Elementare Zahlentheorie

9ter Übungszettel

Abgabe: Donnerstag, 11.06, 12:00 Uhr

(ins Postfach Ihres Tutors)

Bitte bearbeiten Sie drei Aufgaben. Wenn Sie alle vier bearbeiten, zeigen Sie bitte an, welche in die Bepunktung eingehen sollen. Jede Aufgabe wiegt fünf Punkte.

Aufgabe 1. Sei p eine ungerade Primzahl und a teilerfremd zu p. Zeige, daß die Kongruenz

$$x^2 \equiv a \mod p^\alpha$$

für jedes $\alpha \geq 1$ genau $1 + (\frac{a}{p})$ Lösungen hat.

Aufgabe 2. Sei m ungerade und a teilerfremd zu m. Zeige: Die Kongruenz

$$x^2 \equiv a \mod m$$

hat genau $\prod_{p|m} 1 + (\frac{a}{p})$ Lösungen; und ist m überdies quadratfrei, so kann die Voraussetzung, daß a teilerfremd ist, aufgegeben werden.

Aufgabe 3. Sei q von der Form $q = 4^n + 1$. Zeige: q ist eine Primzahl genau dann, wenn $3^{\frac{q-1}{2}} \equiv -1 \mod q$ ist.

Aufgabe 4. Sei $n \in \mathbb{Z}$ nicht durch 3 teilbar. Zeige, daß $m = 4n^2 + 3$ mindestens einen Primfaktor hat, der kongruent $7 \mod 12$ ist. Hint: Bestimme die Primzahlen p, für die -3 quadratischer Rest modulo p ist.