

## Probeklausur Elementare Zahlentheorie

*Beweise werden nur dort erwartet, wo sie ausdrücklich gefordert sind.  
Taschenrechner sind nicht zugelassen.*

1. Welche der folgenden Aussagen über beliebige natürliche Zahlen  $a, b, c, d$  und  $m > 0$  ist wahr, welche ist falsch? Geben Sie im letzteren Fall ein Gegenbeispiel an.
  - (a) Aus  $a \equiv b$  und  $c \equiv d \pmod{m}$  folgt  $ad \equiv bc \pmod{m}$ .
  - (b) Aus  $a \equiv b$  und  $c \equiv d \pmod{m}$  folgt  $a - 2b \equiv c - 2d \pmod{m}$ .
  - (c) Aus  $a^2 \equiv b^2 \pmod{m}$ ,  $a > 0$  und  $b > 0$  folgt  $a \equiv b \pmod{m}$ .
  - (d) Aus  $ac \equiv bc \pmod{mc}$  und  $c \neq 0$  folgt  $a \equiv b \pmod{m}$ .
2. (a) Bestimmen Sie alle Lösungen der folgenden Kongruenzen.

$$5x \equiv 4 \pmod{13}$$

$$6x \equiv -4 \pmod{28}$$

Geben Sie die Antwort jeweils durch Restklassen zum vorgegebenen Modul an.

- (b) Finden Sie alle Lösungen des aus den beiden Kongruenzen in Teil (a) gebildeten Systems.
3. (a) Es seien  $p, q$  und  $r$  verschiedene Primzahlen. Finden Sie den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache der Zahlen  $p^5q^2$  und  $p^3q^3r$ . Geben Sie für diese beiden Zahlen den Wert der Eulerschen  $\varphi$ -Funktion an. (Die Antworten sind durch  $p$  und  $q$  auszudrücken.)
    - (b) Beweisen Sie, dass es keine rationale Zahl gibt, deren Quadrat gleich 8 ist.

4. Zeigen sie durch Reduktion modulo 5, dass die Diophantische Gleichung

$$x^5y + 5x^3 - xy^5 = 1$$

keine Lösung besitzt.

5. Bestimmen Sie einen Entschlüsselungsexponenten für das RSA-Verfahren modulo 143, wenn zur Verschlüsselung der Exponent 7 verwendet wurde.

*b.w.*

6. (a) Finden Sie Vertreter für die primen Restklassen modulo 18 und bestimmen Sie für jeden von ihnen die Ordnung modulo 18.  
(b) Geben Sie eine natürliche Zahl  $g > 1$  an, so dass  $\frac{1}{18}$  im Ziffernsystem zur Grundzahl  $g$  eine Periode der Länge 6 hat.
7. Bestimmen Sie, welche der Zahlen 57, 98 und 117 sich als Summe von zwei Quadraten schreiben lässt.
8. Stellen Sie fest, ob 91 ein quadratischer Rest modulo der Primzahl 181 ist.