Übungen zur Algebraischen Zahlentheorie I

Wintersemester 2010/11

Universität Heidelberg
Mathematisches Institut
Prof. A. Schmidt
Dr. A. Holschbach

Blatt 2
Abgabetermin: Mittwoch, 27.10.2010, 16.15 Uhr

Aufgabe 1.

(a) Ist 67 ein quadratischer Rest modulo 139?

(b) Berechnen Sie das Legendre-Symbol $\left(\frac{701}{997}\right)$.

Aufgabe 2.

(a) Seien m, n zwei teilerfremde natürliche Zahlen, und sei $a \in \mathbb{Z}$. Zeigen Sie: Die Kongruenz

$$x^2 \equiv a \bmod mn$$

ist genau dann lösbar, wenn die beiden Kongruenzen

$$x^2 \equiv a \bmod m \quad \text{und} \quad x^2 \equiv a \bmod n$$

eine Lösung besitzen.

(b) Bestimmen Sie alle Lösungen der Kongruenz

$$x^2 \equiv 29 \bmod 35.$$

Aufgabe 3. Sei $n \in \mathbb{N}$ beliebig. Zeigen Sie:

(a) Jeder Primteiler $p \neq 3$ von $n^2 + n + 1$ erfüllt $p \equiv 1 \bmod 6$.

(b) Jeder Primteiler $p \neq 5$ von $n^2 + n - 1$ erfüllt $p \equiv \pm 1 \bmod 10$.

Aufgabe 4. Sei p eine von 2 und 5 verschiedene Primzahl. Aus der Schule ist bekannt, dass man $\frac{1}{p}$ als periodischen Dezimalbruch schreiben kann; sei l_p die minimale Periodenlänge (Beispiele: $\frac{1}{3} = 0{,}\overline{3} \Rightarrow l_3 = 1$ und $\frac{1}{7} = 0{,}\overline{142857} \Rightarrow l_7 = 6$). Zeigen Sie:

(a) l_p ist ein Teiler von $p - 1$.

(b) l_p teilt $\frac{p-1}{2}$ genau dann, wenn 10 ein quadratischer Rest modulo p ist.

Zusatzaufgabe: Angenommen, p und $q = 2p + 1$ sind ungerade Primzahlen. Zeigen Sie: Dann sind sowohl $(-1)^{(p-1)/2}2$ als auch -4 primitive Wurzeln modulo q.