Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix

# Elementare Zahlentheorie

Sommersemester 2017

**Übungsblatt 7** 6. Juni 2017

**Aufgabe 32.** (Kreisgleichung über $\mathbb{F}_p$ und die Ergäzungssätze des quadratischen Reziprozitätsgesetzes)

Es sei $p > 2$ eine Primzahl. Für $a \in \mathbb{Z}$ mit $p \nmid a$ definieren wir

$$K_a := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \ ; \ x^2 + y^2 \equiv a \pmod{p}\}.$$

Ziel dieser Aufgabe ist es, die Anzahl $\#K_a$ zu bestimmen und daraus einen weiteren Beweis der Ergäzungssätze des quadratischen Reziprozitätsgesetzes herzuleiten. Gehen Sie wie folgt vor:

(a) Zeigen Sie: $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$.

(b) Zeigen Sie: $\displaystyle\sum_{j=0}^{p-1} \left(\frac{j(j-a)}{p}\right) = -1$.

*Hinweis:* Zeigen Sie zunächst für $j \neq 0$, daß $\left(\frac{j^{-1}}{p}\right) = \left(\frac{j}{p}\right)$, wobei $j^{-1} \in \mathbb{F}_p$ das multiplikative Inverse von $j$ modulo $p$ bezeichnet.

(c) Zeigen Sie: $\#K_a = \displaystyle\sum_{j=0}^{p-1} \left(1 + \left(\frac{j}{p}\right)\right)\left(1 + \left(\frac{a-j}{p}\right)\right)$.

*Hinweis:* Überlegen Sie hierzu, daß $\#\{x \in \mathbb{F}_p \mid x^2 \equiv j \pmod{p}\} = 1 + \left(\frac{j}{p}\right)$ gilt.

(d) Folgern Sie: $\#K_a = p - \left(\frac{-1}{p}\right)$.

Wir kommen nun zum Beweis der Ergänzungssätze. Folgende Teilaufgaben sind unabhängig von den vorherigen. Lediglich das Resultat von (d) wird für die Teile (f) und (g) benötigt.

(e) Zeigen Sie: $\#K_2 \equiv 4 + 2\left(\left(\frac{2}{p}\right) + 1\right) \pmod{8}$.

*Hinweis:* Sei $D_4 = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^4 = 1 \rangle$ die Diedergruppe der Ordnung 8. Betrachten Sie die Gruppenwirkung auf $K_2$ von $D_4$, die für $(x, y) \in K_2$ gegeben ist durch

$$\sigma(x, y) := (x, -y) \quad \text{und} \quad \tau(x, y) := (y, x).$$

Sie dürfen davon ausgehen, dass es sich hier um eine wohldefinierte Gruppenwirkung handelt. Für welchen Punkt $(x, y) \in K_2$ hat die Bahn unter dieser Gruppenwirkung die Länge 8? Welche Bahnlänge haben dann die restlichen Punkte?

(f) Folgern Sie den ersten Ergänzungssatz: $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4, \\ -1, & p \equiv 3 \bmod 4. \end{cases}$

(g) Folgern Sie den zweiten Ergänzungssatz: $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$

**Aufgabe 33.** (Berechnung der Jacobi-Symbole)

Berechnen Sie $\left(\frac{2017}{5843}\right)$ und $\left(\frac{13259}{35671}\right)$.

**Aufgabe 34.** (Jacobi-Symbole)

Seien $m, n \in \mathbb{N}$ ungerade und $a \in \mathbb{Z}$, so dass $(a, mn) = 1$.

(a) Zeigen Sie: Ist $m \equiv n \pmod{4|a|}$, so gilt: $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$

(b) Zeigen Sie anhand eines Beispiels mit $a \in \mathbb{N}$ ungerade, dass die Bedingung $m \equiv n \pmod{2a}$ nicht ausreicht.

**Aufgabe 35.** (Spezialfall des Dirichlet'schen Primzahlsatzes)

Zeigen Sie:

(a) Jede Primzahl größer als 3 ist von der Form $6k + 1$ oder $6k - 1$ mit $k \in \mathbb{N}$.

(b) Es gibt unendlich viele Primzahlen der Form $6k - 1$ mit $k \in \mathbb{N}$.

---

**Abgabe:** Am kommenden Montag, den **12. Juni 2017**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/65113368/17_SS_Elementare-Zahlentheorie`