Discrete Mathematics - Exam Cheat Sheet

01017
Discrete Mathematics

Date: 10 December 2025 **Semester:** 2025 Fall

Rasmus Rosendahl-kaa (s255609)

Key Formulas & Quick Reference

Number Theory

Formula	Description
$ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$	Fundamental GCD-LCM relation
$\gcd(a,b) = sa + tb$ for some $s, t \in \mathbb{Z}$	Bézout's identity
$a \equiv b \pmod{m} \iff m \mid (a-b)$	Congruence definition
$a^{-1} \bmod m$ exists $\iff \gcd(a,m) = 1$	Multiplicative inverse exists
$d = \gcd(a,b) \Rightarrow d^2 \mid ab$	GCD constraint on product
$a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$	Fermat's Little Theorem
$a^p \equiv a \pmod{p}$	Fermat's Little Theorem (alt)

Combinatorics

Formula	Description
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$	Binomial coefficient
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$	Binomial theorem
$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{n!}{e}$	Derangements (no fixed points)
$k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$	Absorption identity
$\sum_{k=0}^{n} \binom{n}{k} = 2^n$	Sum of binomial coefficients
$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$	Pascal's identity
$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k}$	Vandermonde's identity
Circular permutations: $(n-1)!$	Arrangements around a circle

Graph Theory

Formula	Description
Q_n: vertices $= 2^n$, edges $= n \cdot 2^{n-1}$	n-cube (hypercube)
K_n: edges $= \binom{n}{2} = \frac{n(n-1)}{2}$	Complete graph
$\sum_{v \in V} \deg(v) = 2\|E\|$	Handshaking lemma
Euler circuit exists $\iff$ all degrees even	Euler's theorem
Euler path exists $\iff$ exactly 0 or 2 odd vertices	Euler path condition
Tree on n vertices has $n-1$ edges	Tree edge count

Set Theory & Inclusion-Exclusion

Formula	**Description**
$\lvert A \cup B\rvert = \lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$	Inclusion-exclusion (2 sets)
$\lvert A \cup B \cup C\rvert = \sum \lvert A_i\rvert - \sum \lvert A_i \cap A_j\rvert + \lvert A \cap B \cap C\rvert$	Inclusion-exclusion (3 sets)
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's law
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's law
Subsets of n-element set: 2^n	Power set cardinality
Even-sized subsets: 2^{n-1}	Half of all subsets

Relations

Property	**Definition**
Reflexive	$\forall x : (x, x) \in R$
Symmetric	$\forall x, y : (x, y) \in R \Rightarrow (y, x) \in R$
Antisymmetric	$\forall x, y : [(x, y) \in R \wedge (y, x) \in R] \Rightarrow x = y$
Transitive	$\forall x, y, z : [(x, y) \in R \wedge (y, z) \in R] \Rightarrow (x, z) \in R$
Equivalence relation	Reflexive + Symmetric + Transitive
Partial order	Reflexive + Antisymmetric + Transitive

Examples + Solutions

Number Theory

Divisibility

Example (Divisibility with $ab \mid cd$)

If a, b, c, d are positive integers such that $ab \mid cd$, which must be true?

Solution:

Key insight: $ab \mid cd$ does NOT imply $a|c$ or $a|d$ individually.

True statement: "If p is a prime that divides a, then $p|c$ or $p|d$"

Proof: If $p|a$ and $ab \mid cd$, then $p \mid cd$. Since p is prime, $p|c$ or $p|d$.

Counterexample: Let $a = 6, b = 1, c = 2, d = 3$. Then $ab = 6 \mid 6 = cd$.

- But $\gcd(a, b) = 6$ does not divide $\gcd(c, d) = 1$
- And $6 \nmid c$ and $6 \nmid d$

Example (GCD as linear combination)

Let a, b be positive integers. Which can NOT necessarily be written as $as + bt$ for $s, t \in \mathbb{Z}$?

Solution:

Bézout's identity: $\gcd(a, b) = as + bt$ for some $s, t \in \mathbb{Z}$.

Any **multiple** of $\gcd(a, b)$ can be written as $as + bt$.

Answer: $\frac{\text{lcm}(a,b)}{\gcd(a,b)} = a\frac{b}{\gcd(a,b)^2}$ is NOT necessarily a multiple of $\gcd(a, b)$.

GCD Constraints

Example (Possible GCD values given product)

Let a, b be positive integers with $ab = 5292 = 2^2 \cdot 3^3 \cdot 7^2$. Which CANNOT be $\gcd(a, b)$?

Options: 1, 3, 36, 42

Solution:

Key fact: If $\gcd(a, b) = d$, then $d^2 \mid ab$.

Check each:
- $d = 1$: $1^2 = 1 \mid 5292$ (valid)
- $d = 3$: $3^2 = 9 \mid 5292$ (valid, since $3^3 \mid 5292$)
- $d = 36 = 2^2 \cdot 3^2$: Need $36^2 = 2^4 \cdot 3^4 \mid 2^2 \cdot 3^3 \cdot 7^2$. But $2^4 \nmid 2^2$!
- $d = 42 = 2 \cdot 3 \cdot 7$: $42^2 = 2^2 \cdot 3^2 \cdot 7^2 \mid 2^2 \cdot 3^3 \cdot 7^2$ (valid)

Answer: 36 cannot be the GCD.

Modular Arithmetic

Example (Congruence cancellation)

If $ac \equiv bc \pmod{m}$, when can we conclude $a \equiv b \pmod{m}$?

Solution:

$ac \equiv bc \pmod{m}$ means $m \mid c(a - b)$.

Cancellation Law: If $\gcd(c,m)=1$, then $a \equiv b \pmod{m}$.

Counterexample when $\gcd(c,m) \neq 1$: $2\cdot 3 \equiv 2\cdot 6 \pmod 6$ (both $\equiv 0$), but $3 \not\equiv 6 \pmod 6$.

Example (Finding multiplicative inverses mod 9)

Find the multiplicative inverse of $n \bmod 9$ for $n = 2, 6, 7$.

Solution:

Inverse exists iff $\gcd(n,9)=1$.

For $n=6$: $\gcd(6,9)=3\neq 1 \rightarrow$

Does not exist

For $n=2$: $\gcd(2,9)=1$. Find x with $2x \equiv 1 \pmod 9$:
- $2\cdot 5 = 10 \equiv 1 \pmod 9 \rightarrow$

  5

For $n=7$: $\gcd(7,9)=1$. Find x with $7x \equiv 1 \pmod 9$:
- $7\cdot 4 = 28 \equiv 1 \pmod 9 \rightarrow$

  4

Chinese Remainder Theorem

Example (System of congruences)

Solve: $x\equiv 1 \pmod 2$, $x \equiv 4 \pmod 5$, $x \equiv 3 \pmod 7$

Solution:

Moduli 2, 5, 7 are pairwise coprime, so unique solution mod $2\cdot 5\cdot 7 = 70$.

Method: Back substitution

Step 1: From $x \equiv 1 \pmod 2$: $x = 1 + 2t_1$

Step 2: Substitute into $x \equiv 4 \pmod 5$: $1 + 2t_1 \equiv 4 \pmod 5 \implies 2t_1 \equiv 3 \pmod 5$

Inverse of 2 mod 5: $2\cdot 3 = 6 \equiv 1$, so $t_1 \equiv 3\cdot 3 = 9 \equiv 4 \pmod 5$

Thus $t_1 = 4 + 5t_2$, giving $x = 1 + 2(4+5t_2) = 9 + 10t_2$

Step 3: Substitute into $x \equiv 3 \pmod 7$: $9 + 10t_2 \equiv 3 \pmod 7 \implies 2 + 3t_2 \equiv 3 \pmod 7 \implies 3t_2 \equiv 1 \pmod 7$

Inverse of 3 mod 7: $3 \cdot 5 = 15 \equiv 1$, so $t_2 \equiv 5 \pmod 7$

Thus $t_2 = 5 + 7t_3$, giving $x = 9 + 10(5) = 59$

Answer: $x \equiv 59 \pmod{70}$

Verify: $59 = 29 \cdot 2 + 1$, $59 = 11 \cdot 5 + 4$, $59 = 8 \cdot 7 + 3$

Functions: Injective/Surjective Analysis

Example (Function classification)

Classify each function:
1. $f : \mathbb{Z}^+ \to \mathbb{N}$ given by $f(x) = \lfloor \log_2(x) \rfloor$
2. $f : \mathbb{N} \to \mathbb{Z}$ given by $f(x) = \begin{cases} \lceil x/2 \rceil & \text{if } x \text{ even} \\ -\lceil x/2 \rceil & \text{if } x \text{ odd} \end{cases}$
3. $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = x^3 + 1$

Solution:

1. $f(x) = \lfloor \log_2(x) \rfloor$, $\mathbb{Z}^+ \to \mathbb{N}$:
- Surjective? Every $n \in \mathbb{N}$ is hit by $x = 2^n$. Yes
- Injective? $f(2) = f(3) = 1$. No
- **Surjective but not injective**

2. Alternating function $\mathbb{N} \to \mathbb{Z}$:
- $f(0) = 0, f(1) = -1, f(2) = 1, f(3) = -2, f(4) = 2, \ldots$
- Surjective? Hits all of $\mathbb{Z}$. Yes
- Injective? Each output appears exactly once. Yes
- **Bijection**

3. $f(x) = x^3 + 1$, $\mathbb{N} \to \mathbb{N}$:
- Injective? x^3 is strictly increasing. Yes
- Surjective? $f(0) = 1, f(1) = 2, f(2) = 9, \ldots$ — skips 3,4,5,6,7,8. No
- **Injective but not surjective**

Using the Function Checker

Example (Checking function properties with `check-function`)

Verify properties of $f(x) = \lfloor \log_2(x) \rfloor$ on domain $\{1, 2, \ldots, 8\}$ onto $\{0, 1, 2, 3\}$:

Solution:

Function f: Injective: No, Surjective: Yes, Bijective: No

Injectivity fails: $\mathrm{f}(2) = \mathrm{f}(3) = 1$

Analysis:

- Mapping: $f(1) = 0, f(2) = 1, f(3) = 1, f(4) = 2, f(5) = 2, f(6) = 2, f(7) = 2, f(8) = 3$
- Not injective because $f(2) = f(3) = 1$ (and others)
- Surjective because all outputs $\{0, 1, 2, 3\}$ are hit

More examples:

Function	Injective	Surjective	Bijective
$f(x) = x^2$ on $\{0, 1, 2, 3\}$ onto $\{0, 1, 4, 9\}$	Yes	Yes	Yes
$f(x) = x \bmod 5$ on $\{0, 1, 2, 3, 4\}$	Yes	Yes	Yes
$f(x) = \lvert x \rvert$ on $\{-2, -1, 0, 1, 2\}$ onto $\{0, 1, 2\}$	No	Yes	No

Graph Theory

Hypercube and Complete Graphs

Example (Edges in Q_n and K_n)

Hypercube Q_n:

- Vertices: 2^n (all n-bit binary strings)
- Each vertex has degree n (can flip any of n bits)
- By handshaking: $2|E| = 2^n \cdot n$, so $|E| = n \cdot 2^{n-1}$

Complete graph K_n:

- Every pair of vertices connected: $|E| = \binom{n}{2} = \frac{n(n-1)}{2}$

For K_{2n}: edges $= \binom{2n}{2} = (2n)\frac{2n-1}{2} = n(2n-1)$

Alternative form: $2\binom{n}{2} + n^2 = n(n-1) + n^2 = n(2n-1)$

Degree Sequences

Example (Valid degree sequence?)

Does a simple graph with degrees $2, 2, 3, 3, 3, 3, 3$ exist?

Solution:

Sum of degrees $= 2 + 2 + 3 + 3 + 3 + 3 + 3 = 19$.

By handshaking lemma: $\sum \deg(v) = 2|E|$ must be even.

Since 19 is odd,

such a graph does not exist.

Euler Circuits

Example (Königsberg Bridge Problem)

A graph has an Euler circuit iff:
1. The graph is connected
2. Every vertex has even degree

A graph has an Euler path iff:
1. The graph is connected
2. Exactly 0 or 2 vertices have odd degree

In Königsberg: degrees are 5, 3, 3, 3 (all odd) → No Euler path or circuit.

Combinatorics

Binomial Theorem

Example (Coefficient in $(2x^2 - 3y^3)^8$)

Find coefficients of $x^8 y^{\{12\}}$ and $x^6 y^9$.

Solution:

General term: $\binom{8}{k}(2x^2)^k(-3y^3)^{8-k} = \binom{8}{k}2^k(-3)^{8-k}x^{2k}y^{3(8-k)}$

For $x^8 y^{\{12\}}$: Need $2k = 8$ and $3(8-k) = 12$.
- $k = 4$ (valid)
- Coefficient: $\binom{8}{4} \cdot 2^4 \cdot (-3)^4 = 70 \cdot 16 \cdot 81 = 90720$

For $x^6 y^9$: Need $2k = 6$ and $3(8-k) = 9$.
- $k = 3$ but $8 - k = 5$, and $3 \cdot 5 = 15 \neq 9$ (invalid)
- Coefficient is 0

Inclusion-Exclusion

Example (Union of four sets)

Each of 4 sets has 200 elements, each pair shares 50, each triple shares 25, all four share 5. Find $|A \cup B \cup C \cup D|$.

Solution:

$|A \cup B \cup C \cup D| = \binom{4}{1} \cdot 200 - \binom{4}{2} \cdot 50 + \binom{4}{3} \cdot 25 - \binom{4}{4} \cdot 5$

$= 4(200) - 6(50) + 4(25) - 1(5) = 800 - 300 + 100 - 5 = 595$

Derangements

Example (Derangement formula and values)

$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ...\right)$

First few values:

- $D_0 = 1$, $D_1 = 0$, $D_2 = 1$, $D_3 = 2$
- $D_4 = 9$, $D_5 = 44$, $D_6 = 265$, $D_7 = 1854$

Recurrence: $D_n = (n-1)(D_{n-1} + D_{n-2})$

Approximation: $D_n \approx \frac{n!}{e}$ (rounds to nearest integer for $n \geq 1$)

Circular Permutations

Example (20 people around a round table)

Count seatings where two arrangements are identical if:

1. Each person has same two neighbors (ignoring direction)
2. Each person has same left AND right neighbor

Solution:

Case 2 (same left AND right neighbor):

- Standard circular permutation: $(n-1)! = 19!$
- Fix one person's position, arrange remaining 19 people.

Case 1 (same two neighbors, ignoring direction):

- Each arrangement counted twice (clockwise vs counterclockwise)
- Answer: $\frac{19!}{2}$

Relations

Example (Classify relations on $\{1, 2, 3, 4, 5, 6\}$)

$R_1 = \{(1,2), (2,3), (1,3), (4,5), (5,6), (4,6)\}$

Solution:

- Reflexive? Missing $(1,1),(2,2),\ldots$ (no)
- Symmetric? $(1,2) \in R$ but $(2,1) \notin R$ (no)
- Antisymmetric? No pair $(x,y),(y,x)$ with $x \neq y$ both present (yes)
- Transitive? $(1,2),(2,3) \in R$ and $(1,3) \in R$; $(4,5),(5,6) \in R$ and $(4,6) \in R$ (yes)
- Transitive and antisymmetric only

Example (Equivalence classes mod 4)

The equivalence relation of congruence modulo 4 on $\mathbb{Z}$:

$$\begin{aligned} [0]_{\text{mod } 4} &= \{\ldots,-8,-4,0,4,8,\ldots\} \\ [1]_{\text{mod } 4} &= \{\ldots,-7,-3,1,5,9,\ldots\} \\ [2]_{\text{mod } 4} &= \{\ldots,-6,-2,2,6,10,\ldots\} \\ [3]_{\text{mod } 4} &= \{\ldots,-5,-1,3,7,11,\ldots\} \end{aligned} \tag{1}$$

These four equivalence classes **partition** the integers.

Partitions of Sets

Example (Partitions of $\mathbb{Z} \times \mathbb{Z}$)

Which are partitions?

(a) $\{(x,y) : x \text{ or } y \text{ odd}\}$ and $\{(x,y) : x \text{ and } y \text{ even}\}$

(b) $\{(x,y) : x \text{ and } y \text{ odd}\}$ and $\{(x,y) : x \text{ and } y \text{ even}\}$

Solution:

Every (x,y) falls into one of 4 categories: EE, OO, EO, OE

(a): "x or y odd" = OO ∪ EO ∪ OE. "x and y even" = EE.
- Disjoint? Yes. Cover everything? Yes.
- **YES, this is a partition**

(b): "x and y odd" = OO. "x and y even" = EE.
- Missing EO and OE!
- **NO, doesn't cover everything**

Proof by Induction

Example (Strong induction: Pie-throwing problem)

Prove: If $2n+1$ people throw pies at their nearest neighbor, at least one survives.

Solution:

Base case ($n = 1$): 3 people. Closest pair (A, B) throw at each other. Third person C's nearest is either A or B. So A and B each receive one pie, C receives 0. C survives.

Inductive step: Assume true for $2k + 1$ people. Consider $2(k + 1) + 1 = 2k + 3$ people.

Let A and B be the closest pair (they throw at each other).

Case 1: No one else throws at A or B. The remaining $2k + 1$ people form an independent group → by IH, at least one survivor.

Case 2: At least one other person throws at A or B. Then ≥ 3 pies hit A or B combined. Remaining pies: $\leq 2k + 3 - 3 = 2k$ for $2k + 1$ people. By pigeonhole, someone survives.

Example (Checkerboard tiling with L-triominoes)

Every $2^n \times 2^n$ checkerboard with one square removed can be tiled by L-triominoes.

Solution:

Base case ($n = 1$): 2×2 board with one square removed = L-triomino.

Inductive step: Assume true for $2^k \times 2^k$. For $2^{k+1} \times 2^{k+1}$ board:

1. Divide into four $2^k \times 2^k$ quadrants
2. The removed square is in one quadrant
3. Place one L-triomino at the center, covering one square from each of the other three quadrants
4. Now each quadrant is a $2^k \times 2^k$ board with one square removed
5. By IH, each can be tiled.

Polynomial Divisibility

Example ($x^n + 1$ divisible by $x + 1$)

For which positive integers n is $x^n + 1$ divisible by $x + 1$?

Solution:

$x + 1 \mid x^n + 1$ iff $x = -1$ is a root of $x^n + 1$.

Evaluate at $x = -1$: $(-1)^n + 1$
- If n odd: $(-1)^n = -1$, so $-1 + 1 = 0$ (root)

- If n even: $(-1)^n = 1$, so $1 + 1 = 2 \neq 0$ (not a root)

Divisible for all odd n, not divisible for any even n.

Pigeonhole Principle

Example (Simple graphs with all distinct degrees)

Can a simple graph on $n \geq 2$ vertices have all distinct degrees?

Solution:

Claim: NO (by pigeonhole)

In a simple graph on n vertices:
- Possible degrees: $0, 1, 2, ..., n - 1$ (that's n values)
- For all degrees distinct, we need exactly $\{0, 1, 2, ..., n - 1\}$

But:
- Degree 0 means isolated (no neighbors)
- Degree $n - 1$ means connected to all others
- These can't coexist! (vertex with degree $n - 1$ would connect to the isolated vertex)

Conclusion: No simple graph on $n \geq 2$ vertices has all distinct degrees.

Hall's Theorem / Matching

Example (Bipartite matching condition)

Hall's Marriage Theorem: A bipartite graph with parts X and Y has a matching saturating X iff for every subset $S \subseteq X$:

$$|N(S)| \geq |S| \quad (2)$$

where $N(S)$ = neighbors of S in Y.

Application: 10 computers, 5 printers. Minimum cables so any 5 computers can print to 5 different printers?

Solution:

Need: every subset of 5 computers has 5 distinct printer neighbors.

If a printer connects to < 6 computers, we could choose 5 computers that don't include any connected to that printer, violating Hall's condition.

Each printer must connect to ≥ 6 computers.

Minimum cables: $5 \times 6 = 30$

Propositional Logic (Truth Sayer/Liar Puzzles)

Example (Truth Sayer and Liar Logic)

Peter says: "At least one of us is a liar." What are Peter and Signe?

Solution:

Let P = "Peter is truth sayer", S = "Signe is truth sayer"

Peter's claim: $\neg P \vee \neg S$

Key: If Peter is a truth sayer, his claim must be true. If he's a liar, his claim must be false.

$$P \Leftrightarrow (\neg P \vee \neg S) \tag{3}$$

P	S	$\neg P \vee \neg S$	$P \Leftrightarrow (\neg P \vee \neg S)$
T	T	F	F
T	F	T	**T**
F	T	T	F
F	F	T	F

Answer: Peter is a truth sayer, Signe is a liar.

Perfect Numbers

Example (Verify perfect numbers)

Show that 6 and 28 are perfect numbers (equal to sum of proper divisors).

Solution:

For 6: Divisors (excluding 6): $1, 2, 3$

$$1 + 2 + 3 = 6 \tag{4}$$

For 28: Divisors (excluding 28): $1, 2, 4, 7, 14$

$$1 + 2 + 4 + 7 + 14 = 28 \tag{5}$$

Theorem: $2^{p-1}(2^p - 1)$ is perfect when $2^p - 1$ is prime (Mersenne prime).

Example: $p = 3$, $2^3 - 1 = 7$ (prime), so $2^2 \cdot 7 = 28$ is perfect.

Set Operations Proofs

Example (Prove $(A - C) \cap (C - B) = \emptyset$)

Solution:

$(A - C)$ = elements in A but not in C

$(C - B)$ = elements in C but not in B

For $x \in (A - C) \cap (C - B)$:
- $x \in A - C$ means $x \in A$ and $x \notin C$
- $x \in C - B$ means $x \in C$ and $x \notin B$

Contradiction: $x \notin C$ and $x \in C$ cannot both be true.

Therefore $(A - C) \cap (C - B) = \emptyset$.

Example (Prove $(B - A) \cup (C - A) = (B \cup C) - A$)

Solution:

LHS: $x \in (B - A) \cup (C - A)$
- $x \in B - A$ or $x \in C - A$
- $(x \in B \land x \notin A)$ or $(x \in C \land x \notin A)$
- $(x \in B \lor x \in C)$ and $x \notin A$

RHS: $x \in (B \cup C) - A$
- $x \in B \cup C$ and $x \notin A$
- $(x \in B \lor x \in C)$ and $x \notin A$

Both sides are equivalent.

Equivalence Relations

Example (Cardinality as equivalence relation)

Let R on sets of real numbers: SRT iff $|S| = |T|$.

Solution:

Reflexive: $|S| = |S|$ (yes)

Symmetric: $|S| = |T| \Rightarrow |T| = |S|$ (yes)

Transitive: $|S| = |T|$ and $|T| = |U| \Rightarrow |S| = |U|$ (yes)

This is an equivalence relation.

Equivalence classes:
- $[\{0, 1, 2\}]$ = all sets with exactly 3 elements
- $[\mathbb{Z}]$ = all countably infinite sets (includes $\mathbb{N}$, $\mathbb{Q}$)

Example (Rational equivalence: $(a, b)R(c, d)$ iff $ad = bc$)

Solution:

This is an equivalence relation (represents fractions $\frac{a}{b} = \frac{c}{d}$).

Reflexive: $a \cdot b = b \cdot a$ (yes)

Symmetric: $ad = bc \Rightarrow cb = da$ (yes)

Transitive: If $ad = bc$ and $cf = de$, then:
- Multiply: $adf = bcf = bde$
- Since $d > 0$: $af = be$ (yes)

This is an equivalence relation.

Equivalence class of $(1, 2)$: all pairs $(k, 2k)$ for $k \in \mathbb{Z}^+$

Generalized Pigeonhole

Example (Generalized pigeonhole for n boxes)

If $n_1 + n_2 + ... + n_t - t + 1$ objects are placed in t boxes, then some box i contains at least n_i objects.

Solution:

Proof by contradiction:

Assume each box i contains fewer than n_i objects (at most $n_i - 1$).

Total objects $\leq (n_1 - 1) + (n_2 - 1) + ... + (n_t - 1) = \sum n_i - t$

But we have $\sum n_i - t + 1$ objects.

$\sum n_i - t + 1 \leq \sum n_i - t$ implies $1 \leq 0$. Contradiction!

Polynomial Division (using auto-div)

Example (Polynomial division with auto-div)

Divide $x^4 + 3x^3 + \frac{5}{2}x + 6$ by $x + 2$:

$$
\begin{array}{r|lllll}
 & & x^3 & +x^2 & -2x & +\frac{13}{2} \\ \hline
x+2 & x^4 & +3x^3 & & +\frac{5}{2}x & +6 \\
 & -(x^4 & +2x^3 & & &) \\ \hline
 & & x^3 & & +\frac{5}{2}x & +6 \\
 & & -(x^3 & +2x^2 & &) \\ \hline
 & & & -2x^2 & +\frac{5}{2}x & +6 \\
 & & & -(-2x^2 & -4x &) \\ \hline
 & & & & \frac{13}{2}x & +6 \\
 & & & & -(\frac{13}{2}x & +13) \\ \hline
 & & & & & -7
\end{array} \tag{6}
$$

Calculation Workspace

Quick Reference: Built-in Typst Functions

Function	Example	Result
`calc.gcd(a, b)`	`calc.gcd(48, 18)`	6
`calc.lcm(a, b)`	`calc.lcm(12, 18)`	36
`calc.fact(n)`	`calc.fact(6)`	720
`calc.binom(n, k)`	`calc.binom(10, 3)`	120
`calc.perm(n, k)`	`calc.perm(5, 3)`	60
`calc.rem(a, b)`	`calc.rem(17, 5)`	2
`calc.quo(a, b)`	`calc.quo(17, 5)`	3
`calc.pow(a, b)`	`calc.pow(2, 10)`	1024

Binomial Coefficients

$$\binom{10}{5} = 252 \tag{7}$$

$$\binom{8}{4} = 70 \tag{8}$$

$$\binom{20}{10} = 184756 \tag{9}$$

$$\binom{15}{7} = 6435 \tag{10}$$

Factorials

$$5! = 120 \tag{11}$$

$$7! = 5040 \tag{12}$$

$$10! = 3628800 \tag{13}$$

Derangements

$$D_4 = 9 \tag{14}$$

$$D_5 = 44 \tag{15}$$

$$D_6 = 265 \tag{16}$$

$$D_7 = 1854 \tag{17}$$

GCD and LCM

$$\gcd(48, 18) = 6 \tag{18}$$

$$\gcd(5292, 36) = 36 \tag{19}$$

$$\gcd(662, 414) = 2 \tag{20}$$

$$\text{lcm}(12, 18) = 36 \tag{21}$$

$$\text{lcm}(24, 36) = 72 \tag{22}$$

Bézout Coefficients (Extended Euclidean Algorithm)

$$\gcd(48, 18) = 6 = (48)(-1) + (18)(3) \tag{23}$$

$$\gcd(35, 15) = 5 = (35)(1) + (15)(-2) \tag{24}$$

$$\gcd(662, 414) = 2 = (662)(-5) + (414)(8) \tag{25}$$

Modular Inverses

$$2^{-1} \equiv 5 \pmod 9 \tag{26}$$

$$6^{-1} \bmod 9 \tag{27}$$

does not exist (since $\gcd(6, 9) = 3 \neq 1$)

$$7^{-1} \equiv 4 \pmod 9 \tag{28}$$

$$3^{-1} \equiv 5 \pmod 7 \tag{29}$$

$$5^{-1} \equiv 5 \pmod{12} \tag{30}$$

Chinese Remainder Theorem

CRT Solution: $x \equiv 59 \pmod{70}$

Verify: 59 ≡ 1 (mod 2), 59 ≡ 4 (mod 5), 59 ≡ 3 (mod 7)

CRT Solution: $x \equiv 68 \pmod{105}$

Verify: 68 ≡ 2 (mod 3), 68 ≡ 3 (mod 5), 68 ≡ 5 (mod 7)

Graph Theory Quick Calculations

$$Q_4 : 16 \text{ vertices}, 32 \text{ edges} \tag{31}$$

$$Q_5 : 32 \text{ vertices}, 80 \text{ edges} \tag{32}$$

$$K_6 : 6 \text{ vertices}, 15 \text{ edges} \tag{33}$$

$$K_{10} : 10 \text{ vertices}, 45 \text{ edges} \tag{34}$$

$$K_{20} : 20 \text{ vertices}, 190 \text{ edges} \tag{35}$$

Inclusion-Exclusion (4 sets with equal intersections)

$$|A \cup B \cup C \cup D| = 4(200) - 6(50) + 4(25) - 5 = 595 \tag{36}$$

Primality and Primes

$$17 \text{ is prime} \tag{37}$$

$$91 \text{ is not prime} \tag{38}$$

$$97 \text{ is prime} \tag{39}$$

There are 10 primes below 30: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

General Linear Congruences

Solve $ax \equiv c \pmod{m}$:

$$3x \equiv 6 \pmod{9} \Rightarrow x \equiv 2 \pmod{3} \tag{40}$$

$$4x \equiv 5 \pmod{9} \Rightarrow x \equiv 8 \pmod{9} \tag{41}$$

$$6x \equiv 15 \pmod{21} \Rightarrow x \equiv 6 \pmod{7} \tag{42}$$

Division with Remainder

$$17 = 5 \cdot 3 + 2 \tag{43}$$

$$100 = 7 \cdot 14 + 2 \tag{44}$$

$$5292 = 36 \cdot 147 + 0 \tag{45}$$

Relation Properties

Relation R_1 on set (1, 2, 3):
- Reflexive: Yes
- Symmetric: Yes
- Antisymmetric: No
- Transitive: Yes
- **Equivalence relation**

Relation R_2 on set (1, 2, 3):
- Reflexive: Yes
- Symmetric: No
- Antisymmetric: Yes
- Transitive: Yes
- **Partial order**

Function Property Checker

Check if functions are injective/surjective/bijective on finite domains:

Usage	Code
Define function	`#let my_func = (x) => calc.floor(calc.log(x, base: 2))`
Check properties	`#let result = check-function( my_func, (1, 2, 3, 4, 5, 6, 7, 8), // domain codomain: (0, 1, 2, 3) // codomain (optional) )`
Display results	`#show-function-check(result, func-name: "f")`

Quick examples:

- $f(x) = \lfloor \log_2(x) \rfloor$: Inj: No, Surj: Yes, Bij: No
- $g(x) = x^2$ on $\{0, 1, 2, 3\}$: Inj: Yes, Surj: Yes, Bij: Yes
- $h(x) = |x|$ on $\{-2, ..., 2\}$: Inj: No, Surj: Yes, Bij: No

Note: Only works for finite domains. For infinite domains ($\mathbb{Z}$, $\mathbb{N}$, $\mathbb{R}$), use mathematical proofs.

Your Calculations Here