

Elementare Zahlentheorie

Sommersemester 2004

8. Übungsblatt

Aufgabe 1 (4 Punkte)

- Bestimmen Sie jeweils eine Primitivwurzel in \mathbb{F}_p für $p = 13, 17$ und 19 .
- Sei nun $p \in \mathbb{P}$ beliebig. Zeigen Sie, dass 4 in \mathbb{F}_p nicht primitiv ist.

Aufgabe 2 (4 Punkte)

Sei $n \in \mathbb{N}$ und $p := 2^{2^n} + 1$ eine Primzahl. Zeigen Sie:

- Genau dann ist $x \in \mathbb{F}_p^\times$ eine Primitivwurzel, wenn $\left(\frac{x}{p}\right) = -1$ ist.
- $7 \bmod p$ ist eine Primitivwurzel von \mathbb{F}_p .

Aufgabe 3 (4 Punkte)

Finden Sie eine Nullstelle von Φ_7 in \mathbb{Z}_{29} .

Hinweis: Konstruieren Sie diese mit Hilfe des Lemma von Hensel.

Aufgabe 4 (4 Punkte)

- Seien $p \in \mathbb{P}$ und $r \in \mathbb{Z}$. Weiter sei r eine primitive Wurzel modulo p . Zeigen Sie, dass dann r oder $r + p$ Ordnung $(p - 1) \cdot p$ modulo p^2 hat.
- Nun sei $p \in \mathbb{P}$ ungerade und r so gewählt, dass r modulo p^2 Ordnung $(p - 1) \cdot p$ hat. Zeigen Sie durch vollständige Induktion:

Für $k \geq 2$ hat r modulo p^k die Ordnung $(p - 1) \cdot p^{k-1} = \varphi(p^k)$.

Hinweis: Wieso ist es hilfreich, erst $r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$ zu zeigen?

ABGABE bis Mittwoch, den **16. Juni 2004, 14:00 Uhr** in den gekennzeichneten Einwurfkästen im Kollegiengebäude Mathematik, 3. OG neben Zimmer 308 oder zu Beginn der Übung.

Beachten Sie auch den Hinweis auf die Vorlesungsevaluation auf der Rückseite.

Liebe Studierende,

in der Woche vom 14.06. bis zum 18.06. wird eine Vorlesungsbefragung via Internet durchgeführt. Sie erhalten dazu in der Vorlesung der nächsten Woche eine Umfrage-Nummer mit einem gültigen Passwort und der entsprechenden URL (Internet-Adresse). Sie können also von jedem Rechner mit Internetzugang aus auf den Fragebogen zugreifen. Selbstverständlich steht Ihnen in dieser Woche auch unser Rechnerpool (Raum -125 im Keller des Mathematik-Gebäudes) zur Verfügung. Die Rechner sind so konfiguriert, daß ein Browser mit der Evaluationsseite geöffnet ist.

Bitte füllen Sie unseren Fragebogen aus. Sie helfen uns, die Qualität unserer Lehre weiter zu verbessern.

Danke!

Andreas Rieder (Studiendekan der Fakultät für Mathematik)