TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Mathias Schulze
Dipl.-Math. Cornelia Rottner
Fachbereich Mathematik

Elementare Zahlentheorie

Sommersemester 2016 - 5.Übungsblatt

Abgabetermin: 23.6.2016, 16:00h

Aufgabe 1. Es sei $p \in \mathbb{P}$ eine ungerade Primzahl. Zeigen Sie:

(a) $\nu_{2,p} = \left|\left\{n \middle| \frac{p-1}{4} < n \leq \frac{p-1}{2}\right\}\right|$;

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

Aufgabe 2.

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

(b) Ist 17 ein quadratischer Rest modulo 6439?

(c) Ist 649 eine 4-te Potenz in $\mathbb{Z}_{859}$?

(d) Ist $X^2 + 11X + 573$ irreduzibel über $\mathbb{Z}_{733}$?

Aufgabe 3. Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $k, m \in \mathbb{Z}$ mit $\text{ggt}(p, km) = 1$. Zeigen Sie: Falls die diophantische Gleichung

$$x^2 - m \cdot y^2 = k \cdot p$$

eine ganzzahlige Lösung hat, so ist das Legendre-Symbol $\left(\frac{m}{p}\right) = 1$. Gilt auch die Umkehrung der Aussage?

Aufgabe 4. Bearbeiten Sie zwei Teilaufgaben Ihrer Wahl:

(a) Sei $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 3 \pmod 4$ und a ein Quadrat modulo p. Zeigen Sie, dass $a^{(p+1)/4}$ eine Lösung von $x^2 \equiv a \pmod p$ ist.

(b) Zeigen Sie mithilfe des Primitivwurzelkriteriums, dass $a = 83$ ein quadratischer Rest modulo $n = 361$ ist und finden Sie eine Lösung der Gleichung $x^2 \equiv a \pmod{361}$.

(c) Sei $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 5 \pmod 8$ und a ein Quadrat modulo p. Finden Sie einen expliziten Ausdruck für eine Lösung der Gleichung $x^2 \equiv a \pmod p$.