**Prof. Dr. A. Huber-Klawitter / Dr. F. Hörmann**
**Proseminar Elementare Zahlentheorie — Winter 2011/12**
Vortragsliste

---

**Literatur:**

- Ireland, K.; Rosen, M.; *A Classical Introduction to Modern Number Theory*, Second Edition, Springer 1990. Chapter 1–8.
- Stefan Müller-Stach; Jens Piontkowski; *Elementare und algebraische Zahlentheorie: Ein moderner Zugang zu klassischen Themen*, Vieweg, 2006
- Scharlau, W.; Opolka, H.; *Von Fermat bis Minkowski*, Springer, 1980

Die Referenzen in den Vortragsbeschreibungen beziehen Sie auf das Buch von Ireland und Rosen. Mit einem * gekennzeichne Vorträge sind tendenziell etwas schwieriger.

1. **[25.10.] Eindeutige Primfaktorzerlegung.** (Chapter 1, §1, Chapter 2, §1)
   - Euklids Beweis für die Unendlichkeit der Primzahlen (Theorem 1, Ch. 2)
   - Zerlegung in Primfaktoren (Lemma 1, Ch. 1)
   - Definition Hauptidealring
   - Führen Sie den g.g.T. ein, beweisen Sie, dass $\mathbb{Z}$ ein Hauptidealring ist (Lemma 2–4, Ch. 1) und erwähnen Sie den euklidischen Algorithmus (Exercises 1,2 p.14)
   - $p|bc \Rightarrow p|b$ oder $p|c$ (Corollary 1, Ch. 1) und eindeutige Primfaktorzerlegung (Theorem 1, Ch. 1)
   - Wenn Zeit bleibt: eindeutige Primfaktorzerlegung für Polynome (§2, Ch. 2)
2. **[8.11.] Einige zahlentheoretische Funktionen.** (Chapter 2, §2)
   - Definiere die zahlentheoretischen Funktionen $\nu$ (Teileranzahl), $\sigma$ (Divisorsumme), $\varphi$ (Eulersche Phi-Funktion), $\mathbf{1}$ Einheit, $I$ (Prop. 2.2.2)
   - Dirichlet Produkt und Möbius' Umkehrformel (Theorem 2, Ch. 2)
   - Formel für die Eulersche $\varphi$-Funktion (2.2.4–2.2.5)
   - Exercise 14/15
   - Wenn Zeit bleibt: Exercises 25/26
3. **[15.11.] Lineare Kongruenzen.** (Chapter 3, §1–§3)
   - Wiederhole die Definition einer (abelschen) Gruppe, zyklischer Gruppe, Nebenklassen und den Satz von Lagrange (bel. Algebrabuch)
   - Kongruenz-/Restklassen als Nebenklassen von $\mathbb{Z}$ modulo $N\mathbb{Z}$
   - Ringstruktur auf der Menge der Restklassen.
   - Lösbarkeit von linearen Kongruenzen (Prop. 3.3.1, Ch. 3 - Corollary 1, 2)

- Einheitengruppe des Rings $\mathbb{Z}/N\mathbb{Z}$ und die Sätze von Euler und Fermat.

4. **[22.11.] Chinesischer Restsatz und Struktur von $(\mathbb{Z}/N\mathbb{Z})^*$.** (Chapter 3, §4, Chapter 4, §1)
   - Chinesischer Restsatz (Theorem 1, Ch. 3, §4)
   - Anwendung auf Einheitengruppen (Proposition 3.4.1)
   - Satz von Willson (Proposition 4.1.1., Corollary)
   - Struktur von $(\mathbb{Z}/p\mathbb{Z})^*$ (Theorem 1)
   - Beispiele von nicht-zyklischen $(\mathbb{Z}/N\mathbb{Z})^*$
   - Die allgemeine Struktur von $(\mathbb{Z}/N\mathbb{Z})^*$ ohne Beweis

5. **[29.11.] Die Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}[\omega]$.** (Chapter 1, §3, §4)
   - Definition von euklidischem Ring (§3, Ch. 1)
   - Euklidische Ringe sind Hauptidealringe (Prop. 1.3.1)
   - Eindeutige Primfaktorzerlegung in Hauptidealringen (Theorem 3, §3)
   - Definition quadratischer Ringe
   - $\mathbb{Z}[i]$ und $\mathbb{Z}[\omega]$ sind euklidisch

6. **[6.12.] Die diophantischen Gleichungen $x^2 + y^2 = p$ und $x^2 + xy + y^2 = p$.**
   - Norm in den Ringen $\mathbb{Z}[i]$ und $\mathbb{Z}[\omega]$
   - Multiplikativität der Norm
   - Bestimmen Sie die Einheiten dieser Ringe (Chapter 1, Exercises 33, 35)
   - Bestimmen Sie die Primelemente dieser Ringe
   - Folgern Sie, dass Primzahlen $p \equiv 1$ modulo 4 Summe zweier Quadrate sind
   - Folgern Sie, dass Primzahlen $p \equiv 1$ modulo 3 von der Form $x^2+xy+y^2$ sind, bzw. v.d.F. $\frac{A^2+27B^2}{4}$
   - Die Anzahl der Lösungen der Gleichung $x^2 + y^2 = n$ (Chapter 17, Prop. 17.6.1) — je nach Zeit mit oder ohne Beweisskizze

7. **[13.12.] Quadratisches Reziprozitätsgesetz I.** (Chapter 5, §1–§2)
   - Definition quadratischer Reste (§1, Ch. 5)
   - Ein einfaches Kriterium (Prop. 5.1.1)
   - Legendre Symbol (Prop. 5.1.2 and Corollaries)
   - Bestimmen Sie $(-1/p)$ und $(2/p)$ (Corollary 3 und Prop. 5.1.3)
   - Das Gaussche Lemma (Lemma p.52)

*8. **[20.12.] Quadratisches Reziprozitätsgesetz II.** (Chapter 5, §3)
   - Ein Beweis des Satzes (Theorem 1, Ch. 5, §2 — wird in §3 gegeben)

9. **[10.1.] Summe von 4 Quadraten.** (Chapter 17, §7)

- Präsentieren Sie Lemma 1 und 2 (§7, Ch. 7)
- Jede positive ganze Zahl ist Summe von 4 Quadraten (Prop. 17.7.1)
- Lemma 3 – Lemma 6
- Proposition 17.7.2. und Corollary
- Explizite Beispiele für Proposition 17.7.2.

10. **[17.1.] Charaktere und Gausssummen.** (Chapter 8, §1–§2)
    - Multiplikative Charaktere (§1, Ch. 8)
    - Prop. 8.1.1–8.1.2
    - Prop. 8.1.5
    - Definition der Gausssumme (§2)
    - Prop. 8.2.1–8.2.2

11. **[24.1.] Jacobisummen und die Kongruenz $x^n + y^n \equiv 1$ modulo $p$.** (Chapter 8, §3–§4)
    - Beispiel auf Seite 92–93
    - Definition der Jacobisumme
    - Theorem 1 und Corollary
    - Beweis von Prop. 8.3.1–8.3.2 (vgl. Vortrag 6)
    - Beweis von Theorem 2
    - Verallgemeinerung §4

*12. **[31.1.] Quadratisches Reziprozitätsgesetz III.**
    - Erklären Sie ohne ausführliche Beweise Kongruenzen algebraischer Zahlen (§1, Ch. 6)
    - Präsentieren Sie den Beweis aus Chapter 6, §3
    - Wenn Zeit bleibt, können Sie etwas aus Chapter 6, §4 präsentieren

*13. **[7.2.] Satz von Legendre.** (Chapter 17, §3)
    - Satz von Legendre (Prop. 17.3.1)
    - Beweisen Sie zunächst die Äquivalenz zu Prop. 17.3.2
    - Exercise 26
    - Beweis von Prop. 17.3.2
      Sie müssen dazu nocheinmal wiederholen, wie die Normabbildung $\mathbb{Q}(\sqrt{b}) \to \mathbb{Q}$ aussieht und dass Sie multiplikativ ist (vgl. Vortrag 6)
    - Erklären Sie die Bedeutung des Hasse-Prinzips und den Beweis (für terniäre quadratische Formen, Corollary auf Seite 275)

*14. **[14.2.] Descent und die Fermatgleichung $x^n + y^n = z^n$ für $n = 3, 4$.** (Chapter 17, §2, §8)