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

8. Übungsblatt

15. Juni 2009

Abgabe der Lösungen bis zum **22. Juni 2009 um 14.$\underline{^{15}}$ Uhr**

Aufgabe 29 (GAUSSsumme zum LEGENDRE–Symbol)

Sei $\zeta : \left\{ \begin{array}{ccc} \mathbb{P} & \to & \mathbb{C} \\ p & \mapsto & \zeta_p \end{array} \right\}$ mit $\zeta_p^\ell \neq 1$ für alle $\ell \in \mathbb{N}$ mit $\ell < p$ und $\zeta_p^p = 1$ für alle $p \in \mathbb{P}$.

Sei $S : \left\{ \begin{array}{ccc} \mathbb{P} & \to & \mathbb{C} \\ p & \mapsto & S_p := \displaystyle\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \cdot \zeta_p^k \end{array} \right\}$.

a) Zeigen Sie $\displaystyle\sum_{k=0}^{p-1} \zeta_p^{jk} = \begin{cases} 0, & \text{falls } p \nmid j \\ p, & \text{falls } p \mid j \end{cases}$ für alle $j \in \mathbb{Z}$ und alle $p \in \mathbb{P}$! (1 Punkt)

b) Zeigen Sie $S_p^2 = \left(\frac{-1}{p}\right) \cdot p$ für alle $p \in \mathbb{P}$! (3 Punkte)

(*Tipp:* Verwenden Sie in einem Faktor Folgerung 2.6 mit einem geeigneten Multiplikator.)

Aufgabe 30 (Quadratische Kongruenz) 5 Punkte

Bestimmen Sie alle $x \in \mathbb{R}$ mit $3x^2 - 13x + 15 \equiv 0 \mod 1325$!

(*Bemerkung:* Für Berechnungen, die mit dem chinesischen Restsatz in Verbindung stehen, dürfen Sie Additionen, Subtraktionen, Multiplikationen und Divisionen mit einem Taschenrechner durchführen.)

Aufgabe 31 (JACOBI–Symbol) 3 Punkte

a) Berechnen Sie $\left(\frac{15694}{12547}\right)$! (1 Punkt)

Geben Sie bei jedem Rechenschritt an, welches Gesetz Sie verwenden!

b) Zeigen Sie, dass $\left(\frac{3}{3^n - 2}\right) = (-1)^{n+1}$ für alle $n \in \mathbb{N} \setminus \{1\}$ gilt! (2 Punkte)

Aufgabe 32 (Primzahlkriterien)

a) Zeigen Sie, dass $n \in \mathbb{N}$ prim ist, wenn es ein $a \in \mathbb{Z}$ mit $(a, n) = 1$ und $\operatorname{ord}_n(a) = n - 1$ gibt! (1,5 Punkte)

b) Zeigen Sie, dass $n \in \mathbb{N} \setminus \{1\}$ mit $2 \nmid n$ genau dann prim ist, wenn es ein $a \in \mathbb{Z}$ mit $(a, n) = 1$, $a^{n-1} \equiv 1 \mod n$ und $a^{\frac{n-1}{p}} \not\equiv 1 \mod n$ für alle $p \in \mathbb{P}$ mit $p \mid (n-1)$ gibt! (2,5 Punkte)