Christian Nelius

2. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Donnerstag, 21.4.2011, bis 13.00 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!**

3. Aufgabe: a) Die Abbildungen $f : \mathbb{N} \longrightarrow \mathbb{Z}$ und $g : \mathbb{Z} \longrightarrow \mathbb{R}$ seien durch die folgenden Zuordnungsvorschriften definiert: $f(n) := n^2 + 1$ $(n \in \mathbb{N})$ bzw. $g(a) := 2a^2 + 3$ $(a \in \mathbb{Z})$. Bestimme alle Urbilder von 9 bzw. 10 unter f. Bestimme alle Urbilder von -1,3 bzw. 5 unter g. Stelle eine Formel für die Zuordnungsvorschrift von $g \circ f$ auf. Läßt sich $f \circ g$ bilden?

b) Die Abbildungen $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ seien für beliebiges $x \in \mathbb{R}$ definiert durch $f(x) := x^2 + 1$ bzw. $g(x) := \dfrac{x+1}{x^4+2}$. Untersuche, ob $f \circ g = g \circ f$ gilt. (5)

4. Aufgabe: a) Begründe, dass durch die Zuordnung $x \longmapsto \dfrac{1}{x-1}$ eine Abbildung $f : \mathbb{Q} \setminus \{1\} \longrightarrow \mathbb{Q} \setminus \{0\}$ definiert ist.

b) Zeichne ein Schaubild von f. Lassen sich Injektivität oder Surjektivität von f aus dem Bild ablesen? Begründe!

c) Beweise, dass die Abbildung f bijektiv ist.

d) Bestimme die Umkehrabbildung von f (es ist insbesondere deren Zuordnungsvorschrift anzugeben).

e) Berechne direkt $(f^{-1} \circ f)(x)$ für $x \in \mathbb{Q} \setminus \{1\}$ unter Benutzung der jeweiligen Zuordnungsvorschrift. (6)

Fortsetzung nächste Seite!

5. Aufgabe: Die Abbildungen $V : \{0,1,2,3,4,5,6,7,8,9\} \longrightarrow \{\alpha,\beta,\gamma,\delta,\varepsilon,\sigma,\eta,\rho,\iota,\kappa\}$ und $W : \{\alpha,\beta,\gamma,\delta,\varepsilon,\sigma,\eta,\rho,\iota,\kappa\} \longrightarrow \{\heartsuit,\emptyset,\diamondsuit,\infty,\triangle,\spadesuit,\nabla,\sharp,\clubsuit,\oplus\}$ seien durch die folgenden Wertetafeln definiert:

x	0	1	2	3	4	5	6	7	8	9
$V(x)$	γ	η	ι	σ	β	α	κ	ε	ρ	δ

y	α	β	γ	δ	ε	σ	η	ρ	ι	κ
$W(y)$	$\oplus$	$\clubsuit$	$\sharp$	∇	$\spadesuit$	$\triangle$	∞	$\diamondsuit$	$\emptyset$	$\heartsuit$

a) Stelle die Wertetabelle für die Hintereinanderausführung $W \circ V$ auf.

b) Verschlüssele die Zahl 87237 mit Hilfe von V, indem jede Ziffer durch ihren Bildwert unter V ersetzt wi rd. Das griechische Alphabet findest du auf meiner Homepage!

c) Verschlüssele $\kappa\alpha\iota\sigma\varepsilon\rho$ mit Hilfe von W.

d) Bei der folgenden Multiplikationsaufgabe, bei der die Ziffern mit $W \circ V$ verschlüsselt wurden, sind die drei mit ? gekennzeichneten Ziffern nicht angegeben worden. Kannst du sie richtig einsetzen? Gibt es nur eine Möglichkeit? (4)

$$\clubsuit \oplus ? \diamondsuit \quad \text{mal} \quad \triangle \sharp \infty \emptyset \quad = \quad \infty \triangle \spadesuit \diamondsuit ? ? \triangle \heartsuit$$

6. Aufgabe: Finde drei sinnvolle Wörter der deutschen Sprache mit mindestens 3 Buchstaben, die durch die Verschiebechiffre V_G wieder in ein sinnvolles Wort der deutschen Sprache verschlüsselt werden. (3)

Achtung!

Schreibe auf die erste Seite deiner Bearbeitung oben rechts eine Punktetabelle der Form

3	4	5	6	**Σ**

in die die Korrektorinnen die Punkte eintragen können. Verfahre bei den folgenden Übungen entsprechend!