

Aufgaben zur Klausurvorbereitung Diskrete und strukturelle Mathematik für Informatiker

*Achtung: so sieht die Klausur natürlich nicht aus!
(In der Klausur selbst wird es weniger Aufgaben geben.)*

1. Aufgabe:

- (i) Sei $G = (V, E)$ ein ebener Graph mit weniger als 30 Kanten. Beweisen sie, daß mind. ein Knoten mit Knotengrad höchstens 4 existiert.
- (ii) Geben Sie ein Gegenbeispiel mit 30 Kanten an, d.h. einen ebenen Graphen mit 12 Knoten, 30 Kanten und Knotengrad mindestens 5 an.

2. Aufgabe:

Sei $G = (V, E)$ ein ebener Graph mit mind. 4 Knoten und Knotengrad $d(v) \geq 3$ für alle Knoten $v \in V$. Zeigen Sie, daß mind. 4 Knoten mit Grad kleiner oder gleich 5 existieren.

3. Aufgabe:

Sei C ein (n, k) -Code.

- (i) Wie viele Codewörter $c \in C$ existieren?
- (ii) Wie groß ist $|B^n|$?
- (iii) Veranschaulichen Sie C auf einem n -dimensionalen Würfel, was für eine Konsequenz hat die Eigenschaft, daß der Hammingabstand mind. 3 ist?

4. Aufgabe:

Warum existiert kein zyklischer $(7,2)$ -Code?

5. Aufgabe:

Es sei G ein Baum mit $|V| = 2m$ Knoten und den Knotengraden $d(x) \leq 3$ für alle $x \in V$. Zeige Sie, daß G höchstens $m + 1$ Endknoten hat.

6. Aufgabe:

Geben Sie eine Zahl zwischen 0 und 494 an, die das System von Kongruenzen

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{9}$$

$$x \equiv 8 \pmod{11}$$

erfüllt.

7. Aufgabe:

Sei $m = 899$ und $e = 11$.

1. Beschreiben Sie, wie Sie im RSA-System eine Zahl zwischen 0 und $m - 1$ verschlüsseln und entschlüsseln. Welche Eigenschaften von m und e sind dafür wichtig? Warum?
2. Verschlüsseln Sie die Zahl 666.
3. Bestimmen Sie den geheimen Schlüssel d . (Tipp: $899 = 29 * 31$.)

8. Aufgabe:

Im Polynomring $\mathbb{Z}_2[x]$ soll der $ggT(f, g)$ bestimmt werden mit

$$f = x^4 + x^3 + x + 1 \quad g = x^5 + x^2 + x + 1$$

9. Aufgabe:

Gegeben ist der (7,4) Hamming-Code aus dem Skript. Berechnen Sie den Hamming-Abstand. Wie viele Fehler lassen sich sicher erkennen, wie viele korrigieren? Warum ist dieser Code linear?