

## Elementare Zahlentheorie – Übungsblatt 10

### Aufgabe 1 (4 Punkte)

Sei  $d \in \mathbb{Z}$  und  $p \equiv 1 \pmod{4d}$  prim. Zeigen Sie, dass  $d$  ein Quadrat modulo  $p$  ist.

### Aufgabe 2 (2 Punkte)

Ist die Gleichung  $X^2 = 14$  in  $\mathbb{Z}/385\mathbb{Z}$  lösbar?

### Aufgabe 3 (4 Punkte)

Bestimmen Sie alle Primzahlen  $p$ , für die 91 ein Quadrat modulo  $p$  ist.

### Aufgabe 4 (4 Punkte)

Sei  $N > 2$  und  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ , so dass  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}$ .  
Zeigen Sie, dass eine solche Matrix keine endliche Ordnung hat.

### Aufgabe 5 (2 Punkte)

Zeigen Sie:

$$\mathbb{R}[X]/(X^2 - d)\mathbb{R}[X] \cong \begin{cases} \mathbb{R} \times \mathbb{R}, & d > 0 \\ \mathbb{C}, & d < 0 \end{cases}.$$

**Abgabe:** Bis Mittwoch, den 25.06.2008, vor Beginn der Übung in den Kasten neben Zimmer 308 des Mathematikgebäudes.