

Mathematik I für die Fachrichtung Informationswirtschaft Übungsblatt 6

Wintersemester 2011/2012

Aufgabe 16 (4 Punkte)

- (a) (1 Punkt) Bestimmen Sie den größten gemeinsamen Teiler von 20622 und 13314.
- (b) (3 Punkte) Berechnen Sie die Inversen bezüglich der Multiplikation in den angegebenen Restklassenkörpern:
- (b1) 9 in \mathbb{Z}_{73}
 - (b2) 22 in \mathbb{Z}_{127}
 - (b3) 16 in \mathbb{Z}_{29}

Aufgabe 17 (4 Punkte)

Bestimmen Sie die Lösungsmengen der folgenden Kongruenzen in \mathbb{Z} :

- (a) (1.5 Punkte) $8x \equiv 10 \pmod{17}$
- (b) (1.5 Punkte) $42x \equiv 6 \pmod{408}$
- (c) (1 Punkt) $x^2 \equiv 4 \pmod{8}$

Aufgabe 18 (4 Punkte)

Ihr Freund möchte Ihnen eine kodierte Nachricht schicken. Dafür wandelt er die Buchstaben A bis Z in Zahlen um ($A = 1, B = 2, \dots, Z = 26$). 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 verschlüsselt. Für das Vorhaben verwendet er die Parameter $p = 11$ und $q = 7$.

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

$$ed \equiv 1 \pmod{\varphi(n)}.$$

- (b) (2 Punkte) Sie empfangen die Meldung

28 21 48 69 28 3 62 1 75 57 48 63,

die unter Verwendung der oben angegebenen Parameter erstellt worden ist. Entschlüsseln Sie diese.

Aufgabe 19 (4.5 Punkte)

Gegeben seien die Permutationen $\pi, \sigma \in S_6$ mit

$$\pi = (3, 2, 5, 6, 4, 1) \quad \text{und} \quad \sigma = (6, 3, 1, 5, 4, 2).$$

- (a) (1.5 Punkte) Berechnen Sie $\pi \circ \sigma$ und $\pi^{-1} \circ \sigma^{-1}$.
- (b) (1 Punkt) Stellen Sie π als Produkt von höchstens vier Transpositionen dar.
- (c) (1.5 Punkte) Berechnen Sie $\sigma^2, \sigma^3, \dots, \sigma^6$.
- (d) (0.5 Punkte) Berechnen Sie σ^{2011} .
-
-

Abgabe der Übungsblätter:

Die bearbeiteten Übungsaufgaben sind bis zum **Montag, den 28.11.2011, 9.45 Uhr** in den Einwurfschlitze **Mathematik I für Informationswirtschaft** im 1. OG des ehemaligen Allianz-Gebäudes einzuwerfen. Schreiben Sie bitte auf jedes Blatt **Name und Matrikelnummer** und heften Sie die Blätter zusammen. Die abgegebenen Aufgaben müssen einzeln und handschriftlich bearbeitet sein.

Besprechung:

Das Übungsblatt wird in der Woche vom **28.11.2011** bis zum **2.12.2011** in den Tutorien besprochen.

Sprechstunden:

Prof. Dr. Christian Wieners: Dienstag, 9.30-11.30 Uhr.
Dipl.-Math. Markus Bürg: Mittwoch, 10.30-11.30 Uhr.