3 Set, Relations, and Functions

3.1 Sets

D 3.2 (Equal sets):

• For sets A and B, $A = B \iff \forall x\,(x \in A \iff x \in B)$.

L 3.1 (Equality of set elemetns and ord. pairs):

• For any sets A and B, $\{A\} = \{B\} \implies A = B$.

Ordered pairs: $(a, b) = (c, d) \iff a = c \wedge b = d$.

Odered pairs via sets: $(a, b) := \{\{a\}, \{a, b\}\}$.

D 3.3 (Subset):

• $A \subseteq B \iff \forall x\,(x \in A \Rightarrow x \in B)$.

L 3.2 (Sets equality and subsets):

• $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$. Equivalently:

$\forall x\,((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) \Leftrightarrow \forall x\,(x \in A \iff x \in B)$.

L 3.3 (Transitivity of subsets):

• For all sets A, B, C, $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$.

D 3.4 (Union and Intersection):

• $A \cup B := \{x \mid x \in A \vee x \in B\}$, $A \cap B := \{x \mid x \in A \wedge x \in B\}$.

Families of Sets: Let $\mathcal{A}$ be a set of sets:

$\bigcap \mathcal{A} := \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}$, $\bigcup \mathcal{A} := \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$.

Example:

$\mathcal{A} = \{\{a, b, c\}, \{a, c\}, \{a, b, c, f\}, \{a, c, d\}\}$,

$\bigcup \mathcal{A} = \{a, b, c, d, e, f\}$, $\bigcap \mathcal{A} = \{a, c\}$.

If I is an index set and $\mathcal{A} = \{A_i \mid i \in I\}$, then $\bigcap_{i \in I} A_i$, $\bigcup_{i \in I} A_i$.

D 3.5 (Set Difference):

• The difference of sets B and A is $B \setminus A := \{x \in B \mid x \notin A\}$.

D 3.6 (Empty Set):

• A set is called *empty* if it contains no elements: $\forall x\,(x \notin A)$.

L 3.5:

• There is exactly **one** empty set, denoted $\varnothing$ or $\{\}$.

L 3.6:

• The empty set is a subset of every set: $\forall A\ (\varnothing \subseteq A)$.

Construction of natural numbers: $S(n) := n \cup \{n\}$ (rec. sucsessor).

D 3.7 (Power Set):

• The power set of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A: $\mathcal{P}(A) := \{S \mid S \subseteq A\}$. If $|A| = k$, then $|\mathcal{P}(A)| = 2^k$. In particular, for a set with k elements, each element may be *included* or *excluded*, giving $2 \times 2 \times \cdots \times 2 = 2^k$ possible subsets.

Example (bit-mask intuition for $\{a, b\}$):

$$\begin{array}{lcl} 00 & \longleftrightarrow & \varnothing \\ 01 & \longleftrightarrow & \{b\} \\ 10 & \longleftrightarrow & \{a\} \\ 11 & \longleftrightarrow & \{a, b\} \end{array}$$

3.2 Relations

D 3.8 (Cartesian product):

• The Cartesian product $A \times B$ of sets A and B is the set of all ordered pairs with first component from A and second from B: $A \times B := \{(a, b) \mid a \in A,\ b \in B\}$. The cardinality satisfies $|A \times B| = |A| \cdot |B|$.

More generally: $\bigtimes_{i=1}^{k} A_i := \{(a_1, \ldots, a_k) \mid a_i \in A_i \text{ for } 1 \le i \le k\}$.

The Cartesian product is *not associative*, since elements are ordered tuples.

Connection to power sets:

If $A = \{a, b, c\}$, $|A| = 3$, then each element may be either *in* or *out*, giving $\{0, 1\}^3 = \{0, 1\} \times \{0, 1\} \times \{0, 1\}$, which represents all subsets of A.

Another example:

$A_1 = \{0, 1\}$, $A_2 = \{d, e\}$, $A_1 \times A_2 = \{(0, d), (0, e), (1, d), (1, e)\}$.

D 3.9 (Relation):

• A (binary) relation ρ from a set A to a set B is a subset of $A \times B$.

If $A = B$, then ρ is called a relation *on* A.

Notation: $(a, b) \in \rho \Rightarrow a \,\rho\, b$, $(a, b) \notin \rho \Rightarrow a \not\rho b$.

For any set S, any subset $\rho \subseteq S \times S$ is a relation on S.

There are 2^{n^2} relations on a set of cardinality n, since $|S \times S| = n^2$ and $|\mathcal{P}(S \times S)| = 2^{n^2}$.

Examples on $\mathbb{Z}$:

- $\le \cup \ge$ is the complete relation $\mathbb{Z} \times \mathbb{Z}$.
- $\le \cap \ge$ is the identity relation: $\{(a, a) \mid a \in \mathbb{Z}\}$.

D 3.11 (Inverse Relation):

• The inverse relation of ρ is $\rho^{-1} := \{(b, a) \mid (a, b) \in \rho\}$.

Equivalently, $b\,\rho^{-1}\,a \iff a\,\rho\,b$.

Interpretations:

- In graphs: reversing all edge directions.
- In matrices: taking the transpose.

D 3.12 (Composition of Relations):

• Let $\rho \subseteq A \times B$ and $\sigma \subseteq B \times C$. The composition $\sigma \circ \rho$ is defined by $\sigma \circ \rho := \{(a, c) \mid \exists b\ ((a, b) \in \rho \wedge (b, c) \in \sigma)\}$. Composition is associative: $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$.

L 3.8:

• Let ρ be a relation from A to B and σ a relation from B to C. Then $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

3.3 Properties of Relations

Name	Formula	Set	Example
Reflexive	$a\rho a$	$\mathrm{id} \subseteq \rho$	$\mathrm{id}, \ge$
Irreflexive	$\neg(a\rho a)$	$\mathrm{id} \cap \rho = \varnothing$	$\ne, >$
Symmetric	$a\rho b \iff b\rho a$	$\rho = \hat{\rho}$	$\mathrm{id}, \equiv \pmod m$
Antisymmetric	$a\rho b \wedge b\rho a \to a = b$	$\rho \cap \hat{\rho} \subseteq \mathrm{id}$	$\ge, \mid$
Transitive	$a\rho b \wedge b\rho c \to a\rho c$	$\rho^2 \subseteq \rho$	$\equiv \pmod m, >$

L 3.9:

• A relation ρ is transitive if and only if $\rho^2 \subseteq \rho$, where $\rho^2 = \rho \circ \rho$.

D 3.18 (Transitive Closure):

• The *transitive closure* of a relation ρ on a set A, denoted ρ^*, is defined by $\rho^* := \bigcup_{n \in \mathbb{N}_{>0}} \rho^n$.

3.4 Equivalence Relation

D 3.19 (Equivalence Relation):

• An equivalence relation on a set A is a relation that is *reflexive*, *symmetric*, and *transitive*.

D 3.20 (Equivalence Class):

• Let θ be an equivalence relation on a set A, and let $a \in A$. The *equivalence class* of a is $[a]_\theta := \{\, b \in A \mid b\,\theta\,a \,\}$.

Example: (congruence modulo 3 on $\mathbb{Z}$): $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

L 3.10:

• The intersection of two equivalence relations on the same set is an equivalence relation.

D 3.21 (Partition):

• A *partition* of a set A is a family $\{S_i \mid i \in I\}$ of subsets of A such that $S_i \cap S_j = \varnothing$ $(i \ne j)$, $\bigcup_{i \in I} S_i = A$.

D 3.22 (Quotient Set):

• Let θ be an equivalence relation on a set A. The set of equivalence classes is denoted by $A/\theta := \{[a]_\theta \mid a \in A\}$, and is called the *quotient set* of A modulo θ.

T 3.11:

• Let θ be an equivalence relation on a set A. Then the set A/θ of equivalence classes forms a partition of A.

3.5 Partial Order Relations

D 3.23 (Partial Order):

• A *partial order* on a set A is a relation that is *reflexive*, *antisymmetric*, and *transitive*.

A set equipped with a partial order $\preceq$ is called a *partially ordered set* (poset), denoted $(A, \preceq)$.

Examples: $(\mathcal{P}(A), \subseteq)$ is a poset, $(\mathbb{N}_{\ge 0}, |)$ is a poset, $(\mathbb{Z}, \preceq)$ is a poset.

Note: $a \prec b \iff a \preceq b \wedge a \ne b$.

D 3.24 (Comparable Elements):

• In a poset $(A, \preceq)$, two elements $a, b \in A$ are called *comparable* if $a \preceq b$ or $b \preceq a$. Otherwise, they are called *incomparable*.

D 3.25 (Total Order):

• Let $(A, \preceq)$ be a poset. If any two elements of A are comparable, then A is called a *totally ordered set* (or *linearly ordered*) by $\preceq$.

Examples: $(\mathbb{Z}, \le)$ and $(\mathbb{Z}, \ge)$ are totally ordered, $(\mathcal{P}(A), \subseteq)$ is not totally ordered if $|A| \ge 2$, $(\mathbb{N}, |)$ is not totally ordered

D 3.26 (Covering Relation):

• In a poset $(A, \preceq)$, an element b *covers* a if:
$a \prec b$ and there is no c with $a \prec c \prec b$ between a and b.

D 3.27 (Hasse Diagram):

• The *Hasse diagram* of a finite poset $(A, \leq)$ is the directed graph whose vertices are the elements of A, and where there is an edge from a to b if and only if b covers a.

Example: $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

D 3.28 (Product Order):

• Let $(A, \preceq_A)$ and $(B, \preceq_B)$ be posets. The product poset $(A \times B, \leq)$ is defined by $(a_1, b_1) \leq (a_2, b_2) \iff a_1 \preceq_A a_2 \ \wedge \ b_1 \preceq_B b_2$.

T 3.12:

• If $(A, \preceq_A)$ and $(B, \preceq_B)$ are posets, then $(A, \preceq_A) \times (B, \preceq_B)$ is a partially ordered set.

T 3.13:

• For posets $(A, \preceq_A)$ and $(B, \preceq_B)$, the relation $(a_1, b_1) \leq_{\text{lex}} (a_2, b_2) \iff a_1 \prec a_2 \ \vee \ (a_1 = a_2 \wedge b_1 \preceq_B b_2)$ defines a partial order on $A \times B$.

D 3.29 (Bounds):

• Let $(A, \preceq)$ be a poset and $S \subseteq A$. For $a \in A$:
• a is *minimal / maximal* if there is no $b \in A$ with $b \prec a$ / $b \succ a$.
• a is the *least / greatest element* of A if $a \preceq b$ / $a \succeq b \ \forall b \in A$.
• a is a *lower / upper bound* of S if $a \preceq b$ / $a \succeq b \ \forall b \in S$.
• a is the *greatest lower bound / least upper bound* of S if it is respectively the greatest / least among all lower / upper bounds of S.

D 3.30 (Well-Ordered Set):

• A poset $(A, \preceq)$ is *well-ordered* if it is totally ordered and every nonempty subset of A has a least element.
• Every subset of a well-ordered set is also well-ordered.

D 3.31 (Meet and Join):

• Let $(A, \preceq)$ be a poset and $a, b \in A$.
• If a and b have a greatest lower bound, it is called the *meet* and denoted $a \wedge b$.
• If a and b have a least upper bound, it is called the *join* and denoted $a \vee b$.

D 3.32 (Lattice):

• A poset $(A, \preceq)$ in which every pair of elements has both a meet and a join is called a *lattice*.

3.6 Functions

D 3.33 (Function):

• A function $f : A \to B$ from domain A to codomain B is a relation from A to B such that:
• For every $a \in A$ there exists $b \in B$ with $a \, f \, b$ (totality).
• For all $a \in A$ and $b, b' \in B$, $a \, f \, b \wedge a \, f \, b' \implies b = b'$ (well-definedness).
We write $f(a) = b$.

D 3.34:

• The set of all functions from A to B is denoted B^A.

D 3.35 (Partial Function):

• A *partial function* satisfies only condition (2) of Definition 3.33.

D 3.36 (Image of a Set):

• Let $f : A \to B$ be a function and $S \subseteq A$. The image of S under f is $f(S) := \{f(a) \mid a \in S\}$.

D 3.37 (Image of a Function):

• The image of f is $\text{Im}(f) := f(A)$.

D 3.38 (Preimage):

• For $T \subseteq B$, the preimage of T under f is $f^{-1}(T) := \{a \in A \mid f(a) \in T\}$.

Example: If $f(x) = x^2$, then $f^{-1}(\{4, 9\}) = \{-3, -2, 2, 3\}$.

D 3.39 (Injective, Surjective, Bijective):

• A function $f : A \to B$ is:
• *Injective*: if $f(a) = f(a') \Rightarrow a = a'$.
• *Surjective*: if $f(A) = B$.
• *Bijective*: if it is both injective and surjective.
A bijection has an inverse function f^{-1}.

D 3.41 (Composition of Functions):

• Let $f : A \to B$ and $g : B \to C$ be functions.
Composition $g \circ f : A \to C$ is defined by $(g \circ f)(a) = g(f(a))$.

L 3.14:

• Function composition is associative: $(h \circ g) \circ f = h \circ (g \circ f)$.

D 3.42:

• Two sets A and B are called *equinumerous*, denoted $A \sim B$, if there exists a bijection $f : A \to B$. Equivalently, $A \sim B \Leftrightarrow |A| = |B|$.
• A set B *dominates* a set A, denoted $A \preceq B$, if $A \sim C$ to some subset $C \subseteq B$. Equivalently, there exists an injective function $f : A \to B$.
• A set A is called *countable* if $A \preceq \mathbb{N}$, and *uncountable* otherwise. Equivalently, A is countable if there exists an injection $f : A \to \mathbb{N}$.

L 3.15:

• The relation $\sim$ is an equivalence relation.
• The relation $\preceq$ is transitive: $A \preceq B \ \wedge \ B \preceq C \ \Rightarrow \ A \preceq C$.
• If $A \subseteq B$, then $A \preceq B$.

T 3.16 (Bernstein-Schröder theorem):

• If $A \preceq B$ and $B \preceq A$, then $A \sim B$.

T 3.17:

• A set A is countable if and only if A is finite or $A \sim \mathbb{N}$.

T 3.18:

• The set $\{0, 1\}^*$ of all finite binary sequences is countable.

T 3.19:

• The set $\mathbb{N} \times \mathbb{N}$ of ordered pairs of natural numbers is countable.

C 3.20:

• If A and B are countable sets, then their Cartesian product $A \times B$ is countable: $A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \implies A \times B \preceq \mathbb{N}$

C 3.21:

• The set of rational numbers $\mathbb{Q}$ is countable.

Idea: Every rational number can be written as $\frac{m}{n}$ with $m \in \mathbb{Z}$ and $n \in \mathbb{N}_{>0}$. Thus $\mathbb{Q} \preceq \mathbb{Z} \times \mathbb{N}$, which is countable.

T 3.22:

• Let A and $\{A_i\}_{i \in \mathbb{N}}$ be countable sets, then:
• For any $n \in \mathbb{N}$, the Cartesian product A^n is countable.
• The union $\bigcup_{i \in \mathbb{N}} A_i$ is countable.
• The set A^* of all finite sequences with elements from A is countable.

D 3.23:

• Let $\{0, 1\}^{\mathbb{N}}$ denote the set of infinite binary sequences, equivalently the set of functions $f : \mathbb{N} \to \{0, 1\}$.

T 3.23:

• The set $\{0, 1\}^{\mathbb{N}}$ is uncountable.

Idea: This follows from *Cantor's diagonal argument*.

D 3.44:

• A function $f : \mathbb{N} \to \{0, 1\}$ is called *computable* if there exists a program such that, for every $n \in \mathbb{N}$, the program outputs $f(n)$ when given input n.

C 3.24:

• There exist uncomputable functions $f : \mathbb{N} \to \{0, 1\}$.

Remark. The Halting Problem gives an explicit example of an uncomputable function.

4 Number Theory

D 4.1:

• Let $a, b \in \mathbb{Z}$. We say that a *divides* b, written • $a \mid b$, if there exists $c \in \mathbb{Z}$ such that • $b = ac$. If $a \neq 0$, then this quotient is unique and $c = \frac{b}{a}$. Every nonzero integer divides 0. The integers 1 and -1 divide every integer.

T 4.1 (Euclid):

• For all integers a and $d \neq 0$, there exist unique integers q and r such that: • $a = dq + r$ and $0 \leq r < |d|$.
Here: d - *divisor*, a - *dividend*, q - *quotient*, r - *remainder*.
The remainder is denoted by • $r = R_d(a)$ or • $r = a \bmod d$.

D 4.2 (Greatest Common Divisor):

• The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the integer d such that • $d \mid a \ \wedge \ d \mid b \ \wedge \ \big(\forall c \, (c \mid a \wedge c \mid b \Rightarrow c \mid d)\big)$.

L 4.3:

• If $a, b \in \mathbb{Z}$ are *relatively prime*, then • $\gcd(a, b) = 1$.

L 4.2:

• For all $m, n, q \in \mathbb{Z}$, • $\gcd(m, n + qm) = \gcd(m, n)$. In particular, • $\gcd\big(m, R_m(n)\big) = \gcd(m, n)$, which is the basis of the Euclidean al-

gorithm.

D 4.4:

• For $a, b \in \mathbb{Z}$, the *ideal generated by a and b*, denoted (a, b), is defined by $(a, b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$. For a single integer a, the ideal generated by a is $(a) = \{ua \mid u \in \mathbb{Z}\}$. Every ideal in $\mathbb{Z}$ can be generated by a single integer.

L 4.3:

• For $a, b \in \mathbb{Z}$, there exists $d \in \mathbb{Z}$ such that $(a, b) = (d)$.

L 4.4:

• Let $a, b \in \mathbb{Z}$, not both zero. If $(a, b) = (d)$, then d is a greatest common divisor of a and b.

C 4.5:

• If $a \in \mathbb{Z}$, then $(a, 0) = (a)$.

C (Bézout):

• For $a, b \in \mathbb{Z}$, not both zero, there exist $u, v \in \mathbb{Z}$ such that $\gcd(a, b) = ua + vb$.

Example: $\gcd(26, 18) = 2 = (-2) \cdot 26 + 3 \cdot 18$.

D 4.5 (Least Common Multiple):

• The *least common multiple* ℓ of positive integers a and b is the integer satisfying $a \mid \ell \ \wedge \ b \mid \ell \ \wedge \ \big(\forall m\,(a \mid m \wedge b \mid m \Rightarrow \ell \mid m)\big)$.

D 4.6:

• A positive integer $p > 1$ is called *prime* if the only positive divisors of p are 1 and p. An integer greater than 1 that is not prime is called *composite*.

T 4.6 (Fundamental Theorem of Arithmetic):

• Every positive integer can be written uniquely (up to the order in which the factors are listed) as a product of primes.

Thus, if $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$, then $\gcd(a, b) = \prod_i p_i^{\min(e_i, f_i)}$, and $\operatorname{lcm}(a, b) = \prod_i p_i^{\max(e_i, f_i)}$. In particular, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$, since $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$.

L 4.7:

• Every composite integer n has a prime divisor $p \leq \sqrt{n}$.

D 4.8 (Congruences):

• For $a, b, m \in \mathbb{Z}$ with $m \geq 1$, we say that a is *congruent* to b modulo m if m divides $a - b$. We write $a \equiv b \pmod{m}$, or simply $a \equiv_m b$. Equivalently, $a \equiv_m b \iff m \mid (a - b)$.

L 4.13:

• For any $m \geq 1$, the relation $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

L 4.14:

• If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$ and $ac \equiv_m bd$.

C 4.15:

• Let $f(x_1, \ldots, x_k)$ be a multivariable polynomial in k variables with integer coefficients, and let $m \geq 1$. If $a_i \equiv_m b_i \quad \text{for } 1 \leq i \leq k$, then $f(a_1, \ldots, a_k) \equiv_m f(b_1, \ldots, b_k)$.

L 4.16:

• For all $a, b, m \in \mathbb{Z}$ with $m \geq 1$:

(i) $a \equiv_m R_m(a)$.

(ii) $a \equiv_m b \iff R_m(a) = R_m(b)$.

C 4.17:

• Let $f(x_1, \ldots, x_k)$ be a multivariable polynomial with integer coefficients, and let $m \geq 1$, then:

$R_m\big(f(a_1, \ldots, a_k)\big) = R_m\big(f(R_m(a_1), \ldots, R_m(a_k))\big)$.

T 4.18:

• The congruence equation $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$. In this case, the solution is unique.

D 4.9:

• If $\gcd(a, m) = 1$, the unique solution $x \in \mathbb{Z}_m$ to the congruence equation $ax \equiv_m 1$ is called the *multiplicative inverse* of a modulo m.

Other notation: $x \equiv_m a^{-1}$ or $x \equiv_m \frac{1}{a}$. The multiplicative inverse can be efficiently computed using the *extended Euclidean algorithm*.

T 4.10 (Chinese Remainder Theorem):

• Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime integers, and let $M = \prod_{i=1}^{r} m_i$. For every list of integers $a_1, \ldots, a_r$ with $0 \leq a_i < m_i \quad \text{for } 1 \leq i \leq r$, the system of congruences $(x \equiv_{m_1} a_1,\ x \equiv_{m_2} a_2,\ \ldots\ ,\ x \equiv_{m_r} a_r)$ has a unique solution x satisfying $0 \leq x < M$.

6 Logic

6.1 Proof Systems

D 6.1 (Proof system):

• A quadruple $\Pi = (\mathcal{C}, \mathcal{P}, \tau, \phi)$

D 6.2 (Sound proof):

• A

7 Algorithms

Euclidean Algorithm

Computing big exponents

Chinese Remainder Theorem

Finding secret key

Finding secret key

Notes from Correction

Sets, relations

Finding elements/subsets:

- List elements of A explicily as a bullet list.
- $x \in A$: candidate set is exactly equal to one of the listed elements.
- $y \subseteq A$: every element of y is also in A.
- $\emptyset$ is a subset of everyset, $\{\emptyset\}$ has 1 element of emptyset.

Simplification of set expressions:

- Draw Venn diagramm.
- Convert expression to boolean logic:

$p, q, r := x \in A, B, C$, then $(A \cap B) \setminus B = (p \wedge q) \wedge \neg(r)$.

Working with cadinalities of sets and combinations:

- $|A \times B| = |A| \cdot |B|$
- If $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$, as they are disjoint.
- Define and split in cases.

Transitivity and Symmetry forces reflexivity:

- Transitivity and Symmetry forces reflexivity: $(a, b), (b, a) \in \rho,\ \rho = \hat{\rho} \Rightarrow (a, a) \in \rho$.

Upper bounds:

- Find lcm of a given set (divisibility) and find multiples of it which are greater than set elements.
- If we want in divisibility relation least upper bound, then find the upper bound that divides all other upper bounds. Otherwise it doesn't exist.

Proving function existence:

- First define if it is totally and well defined function. Then work with given condiitions.

Modular Arithmetic

Computing modulos with big exponents:

- Compute $a^N \pmod p$.
- Find a small k such that $a^k \equiv r \pmod p$.
- Write $N = kq\ (+ r_0)$.

$$a^N = (a^k)^q \cdot a^{r_0} \equiv r^q \cdot a^{r_0} \pmod p.$$

Evaluate and conclude. Example:
$2^6 \equiv -1 \pmod{13}$, $4536 = 6 \cdot 756 \Rightarrow 2^{4536} \equiv (-1)^{756} \equiv 1 \pmod{13}$.

GCD finding:

- $a^n \equiv 0 \pmod A \Rightarrow \gcd(A, B + a^n) = \gcd(A, B)$.
- $\gcd(A, B) = \gcd(A, B \bmod A)$

Euclidean Algorithm:

- $\gcd(A, B) = \gcd(B, A \bmod B)$.
- $A = Bq + r, \quad 0 \le r < B$.
- $\gcd(A, B) = \gcd(B, r)$.
- Repeat until $r = 0$.

Sophie Germain identity to find composite polynomials:

- $a^4 + 4b^4 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2)$.

Finite many solutions for $\varphi(x) = n$ for $x \in \mathbb{N}$:

- Let $n \in \mathbb{N}$ be fixed, and suppose $x \in \mathbb{N}$ satisfies

$$\varphi(x) = n.$$

Write the prime factorization of x as

$$x = \prod_{i=1}^{r} p_i^{e_i},$$

where the p_i are distinct primes and $e_i \ge 1$. Using the formula for Euler's totient function, we obtain

$$n = \varphi(x) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

Hence, for every prime divisor p_i of x, we have

$$p_i - 1 \mid n.$$

Since n has only finitely many divisors, there are only finitely many possible primes p_i that can divide x.

For each such prime p_i, the exponent e_i is bounded: indeed, increasing e_i strictly increases the value of $(p_i - 1)p_i^{e_i - 1}$ and therefore increases $\varphi(x)$. Thus only finitely many choices of the exponents e_i are possible.

Consequently, there are only finitely many natural numbers x such that $\varphi(x) = n$.

Algebra

Finding number of subgroups:

- The number of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ is given by $\sum_{\substack{a \mid m \\ b \mid n}} \gcd(a, b)$.

Generators of max. cyclic subgroups and their order:

- Compute the group orders of $\mathbb{Z}_m^*$ and $\mathbb{Z}_n^*$ separately.
- For finite groups G_1 and G_2 and $(a, b) \in G_1 \times G_2$,

$\operatorname{ord}(a, b) = \operatorname{lcm}\big(\operatorname{ord}(a), \operatorname{ord}(b)\big)$.

- Choose elements of maximal order in each factor to obtain a generator of a largest cyclic subgroup.

Finding isomoprhic groups:

- Testing the equality between multiplicative group orders with $\varphi(m)$ is not sufficient, it's also necessary to check cyclicity to preserve the group structure.

$\mathbb{Z}_8^*$ and $\mathbb{Z}_{12}^*$ are not cyclic: the group $\mathbb{Z}_m^*$ is cyclic $\iff$ $m \in \{2, 4, p^e, 2p^e\}$ where p is an odd prime and $e \ge 1$ exponent (Th 5.15).

Finding GCD of 2 polynomials:

- Let $f_0(x),\ f_1(x) \in \mathbb{F}[x], \quad \deg f_0 \ge \deg f_1$.

$f_0(x) = q_1(x) f_1(x) + r_1(x), \quad \deg r_1 < \deg f_1$
$f_1(x) = q_2(x) r_1(x) + r_2(x), \quad \deg r_2 < \deg r_1$
$r_1(x) = q_3(x) r_2(x) + r_3(x)$
$\vdots$
$r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x)$
$r_{k-1}(x) = q_{k+1}(x) r_k(x)$
$\boxed{\gcd(f_0(x), f_1(x)) = r_k(x)}$

(Optional: normalize $r_k(x)$ to be monic. Take out factors by finding common roots for finding divisors of both polynomials, which after division will be inserted in the next iteration of gcd.)

there exist infinitely many irreducible polynomials in $F[x]$:

- Suppose, towards a contradiction, that there are only finitely many irreducible polynomials in $F[x]$, say $f_1(x), f_2(x), \ldots, f_n(x)$.

Since F is a field, $F[x]$ is a Euclidean domain, and hence every non-constant polynomial factors into irreducible polynomials.

Define $p(x) = f_1(x) f_2(x) \cdots f_n(x) + 1$. Then $p(x) \in F[x]$ and $\deg p(x) \ge 1$.

For each $i \in \{1, \ldots, n\}$, we have $p(x) \equiv 1 \pmod{f_i(x)}$, so $f_i(x)$ does not divide $p(x)$. Therefore, $p(x)$ has no irreducible factor among $f_1(x), \ldots, f_n(x)$.

If $p(x)$ is irreducible, then it is an irreducible polynomial not in the list, a contradiction. If $p(x)$ is reducible, then it factors into irreducible polynomials, none of which can be among $f_1(x), \ldots, f_n(x)$, again a contradiction.

Hence, there must be infinitely many irreducible polynomials in $F[x]$.

Proving a field with polynomials:

- Example: Show $\mathbb{Z}_3[x]_{x^4+x+2}$ is a field:
- show that $\mathbb{Z}_3$ is a field.
- show that $x^4 + x + 2$ is irreducible.

Logic

CNF and DNF equivalence & difference:

- When literals, negation $\neg$ and only exactly one operator among $\wedge, \vee$ shows up in a formula, then it is in both CNF and DNF. Negation applied to non-literals $\rightarrow$ neither CNF or DNF.

For example: CNF $\equiv A \wedge B \wedge \neg C \equiv (A \wedge B \wedge \neg C) \equiv$ DNF

Disproving:

- Find a counter example that shows that a given statement does not hold generally. For example disproving $\mathcal{K} \models K \Longrightarrow \mathcal{K} \vdash_{res} K$:
- Consider $\mathcal{K} := \varnothing$ and $K := \{A, \neg A\}$.

K corresponds to the formula $A \vee \neg A \equiv \top$ and is a tautology. Hence $\models K$, and $\mathcal{K} \models K$ also holds.

Since our clause set is empty, no clauses can be derived. In particular, K cannot be derived, i.e. $\mathcal{K} \nvdash_{res} K$

Soundness of the rule $\vdash_r$:

- **Soundness.** Let F_Γ, F_Δ be the propositional formulas corresponding

to Γ, Δ. Then

$$\Gamma \models \Delta \iff F_\Gamma \to F_\Delta \text{ is a tautology.}$$

Since

$$F_\Gamma \to F_\Delta \equiv \neg F_\Gamma \vee F_\Delta \equiv \top,$$

the rule is sound.

Proving the statement with resolution calculus:

• Example: prove $((A \wedge B) \to C) \wedge (C \to D) \models (A \wedge B) \to D$ (using resolution calculus)

To prove the given statement we can show that $\{((A \wedge B) \to C), (C \to D), \neg((A \wedge B) \to D)\}$ is unsatisfiable

(By **Lemma 6.3** we know $\{F_1, ..., F_k\} \models G$ is equivalent to $\{F_1, ..., F_k, \neg G\}$ *is unsatisfiable*.)