Universität Bielefeld
Prof. W. Hoffmann

WS 2006/07

Klausur 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 ist wahr, welche ist falsch? Geben Sie im letzteren Fall ein Gegenbeispiel an.

   (a) Die Zahl a ist genau dann teilerfremd zu bc, wenn sie sowohl zu b als auch zu c teilerfremd ist.

   (b) Ist $\mathrm{ggT}(a, b, c) = 1$, so ist auch $\mathrm{ggT}(a, bc) = 1$.

   (c) Aus $a^2 \mid b^3$ folgt $a \mid b$.

   (d) Aus $a^3 \mid b^2$ folgt $a \mid b$.

2. (a) Bestimmen Sie alle Lösungen der folgenden Kongruenzen.

   $$\begin{aligned} 6x &\equiv 15 \pmod{21} \\ 9x &\equiv \ \ 8 \pmod{19} \end{aligned}$$

   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. Es seien $p_1, \ldots, p_r$ verschiedene Primzahlen mit der Eigenschaft $p_i \equiv -1 \pmod 4$.

   (a) Zeigen Sie, dass die Zahl $N = 4p_1 \cdot \ldots \cdot p_r - 1$ durch keine der Primzahlen $2, p_1, \ldots, p_r$ teilbar ist.

   (b) Zeigen Sie, dass die Zahl N einen Primfaktor p mit der Eigenschaft $p \equiv -1 \pmod 4$ besitzt.

4. Zeigen sie durch Reduktion modulo 3, dass die Diophantische Gleichung

   $$x^3 + 5x + y^2 + 1 = 0$$

   keine Lösung besitzt.

5. Bestimmen Sie einen Entschlüsselungsexponenten für das RSA-Verfahren modulo 133, wenn zur Verschlüsselung der Exponent 7 verwendet wurde.

b.w.

6. (a) Finden Sie Vertreter für die primen Restklassen modulo 14 und bestimmen Sie für jeden von ihnen die Ordnung modulo 14.

   (b) Geben Sie eine natürliche Zahl $g > 1$ an, so dass $\frac{3}{14}$ im Ziffernsystem zur Grundzahl g eine Periode der Länge 3 hat.

7. Finden Sie alle Lösungen der Kongruenzen

$$\begin{aligned} x^3 - x + 3 &\equiv 0 \pmod{7}, \\ x^3 - x + 3 &\equiv 0 \pmod{49}. \end{aligned}$$

8. Stellen Sie fest, ob 163 ein quadratischer Rest modulo der Primzahl 191 ist.