Albert–Ludwigs–Universität Freiburg
Institut für Mathematik
Abteilung für Reine Mathematik
PD Dr. K. Halupczok
Dipl.–Math. S. Feiler

Übungen zur Vorlesung

Elementare Zahlentheorie

Sommersemester 2009

7. Übungsblatt

08. Juni 2009

Abgabe der Lösungen bis zum **15. Juni 2009 um 14.$\underline{15}$ Uhr**

Aufgabe 25 (Carmichael–Zahlen — Teil 2) 5 Punkte
Eine Zahl $n \in \mathbb{N} \setminus \{1\}$ heißt **Carmichael–Zahl**, wenn $n \notin \mathbb{P}$ ist, aber die Fermat–Kongruenz $a^n \equiv a \bmod n$ für alle $a \in \mathbb{Z}$ erfüllt.

a) Zeigen Sie, dass $n \in \mathbb{N} \setminus \{1\}$ genau dann eine Carmichael–Zahl ist, wenn ein $\mathcal{P} \subseteq \mathbb{P}$ mit $1 < \#\mathcal{P} < \infty$, $n = \prod_{p \in \mathcal{P}} p$ und $(p-1) \mid (n-1)$ für alle $p \in \mathcal{P}$ existiert! (2,5 Punkte)

(Tipp: Sie dürfen Aufgabe 9 verwenden.

Stellen Sie n als $p^k \cdot m$ mit $p \in \mathbb{P}$, $k \in \mathbb{N}$, $m \in \mathbb{N}$ und $p \nmid m$ dar und arbeiten Sie dann mit dem Satz über die Existenz von Primitivwurzeln und dem chinesischen Restsatz!)

b) Zeigen Sie, dass jede Carmichael–Zahl mindestens drei Primfaktoren besitzt und ungerade ist. (1 Punkt)

c) Zeigen Sie, dass 561 die kleinste Carmichael–Zahl ist! (1,5 Punkte)

Aufgabe 26 (Anwendungen des Satzes von Wilson) 3 Punkte
Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$.

a) Zeigen Sie $(p-1)! \equiv (p-1) \bmod \sum_{j=1}^{p-1} j$! (2 Punkte)

b) Zeigen Sie, dass p sowohl $a^p + a \cdot (p-1)!$ als auch $a + a^p \cdot (p-1)!$ teilt! (1 Punkt)

Aufgabe 27 (Lösungen einer Kongruenzengleichung)
Finden Sie alle $x \in \mathbb{Z}$ mit

$$6x^4 + 4x^3 + 3x^2 + 8x + 4 \equiv 0 \bmod 1225 \quad !$$

Verwenden Sie keine elektronischen Hilfsmittel!
(Tipp: Für alle $p \in \mathbb{P} \setminus \{2\}$ ist $\left\{ a \in \mathbb{Z} \,;\, |a| \leq \frac{p-1}{2} \right\}$ ein vollständiges Restsystem modulo p.)

Aufgabe 28 (Legendre–Symbol)
Zeigen Sie, dass $n^2 - n + 41 \in \mathbb{P}$ für alle $n \in \mathbb{N}_0$ mit $n \leq 40$ ist!
(Tipp: Zeigen Sie, dass -163 ein quadratischer Nicht–Rest modulo aller Primzahlen $p \in \mathbb{P}$ mit $p < 41$ ist! Betrachten Sie dann das Polynom $\left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ n & \mapsto & 4n^2 - 4n + 4 \cdot 41 \end{array} \right\}$!)