

4. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 6.5.2011, bis 9.15 Uhr

Gruppen 1 und 2 (Mo): Fach Nr. 3 (orangener Schrank bei D1.348)

Gruppen 3 und 4 (Do): Fach Nr. 11 (orangener Schrank bei D1.348)

Internet: <http://math-www.uni-paderborn.de/~chris>

Schreiben Sie bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel-Nr. und Nr. Ihrer Übungsgruppe. Heften Sie bitte die Seiten zusammen!

Es können **Bonuspunkte** für die Leistungsnachweis-Klausur erworben werden.

Es ist nur Einzelabgabe erlaubt. **Es sind immer Begründungen erforderlich!**

11. Aufgabe: a) Berechne $(37 \bmod 11) + (75 \bmod 11)$ und $(37 + 75) \bmod 11$.

In welchem Verhältnis stehen die beiden Ergebnisse zueinander?

b) Beweise (3.2e): Für $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt:

$$((a \bmod n) + (b \bmod n)) \bmod n = (a + b) \bmod n. \quad (4)$$

12. Aufgabe: a) Die Abbildung $f : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$ sei definiert durch

$$f(r) = (3 \cdot r) \bmod 26 \quad (r \in \mathcal{R}_{26}).$$

1) Stelle die Wertetabelle für f auf. Was läßt sich in Hinblick auf Injektivität bzw. Surjektivität von f aus der Tabelle ablesen?

2) Beweise, dass f injektiv ist. Ist f auch surjektiv?

b) Untersuche, ob die Abbildung $g : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$, die durch $g(r) = (4 \cdot r) \bmod 26$ ($r \in \mathcal{R}_{26}$) definiert ist, injektiv ist.

Hinweis: Bei dieser Aufgabe dürfen keine Ergebnisse aus § 4 benutzt werden! (6)

13. Aufgabe: Eine Permutation der Zahlen $1, 2, 3, 4, 5$, die genau zwei Zahlen $i \neq k$ miteinander vertauscht und die restlichen Zahlen festläßt, heißt eine **Transposition** von 5 Zahlen. Diese Transposition wird mit $\tau_{i,k}$ bezeichnet. So ist z.B. $\tau_{2,4} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$.

a) Berechne $\tau_{2,4} \circ \tau_{2,4}$ und bestimme die Umkehrabbildung von $\tau_{2,4}$.

b) Berechne die Hintereinanderausführung $\tau_{1,2} \circ \tau_{2,3} \circ \tau_{3,4} \circ \tau_{4,5}$.

c) Stelle die Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$ als eine Hintereinanderausführung geeigneter Transpositionen dar. Begründe dein Ergebnis.

Hinweis: Permutationen werden noch in den Gruppen 1 und 2 am Montag behandelt. (4)

Denke an die Punktetabelle!