TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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

Elementare Zahlentheorie

Sommersemester 2016 - 4.Übungsblatt

Abgabetermin: 9.6.2016, 16:00h

Aufgabe 1.

(a) Sei $p \in \mathbb{P}$ eine ungerade Primzahl, $k \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ eine Primitivwurzel modulo p^k. Zeigen Sie:

(i) Ist a ungerade, so ist a eine Primitivwurzel modulo $2 \cdot p^k$.

(ii) Ist a gerade, so ist $a + p^k$ eine Primitivwurzel modulo $2 \cdot p^k$.

(b) Bestimmen Sie eine Primitivwurzel modulo $n = 98$.

Aufgabe 2. Sei $p \in \mathbb{P}$ eine ungerade Primzahl und $a \in \mathbb{Z}$ eine Primitivwurzel modulo p. Zeigen Sie:

(a) $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

(b) Genau dann ist $-a$ ebenfalls eine Primitivwurzel modulo p, wenn $p \equiv 1 \pmod{4}$ gilt.

Aufgabe 3. Sei $p \in \mathbb{P}$ eine Primzahl, $k \in \mathbb{Z}_{>0}$ und $a = p^m \cdot b \in \mathbb{Z}$ mit $\mathrm{ggt}(b, p) = 1$. Zeigen Sie:

(a) Ist $m \geq k$, so hat die Gleichung $x^2 \equiv a \pmod{p^k}$ eine Lösung in $\mathbb{Z}$.

(b) Ist $0 \leq m < k$, so sind die folgenden Aussagen gleichwertig:

(i) $x^2 \equiv a \pmod{p^k}$ hat eine Lösung in $\mathbb{Z}$.

(ii) m ist gerade und die Gleichung $y^2 \equiv b \pmod{p^{k-m}}$ ist in $\mathbb{Z}$ lösbar.

Aufgabe 4. Sei $a \in \mathbb{Z}$. Zeigen Sie:

(a) a ist genau dann quadratischer Rest modulo 2, wenn a ungerade ist.

(b) a ist genau dann ein quadratischer Rest modulo 4 wenn $a \equiv 1 \pmod{4}$.

(c) Die folgenden Aussagen sind gleichwertig:

(i) a ist ein quadratischer Rest modulo 2^k für alle $k \geq 3$.

(ii) a ist ein quadratischer Rest modulo 8.

(iii) $a \equiv 1 \pmod{8}$.