**Übungen zu Elementare Zahlentheorie — Blatt 5**

Prof. Dr. Ulrich Thiel, TU Kaiserslautern — Sommersemester 2021
Abgabetermin: Montag, 28.06.2021, 10:00 Uhr — Dr. Tommy Hofmann

---

Mit Primzahl ist im Folgenden stets eine positive Primzahl gemeint.

**Aufgabe 1.**

(i) Ist die Fermatsche Zahl $F_n = 2^{(2^n)} + 1$ eine Primzahl und $n > 0$, so gilt

$$3^{\frac{F_n - 1}{2}} \equiv -1 \bmod F_n.$$

(ii) Welchen Wert hat das Legendre-Symbol $(\frac{822}{2207})$?

(iii) Ist 17 ein quadratischer Rest modulo 6439?

(iv) Ist das Polynom $X^2 + 11X + 573$ irreduzibel über $\mathbb{Z}/733\mathbb{Z}$?

**Aufgabe 2.** Es sei $p \in \mathbb{P}$ eine ungerade Primzahl, $a = 2$, und $\nu$ definiert wie in Lemma 5.7 (b).

(i) Zeigen Sie, dass

$$\nu = \left| \left\{ n \,\middle|\, \frac{p-1}{4} < n \leq \frac{p-1}{2} \right\} \right|.$$

(ii) Zeigen Sie, dass

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

**Aufgabe 3.** Zeigen Sie:

(i) Eine Zahl $a \in \mathbb{Z}$ ist genau dann quadratischer Rest modulo 2, wenn $a$ ungerade ist.

(ii) Eine Zahl $a \in \mathbb{Z}$ ist genau dann quadratischer Rest modulo 4, wenn $a \equiv 1 \bmod 4$.

(iii) Für eine ungerade Zahl $a \in \mathbb{Z}$ sind die folgenden Aussagen äquivalent:
   (a) $a$ ist quadratischer Rest modulo $2^k$ für alle $k \in \mathbb{Z}$ mit $k \geq 3$,
   (b) $a$ ist quadratischer Rest modulo 8,
   (c) $a \equiv 1 \pmod 8$.

**Aufgabe 4.** Es sei $p$ eine ungerade Primzahl und $a$ teilerfremd zu $p$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) $a$ ist quadratischer Rest modulo $p$,

(ii) $a$ ist quadratischer Rest modulo $p^k$ für alle $k \in \mathbb{Z}_{>0}$.