6. Übungsblatt

MATHEMATIK FÜR INFORMATIKER I (WS 2000/01)

Abgabe: Montag, 4.12.2000 bis **13.00 Uhr !!!**

Der Abgabeort wird noch bekanntgegeben

Internet–Adresse der Vorlesung:

http://math–www.uni–paderborn.de/~chris/index9.html

22. Aufgabe: Es sei $G \subseteq \mathbb{N}$ die Menge der geraden natürlichen Zahlen. Beweise:

a) $G \subset \mathbb{N}$

b) Die Abbildung $f : \mathbb{N} \longrightarrow G$, $n \longmapsto 2n$ ist injektiv un d surjektiv (und damit bijektiv).

c) Gib die Umkehrabbildung $g : G \longrightarrow \mathbb{N}$ von f an und beweise noch einmal explizit, daß $g \circ f = \mathrm{id}_{\mathbb{N}}$ und $f \circ g = \mathrm{id}_G$ gilt. (4)

23. Aufgabe: (Gestellt von M.Noecker) Eine wichtige Rolle spielen bijektive Abbildungen in der Kryptographie. Schon Gaius Julius Caesar (der aus dem *Bellum Gallicum*) benutzte eine Abbildung, um Cicero (der mit den berühmten Reden) geheime Nachrichten zukommen zu lassen. Caesar ging wie folgt vor: Er schrieb die Nachricht in Großbuchstaben A, . . . , Z und ignorierte Satzzeichen. Dann ersetzte er den Text dieses sogenannten *Klartextes* Buchstabe für Buchstabe durch andere. Seine Abbildung φ war die: ersetze A durch D, B durch E usw. Das ergab den *Geheimtext*.

a) Welchen Buchstaben hat Caesar wohl für die Klartextbuchstaben X, Y und Z geschrieben?

b) Wie lautet der Geheimtext für den Klartext: VENI VIDI VICI ?

c) Zeige: die Abbildung φ ist bijektiv. Gib die Umkehrabbildung an, mit der Cicero die Geheimtexte entschlüsselt hat.

d) Der Bote hat den Geheimtext ausgeplaudert. Er lautet: GDVLVWHLQIDFK. Was wird wohl Miraculix, der Hofmathematiker von Vercingetorix (Vorsicht, nur eine dieser Personen ist authentisch) als Entschlüsselung herausbekommen haben? (6)

e) (**Wird nicht korrigiert!**) Entwirf dein eigenes System, indem du die Idee von Caesar nutzt, aber A jetzt nicht durch D, sondern einen anderen Buchstaben deiner Wahl ersetzt. Gib deine Abbildung ψ an, mit der du den Klartext in den Geheimtext übersetzt. Bilde mit ψ deinen Vor- und Nachnamen als Geheimtext ab.

24. Aufgabe: Die folgenden Induktionsbeweise sind **ausführlich** aufzuschreiben:

a) Für $n \in \mathbb{N}$ bezeichne s_n die Summe aller ungeraden natürlichen Zahlen von 1 bis $2n - 1$, d.h. $s_n = 1 + 3 + 5 + \ldots + (2n - 1)$. Berechne s_n für kleine Werte von n (etwa $n = 1, 2, 3, 4, 5$) und suche eine Formel für s_n in Abhängigkeit von n. Beweise die gefundene Formel dann durch vollständige Induktion.

b) Für $n \in \mathbb{N}$ sei $t_n := 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n \cdot (n + 1)$. Beweise durch vollständige Induktion: $\forall\, n \in \mathbb{N} : t_n = \frac{1}{3} n(n + 1)(n + 2)$. (6)