Diskrete Strukturen –Aufgabenblatt 14

Beachten Sie: Soweit nicht explizit angegeben, sind Ergebnisse stets zu begründen!

Hausaufgaben: Abgabe bis zum 12.02.2014 um 12:00

Lesen Sie sich bitte auf der Webpage die Bestimmungen zu den Hausaufgaben genau durch.

Bemerkung: Die auf diesem Blatt erreichten Punkte werden als **Bonuspunkte** gewertet, die noch zum „Passieren" der 2/3-Schranke benutzt werden können; die Maximalpunktzahl bestimmt sich allein aus den Blättern 1 bis (inkl.) 13.

Aufgabe 14.1

Zeigen Sie:

Ist $G = (V, E)$ ein einfacher planerer Graph mit k Zusammenhangskomponenten, dann gilt $|F| - |E| + |V| = 1 + k$.

(F sei die Menge der Flächen, in die der Graph die Ebene unterteilt; wie im Fall $k = 1$ schließt das die „umgebende" Fläche mit ein.)

Aufgabe 14.2

Zeigen Sie: Bis auf Isomorphie gibt es nur endlich viele einfache Graphen $G = (V, E)$, so dass sowohl G als auch $\overline{G} = (V, \overline{E})$ (mit $\overline{E} = \binom{V}{2} \setminus E$) planar sind.

Bemerkung: Machen Sie sich klar, dass die Abschätzung $|E| \leq 3\,|V| - 6$ für jeden einfachen planaren (nicht notwendigerweise zusammenhängenden) Graphen $G = (V, E)$ mit $|V| \geq 3$ gilt.

Aufgabe 14.3

Sei $H \subseteq F \times M$ eine stabile Hochzeit. Wir schreiben fH für den Mann, der der Frau $f \in F$ unter H zugeordnet wird; entsprechend steht Hm für die Frau, die einem Mann $m \in M$ unter H zugeordent wird.

Zeigen Sie, dass eine durch den Gale-Shapely-Algorithmus berechnete Hochzeit H folgende Eigenschaft besitzt:

Ist H' eine weitere stabile Hochzeit, so gilt für jede Frau $f \in F$, dass sie ihren Partner fH bei der Hochzeit H höchstens so sehr präferiert wie ihren Parnter $H'm$ bei der Hochzeit H'.

M.a.W.: Der Gale-Shapely-Algorithmus berechnet für alle Frauen unter allen stabilen Hochzeiten die schlechteste Hochzeit.

Bemerkung: Verwenden Sie, dass eine vom Gale-Shapely-Algorithmus berechnet Hochzeit für alle Männer die beste Hochzeit darstellt.

Aufgabe 14.4 Alle Teilaufgaben werden als eigenständige Aufgaben bewertet.

(a) Zeigen Sie, dass $\langle \mathbb{Z}_{18}^*, \cdot_{18}, 1 \rangle$ zyklisch ist. Geben Sie insbesondere alle Generatoren der Gruppe an.

(b) Bestimmen Sie alle Untergruppen von $\langle \mathbb{Z}_{18}^*, \cdot_{18}, 1 \rangle$.

Aufgabe 14.5 **Alle Teilaufgaben werden als eigenständige Aufgaben bewertet.**

(a) Zeigen Sie, das $H = \{1, 7, 9, 15\}$ eine Untergruppe von $\langle \mathbb{Z}_{16}^*, \cdot_{16}, 1 \rangle$ ist.
Bestimmen Sie inbesondere die Nebenklassen $xH = \{(xh) \mod 16 \mid h \in H\}$ von H.

(b) Bestimmen Sie alle Untergruppen von $\langle \mathbb{Z}_{16}^*, \cdot_{16}, 1 \rangle$.

(c) Geben Sie einen Isomorphismus zwischen den Gruppen $\langle \mathbb{Z}_{16}^*, \cdot_{16}, 1 \rangle$ und $\langle \mathbb{Z}_2, +_2, 0 \rangle \times \langle \mathbb{Z}_4, +_4, 0 \rangle$ an.
(Es reicht, die Abbildung anzugeben.)

Aufgabe 14.6 **Alle Teilaufgaben werden als eigenständige Aufgaben bewertet.**

Sei $N = 55$. Für jedes $e \in \mathbb{Z}$ sei $f_{N,e} \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^* \colon x \mapsto (x^e \bmod N)$.

(a) Überprüfen Sie, dass $(N, 3)$ ein zulässiger öffentlicher Schlüssel für das RSA-Problem ist.

(b) Bestimmen Sie entsprechend der VL das $d \in \mathbb{Z}$ mit $f_{N,d} = f_{N,3}^{-1}$.
Geben Sie alle Rechenschritte der verwendeten Algorithmen an.

Aufgabe 14.7

Zeigen Sie: $g \in \mathbb{Z}_n$ ist ein Generator von $\langle \mathbb{Z}_n, +_n, 0 \rangle$ genau dann, wenn $g \in \mathbb{Z}_n^*$. $(n > 1)$

Bemerkung: Beachten Sie, dass in $\langle \mathbb{Z}_n, +_n, 0 \rangle$ die von a erzeugte Untergruppe von der Gestalt $\langle a \rangle = \{(ka) \bmod n \mid k \in \mathbb{Z}\}$ ist.

Aufgabe 14.8 **Alle Teilaufgaben werden als eigenständige Aufgaben bewertet.**

Sei $\langle G, \cdot, 1 \rangle$ (kurz: G) eine zyklische Gruppe der Ordnung $N := |G|$ mit Generator g. Zeigen Sie:

(a) Jede Untergruppe von G ist zyklisch.

(b) Sei $a \in G$ mit $\mathrm{ord}(a) = n$. Dann gilt $\langle a \rangle = \langle g^{\frac{N}{n}} \rangle$.

(c) Es gibt genau $\varphi(n)$ viele Elemente der Ordnung n in G. (Verwenden Sie das Ergebnis aus HA 14.7.)

Aufgabe 14.9

Zeigen Sie: $\langle \mathbb{Z}_m, +_m, 0 \rangle \times \langle \mathbb{Z}_n, +_n, 0 \rangle$ ist genau dann zyklisch, wenn $\mathrm{ggT}(m, n) = 1$. $(m, n > 1)$

Aufgabe 14.10

Zeigen Sie: Jede Gruppe, deren Ordnung eine Primzahl ist, ist abelsch.

Aufgabe 14.11

Bestimmen Sie 25^{-1} in $\langle \mathbb{Z}_{998}^*, \cdot_{998}, 1 \rangle$ mit Hilfe des erweiterten euklidischen Algorithmus.
Geben Sie alle Zwischenergebnisse an.

Aufgabe 14.12

Sei $\langle S_5, \circ, \mathrm{id} \rangle$ die symmetrische Gruppe der Permutationen über der Menge [5].
Sei $\pi \in S_5$ die Permutation mit

$$\pi(1) = 4, \quad \pi(2) = 1, \quad \pi(3) = 5, \quad \pi(4) = 2, \quad \pi(5) = 3.$$

Bestimmen Sie π^{243}.

Tutoraufgaben: Besprechung in der Woche vom 03.02.2014

Aufgabe 14.1

Sei $\langle G, \cdot, 1\rangle$ (kurz: G) eine endliche, kommutative Gruppe der Ordnung $N := |G|$.

(a) Zeigen Sie: Für jedes $a \in G$ ist $m_a(x) := ax$ eine Permutation von G.

(b) Zeigen Sie: $\prod_{x\in G} x = \prod_{x\in G} m_a(x)$.

(c) Folgern Sie aus (b), dass $a^N = 1$ für alle $a \in G$.

(d) Für $a \in G$ sei $\langle a\rangle := \{a^{-k} \mid k \in \mathbb{Z}\}$. Zeigen Sie: $\langle\langle a\rangle, \cdot, 1\rangle$ ist eine Untergruppe von G.

(e) Zeigen Sie: $\langle a\rangle = \{a^k \mid k \in \mathbb{N}\}$ (nur positive Potenzen von a).

(f) Sei $L \in \mathbb{N}$. Zeigen Sie: Es gilt $\forall a \in G\colon a^L = 1$ genau dann, wenn $\mathrm{ord}(a) \mid L$ für alle $a \in G$ gilt.

(g) Sei λ_G das kleinste gemeinsame Vielfache aller Zahlen aus $\{\mathrm{ord}(a) \mid a \in G\}$. Zeigen Sie: $\lambda_G \mid N$.

(h) Welche der vorangegangenen Resultate gelten auch in endlichen, nicht kommutativen Gruppen?

Aufgabe 14.2

Seien $\langle G_1, \cdot_1, e_1\rangle$ und $\langle G_2, \cdot_2, e_2\rangle$ zwei Gruppen.

Wir definieren auf $G_1 \times G_2$ die Operation $\cdot$ durch

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 h_1, g_2 h_2).$$

Zeigen Sie: $\langle G_1 \times G_2, \cdot, (e_1, e_2)\rangle$ ist eine Gruppe.

Bemerkung: Diese Gruppe wird als das direkte Produkt der beiden ursprünglichen Gruppen bezeichnet und kurz als $\langle G_1, \cdot_1, e_1\rangle \times \langle G_2, \cdot_2, e_2\rangle$ geschrieben.

Aufgabe 14.3

(a) Geben Sie einen Isomorphismus zwischen den Gruppen $\langle \mathbb{Z}_8^*, \cdot_8, 1\rangle$ und $\langle \mathbb{Z}_2, +_2, 0\rangle \times \langle \mathbb{Z}_2, +_2, 0\rangle$ an.

(b) Bestimmen Sie alle Untergruppen von $\langle \mathbb{Z}_8^*, \cdot_8, 1\rangle$.

Aufgabe 14.4

(a) Geben Sie alle Generatoren von $\langle \mathbb{Z}_{11}^*, \cdot_{11}, 1\rangle$ an.

(b) Bestimmen Sie alle Untergruppen von $\langle \mathbb{Z}_{11}^*, \cdot_{11}, 1\rangle$.

Aufgabe 14.5

Sei $N = 2911$ und $f(x) := (x^{17} \bmod N)$.

Zeigen Sie, dass $f(x)$ eine Permutation auf $\mathbb{Z}_N^*$ definiert.

Wie kann man $f^{-1}(x)$ für $x \in \mathbb{Z}_N^*$ effizient berechnen?