Logic

Proof Patterns
- Compos. of Implications: $(A\to B)\land(B\to C)\vDash A\to C$
- Indirect proof: $\neg B\to\neg A\vDash A\to B$
- Modus Ponens: $A\land(A\to B)\vDash B$
- Case Distinction: for any k: $(A_1\lor\dots A_k)\land(A_1\to B)\land\dots(A_k\to B)\vDash B$
- Contradiction: $(\neg A\to B)\land\neg B\vDash A$
- Pigeonhole: set of n objects, partitioned in $k<n$ sets → at least one contains $\geq\lceil\frac{n}{k}\rceil$ objects

General concepts
Syntax: Defines Λ and syntactically correct strings in Λ^*
Semantics: free$(F)\subseteq\{1,\dots,k\}$
Interpr. $\mathcal{A}$: assigns value to sym. ↳ suitable: assigns to all free sym.
function σ: $\sigma(F,\mathcal{A})=\mathcal{A}(F)=\{0,1\}$
model: $\mathcal{A}(F)=1$ / $\mathcal{A}\vDash F$; $\mathcal{A}\vDash M$ for set of formulas
tautology: $\vDash F$
unsatisfiable: $F\vDash\bot$
logical consequence: $F\vDash G$: for every suitable int. for both, a model for F is a model for G
$F\equiv G$ ⟺ $F\vDash G$ and $G\vDash F$
If F and G are formulas, then $\neg F$, $(F\land G)$, $(F\lor G)$ are.

Semantics
$\mathcal{A}(F\land G)=1 \Leftrightarrow \mathcal{A}(F)=1$ and $\mathcal{A}(G)=1$
$\mathcal{A}(F\lor G)=1 \Leftrightarrow \mathcal{A}(F)=1$ or $\mathcal{A}(G)=1$
$\mathcal{A}(\neg F)=1 \Leftrightarrow \mathcal{A}(F)=0$
$\mathcal{A}(\forall x\, G)=1 \Leftrightarrow \mathcal{A}_{[x\to u]}(G)=1$ for all $u\in U$
$\mathcal{A}(\exists x\, G)=1 \Leftrightarrow \mathcal{A}_{[x\to u]}(G)=1$ for some $u\in U$

Prop logic
Syntax: A_i is atomic formula
literal: atom. for. or its neg.
CNF: $(L_{11}\lor\dots\lor L_{1m_1})\land(\dots$ ↳ false rows, opposite
DNF: $(L_{11}\land\dots\land L_{1m_1})\lor(\dots$ ↳ true rows

Pred. logic
Syntax: x_i variable, $f_i^{(k)}$ function, $k=0$: constant, $P_i^{(k)}$ predicate
term: variable x_i is term, $f_i^{(k)}(t_1,\dots,t_k)$ is term
formula: $P_i^{(k)}(terms)$ is atomic for. $\neg F$, $F\land G$, $F\lor G$, $\forall x_i F$, $\exists x_i F$ are formulas
→ Variables are either free or bound
no free var. → closed formula
$F[x/t]$ = substitute free x
Sem.: $\mathcal{A}=(U,\phi,\psi,\xi)$ (structure/interpretation)
U non-empty universe
ϕ assigns func. to func. → $f^{\mathcal{A}}$
ψ assigns func. to pred. → $P^{\mathcal{A}}$
ξ assigns value $\in U$ to var. → $x^{\mathcal{A}}$
value $\mathcal{A}(t)$ for term t:
- $t=x_i$ → $\mathcal{A}(t)=\xi(x_i)$
- $t=f(t_1\dots)$ → $\mathcal{A}(t)=\phi(f)(\mathcal{A}(t_1),\dots)$

truth value $\mathcal{A}(F)$
$\mathcal{A}(F)=\psi(P)(\mathcal{A}(t_1),\dots,\mathcal{A}(t_k))$
- for $F=\forall x G$ / $F=\exists x G$ → sem.

Pred. logic

Lemma 6.7.
x does not occur free in H
$\neg(\forall x F)\equiv\exists x\neg F$
$\neg(\exists x F)\equiv\forall x\neg F$
$(\forall x F)\land(\forall x G)\equiv\forall x(F\land G)$
$(\exists x F)\lor(\exists x G)\equiv\exists x(F\lor G)$
$\forall x\forall y F\equiv\forall y\forall x F$
$\exists x\exists y F\equiv\exists y\exists x F$
$(\forall x F)\land H\equiv\forall x(F\land H)$
$(\forall x F)\lor H\equiv\forall x(F\lor H)$
$(\exists x F)\land H\equiv\exists x(F\land H)$
$(\exists x F)\lor H\equiv\exists x(F\lor H)$
only in this order

Lemma 6.9
$\forall x\, G\equiv\forall y\, G[x/y]$ y not free in G
$\exists x\, G\equiv\exists y\, G[x/y]$
Rectified form: all variables distinct
Prenex form: $Q_1x_1 Q_2x_2\dots G$, Q_i arbitrary quantifiers, G formula free of quantifiers
Lemma 6.11: $\forall x F\vDash F[x/t]$

Lemma 6.1.
- $F\land F\equiv F$, $F\lor F\equiv F$ (idempotence)
- $F\land G\equiv G\land F$, $F\lor G\equiv G\lor F$ (comm.)
- $(F\land G)\land H\equiv F\land(G\land H)$, $(F\lor G)\lor H\equiv F\lor(G\lor H)$ (ass.)
- $F\land(F\lor G)\equiv F$, $F\lor(F\land G)\equiv F$ (absorption)
- $F\land(G\lor H)\equiv(F\land G)\lor(F\land H)$, $F\lor(G\land H)\equiv(F\lor G)\land(F\lor H)$ (distr.)
- $\neg\neg F\equiv F$ (double neg.)
- $\neg(F\land G)\equiv\neg F\lor\neg G$, $\neg(F\lor G)\equiv\neg F\land\neg G$ (de Morgan)
- $F\lor\top\equiv\top$, $F\land\top\equiv F$ (tautol. rules)
- $F\lor\bot\equiv F$, $F\land\bot\equiv\bot$ (unsat. rules)
- $F\lor\neg F\equiv\top$, $F\land\neg F\equiv\bot$

Lemma: F tautology ⟺ $\neg F$ unsatisfiable
Lemma: 3 equivalent statements
1. $\{F_1,F_2,\dots,F_k\}\vDash G$
2. $(F_1\land F_2\dots\land F_k)\to G$ is tautology
3. $\{F_1,F_2,\dots,F_k,\neg G\}$ is unsatisfiable

Logical Calculi
Calculus: finite set of derivation rules: $K=\{R_1,\dots,R_m\}$
Der. rule correct: $M\vdash_R F \Rightarrow M\vDash F$
Calculus sound: $M\vdash_K F\Rightarrow M\vDash F$
Calculus compl.: $M\vdash_K F\Leftarrow M\vDash F$
Derivation/inference rule: $\{F_1,\dots,F_k\}\vdash_R G$ or $\frac{F_1\ F_2\ \dots\ F_k}{G}(R)$

Resolution calculus
clause: set of literals in CNF ↳ $(A\lor B)\land(\neg B\lor C)\to\{A,B\},\{\neg B,C\}$
$\mathcal{K}(F)\overset{def}{=}\{\{L_{11},\dots,L_{1m_1}\},\dots,\{L_{n1},\dots,L_{nm_n}\}\}$
↳ For a formula F in CNF
$\mathcal{K}(M)\overset{def}{=}\bigcup_{F\in M}\mathcal{K}(F)$ → for a set $M=\{F_1,\dots,F_k\}$
resolvent: $K=(K_1\setminus\{L\})\cup(K_2\setminus\{\neg L\})$
The resolution calculus is sound: $\mathcal{K}(M)\vdash_{Res}K\Rightarrow M\vDash K$
$\mathcal{K}(M)\vdash_{Res}\emptyset$ ⟺ M is unsatisfiable
↳ the res.-calculus is not complete!

Proof system
$\Pi=(\mathcal{S},\mathcal{P},\tau,\phi)$
$\mathcal{S}\subseteq\Sigma^*$: statements; $\tau:\mathcal{S}\to\{0,1\}$ truth function
$\mathcal{P}\subseteq\Sigma^*$: proofs; $\phi:\mathcal{S}\times\mathcal{P}\to\{0,1\}$ verification f.
sound: no false s has proof
for all $s\in\mathcal{S}$ with $\exists$ $p\in\mathcal{P}$ s.t. $\phi(s,p)=1$, we have $\tau(s)=1$
compl.: every true st. has proof
for all $s\in\mathcal{S}$ with $\tau(s)=1$, there exists $p\in\mathcal{P}$ with $\phi(s,p)=1$

Th. 6.12: $\neg\exists x\forall y(P(y,x)\leftrightarrow\neg P(y,y))$

Sets, Relations, Functions

Sets
Russell's paradox: $R=\{A\mid A\notin A\}$ does not exist
↳ Case dist.: $R\in R$: ⚡, $R\notin R$: ⚡

Definitions
Def $=$: $A=B\overset{def}{=}\forall x(x\in A\leftrightarrow x\in B)$
$A=B\overset{def}{=}(A\subseteq B)\land(B\subseteq A)$
Def $\subseteq$: $A\subseteq B\overset{def}{=}\forall x(x\in A\to x\in B)$
Def $\cup$: $A\cup B\overset{def}{=}\{x\mid x\in A\lor x\in B\}$ (union)
Def $\cap$: $A\cap B\overset{def}{=}\{x\mid x\in A\land x\in B\}$ (intersection)
Def $\setminus$: $A\setminus B\overset{def}{=}\{x\in A\mid x\notin B\}$
Def $\emptyset$: $\forall x\,\neg(x\in A)$
Def $\mathcal{P}$: $\mathcal{P}(A)\overset{def}{=}\{S\mid S\subseteq A\}$ $\mathcal{P}(\emptyset)=\{\emptyset\}$
↳ $|A|=k\to|\mathcal{P}(A)|=2^k$
Def $\times$: $A\times B=\{(a,b)\mid a\in A\land b\in B\}$
↳ $|A\times B|=|A|\cdot|B|$
↳ $X_{i=1}^{k}A_i=\{(a_1,\dots,a_k)\mid a_i\in A_i$ for $1\le i\le k\}$
Lemma:
$\{a\}=\{b\}\to a=b$
$A\subseteq B\land B\subseteq C\to A\subseteq C$
$\forall A(\emptyset\subseteq A)$

Theorem 3.4
1.-5. of Lemma 6.1
Consistency: $A\subseteq B\Leftrightarrow A\cap B=A\Leftrightarrow A\cup B=B$

Relations
A relation ρ from A to B is a subset of $A\times B$, if $B=A$ it is a relation on A
$id_A=\{(a,a)\mid a\in A\}$
$|A|=n$ → There are 2^{n^2} different relations
Matrix representation: M_{ab} is $1\Leftrightarrow a\,\rho\, b$

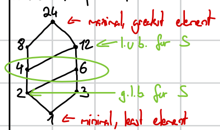
Definitions
inverse: $\hat\rho\overset{def}{=}\{(b,a)\mid(a,b)\in\rho\}$
composition: $\rho\circ\sigma$, $\rho^n\overset{def}{=}\{(a,c)\mid\exists b((a,b)\in\rho\land(b,c)\in\sigma)\}$
For ρ relation on A, ρ^n is the n-fold composition ↳ matrix multiplication
Lemma: composition of relations is associative
Lemma: $\widehat{\rho\circ\sigma}=\hat\sigma\circ\hat\rho$
Reflexive: $a\,\rho\, a$ for all $a\in A$
↳ e.g.: $\le,\ge,\mid$ $<,>$ are not
Symmetric: $a\,\rho\, b\Leftrightarrow b\,\rho\, a$ for all $a,b\in A$
↳ e.g.: $\equiv_m$
Antisym.: $a\,\rho\, b\land b\,\rho\, a\to a=b$ for all $a,b\in A$
↳ e.g.: $\le,\ge,\mid$ on $\mathbb{N}$ $\mid$ on $\mathbb{Z}$ is not
Transitive: $a\,\rho\, b\land b\,\rho\, c\to a\,\rho\, c$ for all $a,b,c\in A$
↳ e.g.: $\le,\ge,<,>,\mid,\equiv_m$
Lemma: ρ is transitive $\Leftrightarrow\rho^2\subseteq\rho$
Transitive Closure: $\rho^*=\bigcup_{n\in\mathbb{N}}\rho^n$
↳ $a\,\rho^*\,b\Leftrightarrow b$ is reachable from a in graph

Equivalence Relation → z.B. $\equiv_m$
↳ reflexive, symmetric, transitive
Equivalence class: $[a]_\theta\overset{def}{=}\{b\in A\mid b\,\theta\, a\}$
Lemma: The intersection of two equivalence relations (on the same set) is an equivalence relation
Partition: $\{S_i\mid i\in I\}$ with $S_i\cap S_j=\emptyset$ for $i\neq j$ and $\bigcup_{i\in I}S_i=A$
A mod θ: $A/\theta\overset{def}{=}\{[a]_\theta\mid a\in A\}$
Theorem: A/θ is a partition of A

Partial Order Relation
↳ reflexive, antisymmetric, transitive, e.g.: $\le,\ge,\mid$
With set A: $(A;\preceq)$ poset, e.g. $(\mathcal{P}(A);\subseteq)$
For a p.o.r.: $a\prec b\overset{def}{=}a\preceq b\land a\neq b$
Comparable: $a\preceq b$ or $b\preceq a$, o.w. incomparable
totally ordered: any two elements comparable
direct product: $(A;\preceq)\times(B;\sqsubseteq)=(A\times B;\le)$
$(a_1,b_1)\le(a_2,b_2)\overset{def}{=}a_1\preceq a_2\land b_1\sqsubseteq b_2$
lex. order: $(a_1,b_1)\le_{lex}(a_2,b_2)\overset{def}{=}a_1\prec a_2\lor(a_1=a_2\land b_1\sqsubseteq b_2)$
cover: $a\prec b$ and $\neg\exists c\ a\prec c\land c\prec b$

Partial Order Relations

Hasse Diagram:
a minimal element: no b with $b\prec a$
a maximal element: no b with $b\succ a$
a least element: $a\preceq b$ for all $b\in A$
a greatest element: $a\succeq b$ for all $b\in A$
a lower bound of $S\subseteq A$: $a\preceq b$ for all $b\in S$
a upper bound of $S\subseteq A$: $a\succeq b$ for all $b\in S$
a great. low. bound of S: a greatest element of all lower bounds
a least upp. bound of S: a least element of all upper bounds
Well-ordered: totally ordered + every subset has a least element
meet $a\land b$: greatest lower bound of a,b
join $a\lor b$: least upper bound of a,b
lattice: all pairs $a,b\in A$ have meet and join



Functions
Def. $f: A\to B$ (domain → codomain)
totally defined: $\forall a\in A\ \exists b\in B\ a\,f\,b$
well-defined: $\forall a\in A\ \forall b,b'\in B$ $(a\,f\,b\land a\,f\,b')\to b=b'$
Def partial function: only well-defined
Def. B^A: set of all functions $A\to B$
$Im(f)$ ← image of f: $f(A)$
$f^{-1}(T)\overset{def}{=}\{a\in A\mid f(a)\in T\}$ preimage
injective: $a\neq a'\to f(a)\neq f(a')$
surjective: for every $b\in B$, $\exists a$ $b=f(a)$
bijective: injective + surjective
composition: $g\circ f$: $g\circ f(a)=g(f(a))$
↳ associative

Countability/Uncountability
equinumerous $A\sim B$: bijection $A\to B$
dominates $A\preceq B$: $A\sim C$ for $C\subseteq B$ or injection $A\to B$
countable: $A\preceq\mathbb{N}$ (finite or $A\sim\mathbb{N}$)
Lemma: i) $\sim$ is equivalence relation
ii) $\preceq$ is transitive
iii) $A\subseteq B\to A\preceq B$
Theorem: For A, A_i ($i\in\mathbb{N}$) countable
i) A^n is countable, $A\times B$ is countable
ii) Union of countable list $A_0,A_1,\dots$ of countable sets is countable
iii) A^* is countable
Cantor: $\{0,1\}^\infty$ uncountable
Contradiction: Assume $\{0,1\}^\infty$ countable. There exists bijection $f:\mathbb{N}\to\{0,1\}^\infty$
$\beta_{i,j}$: j-th bit in i-th sequence $f(i)$
$f(i)=\beta_{i,0}\beta_{i,1}\beta_{i,2}\dots$
$\bar b$ complement bit of $b\in\{0,1\}$. New sequence:
$\alpha=\overline{\beta_{0,0}}\,\overline{\beta_{1,1}}\,\overline{\beta_{2,2}}\dots$
$\alpha\in\{0,1\}^\infty$, but α disagrees in at least 1 bit to all other sequences → f is not bij.
Countable sets: $\mathbb{N}$, $\{0,1\}^*$, $\mathbb{N}\times\mathbb{N}$, $\mathbb{Q}$, $\mathbb{N}^*$
Uncountable sets: $\{0,1\}^\infty$, $\mathbb{N}^\mathbb{N}$, $[0,1]$, $\mathbb{R}$
Def computable: $f:\mathbb{N}\to\{0,1\}$ is computable if there is a program that outputs $f(n)$ for every $n\in\mathbb{N}$
↳ There are uncomputable functions $\mathbb{N}\to\{0,1\}$

Number Theory

Division
$a\mid b\Leftrightarrow\exists c\ \ b=ac$
Euclid's Theorem: $a=dq+r$ $0\le r<|d|$
↳ unique solution for any a, $d\neq0$
gcd: $d\mid a\land d\mid b\land\forall c((c\mid a\land c\mid b)\to c\mid d)$
relatively prime: $\gcd(a,b)=1$
Le.: $\gcd(m,n-qm)=\gcd(m,R_m(n))=\gcd(m,n)$
$(a,b)=\{ua+vb\mid u,v\in\mathbb{Z}\}$
Le. $\forall a,b\ \exists d\ (a,b)=(d)$
$(a,b)=(d)\to\gcd(a,b)=d$
$\gcd(a,b)=ua+vb$
Lcm: $a\mid l\land b\mid l\land\forall m((a\mid m\land b\mid m)\to l\mid m)$
$\forall a$ $a=\prod_i p_i^{e_i}$ p_i → primes
$\gcd(a,b)=\prod_i p_i^{\min(e_i,f_i)}$
$\text{lcm}(a,b)=\prod_i p_i^{\max(e_i,f_i)}$
$\gcd(a,b)\cdot\text{lcm}(a,b)=ab$

Modular Arithmetic
$a\equiv_m b\Leftrightarrow m\mid(a-b)$
Le.: $\equiv_m$ is equivalence relation for $m\ge1$
Le.: $a\equiv_m b$, $c\equiv_m d$
$\Rightarrow a+c\equiv_m b+d$, $ac\equiv_m bd$
$\mathbb{Z}_m:=\{0,\dots,m-1\}$
Le.: $a\equiv_m R_m(a)$
$a\equiv_m b\Leftrightarrow R_m(a)=R_m(b)$
Cor.: $R_m(f(a_1,\dots,a_k))=R_m(f(R_m(a_1),\dots))$
Multip. Inverse: $ax\equiv_m1$ / $x\equiv_m a^{-1}$
↳ $\gcd(a,m)=1\Leftrightarrow x$ exists an is unique
CRT: $m_1,m_2,\dots$ relatively prime
$M=\prod_{i=1}^{r}m_i$
$x\equiv_{m_1}a_1$
$x\equiv_{m_2}a_2$
⋮
has unique sol. $0\le x<M$

Algebra
Monoid $\langle M;*;e\rangle$ $*$ ass, e n.e.
Group $\langle G;*,\hat{},e\rangle$: G1 $*$ ass, G2 $a*e=e*a=a$ G3 $a*\hat a=\hat a*a=e$
Comm./abelian: $a*b=b*a$
Le.: in every Group:
$\widehat{(\hat a)}=a$
$\widehat{a*b}=\hat b*\hat a$
$a*b=a*c\Rightarrow b=c$
$b*a=c*a\Rightarrow b=c$
$a*x=b$, $x*a=b\to x$ unique
Def. $\times$: $\langle G_1\times\dots\times G_n;\diamond\rangle$
$(a_1,\dots,a_n)\diamond(b_1,\dots,b_n)=(a_1*_1b_1,\dots,a_n*_nb_n)$
Le.: $e=(e_1,\dots,e_n)$
$\hat a=(\hat a_1,\dots,\hat a_n)$
Homomorphism: $\langle G,*,\hat{},e\rangle$, $\langle H,\diamond,\tilde{},e'\rangle$
$\psi:G\to H$, $\psi(a*b)=\psi(a)\diamond\psi(b)$
Isomorphism: ψ is bijection: $G\simeq H$
Le.: $\psi(e)=e'$
$\psi(\hat a)=\widetilde{\psi(a)}$
Subgroup: $H\subseteq G$
(1) $a*b\in H$
(2) $e\in H$
(3) $\hat a\in H$ for all $a\in H$
Def. ord(a) = least m: $a^m=e$
ord$(e)=1$, ord$(a)=2\to a^{-1}=a$
Le.: In a finite group, ord is finite
$a^m=a^{R_{ord(a)}(m)}$
$\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}=\{e,a,\dots,a^{ord(a)-1}\}$
$\langle g\rangle$ generator if $G=\langle g\rangle$
ord$(g)=|G|$
Theor.: Cyclic group of order n is isomorphic to $\langle\mathbb{Z}_n;\oplus\rangle$ (abelian)
Lagrange: $H\subseteq G\to|H|\mid|G|$
Cor: ord$(a)\mid|G|$
Cor: $a^{|G|}=e$

$\mathbb{Z}_m^*=\{a\in\mathbb{Z}_m\mid\gcd(a,m)=1\}$
$\varphi(m)=|\mathbb{Z}_m^*|$
$\varphi(m)=\prod_{i=1}^{r}(p_i-1)p_i^{e_i-1}$
Fermat: for all a with $\gcd(a,m)=1$:
$a^{\varphi(m)}\equiv_m1$, thus $a^x\equiv_m a^{R_{\varphi(m)}(x)}$
$a^{p-1}\equiv_p1$ for p prime, $p\nmid a$
Th: $\mathbb{Z}_m^*$ cyclic $\Leftrightarrow m\in\{2,4,p^e,2p^e\}$
($p>2$ prime, $e\ge1$)

Rings
Ring $\langle R;+,-,0,\cdot,1\rangle$
i) $\langle R,+,-,0\rangle$ abelian group
ii) $\langle R,\cdot,1\rangle$ monoid
iii) $a(b+c)=(ab)+(ac)$
$(b+c)a=(ba)+(ca)$ for all a,b,c
comm.: $ab=ba$
Exp.: $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$
Le.: $0a=a0=0$
$(-a)b=-(ab)$
$(-a)(-b)=ab$
$1\neq0$ if R non-trivial
Unit: u is invertible
$(vu=uv=1)$
R^*: set of units (multipl. group)
Def.: $a\mid b\Leftrightarrow b=ac$
Le.: $a\mid b\land b\mid c\Rightarrow a\mid c$
$a\mid b\Rightarrow a\mid bc$ for all c
$a\mid b\land a\mid c\Rightarrow a\mid(b+c)$
Zerodivisor: a z.d.: $ab=0$ for $b\neq0$
Integral domain: comm. ring without z.d.
↳ $\forall a\forall b(ab=0\to a=0\lor b=0)$
Le.: For an integr. domain
$a\mid b\Rightarrow b=ac$ with unique c

Polynomial Rings
Th: R comm ring $\Rightarrow R[x]$ comm. ring
Le.: D integ. dom. $\Rightarrow D[x]$ integr. dom.
$D[x]^*=D^*$ (the constant polynomials)

Fields
→ $\langle R,+,-,0,\cdot,^{-1},1\rangle$ (both abel. groups)
Field F: comm. ring, every element is unit
↳ $F^*=F\setminus\{0\}$
Th: $\mathbb{Z}_p$ field $\Leftrightarrow p$ prime
Th: A field is an integral domain
Def. monic: $a(x)$ monic: leading coeff. $=1$
Def. irred.: $a(x)$, degree ≥1,
divisible only by constant poly. and const. multipl.
Def. gcd: $g(x)\mid a(x)$, $g(x)\mid b(x)$, largest degree, monic
Eucl.: $a(x)=b(x)\cdot q(x)+r(x)$ $\deg(r(x))<\deg(b(x))$
Def. root: α root of $a(x)$: $a(\alpha)=0$
α root of $a(x)\Leftrightarrow(x-\alpha)$ divides $a(x)$
Th.: $a(x)$ with degree d has at most d roots
Polynomial interpolation: A polynomial $a(x)$ of degree $\le d$ is uniquely determined by any $d+1$ values of $a(x)$

Finite Fields
$a(x)\equiv_{m(x)}b(x)\Leftrightarrow m(x)\mid(a(x)-b(x))$
$F[x]_{m(x)}=\{a(x)\in F[x]\mid\deg(a(x))<\deg(m(x))\}$
Le.: $|F[x]_{m(x)}|=q^d$ for $|F|=q$, $\deg(m(x))=d$
Le.: $F[x]_{m(x)}$ is a ring
$F[x]_{m(x)}^*=\{a(x)\in F[x]_{m(x)}\mid\gcd(a(x),m(x))=1\}$
Th: $F[x]_{m(x)}$ field $\Leftrightarrow m(x)$ irreducible
Th: For every prime p and $d\ge1$, there exists an irr. polynomial of degr. d in $GF(q)$.
↳ There exists a finite field with p^d elements.
Th: There exists finite field with q elements
$\Leftrightarrow q$ is power of a prime
Any two fields of size q are isomorphic
Th: multpl group of every finite field $GF(q)$ is cyclic
$GF(q)$: field with q elements → $GF(p)=\mathbb{Z}_p$ for p prime

Applications

Diffie-Hellman
Base: $y=R_p(g^x)$ efficiently computable
↳ computing x computionally infeasible
(Discrete logarithm problem/one-way function)

Alice $\xleftrightarrow{p,g}$ Bob
Alice: select random $x_A\in\{0,\dots,p-2\}$
Bob: select random $x_B\in\{0,\dots,p-2\}$
Alice: $y_A=R_p(g^{x_A})$ $\xrightarrow{y_A}$
Bob: $y_B=R_p(g^{x_B})$ $\xleftarrow{y_B}$
Alice: $k_{AB}=R_p(y_B^{x_A})$
Bob: $k_{BA}=R_p(y_A^{x_B})$
$k_{AB}\equiv_p y_B^{x_A}\equiv_p(g^{x_B})^{x_A}\equiv_p g^{x_Ax_B}\equiv_p(g^{x_A})^{x_B}\equiv_p y_A^{x_B}\equiv_p k_{BA}$
p: prime, g: basis (for group $\mathbb{Z}_p^*$)
For cyclic groups: $p=|G|$, g = generator

RSA:
e-th roots:
Th: G finite group, $e\in\mathbb{Z}$, $\gcd(e,|G|)=1$
$x\to x^e$ is bijection
unique e-th root of y, namely x: $x^e=y$
↳ $x=y^d$, d multpl. inverse of e mod $|G|$: $ed\equiv_{|G|}1$

Alice: random primes p,q
$n=p\cdot q$
$f=\varphi(n)=(p-1)(q-1)$
select e
$d\equiv_f e^{-1}$
Alice $\xrightarrow{n,e}$ Bob
Bob: plaintext $m\in\{1,\dots,n-1\}$
ciphertext $c=R_n(m^e)$
Alice $\xleftarrow{c}$ Bob
Alice: $m=R_n(c^d)$
$\Rightarrow R_n(c^d)=R_n(m^{e\cdot d})=R_n(m^{k\cdot f+1})=R_n(m^{k\cdot f}\cdot m)=R_n(m)=m$

Base: factorizing large n, computing e-th root computionally infeasible

Error-correcting codes
(n,k)-encoding function: injective function $E: A^k\to A^n$
$E((a_0,\dots,a_{k-1}))=(c_0,\dots,c_{n-1})$ (→ codeword) $n>k$
$C=Im(E)=\{E((a_0,\dots,a_{k-1}))\mid a_0,\dots,a_{k-1}\in A\}$ error-correcting code
→ (n,k)-e.c. code over A with $|A|=q$ is a subset of A^n of card. q^k.
Hamming distance: #pos. where two strings of equal length differ
minimum distance: $d_{min}(C)$ = minimum of Hamming distan.
(n,k)-decoding function $D: A^n\to A^k$: t-error correcting for E if $D((r_0,\dots,r_{n-1}))=(a_0,\dots,a_{k-1})$ for any $(r_0,\dots)$ with H.D. at most t from $E((a_0,\dots,a_{k-1}))$.
C is t-error correcting if $\exists E\ \exists D$ with $C=Im(E)$, D t-error-correcting
Th.: C is t-error correcting $\Leftrightarrow d_{min}(C)\ge2t+1$
Polynomial evaluation: $A=GF(q)$, $\alpha_0,\dots,\alpha_{n-1}\in GF(q)$, arbitrary
→ $E((a_0,\dots,a_{k-1}))=(a(\alpha_0),\dots,a(\alpha_{n-1}))$, $a(x)$ is the polynomial
$a(x)=a_{k-1}x^{k-1}+\dots+a_1x+a_0$. $\Rightarrow d_{min}(C)=n-k+1$

(n,k)-code over $GF(2^d)$ can be interpreted as a binary (dn,dk)-code over $GF(2)$. The min. distance is at least that of the original code

How-To

Mengengleichheit
$A=B$ zeigen:
$A \subseteq B$: $x\in A \Rightarrow x\in B$
$B \subseteq A$: $x \in B \Rightarrow x \in A$

Injectivity
$f: A \to B$
$x, x' \in A$ $x=x' \Rightarrow f(x) = f(x')$
oder $f(x)=f(x') \Rightarrow x=x'$

Surjectivity
$f: A \to B$
For every $b \in B$, prove
$\exists a$ $b=f(a)$

Bijectivity
For $f: A\to B$, $|A|=|B|=n$
f bijective $\Leftrightarrow$ f injective
$\Leftrightarrow$ f surjective

Countability
Prove that S countable:
· find injective function $f: S \to A$, A countable
· prove f injective
· prove that $f(s) \in A$ for all $s \in S$

· Prove $S \subseteq A$, where A countable

Uncountability
Prove that S uncountable:
· find injective function $f: B \to S$, B uncountable
· prove that f is injective
· prove $f(b) \in S$ for all $b \in B$

· prove $B \subseteq S$, B uncountable

Euclidian-Algorithm
$\gcd(24, 70)$: $70 \equiv_{24} 22$
$24 \equiv_{22} 2$
$22 \equiv_2 0$
$\gcd(24,70) = 2$ (Letzter $\equiv_n 0$)
→ same for polynomials

Gcd/lcm mit Primfaktor
1. Prime factorization
$60 = 2^2 \cdot 3 \cdot 5 = \Pi_i\, p_i^{e_i}$
$126 = 2 \cdot 3^2 \cdot 7 = \Pi_i\, p_i^{e_i}$
2. $\gcd(a,b) = \Pi_i\, p_i^{\min(e_i, f_i)}$
$\gcd(60, 126) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 6$
3. $\mathrm{lcm}(a,b) = \Pi_i\, p_i^{\max(e_i, f_i)}$
$\mathrm{lcm}(60,126) = 2^2 \cdot 3^2 \cdot 5 \cdot 7$
↳ oder $a\cdot b = \gcd(a,b)\cdot \mathrm{lcm}(a,b)$

Modulo rechnen
$R_m(a^b) \to a^x \equiv_m \pm 1$ finden
$R_{11}(2^{1408}) = R_{11}(2^3 \cdot 2^{1405})$
$= R_{11}(2^3 \cdot (2^5)^{281}) = R_{11}(2^3 \cdot (-1)^{281})$
$= R_{11}(8 \cdot (-1)) = R_{11}(-8) = 3$

e.g. $R_{21}(16^{12})$
→ $\mathbb{Z}_{21}^*$ → $|\mathbb{Z}_{21}^*|$ berechnen
Da $\gcd(16, 21) = 1$
$R_{21}(16^{|\mathbb{Z}_{21}^*|}) = R_{21}(16^{12}) = 1$
Allg.: Für $\gcd(x,n)=1$
$R_n(x^m) = R_n(x^{k \cdot \varphi(n) + r}) = R_n(1 \cdot x^r)$

CRT rechnen
$x \equiv_{m_1} a_1$ $M = \Pi_{i=1}^r m_i$
⋮
$x \equiv_{m_r} a_r$ $x \in \{0, \dots, M-1\}$
1. $M = \Pi_{i=1}^r m_i$
2. $M_i = M / m_i$
3. Find N_i
⇒ $M_i N_i \equiv_{m_i} 1$
4. $x = R_M(\Sigma_{i=1}^r a_i M_i N_i)$

Gleichung modulo
e.g. $2x^2 + 8 \equiv_{13} 6$
⇒ $2x^2 \equiv_{13} 6-8 \equiv_{13} -2$
↳ multipl. inverse von 2 finden
⇒ $14x^2 \equiv_{13} -14$
⇒ $x^2 \equiv_{13} -1 \equiv_{13} 12 \equiv_{13} 25$
⇒ $x = 5$
Wenn x Lösung → auch $-x$ Lös.

Find multipl. inverse
$8x \equiv_{11} 1$

	reverse
$11 = 8(1) + 3$	$3 = 11 - 8(1)$
$8 = 3(2) + 2$	$2 = 8 - 3(2)$
$3 = 2(1) + 1$	$1 = 3 - 2(1)$
$2 = 1(2)$	

Reverse equations:
$1 = 3 - 2(1)$
$1 = 3 - (8 - 3(2))(1) = 3 - (8 - 3(2)) = 3(3) - 8$
$1 = (11 - 8(1))(3) - 8 = 11(3) - 8(4)$
$= 11(3) + 8(-4)$
Thus $-4 \equiv_{11} 7$ is the multiplicative inverse

Iso-/Homomorphismus
· Finde $\psi: G \to H$
· Prove $\psi(a * b) = \psi(a) \cdot \psi(b)$
Für Homomorphismus:
· Prove ψ bijective
Trick: g_1: generator G
g_2: generator H
⇒ $\psi(g_1^x) = g_2^x$

Subgroup
1. For $a,b \in H$ show $a * b \in H$
2. $e \in H$
3. $\hat{a} \in H$ for every $a \in H$

Find generator
1. $|G|$ berechnen
2. $\mathrm{ord}(a) \mid |G|$ ⇒ $\mathrm{ord}(g) \in \{\text{Teiler}\}$
3. Element finden mit $\mathrm{ord}(a) = |G|$

For $\langle \mathbb{Z}_n; + \rangle$ the generators are all $g \in \mathbb{Z}_n$ with $\gcd(g,n)=1$.

Units + Zerodivisors
units: $a \cdot b = 0$ for $b \in R \setminus \{0\}$
zerod.: $a \cdot b = 1$ for $b \in R$
$\mathbb{Z}_m = \underbrace{\mathbb{Z}_m^*}_{\text{units}} \cup \underbrace{\overline{\mathbb{Z}_m^*}}_{\text{zd}} \setminus \{0\} \cup \{0\}$
units: all elements a with $\gcd(a, 12) = 1$
z.d.: rest (all a with $\gcd(a,12) > 1$)

Polynomdivison
$\mathbb{Z}_3[x]$
$2x^3 + x^2 + x + 1 : x + 2 = 2x^2 + 1$
$-(2x^3 + x^2)$
$0 + x + 1$
$-(x + 2)$
$2 = r(x)$

Irreducible
$m(x)$ is irreducible → $m(x)$ has no NS
$\deg = 1$ → all irreducible
$\deg \in \{2,3\}$ → no NS ⇔ irreducible
$\deg = 4$ → NS a ⇒ $(x-a) \mid c(x)$, reducible
no NS ⇒ irreducible or
$a(x) = b(x) \cdot c(x)$,
$b(x), c(x)$ irr. polynomials of degree 2

Find all irr. polynomials
all irr. polynomials of degree 4 over $GF(2)$:
$p(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$
→ eliminate all polynomials with roots:
all with $a_0 = 0$ or $a_3 + a_2 + a_1 + a_0 = 1$
→ eliminate all that are divisible by irr. polynomials of degree 2 (only x^2+x+1)
$(x^2+x+1)^2 = x^4 + x^2 + 1$ eliminate
→ remaining ones are the solutions

Find ZD of $GF(q)[x]_{m(x)}$
· ZD are the polynomials with common factor with $m(x)$
e.g. $m(x) = x^2 + 2x = x(x+2)$ → multiples of x, $(x+2)$

Units of $GF(q)[x]_{m(x)}$
· factorize $m(x)$
e.g. $(x^2+2) = (x+2)(x+1)$
· eliminate all poly. with $\gcd(a(x), m(x)) \neq 1$
for $u(x+2)$, $v(x+1)$ $\gcd(a(x), (x^2+2)) \neq 1$
· rest are the units

Inverse berechnen
Berechne inverse of $x+4$ in $\mathbb{Z}_5[x]_{x^2+1}$
→ Inverse of form $ax+b$
$(x+4)(ax+b) \equiv_{x^2+1} 1$
$(x+4)(ax+b) = ax^2 + bx + 4ax + 4b$
$\equiv_{x^2+1} ax^2 + bx + 4ax + 4b - ax^2 - a$
$\equiv_{x^2+1} \underbrace{(b+4a)}_{0}x + \underbrace{4b-a}_{1} = 1$
$b + 4a \equiv_5 0$ ⇒ $b \equiv_5 -4a \equiv_5 a$
$4b - a \equiv_5 1$
⇒ $4b - a \equiv_5 4a - a \equiv_5 3a \equiv_5 1$
⇒ $2 \cdot 3 \cdot a \equiv_5 2 \cdot 1$
$a \equiv_5 2$
⇒ $a = b = 2$, inverse $2x + 2$

Factorize in dual F
Factorize $a(y) = x \cdot y^3 + x \cdot y^2 + (x+1)y + x$
in $GF(2)[x]_{x^2+x+1}[y]$ in irr. polynomials
$\deg(a(y)) = 3$ ⇒ we search NS
$a(0) = x$
$a(1) = x + x + x + 1 + x = 1$
$a(x) = x^4 + x^3 + (x+1)x + x$
$\equiv x^2 + x + 1 \quad x^4 + x^3 + x^2 - x^2(x^2+x+1) = 0$
⇒ $(y-x) \mid a(x)$
→ Polynomial division $a(y) : (y+x)$
↳ $a(y) = (y+x)(xy^2 + y + 1)$
no roots, thus irr.

Irr. polynomials

$GF(2)$	$GF(3)$	
10	10	1112
11	11	1121
111	12	1201
1011	101	1211
1101	112	1222
10011	122	
11001	1021	
11111	1022	
	1102	

$GF(5)$

10	123	1021	1113
11	124	1024	1114
12	133	1032	1131
14	134	1033	1134
102	141	1042	⋮
103	142	1043	
111	1011	1101	
112	1014	1102	

$GF(7)$

10	101	123	146
11	102	125	152
12	104	131	153
13	113	135	155
14	114	136	163
15	116	141	164
16	122	145	166

$\mathbb{Z}_n^*$ with generators:

$\mathbb{Z}_n^*$	
1	1
2	1
3	1 2
4	1 3
5	1 2 3 4
6	1 5
7	1 2 3 4 5 6
8	1 3 5 7
9	1 2 4 5 7 8
10	1 3 7 9
11	1 2 3 4 5 6 7 8 9 10
12	1 5 7 11
13	1 2 3 4 5 6 7 8 9 10 11 12
14	1 3 5 9 11 13
15	1 2 4 7 8 11 13 14
16	1 3 5 7 9 11 13 15
17	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
18	1 5 7 11 13 17
19	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
20	1 3 7 9 11 13 17 19

Multpl. Inverse

modulo m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1																		
2																			
3	1	2																	
4		X	3																
5	1	3	2	4															
6		X	X	X	5														
7	1	4	5	2	3	6													
8		X	3	X	5	X	7												
9	1	5	X	7	2	X	4	8											
10	1	X	7	X	X	X	3	X	9										
11	1	6	4	3	9	2	8	7	5	10									
12		X	X	X	5	X	7	X	X	X	11								
13	1	7	9	10	8	11	2	5	3	4	6	12							
14		X	5	X	3	X	X	X	11	X	9	X	13						
15	1	8	X	4	X	X	13	2	X	X	11	X	7	14					
16		X	11	X	13	X	7	X	9	X	3	X	5	X	15				
17	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16			
18		X	X	X	11	X	13	X	X	X	5	X	7	X	X	X	17		
19	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18	
20	1	X	7	X	X	X	3	X	9	X	11	X	17	X	X	X	13	X	19
a →	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Cyclic groups

	Anzahl Elements	zyklic?
$\langle \mathbb{Z}_n, \oplus \rangle$	n	for all $n \in \mathbb{N}$
$\langle \mathbb{Z}_n; \oplus\rangle \times \langle \mathbb{Z}_m; \oplus \rangle$	$n \cdot m$	if $\gcd(n,m)=1$
$\langle \mathbb{Z}_n^*, \odot \rangle$	$\varphi(n)$	if $n \in \{2, 4, p^e, 2\cdot p^e\}$ for $p \geq 2$ PZ
$\langle \mathbb{Z}_n^*, \odot \rangle \times \langle \mathbb{Z}_m, \odot \rangle$	$\varphi(n) \cdot \varphi(m)$	if $\gcd(n,m)=1$ and $\mathbb{Z}_{nm}^*$ cyclic

Division in $F[x]$
$a(x) = b(x) \cdot q(x) + r(x)$ and $\deg(r(x)) < \deg(b(x))$
for any $a(x)$ and $b(x) \neq 0$ in a field $F[x]$.

Countability Proofs - reminder: $\{0,1\}^\infty$ is the set of functions $N \to \{0,1\}$

Uncountable

$$S = \{f \in \{0,1\}^N \mid \forall i \in N\ f(i) + f(i+1) \leq 1\}$$

We define an injective function $f: \{0,1\}^\infty \to S$
α_i is the i^{th} bit of the sequence $\alpha \in \{0,1\}^\infty$

$f: \{0,1\}^\infty \to S \quad \alpha \to h$ where $h(k) = \begin{cases} 0 & \text{if } k \equiv_2 1 \\ \alpha_{\frac{k}{2}} & \text{if } k \equiv_2 0 \end{cases}$

$\forall h \in \mathrm{Im}(f)\ \forall i \in N$ either $f(i) = 0$ or $f(i+1) = 0$ and $\forall h \in \mathrm{Im}(h)\ \forall i \in N\ f(i) \leq 1$, thus every function $h \in \mathrm{Im}(f)$ satisfies $\forall i \in N\ f(i) + f(i+1) \leq 1$ and thus is an element of S.

Injectivity:
Let k be the first position where $\alpha_k \neq \beta_k$. Let $f(\alpha) = h_\alpha$ and $f(\beta) = h_\beta$. By construction, $h_\alpha(2 \cdot k) = \alpha_k \neq \beta_k = h_\beta(2 \cdot k)$
$\Rightarrow h_\alpha \neq h_\beta$

Set of equivalence classes $\mathbb{R}/\sim$

$a \sim b \Leftrightarrow a - b \in \mathbb{Z}$

$a - b \in \mathbb{Z}$, thus $\exists x \in \mathbb{Z}$ with $a = x + b$. Consider the interval $(0,1)$. For any $a, b \in (0,1)$ there exists no $x \in \mathbb{Z}$ with $a = x + b$ except $x = 0$. Thus for $a, b \in (0,1)$ $[a]_\sim = [b]_\sim \Rightarrow a = b$. Since $(0,1)$ is uncountable, there are uncountably infinite equivalence classes in $(0,1)$. Thus $\mathbb{R}/\sim$ is also uncountable, since it contains at least all equivalence classes in $(0,1)$.

$S = \{f: N \to \{0,1\} \mid \forall n, m \in N: f(n) = 0 \land n \mid m \to f(m) = 0\}$

Let $\phi: N \to \mathbb{P}$ be a bijection from the natural numbers to the primes. (proof!)
We define $\psi: \{0,1\}^\infty \to S$, i.e. $f \to g$

$g(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \text{ and } n \text{ not prime} \\ f(\phi^{-1}(n)) & \text{otherwise} \end{cases}$

Prove that $\psi(f) \in S$:
Let $f \in \{0,1\}^\infty$ and let $g = \psi(f)$. Let $n \in N$, s.t. $g(n) = 0$.
- If $n = 0$, for all $m \in N$ we have $0 \nmid m$ so that there is nothing to check
- If $n \notin \{0,1\}$ and not prime, thus if $n \mid m$ then $m \neq 1$ and m is not prime, so $g(m) = 0$
- If n is prime, thus if $n \mid m$, m is not prime, so $g(m) = 0$.

ψ injective:
Assume $\psi(f) = \psi(f')$ for some $f, f' \in \{0,1\}^\infty$. Let $g = \psi(f)$ and $g' = \psi(f')$.
This means that for all $n \in N$ $g(n) = g'(n)$. We show that $f(n) = f'(n)$ for all $n \in N$.
Let $n \in N$, since ϕ is bijective we have $n = \phi^{-1}(p)$ for some $p \in \mathbb{P}$. Therefore:

$$\begin{aligned} f(n) &= f(\phi^{-1}(p)) && (n = \phi^{-1}(p)) \\ &= g(p) && (\text{Def. } g) \\ &= g'(p) && (g(n) = g'(n) \text{ for all } n \in N) \\ &= f'(\phi^{-1}(p)) && (\text{Def. } g) \\ &= f'(n) && (n = \phi^{-1}(p)) \end{aligned}$$

Thus ψ is injective.

Countable

$$S = \{A \subseteq N \mid A \text{ or } N \setminus A \text{ is finite}\}$$

We define $f: \{0,1\}^* \to S$
For $b \in \{0,1\}^*$, $b_i = i^{th}$ bit of b, 0-indexed.

$f(b) = \begin{cases} N \setminus A, & \text{if } b_0 = 0 \\ A, & \text{if } b_0 = 1 \end{cases}, \quad A := \{x \in N \mid b_x = 1\}$

$f(b) \in S$: Any bit string is finite and thus has a max x, where $b_x = 1$. Thus A or $N \setminus A$ is finite and thus $f(b) \in S$.
Surjective: For any $x \in S$ we can construct a b, s.t. $f(b) = x$.
We first do a case distinction if x is finite ($b_0 = 1$) or not ($b_0 = 0$). Then we simply set $b_i = 1$ if $i \in x$ / $i \in N \setminus x$. Since x or $N \setminus x$ is finite, the bit string is also finite.

$S = \{f: N \to N \mid \forall x \forall y (x \leq y \to f(x) \geq f(y))\}$

f is monoton falling. $\to$ at some point the functions no longer fall.
For all $f \in S$, $\exists x^* \in N$, s.t. $f(y) = f(x^*)$ for all $y \geq x^*$
We define $g: S \to N^*$
$g(f) = (f(0), f(1), \ldots, f(x^*))$, where $f(y) = f(x^*)$ for all $y \geq x^*$

Injectivity:
Let $f_1, f_2 \in S$ be arbitrary and $x_1^*, x_2^* \in N$ the smallest index, where $f_1(x_1) = f_1(x_1^*)$ and $f_2(x_2) = f_2(x_2^*)$ for all $x_1 \geq x_1^*$ and $x_2 \geq x_2^*$.
Assume $f_1 \neq f_2 \Rightarrow \exists x$ s.t. $f_1(x) \neq f_2(x)$. Let x be the smallest such. It holds that $x \leq x_1^*$ or $x \leq x_2^*$
Assume without loss of generality that $x \leq x_2^*$.
Case 1: $x > x_2^*$: $g(f_1)$ and $g(f_2)$ have different length
Case 2: $x \leq x_2^*$: $g(f_1)$ and $g(f_2)$ differ in pos. x.
Thus $g(f_1) \neq g(f_2)$

$g(f) \in N^*$:
Since $f: N \to N$, $f(x) \in N$. Thus $g(f) = (f(0), f(1), \ldots)$ clearly is a sequence of N. As stated above there always exists an x^*. Thus the sequence is surely finite and thus $g(f) \in N^*$

Other

Y non-empty finite set, $f: N \to Y$ arbitrary. Prove: $\exists$ a strictly increasing function $g: N \to N$, s.t. $f \circ g$ is constant:

For each $y \in Y$, consider the set:
$S_y = \{n \mid f(n) = y\}$
There must at least be one $y \in Y$, s.t. S_y is infinite, since $\bigcup_{y \in Y} S_y = N$.
Fix this y:
Now we define g:
$g(k) = \min(\{n \mid f(n) = y \land (\forall x \in N\ x < k \Rightarrow g(x) < n)\})$

Let $\mathcal{A}$ be the set of all infinite subsets of N. Does every pair of sets $A, B \in \mathcal{A}$ have a least upper bound?

Yes: $A \cup B$ is the least upper bound. Let $T \in \mathcal{A}$ be arbitrary:
$A \subseteq T \land B \subseteq T \Leftrightarrow A \cup B \subseteq T$
There exists always an upper bound, since every $A, B \in \mathcal{A}$ at least satisfies
$A \subseteq N \land B \subseteq N$
Note that $A \cup B \supseteq A$, thus $A \cup B \in \mathcal{A}$

Algebra/N.T. proofs

Fields/Algebras/Rings

How many solutions?

Let $p(x) \in \mathbb{Z}_2[x]$ be an irreducible polynomial of degree 5.
Consider the field $F = \mathbb{Z}_2[x]_{p(x)}$. How many solutions $(a,b) \in F \times F$ does the equation
$a^2 + b^2 + ab = 0$ have

Hint: $(a-b)(a^2+b^2+ab) = a^3 - b^3$

Case distinction:

Case 1: $a = b$

$$a^2 + b^2 + ab = a^2 + a^2 + aa = 3a^2 \equiv_2 a^2$$

Since F is field, the only solution to $a^2 = 0$ is $a = 0$, since the field has no zero divisors.

Case 2: $a \neq b$

$a \neq b \Rightarrow (a-b) \neq 0$. Thus for $a^3 - b^3 = 0$ also $a^2 + b^2 + ab = 0$ (Hint). We show $a^3 - b^3 = 0$ has no solutions.

$|F| = |\mathbb{Z}_2|^{\deg(p(x))} = 2^5 = 32 \Rightarrow |F^*| = 31$ is prime.

$\mathrm{ord}(x) \mid |F^*|$, since $|F^*| = 31$ is prime, $\mathrm{ord}(x) \in \{1, 31\}$ for any x.
Any element has $\mathrm{ord}(x) = 31$ if $x \neq 1$.

$$a^3 - b^3 = 0$$
$$\Rightarrow a^3 = b^3$$
$$\Rightarrow (a^3)^c = (b^3)^c$$
$$\Rightarrow a^{3c} = b^{3c}$$
$$\Rightarrow a^{31h+1} = b^{31h+1} \quad \text{for some } h \in \mathbb{Z}, \text{ since } 3 \cdot c \equiv_{31} 1 \; (\gcd(3,31) = 1)$$
$$\Rightarrow (a^{31})^h \cdot a = (b^{31})^h \cdot b$$
$$\Rightarrow a = b$$

which is a contradiction to $a \neq b$.
Thus the only solution is $(a,b) = (0,0)$

Prove $|H| = \mathrm{ord}(x) \cdot \mathrm{ord}(y)$

Let G be a group and $x, y \in G$, s.t.:

1.) $xy = yx$
2.) $\gcd(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$

Let H be the smallest subgroup containing x and y:
Prove $|H| = \mathrm{ord}(x) \cdot \mathrm{ord}(y)$

First show that $H = \{x^i y^j \mid i \in \{0, \dots, \mathrm{ord}(x)-1\}, j \in \{0, \dots, \mathrm{ord}(y)-1\}\}$ is a subgroup:

1. Let $x^i y^j, x^a y^b \in H$:
$$(x^i y^j)(x^a y^b) = x^i x^a y^j y^b = x^{i+a} y^{j+b}$$
$x^{i+a} = x^r$ with $r = R_{\mathrm{ord}(x)}(i+a) \in \{0, \dots, \mathrm{ord}(x)-1\}$
Same for $y^{j+b} \Rightarrow (x^i y^j)(x^a y^b) \in H$
2. $x^0 y^0 = 1 \in H$
3. $x^i y^j \in H$:
$$(x^i y^j)(x^{\mathrm{ord}(x)-i} y^{\mathrm{ord}(y)-j}) = x^{\mathrm{ord}(x)} y^{\mathrm{ord}(y)} = 1 \cdot 1 = 1$$
$$(x^i y^j)^{-1} = x^{\mathrm{ord}(x)-i} y^{\mathrm{ord}(y)-j} \in H$$

Show that H is the smallest subgroup:
Consider any $J \subseteq G$ containing x and y:
$\{1, x, x^2, \dots, x^{\mathrm{ord}(x)-1}\}$ and $\{1, y, y^2, \dots, y^{\mathrm{ord}(y)-1}\}$ must be subgroups of J.
Since their order needs to divide $|J|$, we have:
$$\mathrm{ord}(x) \mid |J| \text{ and } \mathrm{ord}(y) \mid |J| \Rightarrow \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y)) \overset{2.}{=} \mathrm{ord}(x) \cdot \mathrm{ord}(y) \mid |J|$$
$$\Rightarrow |J| \geq \mathrm{ord}(x) \cdot \mathrm{ord}(y)$$

Prove that $\langle \mathbb{Z}_{15}^*, \odot_{15} \rangle \simeq \langle \mathbb{Z}_{16}^*, \odot_{16} \rangle$

Let $\langle G, *, ^{-1}, e \rangle$ be an abelian group. Let $a, b \in G$ and define $n = \mathrm{ord}(a)$ and $m = \mathrm{ord}(b)$.
We show that if $nm = |G|$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$ then $G \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.
Consider the subset $S \subseteq G$ defined as $S = \{a^x * b^y \mid x \in \mathbb{Z}_n \text{ and } y \in \mathbb{Z}_m\}$
Clearly, S is a subgroup of G. Since $\langle a \rangle \cap \langle b \rangle = \{e\}$, we have $|S| \geq nm = |G|$ so that $S = G$. Consider:
$$\varphi : G \to \mathbb{Z}_n \times \mathbb{Z}_m,$$
$$a^x * b^y \mapsto (x, y)$$
φ is group homomorphism:

$$\begin{aligned}
\varphi(g * h) &= \varphi((a^x * b^y) * (a^{x'} * b^{y'})) && (S = G)\\
&= \varphi(a^{x+x'} * b^{y+y'}) && (* \text{ comm.})\\
&= (x \oplus x', y \oplus y') && (\text{Def. } \varphi)\\
&= (x, y) \oplus (x', y') && (\text{Def. direct product})\\
&= \varphi(a^x * b^y) \oplus \varphi(a^{x'} * b^{y'}) && (\text{Def. } \varphi)\\
&= \varphi(g) \oplus \varphi(h) && (S = G)
\end{aligned}$$

φ is surjective, and since $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm = |G|$, we conclude φ is bijective and thus a group isomorphism.
Now, consider $\langle \mathbb{Z}_{15}^*, \odot_{15} \rangle$:
Direct comp. shows that $\mathrm{ord}(2) = 4$, $\mathrm{ord}(11) = 2$. Since $|\mathbb{Z}_{15}^*| = \varphi(15) = 8$, we have $\mathrm{ord}(2)\mathrm{ord}(11) = |\mathbb{Z}_{15}^*|$. Again, direct comp. shows that $\langle 2 \rangle \cap \langle 11 \rangle = \{1\}$. Therefore, as shown above, we have $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
Consider $\langle \mathbb{Z}_{16}^*, \odot_{16} \rangle$:
Same for $\mathrm{ord}(3) = 4$, $\mathrm{ord}(7) = 2$. Thus $\mathbb{Z}_{16}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.
This shows $\mathbb{Z}_{16}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{15}^*$

Prove ring R is comm. with for all $a \in R \setminus \{0\}$ and all $b, c \in R$ we have $ab = ca \Rightarrow b = c$

For $a \neq 0$:
$$a(ba) = a(ba)$$
$$\Rightarrow a(ba) = (ab)a \quad \text{(associativity)}$$
$$\Rightarrow ba = ab \quad \text{(assumption)}$$
For $a = 0$:
$$ab = 0 * b = 0 = b * 0 = ba$$

Disprove: For any two groups G, H, all subgroups of the direct product group are of the form $G' \times H'$, where $G' \subseteq G$ and $H' \subseteq H$

Counterexample: $G = H = \mathbb{Z}_3$
The subgroups of G and H are $\{0\}$ and $\mathbb{Z}_3$
A subgroup of $G \times H$ is $S = \{(0,0), (1,1), (2,2)\}$
↳ prove that it is a subgroup

Number Theory

Proof $\gcd(a, bc) \mid \gcd(a,b) \cdot \gcd(a,c)$

$\gcd(a,b) = ua + vb$, $\gcd(a,c) = xa + yc$
Thus:
$$\begin{aligned}
\gcd(a,b) \cdot \gcd(a,c) &= (ua + vb)(xa + yc)\\
&= uaxa + uayc + vbxa + vbyc\\
&= (uax + uyc + vbx)a + (vy)bc
\end{aligned}$$
Since $\gcd(a, bc)$ divides both a and bc, it divides everything.

Find $n \in \mathbb{N}$, $5^n \equiv_{23} 1$ and $3^n \equiv_{31} 9$

23 is prime, $5^{22} \equiv_{23} 1$
$$\Rightarrow (5^{22})^h \equiv_{23} 1$$
$$\Rightarrow 5^{22h} \equiv_{23} 1$$
31 is prime, $3^{30} \equiv_{31} 1$
$$\Rightarrow (3^{30})^m \equiv_{31} 1$$
$$\Rightarrow 3^{30m} \equiv_{31} 1$$
$$\Rightarrow 3^{30m+2} \equiv_{31} 9$$
Every n with $n = 22h$, $n = 30m+2$ is a solution.
$$22h = 30m + 2 \Leftrightarrow 11h = 15m + 1$$
$$\Rightarrow 11h \equiv_{15} 1$$
$$\Rightarrow h = 11 \quad \text{(multpl. inverse)}$$
$$\Rightarrow 22 \cdot 11 = 242$$
Thus $n = 242$

Prove that $2^{(2^m)}+1$ and $2^{(2^n)}+1$ rel. pr.

for all $m, n \in \mathbb{N} \setminus \{0\}$ with $m \neq n$
Without loss of gen., assume $m < n$
$$2^{(2^m)} \equiv_{2^{(2^m)}+1} -1$$
$$\Rightarrow (2^{(2^m)})^{2^{n-m}} \equiv_{2^{(2^m)}+1} 1$$
$$\Rightarrow (2^{2^m 2^{n-m}}) \equiv_{2^{(2^m)}+1} 1$$
$$\Rightarrow (2^{2^m 2^{n-m}}) + 1 \equiv_{2^{(2^m)}+1} 2$$
$$\Rightarrow 2^{(2^n)} + 1 \equiv_{2^{(2^m)}+1} 2$$
$$\begin{aligned}
&\gcd(2^{(2^m)}+1, 2^{(2^n)}+1)\\
&= \gcd(2^{(2^m)}+1, R_{2^{(2^m)}+1}(2^{(2^n)}+1))\\
&= \gcd(2^{(2^m)}+1, 2) = \gcd(2, 2^{(2^m)}+1)\\
&= \gcd(2, R_2(2^{(2^m)}+1)) = \gcd(2, 1) = 1
\end{aligned}$$

Prove $ab = cd \Rightarrow a+b+c+d$ is not prime

$a, b, c, d \in \mathbb{N} \setminus \{0\}$
Assume by contradiction that $p = a+b+c+d$ is prime
Thus $\mathbb{Z}_p$ is a field (Theorem).
In this field $a+b+c+d = 0 \Leftrightarrow a = -b-c-d$
Putting that into $ab = cd$:
$$-b^2 - bc - bd = cd$$
$$\Leftrightarrow cd + b^2 + bc + bd = 0$$
$$\Leftrightarrow (b+c)(b+d) = 0$$
Since $a, b, c, d \in \mathbb{N} \setminus \{0\}$, $b+c \neq 0 \neq b+d$. Thus $b+c$, $b+d$ are zerodivisors, which contradicts our assumption that $\mathbb{Z}_p$ is field.

$S \subseteq \mathbb{Z}$ be infinite set, s.t.

i) $a - b \in S$ for any $a \in S$, $b \in S$
ii) $(c) \subseteq S$ for any $c \in S$

Prove that there exists $u \in S$, s.t. $(u) = S$

Let $u > 0$ be the smallest positive integer in S.
(u exists since $S \subseteq \mathbb{Z}$)
By (ii), $(u) \subseteq S$
$S \subseteq (u)$:
Euclid: For any $x \in S$, $\exists h, r \in \mathbb{Z}$ with $0 \leq r < u$, s.t.
$x = h \cdot u + r$
By (ii), $h \cdot u \in S$
$x = h \cdot u + r \Leftrightarrow r = x - (h \cdot u)$, $r \in S$ by (i), $x \in S$, $(h \cdot u) \in S$.
However since $0 \leq r < u$ and our assumption that $u > 0$ is the smallest positive integer in S, we have $r = 0$. Thus $x = h \cdot u + r \Leftrightarrow x = h \cdot u \Rightarrow x \in (u)$.
Therefore $(u) \subseteq S \wedge S \subseteq (u) \Rightarrow S = (u)$

Prove for $a^2 = b^3 + 2$, $\exists q$ $a^2 = 4q + 1$

$a^2 = 4q + 1 \Leftrightarrow a^2 \equiv_4 1$
For any $x \in \mathbb{Z}$, we have:

- if $x \equiv_4 0$, then $x^2 \equiv_4 0$, $x^3 \equiv_4 0$
- if $x \equiv_4 1$, then $x^2 \equiv_4 1$, $x^3 \equiv_4 1$
- if $x \equiv_4 2$, then $x^2 \equiv_4 0$, $x^3 \equiv_4 0$
- if $x \equiv_4 3$, then $x^2 \equiv_4 1$, $x^3 \equiv_4 3$

Thus, we have:
$R_4(a^2) \in \{0, 1\}$
$R_4(b^3) \in \{0, 1, 3\} \Rightarrow R_4(b^3 + 2) \in \{1, 2, 3\}$
$a^2 = b^3 + 2 \Rightarrow R_4(a^2) = R_4(b^3 + 2)$, thus we must have $R_4(a^2) = R_4(b^3 + 2) = 1$
Thus $R_4(a^2) \equiv_4 1 \Leftrightarrow a^2 \equiv_4 1$

Find all sol. $0 \leq x < 195$ for

$$2 \cdot x^2 + 8 \equiv_{13} 6$$
$$x \equiv_{15} 2$$

$$2 \cdot x^2 + 8 \equiv_{13} 6$$
$$2x^2 \equiv_{13} 6 - 8 \equiv_{13} -2 \equiv_{13} 11$$
→ Find multpl. inverse of 2 → 7
$$7 \cdot 2 \cdot x^2 \equiv_{13} 7 \cdot 11$$
$$x^2 \equiv_{13} 12 \equiv_{13} 25$$
$$x \equiv_{13} 5, \quad x \equiv_{13} -5 \equiv_{13} 8$$
→ quadratic equations have two solutions: $\pm x$
Thus we have:

$x \equiv_{13} 5$ $\quad$ $x \equiv_{13} 8$
$x \equiv_{15} 2$ $\quad$ $x \equiv_{15} 2$

↳ solve both equations with CRT

Prove $m \equiv_4 n \Leftrightarrow 2003^m \equiv_{10} 2023^n$ for all $m, n \in \mathbb{N}$

$$2003^m \equiv_{10} 2023^n$$
$$\Leftrightarrow R_{10}(2003^m) = R_{10}(2023^n)$$
$$\Leftrightarrow R_{10}(3^m) = R_{10}(3^n)$$
$$\Leftrightarrow R_{10}(3^{R_{\varphi(10)}(m)}) = R_{10}(3^{R_{\varphi(10)}(n)})$$
$$\Leftrightarrow R_{10}(3^{R_4(m)}) = R_{10}(3^{R_4(n)})$$
$$\Leftrightarrow R_4(m) = R_4(n) \qquad (1)$$
$$\Leftrightarrow m \equiv_4 n$$
(1) can be verified by computing all remainders of 3^h, $h \in \{0, 1, 2, 3\}$. Since they are all distinct, it implies $R_4(m) = R_4(n)$

Logic

Semantics proof

$\forall x \neg(F \wedge G) \models \neg((\forall x F) \wedge (\forall x G))$

Let $\mathcal{A}$ be a suitable interpretation for both formulas and also a model for $\forall x \neg(F \wedge G)$:

$\mathcal{A}(\forall x \neg(F \wedge G)) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(\neg(F \wedge G)) = 1$ for all $u \in U$ (Sem. $\forall$)

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F \wedge G) = 0$ for all $u \in U$ (Sem. $\neg$)

By sem. of $\wedge$, $\mathcal{A}_{[x \mapsto u]}(F \wedge G) = 1$ for all $u \in U$ iff. $\mathcal{A}_{[x \mapsto u]}(F) = 1$ and $\mathcal{A}_{[x \mapsto u]}(G) = 1$ for all $u \in U$. Hence we have $\mathcal{A}_{[x \mapsto u]}(F \wedge G) = 0$ for all $u \in U$ iff. for all $u \in U$ either $\mathcal{A}_{[x \mapsto u]}(F) = 0$ or $\mathcal{A}_{[x \mapsto u]}(G) = 0$ (or both).

Case distinction:

Case 1: $\mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 0$ for all $u \in U$ (as stated above)

$\Rightarrow \mathcal{A}(\forall x G) = 0$ (Sem. $\forall$)

$\Rightarrow \mathcal{A}((\forall x F) \wedge (\forall x G)) = 0$ (Sem. $\wedge$)

$\Rightarrow \mathcal{A}(\neg((\forall x F) \wedge (\forall x G))) = 1$ (Sem. $\neg$)

Case 2: $\mathcal{A}_{[x \mapsto u]}(F) = 0$ for some $u \in U$

$\Rightarrow \mathcal{A}(\forall x F) = 0$ (Sem. $\forall$)

$\Rightarrow \mathcal{A}((\forall x F) \wedge (\forall x G)) = 0$ (Sem. $\wedge$)

$\Rightarrow \mathcal{A}(\neg((\forall x F) \wedge (\forall x G))) = 1$ (Sem. $\neg$)

New operator $\diamond$

Sem.: $\mathcal{A}((F \diamond G)) = 1 \Leftrightarrow \mathcal{A}(F) = 0$ or $\mathcal{A}(G) = 1$

Prove: $\forall x (F \diamond G) \models (\forall x F) \diamond (\forall x G)$

Let $\mathcal{A}$ be suitable intp. for both interpretations and a model for $\forall x (F \diamond G)$.

$\mathcal{A}(\forall x (F \diamond G)) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F \diamond G) = 1$ for all $u \in U$ (Sem. $\forall$) (1)

Case distinction:

Case 1: $\mathcal{A}(\forall x (G)) = 1$

$\Rightarrow \mathcal{A}((\forall x F) \diamond (\forall x G)) = 1$ (Sem. $\diamond$)

Case 2: $\mathcal{A}(\forall x (G)) = 0$

$\Rightarrow$ not $(\mathcal{A}(\forall x (G)) = 1))$ (Def. $\mathcal{A}$)

$\Rightarrow$ not $(\mathcal{A}_{[x \mapsto u]}(G) = 1$ for all $u \in U)$ (Sem $\forall$)

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 0$ for some $u \in U$

with (1):

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 0$ for some $u \in U$ and $\mathcal{A}_{[x \mapsto u]}(F \diamond G) = 1$ for all $u \in U$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 0$ and $\mathcal{A}_{[x \mapsto u]}(F \diamond G) = 1$ for some $u \in U$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F) = 0$ for some $u \in U$ (Sem. $\diamond$)

$\Rightarrow$ not$(\mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U)$

$\Rightarrow$ not$(\mathcal{A}(\forall x F) = 1)$

$\Rightarrow (\mathcal{A}(\forall x F) = 0)$

$\Rightarrow \mathcal{A}((\forall x F) \diamond (\forall x G)) = 1$ (Sem $\diamond$)

$\neg F \wedge \forall x F \models G$

Let $\mathcal{A}$ be a suitable interpretation for both and a model for LHS

$\mathcal{A}(\neg F \wedge \forall x F) = 1$

$\Rightarrow \mathcal{A}(\neg F) = 1$ and $\mathcal{A}(\forall x F) = 1$ (Sem. $\wedge$)

$\Rightarrow \mathcal{A}(\neg F) = 1$ and $\mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U$ (Sem. $\forall$)

Case 1: x does not occur free in F

$\Rightarrow \mathcal{A}(\neg F) = 1$ and $\mathcal{A}(F) = 1$ $\Rightarrow$ Contradiction

Case 2: x occurs free in F

$\Rightarrow \mathcal{A}(\neg F) = 1$ and $\mathcal{A}_{[x \mapsto u]}(F) = 1$ for $u = x^{\mathcal{A}}$ $\Rightarrow$ Contradiction

Thus LHS is unsatisfiable and by def of $\models$ the statement is trivially true

$F \models \exists x F$

Let $\mathcal{A}$...

$\mathcal{A}(F) = 1$

Case distinction:

Case 1: x does not occur free in F

$\mathcal{A}(F) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U$ (since $\mathcal{A}$ indp. of x)

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F) = 1$ for some $u \in U$

$\Rightarrow \mathcal{A}(\exists x F) = 1$ (Sem. $\exists$)

Case 2: x occurs free in F

$\mathcal{A}(F) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto x]}(F) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F) = 1$ for some $u \in U$ $(x \in U)$

$\Rightarrow \mathcal{A}(\exists x F) = 1$

$\forall x (F \vee G) \models F \vee (\exists x G)$

Let $\mathcal{A}$...

$\mathcal{A}(\forall x (F \vee G)) = 1$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F \vee G) = 1$ for all $u \in U$ (Sem. $\forall$)

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(F) = 1$ or $\mathcal{A}_{[x \mapsto u]}(G) = 1$ (Sem. $\vee$)
for all $u \in U$

Case 1: $\mathcal{A}_{[x \mapsto u]}(F) = 0$ for some $u \in U$

$\mathcal{A}_{[x \mapsto u]}(F) = 0$ for some $u \in U$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 1$ for all $u \in U$

$\Rightarrow \mathcal{A}_{[x \mapsto u]}(G) = 1$ for some $u \in U$

$\Rightarrow \mathcal{A}(\exists x G) = 1$ (Sem $\exists$)

$\Rightarrow \mathcal{A}(F \vee (\exists x G)) = 1$ (Sem. $\vee$)

Case 2: $\mathcal{A}_{[x \mapsto u]}(F) = 1$ for all $u \in U$

Case 2.1.: x occurs free in F

$\Rightarrow \mathcal{A}_{[x \mapsto x^{\mathcal{A}}]}(F) = 1$ $(x^{\mathcal{A}} \in U)$

$\Rightarrow \mathcal{A}(F) = 1$

$\Rightarrow \mathcal{A}(F \vee (\exists x G)) = 1$ (Sem. $\vee$)

Case 2.2.: x does not occur free in F

$\Rightarrow \mathcal{A}(F) = 1$ (x not free in F)

$\Rightarrow \mathcal{A}(F \vee (\exists x G)) = 1$

Proof system - combine into Π_3

$\tau_3(s_1, s_2) = 1 \Leftrightarrow \tau_1(s_1) \neq \tau_2(s_2)$

$\phi_3((s_1, s_2), (p_1, p_2)) = 1 \Leftrightarrow \phi_1(s_1, p_1) \neq \phi_2(s_2, p_2)$

(Dis) Prove: Π_3 is complete $\Rightarrow \Pi_1$ or Π_2 complete

Counterexample: $S_1 = P_1 = \{0\}$, $\tau_1(0) = 1$, $\phi_1(0,0) = 0$
$\Pi_1 = \Pi_2$

$\tau_3(s_1, s_2) = 1 \Leftrightarrow \tau_1(s_1) = 1$ or $\tau_2(s_2) = 1$

$\phi_3((s_1, s_2), (p_1, p_2)) = 1 \Leftrightarrow \phi_1(s_1, p_1) = 1$ or $\phi_2(s_2, p_2) = 1$

(Dis) Prove: If Π_3 complete $\Rightarrow \Pi_1$ or Π_2 complete

Indirect proof:

Assume both Π_1, Π_2 incomplete:

$\exists s_1 \in S_1$ $\tau_1(s_1) = 1$ but $\phi_1(s_1, p_1) = 0$ for all $p_1 \in P_1$

$\exists s_2 \in S_2$ $\tau_2(s_2) = 1$ but $\phi_2(s_2, p_2) = 0$ for all $p_2 \in P_2$

Consider $(s_1, s_2) \in S_1 \times S_2$

$\tau_1(s_1) = 1$ and $\tau_2(s_2) = 1 \Rightarrow \tau_3(s_1, s_2) = 1$

However:

$\phi_1(s_1, p_1) = 0$ and $\phi_2(s_2, p_2) = 0$ for all $p_1 \in P_1$, $p_2 \in P_2$

$\Rightarrow \phi_3((s_1, s_2), (p_1, p_2)) = 0$ for all $(p_1, p_2) \in P_1 \times P_2$

Thus Π_3 is incomplete and the statement holds

(Dis) Prove: Π_3 sound $\Rightarrow \Pi_1$ or Π_2 sound

Indirect proof:

Assume both Π_1, Π_2 not sound

$\exists s_1 \in S_1$ $\exists p_1 \in P_1$ $\tau_1(s_1) = 0$ but $\phi_1(s_1, p_1) = 1$

$\exists s_2 \in S_2$ $\exists p_2 \in P_2$ $\tau_2(s_2) = 0$ but $\phi_2(s_2, p_2) = 1$

Thus $\tau_3(s_1, s_2) = 0$, but $\phi_3((s_1, s_2), (p_1, p_2)) = 1$

Π_3 is not sound.

(Dis) Prove: Π_1 or Π_2 complete $\Rightarrow \Pi_3$ complete

Counterexample:

$S_1 = S_2 = \{0\}$ and $P_1 = P_2 = \{0\}$

$\tau_1(0) = 0$, $\phi_1(0,0) = 0$, $\tau_2(0) = 1$, $\phi_2(0,0) = 0$.

Π_1 complete.

$\tau_3(0,0) = 1$, since $\tau_2(0) = 1$, but

$\phi_3((0,0), (p_1, p_2)) = 0$ for all $(p_1, p_2) \in P_1 \times P_2 = \{(0,0)\}$

Π_3 is not complete.

$\overline{\Pi} = (S, P, \overline{\tau}, \overline{\phi})$

$\overline{\tau}(s) = 1 \Leftrightarrow \tau(s) = 0$

$\overline{\phi}(s, p) = 1 \Leftrightarrow \phi(s, p) = 0$

(Dis) Prove: Π sound $\Rightarrow \overline{\Pi}$ complete

Counterexample:

$S = \{s\}$, $P = \emptyset$ $\Rightarrow$ only if $P = \emptyset$

$\tau(s) = 0$

Π sound

$\overline{\tau}(s) = 1$

$\overline{\Pi}$ is not complete

(Dis) Prove: Π complete $\Rightarrow \overline{\Pi}$ sound

Counterexample:

$S = \{s\}$, $P = \{p, q\}$

$\tau(s) = 1$, $\phi(s, p) = 1$, $\phi(s, q) = 0$

Π complete.

$\overline{\tau}(s) = 0$, $\overline{\phi}(s, q) = 0$

$\overline{\Pi}$ is not sound.

Applications

Diffie-Hellman

1. Diffie-Hellman protocol with $\langle \mathbb{Z}_n, + \rangle$ with generator $g \in \mathbb{Z}_n$. Show that this protocol is insecure.

→ We have $\gcd(g, n) = 1$. Thus Eve can compute the multpl. inverse with the extended GCD algorithm to find $a \cdot g \equiv_n 1$. Then she can compute $h_{AB} = R_n(a \cdot y_A \cdot y_B)$

$h_{AB} \equiv_n g \cdot x_A \cdot x_B \equiv_n g \cdot x_A \cdot (a \cdot g) \cdot x_B \equiv_n a \cdot (g \cdot x_A) \cdot (g \cdot x_B) \equiv_n a \cdot y_A \cdot y_B$

2. Thus the protocol is insecure for every cyclic group, since all cyclic groups are isomorphic to $\langle \mathbb{Z}_n, + \rangle$. Is this true

→ No. With an isomorphism we could compute x with $g^x = y$ easily with $\varphi(g)^x = \varphi(y)$, since then we would be in the natural numbers $\mathbb{Z}_n$. However, this is false, since finding an isomorphism also isn't always easy.

Exercise:

$\langle \mathbb{Z}_{42}; \oplus \rangle$, $g = 17$, $y_A = 28$, $y_B = 10$, $h = ?$

$y_A = R_{42}(17^{x_A}) \equiv_{42} 17^{x_A} \equiv_{42} 28$

$\Leftrightarrow 17 \cdot x_A \equiv_{42} 28$

$17 \cdot x \equiv_{42} 1 \Leftrightarrow x = 5 \Rightarrow x_A \equiv_{42} 5 \cdot 28 = 140 \equiv_{42} 14$

$\Rightarrow h_{AB} \equiv_{42} 10^{14} \equiv_{42} 10 \cdot 14 = 140 \equiv_{42} 14$

$\langle \mathbb{Z}_{15}^*, \odot \rangle$, $g = 2$, $y_A = 8$, $h_{AB} = 2$, $y_B = ?$

$y_A = R_{15}(2^{x_A}) \Leftrightarrow 2^{x_A} \equiv_{15} 8 \Rightarrow x_A = 3$

$h_{AB} = R_{15}(y_B^{x_A}) \Leftrightarrow y_B^3 \equiv_{15} 2 \Rightarrow y_B = 8$

RSA

RSA with three keys $(n_1, 3), (n_2, 3), (n_3, 3)$. Message m is encrypted for each of them, resulting in c_1, c_2, c_3. How can an attacker use this to compute m?

→ If n_1, n_2, n_3 are not relatively prime:
E.g. $\gcd(n_1, n_2) > 1$. Then we can compute $g = \gcd(n_1, n_2)$ and thus factorize n_1. Then we can decrypt c_1.
If n_1, n_2, n_3 are relatively prime:
We can compute x with CRT:

$x \equiv_{n_1} c_1$
$x \equiv_{n_2} c_2$
$x \equiv_{n_3} c_3$

$m^3 \equiv_{n_i} c_i$ is also a solution. Since $0 \le m < n_i$ we have $0 \le m^3 < n_1 \cdot n_2 \cdot n_3 = N$. Since x is unique in $0 \le x < N$, $x = m^3$. Thus we can compute $m = \sqrt[3]{x}$ efficiently.

Error-Correcting

Polynomial Interpolation

We have a key $s \in GF(q)$ with a polynomial

$a(x) = a_{t-1} x^{t-1} + \dots + a_1 x + s$

Each general $G_1, \dots, G_n$ receives a share $s_i = a(\alpha_i)$.

a) Show that the key can be determined uniquely by t shares

→ Polynomial interpolation. The polynomial is uniquely determined by t shares, since it has degree $t-1$.

b) How many values $\in GF(q)$ are possible for s, if one collected $t-1$ shares.

→ q possibilities. For every $s \in GF(q)$ there exists a polynomial $a(x)$ of degree at most $t-1$, such that all shares are fulfilled.

Prove that for any two rel. prime numbers $m, n > 0$, $\langle \mathbb{Z}_{nm}^*, \odot \rangle$ is isomorphic to $\langle \mathbb{Z}_n^*, \odot \rangle \times \langle \mathbb{Z}_m^*, \odot \rangle$

$f: \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ with $f(x) = (R_n(x), R_m(x))$

f function: $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ for all $x \in \mathbb{Z}_{nm}^*$

Let $x \in \mathbb{Z}_{nm}^*$, thus $\gcd(x, nm) = 1$. Let $d = \gcd(x, n)$. Then $d \mid x$ and $d \mid n$, which implies that $d \mid x$ and $d \mid nm$, so by the definition of gcd, $d \mid \gcd(x, nm)$. Hence $d \mid 1$, so $d = 1$. Thus $\gcd(R_n(x), n) = \gcd(x, n) = 1$, so $R_n(x) \in \mathbb{Z}_n^*$

Analogous for $R_m(x) \in \mathbb{Z}_m^*$

f surjective:

Take any $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Since $\gcd(m, n) = 1$, by CRT, there exists an $x \in \mathbb{Z}_{nm}$ such that $(R_n(x), R_m(x)) = (a, b)$. To show that $x \in \mathbb{Z}_{nm}^*$, assume by contradiction that $d = \gcd(x, nm) > 1$. Let p be an arbitrary prime in the decomposition of d. Since $p \mid nm$, by lemma 4.7, $p \mid n$ or $p \mid m$. In the first case, since also $p \mid x$, we get $p \mid \gcd(x, n)$. But $\gcd(x, n) = \gcd(R_n(x), n) = \gcd(a, n) = 1$ (since $a \in \mathbb{Z}_n^*$), so this is a contradiction. Analogously, in the second case we get $p \mid \gcd(b, m)$.

f injective:

By CRT, the x defined above is unique in $\mathbb{Z}_{nm}$, hence it is also unique in $\mathbb{Z}_{nm}^*$.

f homomorphism:

$f(a \odot_{nm} b) = (R_n(a \odot_{nm} b), R_m(a \odot_{nm} b)) = (R_n(R_{nm}(ab)), R_m(R_{nm}(ab))) = (R_n(ab), R_m(ab)) = (R_n(R_n(a) \cdot R_n(b)), R_m(R_m(a) \cdot R_m(b)))$

$= (R_n(a) \odot_n R_n(b), R_m(a) \odot_m R_m(b)) = (R_n(a), R_m(a)) * (R_n(b), R_m(b)) = f(a) * f(b)$