Zahlentheorie:

Primfaktorzerlegung (Existenz)
-1: Multiplikativ neutral
-Jede Primzahl gemäss Definition
-Rest: Widerspruch Beweis: Angenommen es gibt Zahlen ohne Primfaktor Zerlegung, n, kleinste davon, $n>1$. Da n weder 1 noch prim, besitzt n nicht triviale Teiler $\exists a,b: a \cdot b = n$ $1<a,b<n$. a und b müssen beide in Primzahlen zerlegbar, da n kleinste nicht zerlegbare. $a = \prod p_a$, $b = \prod p_b$ $\rightarrow n = a \cdot b = \prod a \cdot \prod p_b$ ↙
Primfaktorzerlegung (Eindeutigkeit) n = kleinste Zahl mit mehreren: Angenommen, $n = p \cdot q = a \cdot b$, p,q prime, $a \neq b$. Lemma v. Euklid: Teilt p ein Produkt → dann teilt p auch einen Faktor. da q prime, muss p, b teilen. p kommt also in beiden Zerlegungen auf. Dann muss auch n/p mehrere Zerlegungen haben ↙

Beweissysteme:

Direkter Beweis: $S \Rightarrow T$, S angenommen, T nachweisen
Indirekter Beweis: $\neg T$ Falsch $\Rightarrow \neg S$ Falsch
Beweisschritt: $(S \Rightarrow U, U \Rightarrow T) \Rightarrow (S \Rightarrow T)$
Beweis mit Modus-Einteilung: Finden Verwendung R mit $R \Rightarrow S$
Beweis durch Fallunterscheidung: $R_i \Rightarrow S$ $(i \in \{1,\dots,k\})$
Wiedersprüchsbeweis: T führt an, setzt S falsch voraus, Annahme T wahr ↳ Beweis T falsch.
Existenzbeweis: $\exists x P(x)$ für best. Universum und Prädikat P
Beweis mittels Gegenbeispiel: $\neg\forall x P(x) \equiv \exists x \neg P(x)$

Relationsbeweise:

Komposition v. Relationen: $a \rho\sigma c \Leftrightarrow \exists b: (a \rho b \wedge b \sigma c)$
$\rho(\sigma\tau) = (\rho\sigma)\tau$: $\rho(\sigma\tau) \subseteq (\rho\sigma)\tau$ (und umgekehrt)
Sei: $a \rho b \wedge b \sigma c \wedge c \tau d \rightarrow a \rho(\sigma\tau) d$

Transitivität: $\forall a,b,c: (a \rho b \wedge b \rho c) \rightarrow (a \rho c)$
($\Leftarrow$) Falls $a \rho b$ und $b \rho c$, dann $a \rho^2 c \rightarrow a \rho c$, da $\rho^2 \subseteq \rho$
($\Rightarrow$) Sei ρ transitiv und $a \rho^2 b$ für einige a, b ∈ Z:
$a \rho b$. Per Definition $a \rho^2 b \rightarrow \exists c: a \rho c \rho b$, Transitivität ~~bezogt: $a \rho b$~~ impliziert: $a \rho b$ □

Chinese Remainder Theorem:

Falls ein Set $|M| = n$ in k Partitionen, $k<n$ geteilt wird, hat min. 1 Set $\lceil n/k \rceil$ Elemente.
Beweis durch Wiederspruch: angenommen alle Sets haben max $\lceil n/k \rceil - 1$ Elemente, dann gibt es max $k(\lceil n/k \rceil - 1)$ Elemente, was weniger als n ist, da
$k(\lceil n/k \rceil) < (n+1)k = n+k$ Theorem 2.9
↳ evt. $< (\binom{n}{2}+1)k = n+k$

T sei $\rho = |$ (teilt): $a|b \rightarrow ax = b$. $b|c \rightarrow by = c$. $\rightarrow \underbrace{a}_{b} \underbrace{xy}_{z} = c \rightarrow az = c$ ↳ $a|c$

Vorsicht:

ist $n^2 - n + 41$ prime? Scheinbar ja, aber $n = 41 \Rightarrow 41^2 - 41 + 41$, 41^2 nicht prime!
$(A \cup B) = (A \cup C) \not\Rightarrow B = C$, C könnte = AUB sein!
$A = \{1,2\}$, $B = \{3,4\}$, $C = \{1,2,3,4\}$, $A \cup B = A \cup C = \{1,2,3,4\} = C$

Nullteiler in $\langle \mathbb{Z}_n, \odot \rangle$:

z.B. $\mathbb{Z}_{10}$: PFZ: $10 = 2 \cdot 5$
$ggT(a,n)>1$: ↳ [2], [5] sowie vielfache < 10: [4], [6], [8]
$ggT(a,n)=1$: ↳ Einheiten: [1], [3], [7], [9] alle nicht nullteiler

Lemma v. Euklid (L 4.7)

Falls n prime ∧ $n | (x_1 \cdot x_2 \cdot \dots \cdot x_k) \rightarrow n | x_i$ $i \in \{1,\dots,k\}$
Induktion: $n=1$ ✓, $k \rightarrow k+1$: $n | (x_1 \cdot \dots \cdot x_n \cdot x_{n+1})$, sei $y = (x_1 \cdot \dots \cdot x_k)$, $p | y x_{k+1}$
falls $p | y$: $p | x_i$, $i \in \{1,k\}$
falls $p \nmid y$: $ggT(p,y) = 1 \rightarrow (up + vy) = 1 \rightarrow$ ↯
$x_{k+1} = (up + vy) x_{k+1} = (ux_{k+1})p + v(yx_{k+1})$
$\rightarrow p | x_{k+1}$

Gaps between Primes:

können beliebig gross sein: für jedes $k \in \mathbb{N}$ existiert $n \in \mathbb{N}$
$\rightarrow \{n, n+1, \dots, n+k-1\}$ hat keinen Prim
Sei $n = (k+1)! + 2$, $\forall 2 \leq i \leq k+1$, i teilt $(k+1)! = n-2$
$\rightarrow i$ teilt $(k+1)! + i = n \neq 2 + i$, weshalb $\{n, \dots, n+k-1\}$ nicht prime.

Multiplikativ Inverses:

$ax \equiv_n 1$ hat Lösung $x \in \mathbb{Z}_n$, falls $ggT(a,m) = 1$
$ax = km + 1$, da $ggT(a,m)$ sowohl a als auch m teilt, teilt er auch $ax - km$. $ax - km = 1 \rightarrow ggT(a,m) = 1$
$\rightarrow$ falls $ggT(a,m) > 1 \rightarrow$ keine Lösung!
gemäss Lemma 4.4 $\rightarrow \exists u,v: ua + vm = ggT(a,m) = 1$
$vm \equiv_m 0 \rightarrow ua \equiv_m 1 \rightarrow x = u$ ist Lösung in $\mathbb{Z}$
$\rightarrow R_m(u)$ ist Lösung in $\mathbb{Z}_m$ eindeutig (siehe Modulo)

Zyklische Gruppen:

Eine Zyklische Gruppe der Ordnung n ist isomorph zu $\langle \mathbb{Z}_n, \oplus \rangle$ und dadurch abelsch
↳ Sei $G = \langle g \rangle$ zyklisch, order n, mit e als neutral
↳ bijektion, $\mathbb{Z}_n \rightarrow G$: $i \mapsto g^i$ ist Gruppen isomorphismus, da $i \oplus j \mapsto g^{(i)} = g^i * g^j$, $\ominus i \mapsto g^{-1}$, $0 \mapsto e$
endlich ≠ zyklisch

Sei G eine eine endliche Gruppe, $\rightarrow a^{|G|} = e$ $\forall a \in G$
↳ $|G| = k \cdot ord(a) \rightarrow a^{|G|} = a^{k \cdot ord(a)} = (a^{ord(a)})^k = e^k = e$
Jede |Gruppe| = prime ist zyklisch, jedes $a \in G$ ist $\langle a \rangle$ ausser e
↳ $|G| = p$ $\forall a \in G$ $ord(a) \mid |G|$ $\leq \begin{matrix} ord(a)=1 \rightarrow a=e \\ ord(a)=p \rightarrow a \neq \langle p \rangle = G \end{matrix}$

Urbild:

$A = \{1,2,3,4\}$, $B = \{a,b,c,d\}$ $f: A \rightarrow B$

$1 \mapsto a$
$2 \mapsto a$
$3 \mapsto b$
$4 \mapsto d$

$f = \{(1,a), (2,a), (3,b), (4,d)\}$

Theorem 5.15

$\mathbb{Z}_m^*$ ist zyklisch für $m = 2$, $m = 4$, $m = p^e$, $m = 2p^e$
p = ungerade prime, $e \geq 1$
z.B. $\mathbb{Z}_{19}^* = \langle 2 \rangle$: 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1
$G = \langle 2 \rangle, \langle 3 \rangle, \langle 10 \rangle, \langle 13 \rangle, \langle 14 \rangle, \langle 15 \rangle$

Quiz 4:

Potenzmenge, P(A): $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \emptyset\}\} = \{\emptyset, \{\emptyset\}\}$
$P(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
Kardinalität, A, B beliebig:
$|B \cup (A \times \emptyset)| = |B|$, $|CA \times \emptyset| = 0$
$|A \cap (B \cap \bar{B})| = 0$, $|CB \cap \bar{B})| = 0$
Fibonacci: $f_0 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, $n \geq 2$
z.Z.: $n \geq 0$: $f_{n+2} = 1 + \sum_{i=1}^{n} f_i$
Induktion: $n=1$: $f_3 \overset{IA}{=} f_2 + f_1 = 1 + f_1 = 2$ ✓
Schritt: $f_{(n+1)+2} = f_{n+3} \overset{IA}{=} (1 + \sum_{i=1}^{n} f_i) + f_{n+1} = 1 + \sum_{i=1}^{n+1} f_i$

Quiz 5:

A, B, C, beliebige Mengen:
$A \cup B = A \cup C \Rightarrow B = C$ Falsch z.B. $C = A \cup B$
$A \cap B = A \cap C \Rightarrow B = C$ Falsch: $A = \{1\}$, $B = \{2\}$, $C = \{3\}$
$(A \cup B) - (A \cap B) = (A \cup C) - (A \cap C) \Rightarrow B = C$ Wahr
$A \times B = B \times A$ Falsch
ρ relation auf A, $|A| > 0$
falls ρ nicht reflexiv $\rightarrow \rho$ irreflexiv Falsch
falls ρ irreflexiv $\rightarrow \rho$ nicht reflexiv Wahr
falls ρ symetrisch $\rightarrow \rho$ nicht antisymetrisch Falsch
falls ρ antisymetrisch $\rightarrow \rho$ nicht symetrisch Wahr

Quiz 6:

Def Äquivalenz-Relation: reflexiv, symetrisch, transitiv
Def partionelle Ordnung: reflexiv, antisymetrisch, transitiv
$A = \{2,3,4,5,6,7,8\}$, $\rho = (\mid \cup =)$, ρ = Äquivalenzrelation
Äquivalenzklassen: $\{2,3,4,6,8\}$, $\{5\}$, $\{7\}$

Quiz 7:

$ggT(15,18)$, $kgV(15,18)$: $15 = 2^0 \cdot 3^1 \cdot 5^1$, $18 = 2^1 \cdot 3^2 \cdot 5^0$
ggT: $2^0 \cdot 3^1 \cdot 5^0 = 3$, kgV: $2^1 \cdot 3^2 \cdot 5^1 = 90$ oder EEA für ggT und $kgV(a,b) = \frac{a \cdot b}{ggT(a,b)}$
$ggT(15,18) = 15u + 18v \rightarrow$ EEA/Raten: $u = -1$, $v = 1$
$R_m(a+b) \neq R_m(a) + R_m(b)$ teilweise, nicht immer.
Sei $m = 9$, $a = 3$, $b = 4$: $R_9(3+4) = R_9(7) = 7 \neq 3 + 4 = R_9(3) + R_9(4)$ ✓
Sei $m = 2$, $a = b = 1$: $R_2(1+1) = R_2(2) = 0 \neq 2 = 1+1 = R_2(1) + R_2(1)$
$n^3 + 2n$ durch 3 teilbar für alle n? Ja!
$R_3(n) = 0$: $R_3(n^3+2n) = R_3(0^3+2\cdot 0) = R_3(0) = 0$ ✓
$R_3(n) = 1$: $R_3(n^3+2n) = R_3(1^3+2\cdot 1) = R_3(3) = 0$ ✓
$R_3(n) = 2$: $R_3(n^3+2n) = R_3(2^3+2\cdot 2) = R_3(12) = 0$ ✓
In allen Fällen $R_3(n^3+2n) = 0 \rightarrow n^3+2n$ durch 3 teilbar

Quiz 8:

Gruppe, Monoid, weder noch?
$\langle R, \cdot \rangle$: Monoid
$\langle \mathbb{N} \setminus \{0\}, 1 \rangle$: Weder noch
$\langle P(\mathbb{N}), \cap \rangle$: Monoid
$\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$: Gruppe + Monoid
$\langle S, * \rangle$, e, e' neutral z.Z.: $e = e' \overset{e' \text{ n.}}{=} e * e' \overset{e \text{ n.}}{=} e'$
$\langle S, *, e \rangle$, b, c inverse v. a: $b \overset{e \text{ n.}}{=} b * e = b * (a * c) \overset{\text{assoziation}}{=} (b * a) * c \overset{b \text{ inverse } e \text{ n.}}{=} e * c = c$
$b = c$, a hat nur 1 Inverses!

$\mathbb{N}$ = Natürliche Zahlen, $\mathbb{Z}$ = Ganze Zahlen
$\mathbb{Q}$ = Rationale Zahlen, $\mathbb{R}$ = Reelle Zahlen
$\mathbb{C}$ = Komplexe Z