4. Übungsblatt zu der Vorlesung

"Diskrete und Numerische Mathematik für Informatiker"

Frankfurt, den 3.5.2016

Abgabetermin: 10.5.2016, 12:00 – vor der Vorlesung

13.) Es sei $n \in \mathbb{N}$ mit $n \geq 2$ fixiert. Ferner sei T_n die Menge der – positiven – Teiler von n, und für $t \in T_n$ setze

$$A_t := \{k \in \mathbb{N} \,|\, 1 \leq k \leq t,\ ggT(k,t) = 1\},$$
$$B_t := \{k \in \mathbb{N} \,|\, 1 \leq k \leq n,\ ggT(k,n) = t\}.$$

Insbesondere ist also stets $|A_t| = \varphi(t)$. Sind $d, t \in T_n$ mit $d \cdot t = n$, so heißen d, t *komplementäre Teiler von* n; dabei *kann* auch $d = t$ sein. Beweisen Sie:

i) Die Mengen $B_t, t \in T_n$, bilden eine disjunkte Zerlegung der Menge $J_n = \{1, ..., n\}$; das heißt: Jedes $k \in J_n$ ist in genau einer der Mengen B_t für passendes $t \in T_n$ enthalten.

ii) Sind d, t komplementäre Teiler von n, so ist die Abbildung $f : A_d \to B_t$, definiert durch $f(k) := t \cdot k$ eine Bijektion.

iii) Es gilt:

$$\sum_{d \in T_n} \varphi(d) = n.$$

(6 Punkte)

14i) Es sei M eine endliche Menge mit $|M| \geq 2$, und $f : M \to M$ sei eine *Involution*; das ist eine Abbildung mit $f \circ f = id_M$. Ferner bezeichne $F := \{m \in M \,|\, f(m) = m\}$ die Menge der *Fixpunkte* von f. Beweisen Sie: $|M| \equiv |F| \ mod\ 2$.
Insbesondere folgt: Ist f fixpunktfrei, so ist $|M|$ eine gerade Zahl.

ii) Beweisen Sie: Für jedes $n \in \mathbb{N}$ mit $n \geq 3$ ist $\varphi(n)$ eine gerade Zahl.

Hinweis zu ii): Konstruieren Sie – mit Begründung und für A_n (mit $t = n$) wie in Aufgabe 13) – eine fixpunktfreie Involution $f : A_n \to A_n$.

(6 Punkte)

15i) Chiffrieren Sie das Wort

BUNDESNACHRICHTENDIENST

mittels der in Beispiel 3.4 vorgestellten Stromchiffrierung.

ii) Entscheiden Sie – mit Begründung – ob die in i) erhaltene natürliche Zahl eine Primzahl ist.

(4 Punkte)

16.) Wie lautet der Klartext, der zu folgendem mittels einer Skytala-Verschlüsselung chiffrierten Geheimtext gehört – der aber zeilenweise zu lesen ist?

$$ISADTPIHEHNNCSDIROOILTAIHTAEAS$$
$$NFEZCSWESSNISFIUKTUJSESTCRCKE$$

(4 Punkte)