UNIVERSITÄT PADERBORN

Institut für Mathematik
Prof. Dr. Fabian Januszewski

Proseminar im Sommersemester 2022: Elementare Zahlentheorie

(1) **Teilbarkeitslehre I.** Wir lernen die Grundbegriffe der Teilbarkeitslehre in im Ring $\mathbb{Z}$ der ganzen Zahlen kennen: Division mit Rest, Teilbarkeit als Relation, Definition größter gemeinsamer Teiler. [EZ], Abschnitte 1.4.1, 1.4.2 und Definition 1.4.8 aus Abschnitt 1.4.3.

(2) **Teilbarkeitslehre II.** Der erweiterte Euklidische Algorithmus in $\mathbb{Z}$: Existenz größter gemeinsamer Teiler, Lemma von Bézout, Teilerfremdheit. [EZ], Abschnitte 1.4.3, 1.4.4 und 1.4.5.

(3) **Teilbarkeitslehre III.** Primzahlen und eindeutige Primfaktorzerlegung. [EZ], Abschnitte 1.4.5 und 1.4.6 bis Korollar 1.4.32, sowie die Unendlichkeit der Menge der Primzahlen (Satz 1.4.37 aus Abschnitt 1.4.7).

(4) **Irrationalität n-ter Wurzeln.** Kriterien wann eine ganze bzw. rationale Zahl eine n-te Potzenz ist (Korollare 1.4.33 und 1.4.34 in [EZ]), sowie ihre Verallgemeinerung auf Wurzeln von Polynomgleichungen (Bemerkung 1.4.35, ggf. Beispiel 1.4.36).

(5) **Kongruenzrechnung I.** Der endliche Ring $\mathbb{Z}/n\mathbb{Z}$, seine Einheiten und die Eulersche φ-Funktion, sowie die Anwendung auf Zyklizität endlicher Gruppen: Abschnitte 1.5.1 & 1.5.2 in [EZ].

(6) **Kongruenzrechnung II.** Der chinesische Restsatz für $\mathbb{Z}/n\mathbb{Z}$ (Satz 1.5.13 in [EZ]), Anwendung auf simultane Kongruenzen, Eulers φ-Funktion & zyklische Gruppen. Dies ist der Inhalt von Abschnitt 1.5.3 in [EZ].

(7) **Endliche Körper.** Die endlichen Körper $\mathbb{F}_p$ und ihre Einheitengruppe, Primitivwurzeln & der Begriff der Ordnung eines Gruppenelementes. [EZ] Abschnitt 1.5.4.

(8) **Quadrate in $\mathbb{F}_p$.** Abschnitt 1.5.7 in [EZ]: Quadrate in $\mathbb{F}_p$ und eine Anwendung auf die Faktorisierung bzw. Nullstellenbestimmung quadratischer Polynome über $\mathbb{F}_p$.

(9) **Quadratische Reziprozität.** Für zwei verschiedene Primzahlen p und q gibt es einen fundamentalen Zusammenhang zwischen der Frage, ob p ein Quadrat modulo q ist und ob q ein Quadrat modulo p ist. Dies ist der Inhalt von Abschnitt 1.5.8 in [EZ].

(10) **Primzahlen revisited: Das Sieb von Eratosthenes.** Das Sieb von Eratosthenes ist ein sehr effizienter Algorithmus, um sämtliche Primzahlen $\leq N$ zu bestimmen: Abschnitt 1.4.7 ab Bemerkung 1.4.42 bis einschließlich der Formulierung des Primzahlsatzes (Satz 1.4.49).

(11) **Das quadratische Sieb I.** In diesem Vortrag soll die Grundidee des quadratischen Siebs erklärt werden: Wir verwandeln das Faktorisierungsproblem in zwei Teilprobleme: Finde Relationen über einer Faktorbasis & Löse eine großes LGS über $\mathbb{F}_2$. Abschnitt 1.5.9 aus [EZ] bis einschließlich Unterabschnitt zur Anpassung der Faktorbasis.

(12) **Das quadratische Sieb II.** Abschnitt 1.5.9 ab Unterabschnitt „Sieben von Relationen“, inklusive Parameterwahl (ggf. als Skizze). Ausführliche Beispiele sind dem dritten Vortrag vorbehalten. Daher sollte ein kleines Beispiel mit ca. 3 Relationen vorbereitet werden.

(13) **Das quadratische Sieb III.** Implementiere das quadratische Sieb selbst in Python und arbeite auf dieser Grundlage ein etwas größere Beispiele aus, um diese inklusive Parameterwahlen zu präsentieren.

Literatur

[EZ] F. Januszewski, Skriptum *Elementare Zahlentheorie*, 2021.