EXAMEN, ZAHLENTHEORIE

Teilbarkeit in $\mathbb{Z}$

- Definition der Teilbarkeit; Definition ggT, kgV; Definition Primzahl
- Rechenregeln (Beweise!!)
- Fundamentalsatz der elementaren ZT (Beweis)
- Euklidischer Algorithmus (Anwendung ($\longrightarrow$ ggT)!! & Beweis)

Lineare diophantische Gleichungen

- Existenz und Eindeutigkeit von Lösungen linearer Gleichungen
- Kongruenzrechnung, Modulrechnung (Kalkül beherrschen): (Anwendung!! & Beweis)
- Simultane Kongruenzen; Chinesischer Restesatz (Anwendung!! & Beweis!) $\longrightarrow$ "Zusammenbauen" von Lösungen (zu teilerfremden Moduln)

Restklassenringe $\mathbb{Z}/m$

- Zusammenhang mit Modulrechnung; Übersetzung von Begriffen und Ergebnissen (?)
- Ringstruktur (Beweis); Endlichkeit der $\mathbb{Z}/m$; $\mathbb{Z}/m$ Körper $\Leftrightarrow$ m Primzahl (? Beweis)
- Prime Restklassengruppe: Satz von Gauß über die Zyklizität (ohne Beweis);
- Primitivwurzeln: Existenz, Anzahl; Indexrechnung $\longrightarrow$ Lösung von Exponentialgleichungen

Quadratische Reste

- Definition Legendre-Symbol; Rechenregeln; Eulerkriterium; QRG & Ergänzungssätze (ohne Beweis); Zusammenhang mit Primitivwurzeln
- Definition Jacobi-Symbol; Rechenregeln; Eulerkriterium; QRG & Ergänzungssätze (ohne Beweis); (Anwendungen!! $\longrightarrow$ Berechnung von Legendre-Symbolen)

Zahlentheoretische Funktionen

- Definition "Zahlentheoretische Funktion"; Beispiele: φ, μ, Teileranzahlfunktion etc.
- $\varphi(m)$ = Anzahl der Elemente in $(\mathbb{Z}/m)^*$.
- Faltung, Definition; ZT-Funktionen bilden einen Ring (mit der Faltung als Produkt) $\longrightarrow$ Rechenregeln für die Faltung (Beweis).
- Möbiussche Umkehrformel (Beweis & Anwendungen)
- Definition multiplikative Funktionen (& strikt multiplikativ); Beispiele: φ, μ, Teileranzahlfunktion etc. (aber nicht alle ZT-Funktionen sind multiplikativ)
- Die Faltung zweier multiplikativer Funktionen ist multiplikativ. $\longrightarrow$ Nachweis für Multiplikativität) (Beweis! & Anwendungen!!)

Algebraische Kongruenzen bzw. Polynomkongruenzen (?)

- Reduktion einer Kongruenz $f(x) \equiv 0 \pmod{m}$ auf $\pmod{p^l}$ (Chinesischer Restesatz)
- "Liften" einer Lösung $\pmod{p^l}$ nach $\pmod{p^{l+1}}$ (Hensellemma (?))

Summen von Quadraten (?)

- $p \neq 2$ Primzahl $\Rightarrow$ p besitzt eine Darstellung als Summe zweier Quadrate genau dann, wenn $p \equiv 1 \pmod{4}$.
- Jede Zahl ist als Summe von 4 Quadratzahlen darstellbar.
- Eine Zahl $n \equiv 7 \pmod{8}$ besitzt keine Darstellung als Summe von 3 Quadraten (Beweis!!).

g-adische Entwicklung (?)