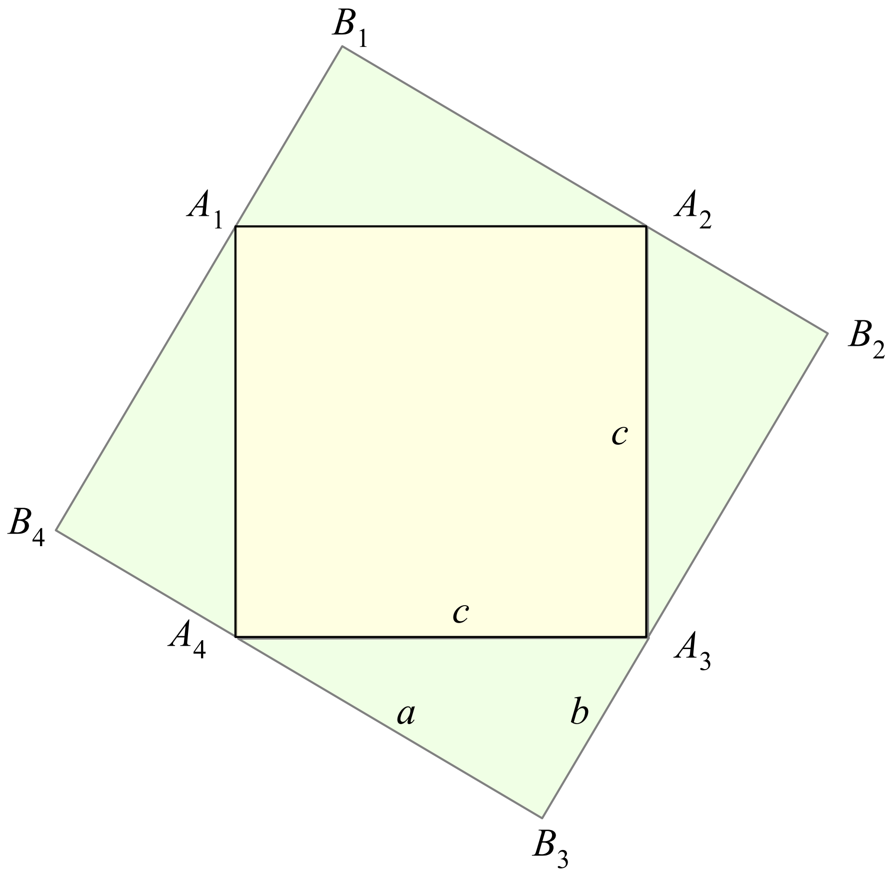
$$4 \cdot \tfrac{1}{2}ab + c^2 = (a+b)^2$$

This yields

$$2ab + c^2 = a^2 + 2ab + b^2$$

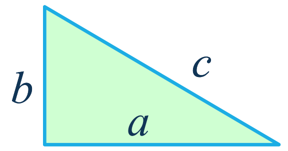
Therefore

$$c^2 = a^2 + b^2 \quad \blacksquare$$



Proofs

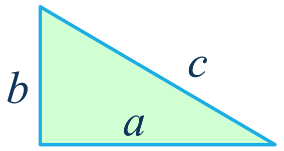
Pythagorean Theorem: Let a, b, and c be the width, height, and hypotenuse of a right triangle. Then $a^2 + b^2 = c^2$.



Intuition: The value c^2 represents the area of a $c \times c$ square. So there should be a way to slice a $c \times c$ square into pieces that can be then reassembled to form a $a \times a$ square and a $b \times b$ square.

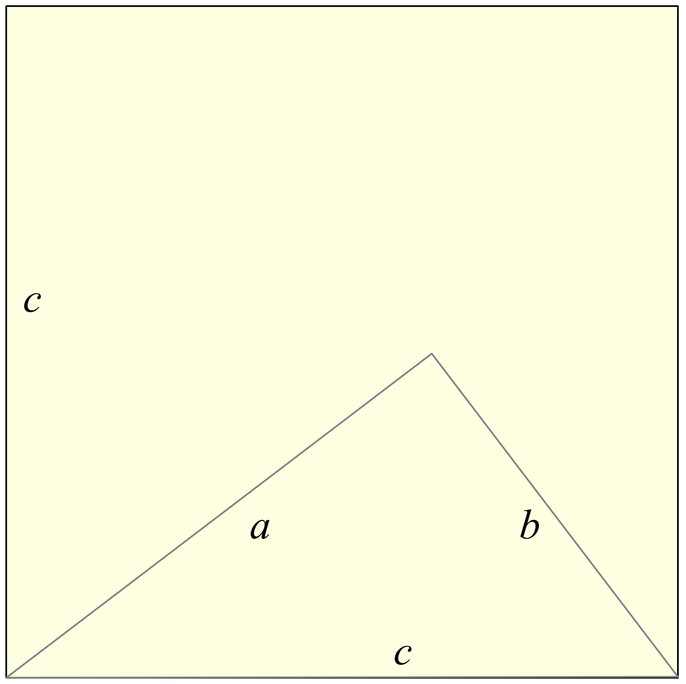
Proofs

Pythagorean Theorem: Let a, b, and c be the width, height, and hypotenuse of a right triangle. Then $a^2 + b^2 = c^2$.



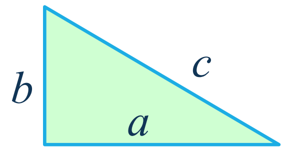
Proof 2:

Draw a $c \times c$ square with one edge being the c edge of our triangle (in yellow).



Proofs

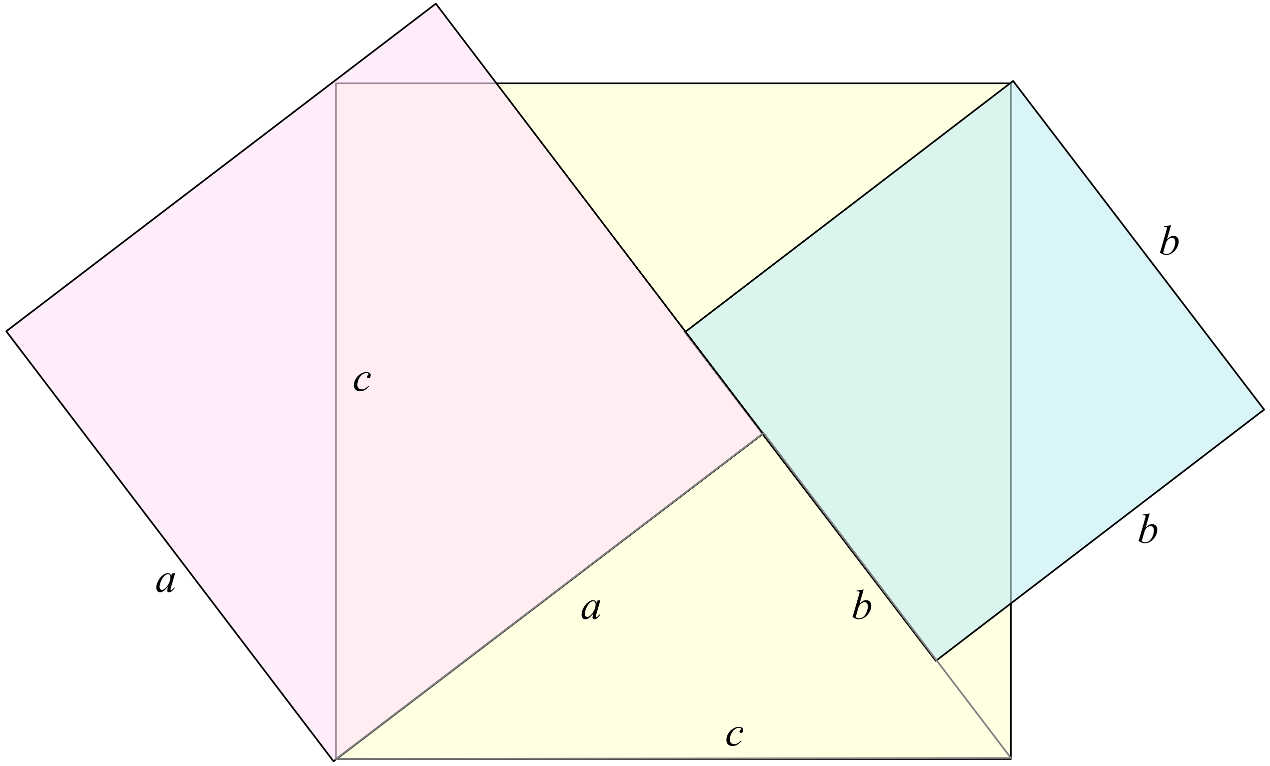
Pythagorean Theorem: Let a, b, and c be the width, height, and hypotenuse of a right triangle. Then $a^2 + b^2 = c^2$.



Proof 2:

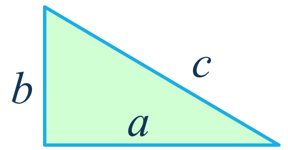
Draw a $c \times c$ square with one edge being the c edge of our triangle (in yellow).

Draw an $a \times a$ square (pink) and a $b \times b$ square (blue) as in the picture.



Proofs

Pythagorean Theorem: Let a, b, and c be the width, height, and hypotenuse of a right triangle. Then $a^2 + b^2 = c^2$.



Proof 2:

Draw a $c \times c$ square with one edge being the c edge of our triangle (in yellow).

Draw an $a \times a$ square (pink) and a $b \times b$ square (blue) as in the picture.

This creates three pairs of identical triangles that can be rearranged following the arrows, convering the yellow square into the pink and the blue squares. ■