Universität Karlsruhe (TH)
Forschungsuniversität · gegründet 1825
Institut für Angewandte
und Numerische Mathematik

Mathematik für die Fachrichtung Informationswirtschaft I

Prof. Dr. Andreas Rieder, PD Dr. Nicolas Neuss

7. Übungsblatt

Aufgabe 1: (3 Punkte)
Es sei $m > 0$ und $a, b, c, d \in \mathbb{Z}$ mit $a \equiv b \bmod m$ und $c \equiv d \bmod m$. Zeigen Sie:

a) $a + c \equiv (b + d) \bmod m$,

b) $ac \equiv bd \bmod m$.

c) $a^k \equiv b^k \bmod m$ für alle $k \geq 0$.

Aufgabe 2: (5 Punkte)

a) Lösen Sie $2x \equiv 1 \bmod 3$ in $\mathbb{Z}_3$ und in $\mathbb{Z}$.

b) Bestimmen Sie mit dem Euklidischen Algorithmus Zahlen $k, l \in \mathbb{Z}$ mit $17k+5l = 1$. Verwenden Sie dieses Resultat, um alle Lösungen $x \in \mathbb{Z}$ von $5x \equiv 10 \bmod 17$ zu bestimmen.

c) Bestimmen Sie alle Lösungen von $x^2 \equiv -1 \bmod 5$ in $\mathbb{Z}$.

d) Bestimmen Sie alle Lösungen von $x^2 \equiv -1 \bmod 8$ in $\mathbb{Z}$.

e) Lösen Sie $x^3 - 2x^2 + x \equiv 0 \bmod 11$ in $\mathbb{Z}_{11}$ und in $\mathbb{Z}$.

Aufgabe 3: (4 Punkte)
Zeigen Sie, dass die Zahlen 5^{57} und 17^{73} kongruent modulo 27 sind.
Hinweis: Verwenden Sie den Satz von Fermat-Euler (für teilerfremde natürliche Zahlen a und m gilt $a^{\varphi(m)} \equiv 1 \bmod m$).

Aufgabe 4: (4 Punkte)
Es sei $p = 31$ und $q = 43$, $n = pq$ sowie $e = 11$. Jemand hat eine Botschaft x als $y \equiv x^e \bmod n$ verschlüsselt und $y = 268$ erhalten.

a) (3 Punkte) Wie lautet die Entschlüsselungsvorschrift?

b) (1 Punkt) Was ist x?
Hinweis: Verwenden Sie für diesen Teil Maxima oder ein anderes CAS zum Rechnen (schreiben Sie dann aber bitte auch den Befehl zur Lösung auf). Mit einem normalen Taschenrechner oder per Hand ist es etwas mühsam.

Abgabe: Werfen Sie Ihre Löungen bis zum **18.12.2006**, **11.00 Uhr** in den Einwurfschlitz „Mathematik I für Informationswirte“ im Treppenhaus des Mathematik-Gebäudes, 1. OG, gegenüber von Zimmer 112. Schreiben Sie bitte auf **jedes** Ihrer Blätter Ihren Namen, Ihre Gruppe (A-D) sowie Ihre/n Tutor/-in.