Institut für Angewandte und
Numerische Mathematik

PD Dr. Nicolas Neuß
Dipl.-Math. techn. Hannes Gerner

22.11.2010

Mathematik I für die Fachrichtung Informationswirtschaft (Wintersemester 2010/2011)

Übungsblatt 6

Bearbeitungszeitraum: 22.11.2010-29.11.2010

Aufgabe 1

(1+1+1+1 Punkte)

Berechnen Sie mit Hilfe des Euklidischen Algorithmus' die Inversen der folgenden Zahlen in den angebenen Restklassenkörpern:

(a) 9 in $\mathbb{Z}_{29}$,

(b) 22 in $\mathbb{Z}_{73}$,

(c) 16 in $\mathbb{Z}_{57}$,

(d) 17 in $\mathbb{Z}_{127}$.

Aufgabe 2

(2+2 Punkte)

Ihr Freund möchte Ihnen eine kodierte Nachricht schicken. Dafür wandelt er die Buchstaben A bis Z in Zahlen um ($A = 1, B = 2, \ldots, Z = 26$). Für das Leerzeichen verwendet er die Zahl 27 und für das Ausrufezeichen 28. So bildet er aus seinem Klartext eine Zahlenfolge, die er mit dem RSA-Verfahren chiffriert. Für das Verfahren verwendet er die Parameter

$$p = 11, q = 7, \text{ woraus } n = 77 \text{ und } \varphi(n) = 60 \text{ folgt.}$$

(a) Bestimmen Sie zu $e = 17$ die Zahl $d \in \{1, 2, \ldots, \varphi(n) - 1\}$ mit

$$ed \equiv 1 \mod \varphi(n).$$

(b) Sie empfangen die Meldung

62 1 48 57 3 69 4 24 48 69 44 45 1 24 24 3 63,

die unter Verwendung der oben angegebenen Parameter erstellt worden ist.

Entschlüsseln Sie diese.

Aufgabe 3

(1+1+1+1 Punkte)

Bestimmen Sie alle Lösungen $x \in \mathbb{Z}$ der Kongruenzen

(a) $8x \equiv 10 \mod 17$,

(b) $x^2 \equiv 4 \mod 8$,

(c) $x^2 \equiv -4 \mod 7$,

(d) $42x \equiv 6 \mod 408$.

Verwenden Sie für (b) und (c) folgenden Satz:
Sei $m \in \mathbb{Z}$, $m \neq 0$ und $b \in \mathbb{Z}_m$. Die Kongruenz $x^2 \equiv b \mod m$ ist genau dann in $\mathbb{Z}$ lösbar, wenn die Gleichung $z^2 = b$ in $\mathbb{Z}_m$ lösbar ist. In diesem Fall sind alle Lösungen der Kongruenz gegeben durch $x = z_0 + km$ für $k \in \mathbb{Z}$ und z_0 ist Lösung von $z^2 = b$ in $\mathbb{Z}_m$.

Aufgabe 4 (4 Punkte)

Seien $m, n \in \mathbb{N}$ mit $m > n$. Zeigen Sie: Zwei hintereinander ausgeführte Schritte des Euklidischen Algorithmus' zur Berechnung von $\mathrm{ggT}(m, n)$ führen mindestens zu einer Halbierung der Zahlen m und n.
Hinweis: Sie können annehmen, dass der Euklidische Algorithmus nicht abbricht.

Abgabe
Werfen Sie Ihre Lösungen bis zum **Montag, den 29. November 2010, 09.40 Uhr** in den mit "Mathematik für die Fachrichtung Informationswirtschaft" gekennzeichneten Abgabekasten im 1.OG des C-Teils des Allianz-Gebäudes (Kaiserstr. 93) ein. Schreiben Sie bitte auf **jedes** Ihrer Blätter Ihren Namen, Ihre Matrikelnummer und Ihre Übungsgruppe.