Fachbereich Mathematik
Thomas Markwig Sommersemester 2008, Blatt 4

Elementare Zahlentheorie

Abgabetermin: Donnerstag, 05/06/2008, 12:00

Fernstudenten reichen alle Aufgaben ein und ersetzen den hier angegebenen Abgabetermin durch den ihnen mitgeteilten. Für alle anderen Studenten ist die Aufgabe 16 eine Präsenzaufgabe, deren Lösung nicht eingereicht werden muß.

Für die Lösung der Aufgaben 15 und 16 wird die Vorlesung vom 2.6. benötigt.

Aufgabe 13: Es sei $(G, \cdot)$ eine Gruppe, $g \in G$ mit $o(g) < \infty$ und $k \in \mathbb{Z}$. Zeige

$$o\left(g^k\right) = \frac{o(g)}{\mathrm{ggt}(o(g), k)}.$$

Aufgabe 14: Es sei $p \in \mathbb{P}$ und $k \in \mathbb{Z}_{>0}$. Zeige:

a. Die Abbildung

$$\pi : \mathbb{Z}_{p^{k+1}}^* \longrightarrow \mathbb{Z}_{p^k}^* : \overline{z}_{p^{k+1}} \mapsto \overline{z}_{p^k}$$

ist ein Gruppenepimorphismus und $|\mathrm{Ker}(\pi)| = p$.

b. Für $a \in \mathbb{Z}$ mit $\mathrm{ggt}(a, p) = 1$ gilt

$$o\left(\overline{a}_{p^{k+1}}\right) \in \left\{o\left(\overline{a}_{p^k}\right), p \cdot o\left(\overline{a}_{p^k}\right)\right\}.$$

Aufgabe 15: Es sei $2 \neq p \in \mathbb{P}$, $k \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ eine Primitivwurzel modulo p^k. Zeige:

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

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

Aufgabe 16: Bestimme Primitivwurzeln modulo n für $n = 98$ und $n = 2197$.