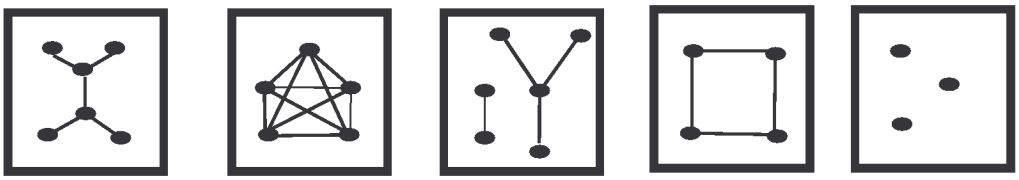
Aufgabensammlung zur Vorlesung "Diskrete Algebraische Strukturen" im Sommersemester 2010 bei Dr. M. Junker

19. 07. 2010

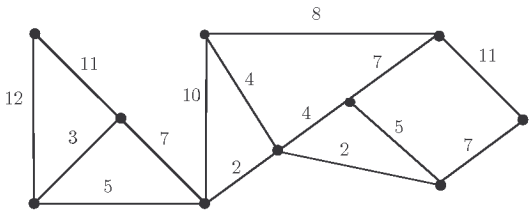
---

1. Betrachten Sie die folgenden Graphen:



   Welche von diesen Graphen sind Bäume, welche sind Wälder, welche bipartit, welche 3-färbbar, welche zusammenhängend?

2. Geben Sie einen minimal aufspannenden Baum für den folgenden Graphen an:



3. Seien $(G, \circ), (H, \circ)$ zwei Gruppen. Dann definiert man das direkte Produkt $(G \oplus H, \circ)$ mit $G \oplus H = \{(g, h) \mid g \in G, h \in H\}$, wobei für $g_1, g_2 \in G$, $h_1, h_2 \in H$ gilt: $(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ g_2, h_1 \circ h_2)$. Zeigen Sie:

   Für $m, n \in \mathbb{N}$ gilt: $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ genau dann, wenn m und n teilerfremd sind.

4. Seien $(G, \circ), (H, \circ)$ zwei Gruppen, e_H das neutrale Element von H und $\varphi : G \to H$ ein Gruppenhomomorphismus.

   Zeigen Sie: Der Kern von φ, $\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$, ist eine Untergruppe von G und das Bild von φ, $\mathrm{im}(\varphi) = \varphi(G)$, ist eine Untergruppe von H.

5. Sei $(G, \circ)$ eine Gruppe. Der Zentralisator von G ist gegeben durch $Z(G) = \{h \in G \mid h \circ g = g \circ h \quad \forall\, g \in G\}$.

   Zeigen Sie: Der Zentralisator ist eine Untergruppe von G.

6. Zeigen Sie, dass $((\mathbb{Z}/15\mathbb{Z})^*, \cdot)$ nicht zyklisch ist.

7. Berechnen Sie $\varphi(5)$, $\varphi(6)$, $\varphi(7)$, $\varphi(8)$, $\varphi(9)$, $\varphi(10)$, $\varphi(11)$ und $\varphi(12)$.

8. Seien $p \neq q$ zwei Primzahlen und φ die Eulersche φ-Funktion. Berechnen Sie $\varphi(p^2q^2)$ zum Beispiel mit Hilfe der Einschluss-Ausschluss-Formel.

9. Zeigen Sie, dass die Drehgruppe des Würfels die Symmetriegruppe S_4 ist.

   Hinweis. Symmetrien des Würfels permutieren die vier Raumdiagonalen.

10. (a) Zeigen Sie mit Hilfe des kleinen Satzes von Fermat, dass 9 keine Primzahl ist.
    (b) Berechnen Sie 1764^{2013} mod 2011.

11. Gegeben seien die Primzahlen $p = 3001$ und $q = 4001$, wobei dann $\varphi(pq) = (p-1)(q-1) = 12\,000\,000$ gilt. Dazu teilerfremd ist z.B. die 1331. Berechnen Sie 1331^{-1} in $(\mathbb{Z}/\varphi(pq)\mathbb{Z})^*$.

12. Sie haben einen Wasserhahn, zwei Krüge, die 7 bzw. 9 Liter fassen, und sollen nun einen Liter Wasser abmessen. Wie gehen Sie vor?

    Anleitung. Ihr Lösungsansatz sollte allgemein für einen Krug mit m und einen Krug mit n Litern Fassungsvermögen funktionieren, wobei $\mathrm{ggT}(m, n)$ Liter abgemessen werden sollen.

13. Die Matrizen $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ lassen sich zum Beispiel als Matrizen über $\mathbb{F}_3$ oder $\mathbb{F}_5$ auffassen. Berechnen Sie jeweils das Produkt.

14. Der (alte) ISBN-10-Code bei Büchern besteht aus neun Ziffern $a_1, \ldots, a_9$ plus eine Prüfziffer a_{10}, die gerade so gewählt ist, dass

$$\sum_{i=1}^{10} i \cdot a_i \equiv 0 \bmod 11$$

    ist. (Sollte man als Prüfziffer die 10 nehmen müssen, schreibt man ein X.) Der (neue) ISBN-13-Code besteht nun aus zwölf Ziffern $b_1, \ldots, b_{12}$ plus einer Prüfziffer b_{13}, die so gewählt ist, dass

$$\sum_{i=1}^{6} (b_{2i-1} + 3b_{2i}) + b_{13} \equiv 0 \bmod 10$$

    ist. Zeigen Sie, dass die Gleichungen nicht mehr stimmen, falls

    (a) bei beiden Codes eine der Ziffern nicht stimmt,
    (b) beim alten Code zwei verschiedene Ziffern vertauscht sind und

(c) die Prüfsumme beim neuen Code nicht immer erkennt, wenn zwei verschiedene Ziffern vertauscht sind.

15. Kodieren Sie wie in der Vorlesung beschrieben den Text „SICHER“ mit dem RSA-Verfahren, wobei $n = 2773$ und $e = 17$ gewählt wird. Ersetzen Sie dazu zunächst jeden Buchstaben gemäß A=01, B=02, ..., Z=26 durch zwei Ziffern und kodieren Sie dann je vier aufeinander folgende Ziffern mit dem RSA-Verfahren.

16. Finden Sie eine natürliche Zahl $n < 170$, so dass $n \mod 5 \equiv 3$, $n \mod 4 \equiv 2$ und $n \mod 7 \equiv 5$.

    Hinweis: Chinesischer Restsatz

Abgabe: keine Abgabe