Diskrete Mathematik

by Danny Camenisch

Logic

D 2.1. A mathematical statement (true or false) is a proposition

A	B	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

$\wedge$ conjunction

$\vee$ disjunction

$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$, $A \to B \equiv \neg A \vee B$ notational convention

General Concepts

D.6.4. Syntax symbols that are allowed and which combinations.
D.6.5. Semantics define a function free, which assigns each F a set of indeces that are free symbols.
D.6.6. An interpretation $\mathcal{A}$ assigns each symbol a value.
D.6.7. $\mathcal{A}$ is suitable if it assigns a value for all free symbols.
D.6.8. The semantics also define a function $\sigma(F, \mathcal{A}) = \{0,1\}$ or $\mathcal{A}(F)$, giving the truth value of F under $\mathcal{A}$.
D.6.9. If $\mathcal{A}(F)=1$, then is $\mathcal{A}$ a model for F or even a set of formulas M. One writes $\mathcal{A} \models F$, $\mathcal{A} \models M$, $\mathcal{A} \not\models F$.

Satisfiability, Tautology, Consequence, Equivalence

D.6.10. F is satisfiable if there exists a model and unsatisfiable $\perp$ otherwise.
D.6.11. F is a tautology $\top$ if it is true for every suitable $\mathcal{A}$.
D.6.12. G is a logical consequence of F ($F \models G$) if every suitable interpretation for both F, G, is a model for G, if it is a model for F. ($F \leq G$)
D.6.13. F and G are equivalent $F \equiv G$ if $F \models G$ and $G \models F$.
D.6.14. If F is a tautology one writes $\models F$.
L.6.2. F is a tautology iff $\neg F$ is unsatisfiable.
L.6.3. These statements are equivalent:
- $\{F_1, \dots, F_k\} \models G$
- $\{F_1 \wedge F_2 \wedge \dots \wedge F_k\} \to G$ is a tautology
- $\{F_1, \dots, F_k, \neg G\}$ is unsatisfiable.

Logical Operators $\vee \wedge \neg$

D.6.15. If F and G are formulas, so are $\neg F$, $F \vee G$, $F \wedge G$
D.6.16.
- $\mathcal{A}(F \wedge G) = 1 \iff \mathcal{A}(F)=1$ and $\mathcal{A}(G)=1$
- $\mathcal{A}(F \vee G) = 1 \iff \mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$
- $\mathcal{A}(\neg F) = 1 \iff \mathcal{A}(F)=0$

These are again used in D 6.24 / D.6.36
Prop. Logic / Pred. Logic

L.6.1.
1) $F \wedge F \equiv F$ and $F \vee F \equiv F$ idempotence
2) $F \wedge G \equiv G \wedge F$ and $F \vee G \equiv G \vee F$ commutativity
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ same for $\vee$ associativity
4) $F \wedge (F \vee G) \equiv F$ and $F \vee (F \wedge G) \equiv F$ absorption
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ distributive law
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ distributive law
7) $\neg\neg F \equiv F$ double negation
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ and $\neg(F \vee G) \equiv \neg F \wedge \neg G$ de Morgan's rules
9) $F \vee \top \equiv \top$ and $F \wedge \top \equiv F$ tautology rules
10) $F \vee \perp \equiv F$ and $F \wedge \perp \equiv \perp$ unsatisfiability rules
11) $F \vee \neg F \equiv \top$ and $F \wedge \neg F \equiv \perp$

Logical Calculi

Hilberti-Style Calculi

D.6.17 derivation rule $\{F_1, \dots, F_k\} \vdash_R G$ or $\frac{F_1, \dots, F_K}{G}$ (R)
D.6.18 Applyind a derivation rule means:
- Select $N \subseteq M$
- Specify $N \vdash_R G$
- $M \cup \{G\}$

D.6.19. A calculus K is a finite set of deriviation rules.
D.6.20. A derivation of a formula from M in K, is a finite sequence of applications of $R \in K$.
D.6.21. A derivation rule is correct if $\forall M, F \quad M \vdash_R F \Rightarrow M \models F$.
D.6.22. A calculus is sound / correct if $M \vdash_K F \Rightarrow M \models F$.
A calculus is complete if $M \models F \Rightarrow M \vdash_K F$.
L.6.4. If $\{F_1, \dots, F_k\} \vdash_K G$, then $\models (F_1 \wedge \dots \wedge F_k) \to G$.

We can extend calculi by adding sequences of rule applications.

Ex. Calculi

complete & not sound : $K = \{R\}$ where $\vdash_R F$
not complete & sound : $K = \{R\}$ where $\{F\} \vdash_R F$

Propositional Logic

D.6.23. Syntax: An atomic formula is of the form A_i.
A formula is defined as in D.6.15.
D.6.24. Semantics: D.6.16.
D.6.25. A literal is an atomic formula or its negation.
D.6.26. Conjunctive Normal Form: $(L \vee L \vee L) \wedge (\dots) \dots$
D.6.27. Disjunctive Normal Form: $(L \wedge L \wedge L) \vee (\dots) \dots$
T.6.5 Every formula is $\equiv$ to a DNF/CNF formula.

Given F calculate the truth table:
DNF: (Row 1) $\vee$ (Row 2) ... only the rows which are true
↳ $(A_1 \wedge A_2 \dots)$ A_i: A_i if $=1$ else $\neg A_i$
CNF (Row 1) $\wedge$ (Row 2) ... only the rows which are false
↳ $(A_1 \vee A_2 \dots)$ A_i: A_i if $=0$ else $\neg A_i$

Ex. Prove that the resolution calculus is not complete.
Let $F = A$ and $G = A \vee B$ we know $F \models G$. But we can't derive $\mathcal{K}(A \vee B)$ from $\mathcal{K}(A)$ using the res. calc.

Resolution Calculus

sound, but not complete

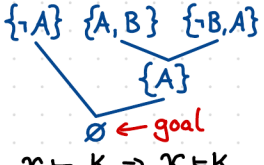
The resolution calculus is used to prove unsatisfiability and logical consequence (since $M \models F$ is true only if $M \cup \{\neg F\}$ is unsatisfiable L.6.3.). The formulas have to be in CNF.

D.6.28. A clause ($L \wedge L \wedge L$) is a set of literals.
D.6.29. A set of clauses is denoted $K(F)$ — $K(M)$ is the union of all $K(F)$.

The empty clause is unsatisfiable and the empty clause set is a tautology.

D.6.30. A clause K is resolvent if K_1 and K_2 contain a literal $L \in K_1$, $\neg L \in K_2$ and
$K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

Resolution steps must be carried out one by one. To be consistent one can write $\{K_1, K_2\} \vdash_{Res} K$. The resolution calculus can be denoted $Res = \{res\}$



L.6.6. The resolution calculus is sound. $\mathcal{K} \vdash_{res} K \Rightarrow \mathcal{K} \models K$
T.6.7. A set M is unsatisfiable iff $\mathcal{K}(M) \vdash_{res} \emptyset$.

Predicate Logic

D.6.31. Syntax:
- variable: x_i, $i \in \mathbb{N}$
- function: $f_i^{(k)}$, $i,k \in \mathbb{N}$, where k = # arguments
- predicate: $P_i^{(k)}$, $i,k \in \mathbb{N}$, where k = # arguments

defined inductively {
- term: t_i, variables and functions
- formulas:
  - predicates are atomic formulas
  - if F and G are formulas, so are $\neg F$, $F \vee G$, $F \wedge G$
  - if F is a formula, so is $\forall x F$ and $\exists x F$

D.6.32. Every variable is either bound or free, F is closed if all variables are bound.
D.6.33. For F, $F_{[x/t]}$ denotes the formula obtained by replacing every free x with the term t.
D.6.34. Semantics: a interpretation $\mathcal{A} = (U, \phi, \psi, \xi)$ is a tuple:
- U = universe
- ϕ = function assigning function : $f^{\mathcal{A}}$
- ψ = function assigning predicate: $P^{\mathcal{A}}$
- ξ = function assigning free variables.

D.6.35. $\mathcal{A}$ is suitable if all functions, predicates and free variables of F are defined.
D.6.36. The value of a term is defined:
- $\mathcal{A}(t) = \xi(t)$ if variable
- $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n))$ if function

The truth value of a formula:
- $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$ if predicate
- $\mathcal{A}(\forall x F) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(F) = 1 \text{ for } \underline{\text{all}}\ u \in U \\ 0 & \text{else} \end{cases}$
$\mathcal{A}(\exists x F)$ — some

L.6.8. For all F, G and H where x does not occure free in H:

1) $\neg(\forall x F) \equiv \exists x \neg F$	6) $\exists x \exists y F \equiv \exists y \exists x F$
2) $\neg(\exists x F) \equiv \forall x \neg F$	7) $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
3) $(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$	8) $(\forall x F) \vee H \equiv \forall x (F \vee H)$
4) $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$	9) $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
5) $\forall x \forall y F \equiv \forall y \forall x F$	10) $(\exists x F) \vee H \equiv \exists x (F \vee H)$

L.6.9. If one replaces a subformula of F, with a equivalent formula, then the resulting formula is equivalent to F.

L.6.10. For a formula G in which y does not occure:
- $\forall x G \equiv \forall y\, G_{[x/y]}$ and - $\exists x G \equiv \exists y\, G_{[x/y]}$

D.6.37. A formula in which no variable occurs as both bound and free and in which all variables after quantifiers are distinct, is in rectified form.

L.6.11. $\forall x F \models F_{[x/t]}$ for any t. $\Rightarrow \forall x \models F$

D.6.38. A formula of the form $Q_1 x_1 Q_2 x_2 \ldots F$ where Q_i is a quantifier and G does not contain any quantifiers is said to be in prenex form.
$\Rightarrow$ To achieve first rectivied form, then L.6.8.

T.6.12. For every formula, there is a equivalent formula in prenex form.

Prenex: ① rename bound variables ② remove all $\rightarrow$ ③ apply de Morgan ④ shift $\exists, \forall$ to front

T.6.13. $\neg \exists x \forall y (P(y,x) \leftrightarrow P(y,y))$

Ex. Prove $\forall x (F \wedge G) \models (\forall x F) \wedge G$.

Let F and G be any suitable formulas. Let A be any structure suitable for $\forall x (F \wedge G)$ and $(\forall x F) \wedge G$.
Assume $A(\forall x (F \wedge G)) = 1$

sem $\forall$ $\Rightarrow$ $A_{[x \to u]}(F \wedge G) = 1$ for any $u \in U^A$

sem $\wedge$ $\Rightarrow$ $A_{[x \to u]}(F) = 1$ and $A_{[x \to u]}(G) = 1$ for any $u \in U^A$
$\Rightarrow$ $A_{[x \to u]}(F) = 1$ for any $u \in U^A$ and $A_{[x \to u]}(G) = 1$ for any $u \in U^A$

sem $\forall$ $\Rightarrow$ $A(\forall x F) = 1$ and $A_{[x \to u]}(G) = 1$ for any $u \in U^A$

Case 1: x does not occur free in G
Then for any u, we have $A_{[x \to u]}(G) = A(G)$.
So $A(G) = A_{[x \to u]}(G) = 1$.

Case 2: x does occur free in G
Then x occurs free in $(\forall x F) \wedge G$. So if A is suitable it defines $x \in U^A$. Since $A_{[x \to y]}(G) = 1$ for all $u \in U^A$, we have in particular for $u = x^A$, $A_{[x \to x^A]}(G) = 1$. So $A(G) = A_{[x \to x^A]}(G) = 1$.

Therefore $A(\forall x F) = 1$ and $A(G) = 1 \overset{\text{sem } \wedge}{\Rightarrow} A((\forall x F) \wedge G) = 1$

Proof Systems

D.6.1. A proof system is a quadruple $\Pi = (S, P, \tau, \phi)$.
- $s \in S$: statement - $\tau: S \to \{0,1\}$ truth function
- $p \in P$: proof - $\phi: S \times P \to \{0,1\}$ verification function

D.6.2. A proof system is sound if no false statement has a proof.

D.6.3. A proof system is complete if every true statement has a proof.

Ex. Proof Systems: $S = P = \{0,1\}^3$

complete & not sound: $\tau(s) = 1$ if s contains at most one 0.
$\phi(s,p) = 1$ if s contains at most two 0 and $s = p$

not complete & sound: $\tau(s) = 1$ if s contains at least one 1
$\phi(s,p) = 1$ if $d(s,p) = 3$ and p contains exactly one 0
↳ Hamming Distance

Proof Patterns

Composition of Implication D2.13. If $S \Rightarrow T$ and $T \Rightarrow U$ are both true, then $S \Rightarrow U$ is true. L2.5 $(A \to B) \wedge (B \to C) \models A \to C$

Direct Proof of an Impl. D2.14. Proof $S \Rightarrow T$ by assuming S and proving T under this assumption.

Indirect Proof of an Impl. D2.15. Proof $S \Rightarrow T$ by assuming $\neg T$ and proving $\neg S$ under this assumption.

Modus Ponens D2.16 Prove S by finding R, proving R and then proving $R \Rightarrow S$. L 2.7. $A \wedge (A \to B) \models B$.

Case Distinction D2.17. Prove S by finding a list $R_1, \ldots, R_k$ (cases), proving one R_i and prove for all $R_i \Rightarrow S$.

Proof by Contradiction D2.18 Prove S by finding T, proving T is false and then prove T is true under the assumption that S is false.

Existence Proof D2.19. Prove that S is true for at least one $x \in \mathcal{X}$, if true constructive else non-constructive.

Pigeonhole Principle T 2.10. If a set of n objects is split into $k < n$ sets, then atleast one set contains $\lceil \frac{n}{k} \rceil$ objects.

Proof by Counterexample D2.20 Prove by counterexample that S is not true for all x.

Proof by Induction Prove $P(0)$ Basis Step, then prove for any n $P(n) \Rightarrow P(n+1)$ Induction Step.

Sets, Relations and Functions

Sets

D.3.1. $|A|$ = cardinality = # elements in a finite set A

D.3.2. $A = B \Leftrightarrow \forall x (x \in A \wedge x \in B)$
D.3.3. $A \subseteq B \Leftrightarrow \forall x (x \in A \to x \in B)$ $\Big\} \Rightarrow A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

D.3.4. $\emptyset = \{\}$ $\Rightarrow$ L.3.3. $\forall A (\emptyset \subseteq A)$

D.3.5. Powerset: $\mathcal{P}(A) = \{S \mid S \subseteq A\}$ $\quad \mathcal{P}(\emptyset) = \{\emptyset\}$

D.3.6. Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$
Intersection: $A \cap B = \{x \mid x \in A \vee x \in B\}$

D.3.7. Complement: $\bar{A} = \{x \in U \mid x \notin A\}$ for some universe U.

D.3.8. Difference: $B \setminus A = \{x \in B \mid x \notin A\}$

T.3.4.
- Idempotence: $A \cup A = A$, $A \cap A = A$
- Commutativity: $A \cap B = B \cap A$, $A \cup B = B \cup A$
- Associativity: $A \cap (B \cap C) = (A \cap B) \cap C$ same for $\cup$
- Absorbtion: $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$
- Distributivity: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ same for $\cup$
- Consistency: $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$

D.3.9. Cartesian Product: $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$ ordered pairs

Relations

$\emptyset \times A = \emptyset$ $\quad (a,b) \in (A \times B) \Rightarrow a \in A \wedge b \in B$

D.3.10. A relation ρ from set A to B is a subset of $A \times B$, if $B = A$, its a relation on A.

D.3.11. The identity relation on A is denoted id_A.

D.3.12. The inverse of ρ is $\hat{\rho} = \{(b,a) \mid (a,b) \in \rho\}$.

D.3.13. If ρ, σ are relations then $\rho \circ \sigma = \{(a,c) \mid \exists b ((a,b) \in \rho \wedge (b,c) \in \sigma)\}$ is their composition.

L.3.6. $\widehat{\rho \circ \sigma} = \hat{\sigma} \circ \hat{\rho}$

calculate ρ^2 etc. by matrix multiplication, for ρ^* add $\rho + \rho^2 + \rho^3 \ldots$

Special Properties

D3.14. Reflexive: $a \rho a$ is true for all $a \in A$, $id \subseteq \rho$
Irreflexive: $a \rho a$ is false for $\forall a$

D.3.16. Symetric: $a \rho b \Leftrightarrow b \rho a$ is true for all $a, b \in A$

D.3.17. Antisymetric: $(a \rho b \wedge b \rho a) \Rightarrow a = b$ is true for all $a, b \in A$

D.3.18. Transitive: $(a \rho b \wedge b \rho c) \Rightarrow a \rho c$ is true for all $a, b, c \in A$

L.3.7. A relation is transitive iff $\rho^2 \subseteq \rho$. D.3.19. ρ^* transitive closure

Equivalence Relations and Posets

D.3.20. An equivalence relation is reflexive, symetric & transitive.

D.3.21. For θ on A, $[a]_\theta$ is an equivalence class, defined as $[a]_\theta = \{b \in A \mid b \theta a\}$.

L.3.8. Two intersections of equiv. relations form a equiv. relation.

T.3.9 The quotient set A/θ of equivalence classes of θ on A is a partition of A.

Ex. Let ρ, σ be equivalence relations, prove that $\rho \circ \sigma$ is a equiv. relation if $\rho \circ \sigma = \sigma \circ \rho$.

reflexive: $\forall a \in A\ (a \rho a \wedge a \sigma a)$ | ρ, σ reflexive
$\Rightarrow \forall a \in A\ (a \rho \circ \sigma a)$ | def $\circ$

symetric: For any $a, b \in A$, $(a,b) \in \rho \circ \sigma$
$\Rightarrow (b,a) \in \widehat{\rho \circ \sigma}$ | def inverse
$\Rightarrow (b,a) \in \widehat{\sigma \circ \rho}$ | $\rho \circ \sigma = \sigma \circ \rho$
$\Rightarrow (b,a) \in \hat{\rho} \circ \hat{\sigma}$ | L. 3.6.
$\Rightarrow (b,a) \in \rho \circ \sigma$ | symetrie of ρ, σ

transitive: For any $a, b, c \in A$, show $\rho \circ \sigma = (\rho \circ \sigma)^2$ which will prove transitivity L.3.7.

$(\rho \circ \sigma) \circ (\rho \circ \sigma) \overset{\text{Ass.}}{=} \rho \circ (\sigma \circ \rho) \circ \sigma \overset{\text{Asu.}}{=} \rho \circ (\rho \circ \sigma) \circ \sigma$
$\overset{\text{Ass}}{=} \rho^2 \circ \sigma^2 = \rho \circ \sigma$ (since ρ, σ are transitive)

D.3.24. A partial order on a set is reflexive, antisymetric and transitive. A set with a partial order $\preccurlyeq$ is called a poset.

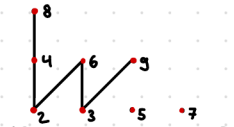
D.3.25. For a poset two elements are comparable if $a \preccurlyeq b$ or $b \preccurlyeq a$.

D.3.26. If all elements are comparable, then A is totally-ordered

D.3.27. In a poset an element b covers a, if $a \prec b$ and there exists no c, $a \prec c$ and $c \prec b$.

$$a \prec b \iff a \preccurlyeq b \wedge a \neq b$$

D.3.28. The Hasse diagram of a poset, is a directed graph whose vertices are $\in A$ and the edge (a,b) means that a covers b.



$(\{2,3,4,5,6,7,8,9\}; |)$

T.3.10. $(a_1,b_1) \leq (a_2,b_2) \iff a_1 \preccurlyeq a_2 \wedge b_1 \sqsubseteq b_2$ is a p.o. relation

T.3.11. $(a_1,b_1) \leq (a_2,b_2) \iff a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$, lex. order, is a p.o. relation

D.3.29. Special Elements: let $(A;\preccurlyeq)$ be a poset and $S \subseteq A$.

1. $a \in A$ is a min./max element, if $\nexists b$ with $b \prec a / a \prec b$.
2. $a \in A$ is the least/greatest element, if for $\forall b$ $a \preccurlyeq b / b \preccurlyeq a$.
3. $a \in A$ is the lower/upper bound of S if $\forall b \in S$ $a \preccurlyeq b / b \preccurlyeq a$.
4. $a \in A$ is the greatest lower bound/least upper bound of S if a is the greatest/least element of all lower/upper bounds of S.

D.3.30. A is well-ordered if it is totally ordered and every subset has a least element.

D.3.31. If $\{a,b\}$ have a greatest lower bound $a \wedge b$ it is called the meet, if they have a lowest upper bound $a \vee b$ it is called a join.

D.3.32. If all pairs of elements in a poset have a meet and join, it is called a lattice.

Ex. Show that $\forall a \forall b ((a \rho b \wedge b \rho a) \to a = b)$ iff $\rho \cap \hat{\rho} = id$

Let $(a,b) \in \rho \cap \hat{\rho}$ be arbitrary

$(a,b) \in \rho \cap \hat{\rho} \wedge \rho \cap \hat{\rho} \subseteq id$

$\iff (a,b) \in \rho \wedge (a,b) \in \hat{\rho} \to (a,b) \in id$

$\iff (a,b) \in \rho \wedge (b,a) \in \rho \to (a,b) \in id$

$\iff (a \rho b \wedge b \rho a) \to a = b$

$\iff \rho$ is antisymmetric

Functions

D.3.33. A function $f: A \to B$ from a domain to a codomain is a relation afb with special properties:

1. $\forall a \in A \; \exists b \in B \; afb$ — totally defined
2. $\forall a \in A \; \forall b,b' \in B \; (afb \wedge afb') \to b = b'$ — well-defined

D.3.34. The set of all functions $f: A \to B$ is denoted B^A

D.3.35. A partial function is a relation such that 2. is true.

D.3.36. If $S \subseteq A$, then the image of S is $f(S) = \{f(a) \mid a \in S\}$

D.3.37. The subset $f(A)$ of B is called the image of f $\mathrm{Im}(f)$.

D.3.38. For $T \subseteq B$, the preimage $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$.

D.3.39. Injective: if $a \neq b$, then $f(a) \neq f(b)$.
Surjective: if $f(A) = B$, $\forall b \in B \; \exists a \; f(a) = b$
Bijective: injective and surjective D.3.40 $\Rightarrow$ has inverse f^{-1}

For $f: A \to B$ and $g: B \to A$ we can say that f is injective iff g is surjective.

There are $|B|^{|A|}$ functions: $A \to B$

D.3.41. The composition is defined $(g \circ f)(a) = g(f(a))$

L.3.12. Function composition is associative.

Ex. Prove that for $f: A \to A$ exist a g such that $g \circ f = id$ iff f is injective.

$\Rightarrow$ Consider $f(a) = f(b)$

$$\begin{aligned} a &= (g \circ f)(a) \\ &= g(f(a)) \\ &= g(f(b)) \\ &= (g \circ f)(b) \\ &= b \end{aligned}$$

$\Leftarrow$ We construct g as follows for any $b \in \mathrm{Im} f$ $g(b) = f(a)$ where $f(a) = b$. For $b \notin \mathrm{Im} f$, $g(b) = b$. We get $g \circ f = id$, because $\forall a \in A$, $f(a) \in \mathrm{Im} f$, so $g(f(a)) = a$. $\square$

Ex. Prove that every $a \in D \setminus \{0\}$ is a unit:

We define $f_a: D \to D$, $x \to a \cdot x$.

injective: Assume $x, y \in D$ $x \neq y$ and $f_a(x) = f_a(y)$.

$$0 = f_a(y) - f_a(y) = a \cdot y - a \cdot x = a \cdot y + a \cdot (-x) = a \cdot (y - x)$$

since $a \neq 0$, $y - x$ has to be 0 and thats the case if $x = y$. Else a would be a zero divisor.

surjective: If f_a was not injective we would have $y \notin \mathrm{Im}(f_a)$ for some $y \in D$. Which for finite D implies $|\mathrm{Im}(f_a)| < |D|$. This is a contradiction to the fact that f_a is injective, therefore is f_a surjective and also bijective.

The inverse of a is $f_a^{-1}(1)$ and therefore is a a unit. $\square$

Ex. $F: \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, $f \to f \circ f$ prove that F is not surjective.

Hint: use $h(0) = 1$ $h(1) = 0$ and $h(x) = x$ for $x \geq 2$.

Assume F is surjective then there must be a g such that $g \circ g = h$.

Case: $g(0) = 0 \Rightarrow (g \circ g)(0) = g(0) = 0 \Rightarrow$ contradiction

Case: $g(1) = 1 \Rightarrow (g \circ g)(1) = g(1) = 1 \Rightarrow$ contradiction

Case: $g(0) = 1$, $g(1) = 0 \Rightarrow (g \circ g)(0) = g(1) = 0 \Rightarrow$ contradiction

Case: $g(0) = x$, $g(1) = y$ with $x, y \geq 2$

$\Rightarrow (g \circ g)(0) = g(x) = 1$ since $h(0) = 1$ but this contradicts $h(x) = x$

Countability

D.3.42. i) A and B are equinumerous, $A \sim B$, if there exists a bijection $A \to B$.

ii) B dominates A, $A \preccurlyeq B$, if $A \sim C$ for $C \subseteq B$ or if there exist an injective function $A \to B$.

iii) A is countable iff $A \preccurlyeq \mathbb{N}$. $\mathbb{N}$ is countable

L.3.13. i) $\preccurlyeq$ is transitive ii) $A \subseteq B \Rightarrow A \preccurlyeq B$

T.3.14. $A \preccurlyeq B \wedge B \preccurlyeq A \Rightarrow A \sim B$

T.3.15. A is countable iff A is finite or $A \sim \mathbb{N}$.

Cantors diagonalization argument:

We define α_{ij} as the j-th digit of the i-th sequence $f(i) = \alpha_{i0}\alpha_{i1}\alpha_{i2}\ldots$. We further define $\widehat{\alpha_{ij}} = \alpha_{jj} + 1$. Now we take $\beta = \widehat{\alpha_{00}}\,\widehat{\alpha_{11}}\,\widehat{\alpha_{22}}\ldots$ From this definition it is clear that β is different from all $f(i)$ by at least one digit.

Countable sets

T.3.16 $\{0,1\}^*$

T.3.17 $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$

C.3.19 $\mathbb{Q}$

T.3.20. i) the set of n-tuples over A
ii) union of countable sets
iii) The set A^* of finite sequences of A

T.3.21. $\{0,1\}^\infty$ is uncountable $\Rightarrow \mathbb{R}$ uncountable

D.3.44. A function $f: \mathbb{N} \to \{0,1\}$ is computable if there exist a program $p \in \{0,1\}^*$ that can compute $f(n)$ for all $n \in \mathbb{N}$.

Ex. Is the set of all zigzag functions countable?
($f: \mathbb{N} \to \mathbb{N}$ so that $f(n) < f(n+1)$, $f(n-1) > f(n)$)
We will prove that the subset $A' = \{f \mid n \text{ odd} \Rightarrow f(n) = 0\}$ is uncountable. We create a bijective mapping $\phi: A' \to \mathbb{N}_+^\infty$, $f \to f(0)f(2)f(4)\ldots$. As ϕ is bijective and $\mathbb{N}_+^\infty$ is uncountable, A' is uncountable and therefore also A.

Ex. Prove that set of equivalence relations S is uncountable.
We define $f: \mathcal{P}(\mathbb{N} \setminus \{0\}) \to S$, consider $A \in \mathcal{P}(\mathbb{N} \setminus \{0\})$. We partition $\mathbb{N}$ into $A \cup \{0\}$ and $\mathbb{N} \setminus A \cup \{0\}$ and define the equivalence relation $f(A)$ such that two numbers are related if they are in the same partition. Clearly f is injective since for two sets A and A', the equivalence class of 0 are different, hence $f(A) \neq f(A')$. T.3.21. elements of $\mathcal{P}(\mathbb{N} \setminus \{0\})$ correspond to $\{0,1\}^\infty$ and therefore it is uncountable.

Number Theory

Division

D.4.1. If a divides b we write $a \mid b$, $a \cdot c = b$. c is the unique quotient, b is the multiple and a is the divisor.

T.4.1. For all integers a and $d \neq 0$, the exist unique q and r so that $a = d \cdot q + r$ and $0 \leq r < |d|$.

D.4.2. For $a, b \in \mathbb{Z}$ (not both 0), $d \in \mathbb{Z}$ is the greatest common divisor, if $d \mid a \wedge d \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \to c \mid d)$

D.4.3. If $\gcd(a,b) = 1$, then a, b are relatively prime.

L.4.2. $\gcd(m, n - qm) = \gcd(m, n)$
$\Rightarrow$ euclid alg. $\gcd(m,n) = \gcd(R_n(m), m) = \ldots$

D.4.4. The ideal of $a, b \in \mathbb{Z}$ is $(a,b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$
$a \in \mathbb{Z}$ is $(a) = \{u \cdot a \mid u \in \mathbb{Z}\}$

L.4.3. For $a, b \in \mathbb{Z}$ there exists $d \in \mathbb{Z}$, $(a,b) = (d)$

L.4.4. If $(a,b) = (d)$, then $d = \gcd(a,b)$.
$\Rightarrow \gcd(a,b) = ua + vb$, $u, v \in \mathbb{Z}$

D.4.5. The least common multiple l of $a, b \in \mathbb{Z}$, denoted $\mathrm{lcm}(a,b)$, is defined as $a \mid l \wedge b \mid l \wedge \forall c ((a \mid c \wedge b \mid c) \to l \mid c)$

Primes

D.4.6. A positive integer $p > 1$ is a prime iff the only positive divisors of p are p and 1. Else a number is a composit.

T.4.6. Every positive integer can be written uniquely as the products of primes.

We can write $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$. Now we have $\gcd(a,b) = \prod_i p_i^{\min(e_i, f_i)}$ and $\mathrm{lcd} = \prod_i p_i^{\max(e_i, f_i)}$. We can see that $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = a \cdot b$, since $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$.

Congruences and Modular Arithmetic

D. 4.8. For $a,b,m \in \mathbb{Z}$, $m \geq 1$ we say a is congruent to b modulo m, if m divides $a-b$.

$$a \equiv_m b \iff m \mid a-b$$

L. 4.13. For any $m \geq 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$.

L. 4.14. $a \equiv_m b$ and $c \equiv_m d \Rightarrow a+c \equiv_m d+b$ and $ac \equiv_m bd$.

C. 4.15. $f(a_1,\dots,a_k) \equiv_m f(b_1,\dots,b_k)$ for $a_i \equiv_m b_i$.

L. 4.16. i) $a \equiv_m R_m(a)$
ii) $a \equiv_m b \iff R_m(a) = R_m(b)$

C. 4.17. $R_m(f(a_1,\dots,a_k)) = R_m(f(R_m(a_1),\dots,R_m(a_k)))$

$\Rightarrow$
- $R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$
- $R_m(a+b) = R_m(R_m(a) + R_m(b))$
- $R_m(a^b) = R_m(R_m(a)^b)$

From Fermants little theorem and Eulers theorem:

$$\boxed{\text{If } \gcd(m,a)=1, \text{ then } R_m(a^b) = R_m(a^{R_{\varphi(m)}(b)})}$$

Ex. Prove that if $s(a) = s(2a)$ (s denotes sum of digits) then $9 \mid a$. Use fact that $R_9(a) = R_9(s(a))$

$R_9(a) = R_9(s(a)) = R_9(s(2\cdot a)) = R_9(2a) = R_9(2)\cdot R_9(a)$
$\Rightarrow R_9(a) = 2 \times R_9(a)$
$\Rightarrow R_9(a) = 0$

Ex. Prove that for all $a,b \in \mathbb{Z}$ such that $a^2+b^2 \equiv_7 0$ it holds that $a^2 \equiv_7 0$ and $b^2 \equiv_7 0$.

Note that $R_7(x) \in \{0,1,2,3,4,5,6\} \Rightarrow R_7(x^2) \in \{0,1,2,4\}$

$0 = R_7(a^2+b^2) = R_7(R_7(a^2) + R_7(b^2))$
therefore $R_7(a^2) = R_7(b^2) = 0$

Ex. Prove that for all $a,b,c \in \mathbb{Z}\setminus\{0\}$, if $a \mid bc$ and $\gcd(a,b)=1$ then $a \mid c$.

$\gcd(a,b)=1 \Rightarrow ua+vb=1$ for some $u,v \in \mathbb{Z}$
$a \mid bc \Rightarrow bc = ad$

$c = 1c = (ua+vb)\cdot c = uac + vbc = uac + vad = (uc+vd)\cdot a$
$\Rightarrow a \mid c$

Ex. Prove that for all $n \geq 2$, if $3 \nmid n$, then n^2+2^n is not prime.

Case 1: n is even ($n=2k$):
$(2k)^2 + 2^n = 4\cdot k^2 + 2\cdot 2^{n-1} \Rightarrow 2 \mid (n^2+2^n)$

Case 2: n is odd:
$R_3(n^2) = R_3(R_3(n)\cdot R_3(n)) \Rightarrow R_3(1\cdot 1) = 1$ or $R_3(2\cdot 2) = 1$
$\Rightarrow R_3(R_3(n^2) + R_3(2^n)) = R_3(1 + R_3(2^{R_{\varphi(3)}(n)})) = R_3(2+1) = 0$
$\Rightarrow 3 \mid (n^2+2^n)$

Multiplicative Inverse

L. 4.18. $ax \equiv_m 1$ has a unique solution $x \in \mathbb{Z}$ iff $\gcd(a,m)=1$.

D. 4.9. This solution is called the multiplicative inverse $x \equiv_m a^{-1}$. It only exists if $\gcd(a,m)=1$.

Ex. $\gcd(3,26) =$

$26 = 8\cdot 3 + 2$
$3 = 1\cdot 2 + 1$

$9 \equiv_{26} 3^{-1}$
$3\cdot 9 \equiv_{26} 1$

Backwards:
$2 = 26 - 8\cdot 3$
$1 = 3 - 1\cdot 2 = 3 - 1\cdot(26 - 8\cdot 3)$
$= 3 - 1\cdot 26 + 8\cdot 3$
$= \underline{9\cdot 3} - 1\cdot 26$

CRT

T. 4.19. Let $m_1, m_2, \dots, m_r$ be pairwise relatively prime and let $M = \prod_{i=1}^r m_i$. For every list $a_1,\dots,a_r$ with $0 \leq a_i < m_i$ for $i=1,\dots,r$ the system

$$x \equiv_{m_1} a_1 \quad \vdots \quad x \equiv_{m_r} a_r$$

has a unique solution x, with $0 \leq x < M$.

Ex. $x \equiv_3 2$, $x \equiv_4 1$, $x \equiv_5 4$, $M = 60$

1. $M_i = \frac{M}{m}$: $M_1 = 20$, $M_2 = 15$, $M_3 = 12$
2. $N_i M_i \equiv_{m_i} 1$: $N_1 \cdot 20 \equiv_3 1 \Rightarrow N_1 = 2$, $N_2 \cdot 15 \equiv_4 1 \Rightarrow N_2 = 3$, $N_3 \cdot 12 \equiv_5 1 \Rightarrow N_3 = 3$
3. $\sum_{i=1}^r a_i \cdot M_i \cdot N_i = 2\cdot 20\cdot 2 + 1\cdot 15\cdot 3 + 4\cdot 12\cdot 3 \equiv_M \underline{\underline{29}}$

If we have something like $x \equiv_{12} 8$, $x \equiv_{15} 2$ we need to decompose since $\gcd(12,15) \neq 1$.

We get: $x \equiv_3 2$, $x \equiv_4 0$; $x \equiv_3 2$, $x \equiv_5 2$ — need to be equal, else no solution

$2x^2 + 8 \equiv_{13} 6 \Rightarrow 2x^2 \equiv_{13} -2 \equiv_{13} 11 \equiv_{13} 24 \Rightarrow x^2 \equiv_{13} 12 \equiv_{13} 25 \Rightarrow x \equiv_{13} \pm 5$

Diffie-Hellman

Idee: Encryption using a one-way function (easy to calculate, hard to reverse).

Alice	g: generator, p: large prime	Bob
a = random number in $\{0,\dots,p-2\}$		b = random number in $\{0,\dots,p-2\}$
$y_A = g^a \bmod p$		$y_B = g^b \bmod p$
$k_{AB} = y_B^a = g^{b\cdot a}$		$k_{BA} = y_A^b = g^{a\cdot b}$

Man in the middle can only get y_B and y_A.

Algebra

D. 5.1. An operation on a set S is a function: $S^n \to S$, where $n \geq 0$ is the arity.

D. 5.2. An algebra is a pair $\langle S;\Omega\rangle$, where S is a set and Ω a list of operations.

Monoids and Groups

D. 5.3. A left/right neutral element is an element $e \in S$ such that $\forall a \in S$ $e \times a = a$ / $a \times e = a$. If both are true it is simply a neutral element.

L. 5.1. $\langle S;\Omega\rangle$ can only have one NE.

D. 5.4. A binary operation is associative if $a\times(b\times c) = (a\times b)\times c$.

D. 5.5. A monoid is an algebra $\langle M;\times,e\rangle$, where $\times$ is associative and e is the NE.

D. 5.6. A left/right inverse of an element $a \in S$, is a $b \in S$ such that $b\times a = e$ / $a \times b = e$. If both are true its simply an inverse.

D. 5.7. A group is an algebra $\langle G;\times,\hat{\ },e\rangle$ satisfying the axioms:

⚠
G1. $\times$ is associative
G2. e is a NE, $a\times e = e\times a = a$
G3. $\forall a \in G\ \exists \hat{a}$ $a\times\hat{a} = e = \hat{a}\times a$

D. 5.8. A group/monoid is commutative/abelain if $a\times b = b\times a$.

L. 5.3. For groups we have:
i. $\hat{(\hat{a})} = a$
ii. $\widehat{a\times b} = \hat{b}\times\hat{a}$
iii. $a\times b = a\times c \Rightarrow b = c$
iv. $b\times a = c\times a \Rightarrow b = c$
v. $a\times x = b$ has a unique solution.

Ex.
$\widehat{a\circ b}\circ(a\circ b) = e$ G3.
$\widehat{a\circ b}\circ(a\circ b)\circ\hat{b} = e\circ\hat{b}$
$\widehat{a\circ b}\circ(a\circ b)\circ\hat{b} = \hat{b}$ G2.
$\widehat{a\circ b}\circ a\circ(b\circ\hat{b}) = \hat{b}$ G1.
$\widehat{a\circ b}\circ a\circ e = \hat{b}$ G3.

$\widehat{a\circ b}\circ a = \hat{b}$ G2.
$(\widehat{a\circ b}\circ a)\circ\hat{a} = \hat{b}\circ\hat{a}$
$\widehat{a\circ b}\circ(a\circ\hat{a}) = \hat{b}\circ\hat{a}$ G1.
$\widehat{a\circ b}\circ e = \hat{b}\circ\hat{a}$ G3.
$\widehat{a\circ b} = \hat{b}\circ\hat{a}$ G2.

The Structure of Groups

D. 5.9. The direct product of n Groups is the algebra $\langle G_1\times\dots\times G_n;\cdot\rangle$, where $\cdot$ is a component wise operation.

D. 5.10. A function ψ from group G to Group H is a group homomorphism if for all $\psi(a\times b) = \psi(a) * \psi(b)$. If ψ is bijective it is a isomorphism, we write $G \simeq H$.

L. 5.5. A group homomorphism ψ satisfies:
- $\psi(e) = e'$
- $\psi(\hat{a}) = \widehat{\psi(a)}$

Ex. Prove $\phi(e) = e'$:
$\phi(e) = \phi(e\cdot e)$
$\widehat{\phi(e)}\cdot\phi(e) = \widehat{\phi(e)}\cdot\phi(e)\cdot\phi(e)$
$e' = \phi(e)$

When proving that something is a isomorphism we need to prove that:
- It's a homomorphism
- ϕ is bijective

$\langle\mathbb{Z};+\rangle$ is isomorph to $\langle G;+\rangle$ where $G = \{2x \mid x \in \mathbb{Z}\}$

D. 5.11. A subset $H \subseteq G$ is a subgroup if H is a group, meaning if its closed with respect to all operations:
- $a\times b \in H$
- $e \in H$
- $\hat{a} \in H$

D. 5.12. The order of $a \in G$, $\mathrm{ord}(a)$ is the least $m \geq 1$ such that $a^m = e$, if no such m exists the $\mathrm{ord}(a) = \infty$.

L. 5.6. In a finite group every element has a finite order.

Ex. For any two $a,b \in G$ we have $\mathrm{ord}(a*b) = \mathrm{ord}(b*a)$

We only need to prove $\mathrm{ord}(a\times b) \geq \mathrm{ord}(b\times a)$. Let $\mathrm{ord}(a\times b) = n$

$(a*b)^n = e$
$\iff (a\times b)*(a\times b)*\dots*(a\times b) = e$
$\Rightarrow b*(a\times b)*\dots*(a\times b)*a = b*a$
$\iff b*a*(b*a)*\dots*(b*a) = b*a$
$\Rightarrow \hat{a}*\hat{b}*b*a*(b*a)*\dots*(b*a) = \hat{a}*\hat{b}*b*a$
$\iff (b*a)^n = e$

D.5.13. For a finite group G, $|G|$ is called the order of G.
D.5.14. For $a \in G$, the group generated by a, $\langle a \rangle$, is defineded as $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.
D.5.15. A group $G = \langle g \rangle$ is called cyclic and g is called a generator of G. g^{-1} is also a generator.

Finding generators

$\langle \mathbb{Z}_m ; \oplus \rangle$: all elements a with $\gcd(a,m) = 1$

$\langle \mathbb{Z}_m^* ; \odot \rangle$:
- calculate order of group
- for all $d \mid$ order check each element a if $a^d = 1$ if not a is a generator, realize for order $= 16$ $d = \{1,2,4,8,16\}$ we only need to check $a^8 = 1$

Same goes for generators of $F[x]^*_{m(x)}$ etc.

Reality-Check: # generators $= \varphi(\text{order})$

T.5.7. A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n ; \oplus \rangle$ and therefore commutative. All groups of prime order are commutative
$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if $\gcd(m,n) = 1$
T.5.8. Lagrange If $H \leq G$, then $|H|$ divides $|G|$.
C.5.9. For a finite group G, the order of $a \in G$ divides $|G|$.
C.5.10. For a finite group G, $a^{|G|} = e$.
C.5.11. Every group of prime order is cyclic and every element except the NE is a generator.
D.5.16. $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a,m) = 1\}$ Multiplicative group
D.5.17. Euler function $\varphi(m) = |\mathbb{Z}_m^*| = p - 1$ if $m =$ prime
L.5.12. If $\prod_{i=1}^r p_i^{e_i}$ is the prime factorization of m, then

$$\varphi(m) = \prod_{i=1}^r \underbrace{(p_i - 1)\, p_i^{e_i - 1}}_{= p_i^{e_i} - p_i^{e_i - 1}}$$

T.5.13. $\langle \mathbb{Z}_m^* ; \odot, ^{-1}, 1 \rangle$ is a group.
C.5.14. For all $m \geq 2$ and $\gcd(a,m) = 1$, $a^{\varphi(m)} \equiv_m 1$ and for all primes p with $p \nmid a$ $a^{p-1} \equiv_p 1$
T.5.15. $\mathbb{Z}_m^*$ is cyclic iff $m = 2$, $m = 4$, $m = p^e$ or $m = 2p^e$, where p is an odd prime and $e \geq 1$.

Inverse of a: $a^{\varphi(m)-1} = \hat{a}$

Ex. Claim: for $\gcd(m,n) = 1$, $\phi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $x \to (R_m(x), R_n(x))$ is a isomorphism.

Homomorphism:
$$\begin{aligned}\phi(x \oplus y) &= (R_m(x \oplus y), R_n(x \oplus y)) \\ &= (R_m(x+y), R_n(x+y)) \\ &= (R_m(R_m(x) + R_m(y)), R_n(R_n(x) + R_n(y))) \\ &= (R_m(x), R_n(x)) + (R_m(y), R_n(y)) \\ &= \phi(x) + \phi(y)\end{aligned}$$

Bijective: By CRT we know that a one-to-one relation between $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ exists. We will show that it's injective. Assume $x \neq y$ and $\phi(x) = \phi(y)$. This follows from the fact that x, y are solutions of $a \equiv_m \phi(x)$, $a \equiv_n \phi(y)$. Given $x + y < m \cdot n$ and $\phi(x) < m$, $\phi(y) < n$ we have by CRT that a is unique $\Rightarrow x = y$. Therefore it's injective. Since $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$ it is also surjective. $\square$

Ex. Let G be a finite, non-empty set and $*$ a binary operation on G. Let $*$ be associative and commutative. Let $\forall a,b,c \in G$ $a * b = a * c$ then $b = c$. Prove that G is a group.

We know $\forall a \in G\ \exists n,m \in \mathbb{N}\ (n < m \wedge a^n = a^m)$, since G is finite.

① $e \in G$: $z = m - n \Rightarrow a^z \cdot a^n = a^{(m-n)+n} = a^m = a^n \Rightarrow a^z$ is e
Show $a^z = e$ for all $b \in G$: $a * b = (a * e) * b = a * (e * b)$
$\Rightarrow b = (e * b) = (b * e)$

② $\hat{a} \in G$: $\forall a \in G$ $a^z = e$ $e = a^{m-n}$ then $\hat{a} = a^{m-n-1}$ since $a^{m-n-1} * a = a^{m-n} = e$.

Ex. Prove that if $G \leq \langle \mathbb{Z}; + \rangle$, then $G = \{n \cdot d \mid n \in \mathbb{Z}\}$ for some $d \in \mathbb{Z}$.
Proof by contradiction. Let d be the smallest element in G. We assume $\nexists d' \{n \cdot d' \mid n \in \mathbb{Z}\}$. If we now set $d' = d$ we have that $\exists g \in G$ for which $d \nmid g$. W.o.l.g let $g > 0$, then $g = k \cdot d + r$ with $0 < r < d$. But because G is closed under $+$ and $-$ we have $r = g - k \cdot d \in G$. But we assumed d is the smallest element which is a contradiction! Therefore G has to be of the form $\{n \cdot d \mid n \in \mathbb{Z}\}$.

RSA

T.5.16. Let G be a finite group and $e \in \mathbb{Z}$ with $\gcd(e, |G|) = 1$. Then is $x \to x^e$ a bijection and x is the e-th root of $y \in G$, $y = x^e$. $x = y^d$, where d is the multiplicative inverse of e mod $|G|$, $e \cdot d \equiv_{|G|} 1$.

$\Rightarrow$ Without $|G|$ it's hard to calculate the e-th root

Alice	insecure channel	Bob
p, q large primes		
$n = p \cdot q$		
$f = (p-1)(q-1) = \varphi(n)$		
select $e \in \mathbb{Z}_n^*$	$\xrightarrow{n, e}$	$m =$ message
$d \equiv_f e^{-1}$		
$m = R_n(y^d)$	$\xleftarrow{y}$	$y = R_n(m^e)$

Ex. Prove that for all $m \in \mathbb{Z}_n$, we have $m^{de} \equiv_p m$, where $n = p \cdot q$ and $de \equiv_{\varphi(n)} 1$.

$de - 1 = (p-1)(q-1) \cdot k$
$de = (p-1)(q-1) \cdot k + 1$

Case 1: $m = k \cdot p$ therefore it is trivial that $m^{de} \equiv_p 0 \equiv_p m$

Case 2: $m \neq k \cdot p$ $m^{(p-1)(q-1) \cdot k + 1}$
$= m^{(p-1)(q-1) \cdot k} \cdot m = m^{((q-1) \cdot k) \cdot p - 1} \cdot m$
$\equiv_p 1 * m$ by C.5.14

Ex. Prove that if $m^{de} \equiv_p m$ and $m^{de} \equiv_q m$ then $m^{de} \equiv_{q \cdot p} m$
Define $x \equiv_p m$, $x \equiv_q m$ clearly m^{de} and m are two solutions, by CRT, all solutions are congruent modulo $p \cdot q = n$, hence $m^{de} \equiv_n m$.

Rings

D.5.18. A ring is an algebra for which:
i) $\langle R; +, -, 0 \rangle$ is a commutative group
ii) $\langle R; \cdot, 1 \rangle$ is a monoid
iii) left and right distributive law is true
A ring is commutative if the multiplication is comm.
L.5.17 i) $0a = a0 = 0$ ii) $(-a)b = -(ab)$ iii) $(-a)(-b) = ab$
iv) if R is non-trivial $\Rightarrow 1 \neq 0$
D.5.19. Characteristic of a ring: order of 1 in the additive group, 0 if it's not finite.

Commutative rings:
D.5.20. $a, b \in R$ we say a divides b, $a \mid b$ if $\exists c \in R$ $a \cdot c = b$.
⚠ all non-zero elemenet divide 0
L.5.18 i) if $a \mid b$ and $b \mid c$ then $a \mid c$
ii) if $a \mid b$ then $a \mid b \cdot c$ $\forall c \in R$
iii) if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
D.5.21. gcd for rings (D.4.2.)
D.5.22. Zerodivisor: $a, b \in R$, $a \neq 0$, $b \neq 0$, $ab = 0$, then are a, b zerodivisors.

Finding zerodivisors: all elements $a \in \mathbb{Z}_m$ such that $\gcd(a, m) \neq 1$

$\langle \mathbb{Z}_n ; + \rangle$ is isomorphic to $\langle \mathbb{Z}_p ; + \rangle \times \langle \mathbb{Z}_q ; + \rangle$ iff $n = p \cdot q$ and $\gcd(p, q) = 1$. (follows from CRT)

D.5.23. Unit: $u \in R$ is a unit if it is invertible, $uv = vu = 1$, $v = u^{-1}$.
The set of units of R is denoted R^*.
L.5.19. For a ring R, R^* is a multiplicative group.

Finding units all elements a such that $\gcd(a, m) = 1$

Order of $F[x]^*_{m(x)}$: L.5.33. $|F[x]_{m(x)}| = |F|^{\deg(m(x))}$
D.5.26. $|F[x]^*_{m(x)}| = |F[x]_{m(x)}| - 1$
↳ if $F[x]_{m(x)}$ is a field

D.5.24. An integral domain is a commutative, non-trivial ring without zerodivisors.
L.5.20. In an integral domain with $a \mid b$, $b = ac$, c is unique and can be denoted $c = b/a$.
$\mathbb{Z}_m$ can only be a integral domain if m is prime. needs proof
D.5.25. A polynomial $a(x)$ over R is $a(x) = \sum_{i=0}^{d} a_i x^i$ for some $d \geq 0$ and $a_i \in R$. $\deg(a(x))$ is equal to the largest $i \neq 0$. If all $a_i = 0$ it has degree $-\infty$. $R_{[x]}$ denotes the set of polynomials over R.
T.5.21. For any ring R, $R_{[x]}$ is a ring.
L.5.22. i) if D is an integral domain, then so is $D_{[x]}$.
ii) the units of $D_{[x]}$ are the constant polynomials that are units of D: $D^* = D_{[x]}^*$

Calculate mod in $\mathbb{Z}_5[x]_{x^2+1}$: simply substitute x^2 with 4 since $x^2 + 1 \equiv_{x^2+1} 0$, $x^2 \equiv_{x^2+1} -1$ $x^2 \equiv_{x^2+1} 4$.

Ex. Let $\langle R;+,-,0,\cdot,1\rangle$ be any ring such that $a^2=a$ prove $a+a=0$.

$(a+a)=(a+a)\cdot(a+a)$
$= aa+aa+aa+aa$
$= a+a+a+a$
$\Rightarrow 0 = a+a$

Now prove commutativity:

$a+b=(a+b)(a+b)$
$= aa+ab+ba+bb$
$= a+ab+ba+b$
$\Rightarrow 0=a+a$
$-a=a$

$a+b+(-a)+(-b)=ab+ba$
$0=ab+ba$
$-(ab)=ba$
$ab=ba$

Ex. List all elements $R\setminus R^\times$ $(R=\mathbb{Z}_7[x]_{x^2+x+1})$

We have to remove all units. $x^2+x+1=(x+3)\cdot(x+5)$ all elements that are not a linear combination of these factors are units. Therefore $R\setminus R^\times$ = all multiples of $x+3$ and $x+5$.

Ex. Let R be a ring. Prove that if $1-ab$ has a multiplicative inverse c, then $1-ba$ has the multiplicative inverse $1+bca$.

Assume $(1-ab)\cdot c=1$ (List all steps)

$(1-ba)\cdot(1+bca)=(1-ba)+(1-ba)\cdot bca = 1-ba+bca-babca$
$=1+b(-a+ca-abca)=1+b((-1+c-abc)\cdot a)$
$=1+b((-1+(1-ab)\cdot c)\cdot a)=1+b\cdot((-1+1)\cdot a)=1+b\cdot(0\cdot a)=1$

Fields

D.5.26. A field F is a non-trivial commutative ring in which every element $\neq 0$ is a unit: $F^\times = F\setminus\{0\}$.

T.5.23. $\mathbb{Z}_p$ is a field iff p is prime. $\mathbb{Z}_p = GF(p)$

T.5.24. Every field is an integral domain.

unit $\Rightarrow$ not zerodivisor $uv=0 \Rightarrow v=1\cdot v=u^{-1}uv=u^{-1}\cdot 0=0$ □

D.5.27. A polynomial $a(x)\in F_{[x]}$ is called monic if the leading coefficient is 1.

D.5.28. A polynomial $a(x)\in F_{[x]}$ with degree ≥ 1 is called irreducible if it's divisible only by a constant polynomial or a constant multiple of $a(x)$.

D.5.29. The monic polynomial of largest degree such that $g(x)|a(x)$ and $g(x)|b(x)$ is the gcd of $a(x)$ and $b(x)$.

T.5.25. For any $a(x)$ and $b(x)\neq 0$ in $F_{[x]}$, there exists a unique monic $q(x)$ and a unique $r(x)$ such that:
$a(x)=q(x)\cdot b(x)+r(x)$ and $\deg(b(x))\geq\deg(r(x))$

Polynomials as Functions

D.5.33. Let $a(x)\in R_{[x]}$, $\alpha\in R$ for which $a(\alpha)=0$ is called a root of $a(x)$.

L.5.28. For a field F, $\alpha\in F$ is a root if $x-\alpha$ divides $a(x)$.

C.5.29. A polynomial of deg. 2 or 3 is irreducible iff it has no roots.

D.5.34. If α is a root of $a(x)$, then its multiplicity is the highest power of $(x-\alpha)$ dividing $a(x)$.

T.5.30. For a field F, a nonzero polynomial of degree d has at most d roots, counting multiplicities.

L.5.31. A polynomial $a(x)\in F_{[x]}$ of degree d can be uniquely determined by $d+1$ values.

$$\alpha(x)=\sum_{i=1}^{d+1}\beta_i u_i(x) \text{ where } u_i(x)=\frac{(x-\alpha_1)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)}{(\alpha_i-\alpha_1)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)}$$

gcd of two polynomials: apply euclid. algoritm

Ex. $\gcd(x^3+x+2,\ x^2+x+1)=\gcd(x^2+x+1,\ x+3)=\gcd(x+3,0)$
$=x+3$ always divide by the smaller polynomial and keep the remainder

Ex. $2x+1\in\mathbb{Z}_7[x]_{x^2+x+1}$ find the multiplicative inverse.

① Divide $x^2+x+1+1$ by $2x+1$ to get the result.

Irreducibility of Polynomials:

- deg 1 always irreducible
- deg 2/3 irreducible if they have no root C.5.30.
- deg 4 irreducible if they have no root or factor deg 2
- deg 5 irreducible if they have no root or factor deg 2/3

Ex.

GF(2)	GF(3)		GF(5)		
10	10	1112	10	123	1021
11	11	1121	11	124	1024
111	12	1201	12	133	1032
1011	101	1211	14	134	1033
1101	112	1222	102	141	1042
10011	122	10012	103	142	⋮
11001	1021		111	1011	
11111	1102		112	1014	

GF(7)

10	15	113	125	145	163	1004	1026	1052
11	16	114	131	146	164	1005	1032	1055
12	101	116	135	152	166	1011	1035	1062
13	102	122	136	153	1002	1016	1041	1065
14	104	123	141	155	1003	1021	1046	1101

Ex. Solve $y^2+(x^2+1)\cdot y+(x^2+x+1)=0$ for $y\in A$.

We try to find the roots of the polynomial. We do this by inserting elements of A for y. Once we find such a element r we can divide by $y-r$ to get $y+r'$ where r' is the second root.

Finite Fields

D.5.35. Let $m(x)$ be a polynomial of deg. d over F. Then $F[x]_{m(x)}=\{a(x)\in F[x] \mid \deg(a(x))<d\}$.

L.5.33. Let F be a finite field with q elements and let $m(x)$ be of degree d over F. Then $|F[x]_{m(x)}|=q^d$.

L.5.34. $F[x]_{m(x)}$ is a ring with respect to addition and multiplication modulo $m(x)$.

L.5.35. $F[x]^\times_{m(x)}=\{a(x)\in F[x]_{m(x)} \mid \gcd(a(x),m(x))=1\}$

T.5.36. The ring $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible.

T.5.39. $|GF(q)|=q-1$ for $q=p^e$, p=prim $e\geq 1$

If F is a field $F[x]$ can't be a field.

Proof: At least one element in $F[x]$ has no inverse. Given at least two elements we have $0,1\in F$ and $0\neq 1$. Now we multiply two polynomials of degree d, d', which will yield a polynomial of degree $d+d'\geq d$ as $a_d\cdot b_{d'}\neq 0$ (no zerodivisors). Multiplication only increases the degree, it follows that a polynomial with $d\geq 1$ does not have an inverse. Therefore is $F[x]$ not a field.

Constructing finite field with p^d elements:

- pick $GF(p)$
- pick $m(x)$ of degree d in $GF(p)$ that is irreducible

$\Rightarrow GF(p)[x]_{m(x)}$

Ex.

monoid	:	$\langle\mathbb{Z};+,0\rangle$
group	:	$\langle\mathbb{Z};+,-,0\rangle$, $\langle\mathbb{Z}[x];+,-,0\rangle$
ring	:	$\langle\mathbb{R};+,-,0,\cdot,1\rangle$, $\mathbb{Z}\times\mathbb{Z}$
finite ring	:	$\langle\mathbb{Z}_m;+,-,0,\cdot,1\rangle$
integral domain	:	$\mathbb{Z}$, $\mathbb{Z}_{prime}$, $\mathbb{Q}[x]$
field	:	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, GF
finite field	:	$\mathbb{Z}_{prime}$

$\langle G;+,-,0,\cdot,1\rangle$ are left away for simplicity

Ex. Let F be a finite Field, prove that there exists $f(x)\in F[x]$ which has no roots.

1. Let $g(x)=\prod_{\alpha\in F}(x-\alpha)$, clearly $g(\alpha)=0$ for all $\alpha\in F$
2. Now let $f(x)=g(x)+1$, since $\forall\alpha\in F\ g(\alpha)=0$, it follows that $\forall h\in F\ f(h)=1$.

Application: ECC

D.5.36. A (n,k)-encoding function maps A^k to A^n, where $n>k$, the result is called a codeword.

D.5.37. An (n,k)-ECC over A with $|A|=q$ is a subset of A^n with cardinality q^k.

D.5.38. Hamming Distance: number of positions in which two strings over A differ.

D.5.39. Minimum Distance: minimal Hamming distance between any two codewords of an ECC.

D.5.40. A decoding function D for an (n,k)-encoding function is a function $D: A^n\to A^k$.

T.5.40. A ECC with minimum distance d is t-error correcting iff $d\geq 2t+1$.

T.5.41. Let $A=GF(q)$ and let $\alpha_0,\dots,\alpha_{n-1}\in A$. The encoding function $E((a_0,\dots,a_{k-1}))=(a(\alpha_0),\dots,a(\alpha_{n-1}))$, where $a(x)=a_{k-1}x^{k-1}+\dots+a_0$. This ECC has minimum distance $n-k+1$.

Good Luck & you can do this!