Klausur 2000

1. Aufgabe: **2+2+2+4 Punkte**

(a) Zeichnen Sie einen Graphen mit 6 Knoten und 16 Kanten, oder beweisen Sie, dass es keinen solchen Graphen gibt. $|E| \leq \frac{1}{2}|V|(|V|-1)$ (Kanten, Knoten)
keinen Graphen

(b) Zeichnen Sie einen planaren Graphen mit 6 Knoten und 13 Kanten, oder beweisen Sie, dass es keinen solchen Graphen gibt. $|E| \leq 3|V| - 6$

(c) Zeichnen Sie einen planaren Graphen mit 6 Knoten und 12 Kanten, bei dem jeder Knoten Grad 4 hat, oder beweisen Sie, dass es keinen solchen Graphen gibt.

(d) Zeichnen Sie einen planaren Graphen mit 11 Kanten, bei dem jeder Knoten mindestens Grad 4 hat, oder beweisen Sie, dass es keinen solchen Graphen gibt.

(Zur Vermeidung von Spitzfindigkeiten:
Wie in der Vorlesung werden hier nur "einfache" Graphen betrachtet: Zwischen verschiedenen Knoten darf maximal eine Kante vorkommen, und Kanten gibt es nur zwischen verschiedenen Knoten.)

2. Aufgabe: **1+2+2+2+3 Punkte**

(a) Was ist der Sinn von Kryptographie? Nennen Sie eine entscheidende Eigenschaft, die RSA von älteren Verschlüsselungsmethoden unterscheidet, und beschreiben Sie, warum diese Eigenschaft viele heutige praktische Anwendungen erst möglich macht.

(b) Welche mathematischen Voraussetzungen sind für einen RSA-Code erforderlich? Wie nimmt man Verschlüsselung und Entschlüsselung vor, und welcher mathematische Sachverhalt führt dazu, dass die Entschlüsselung funktioniert? Fermat: $x^{\varphi(m)} \equiv 1 \mod m$
(Hinweis: Sie dürfen davon ausgehen, dass $x \neq p, q$ ist.)

(c) Welche beiden Teilschritte müsste jemand erfolgreich durchführen, um einen RSA-Code zu knacken? Welcher davon ist in der Praxis sehr schwer, und warum ist der andere relativ einfach?

(d) Gegeben seien $m = 91$ und $e = 5$. Verschlüsseln Sie $x = 15$.

(e) Knacken Sie den Code aus (d), d.h. bestimmen Sie den geheimen Schlüssel d.

p q

3. Aufgabe: **1+5+2+2 Punkte**

(a) Bestimmen Sie anhand der Primfaktorzerlegung der natürlichen Zahl 60 die Zahl ihrer Teiler.

(b) Zerlegen Sie $f(x) = x^6+1 \in \mathbb{Z}_2[x]$ in irreduzible Faktoren und bestimmen Sie damit die Zahl der Polynome $g(x) \in \mathbb{Z}_2[x]$, die Teiler von $f(x)$ sind. Welche Grade kommen bei Teilern von $f(x)$ vor?

(c) Entscheiden Sie, ob es eine Zahl $x \in [0, 39]$ gibt, die die Kongruenzen

$$x \equiv 1 \pmod 2$$

$$x \equiv 2 \pmod 4$$

$$x \equiv 3 \pmod 5$$

erfüllt. (Falls nein: Beweis; falls ja: Berechnung!)

(d) Entscheiden Sie, ob es eine Zahl $x \in [0, 29]$ gibt, die die Kongruenzen

$$x \equiv 1 \pmod 2$$

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

erfüllt. (Falls nein: Beweis; falls ja: Berechnung!)

4. Aufgabe: **1+3+3+3 Punkte**

(a) Sowohl in der Codierungstheorie als auch in der Kryptographie geht es um die Verschlüsselung von Daten. Nennen Sie zwei entscheidende Unterschiede dieser Verschlüsselungen!

(b) Geben Sie einen $(42, 41)$-Code mit Hammingabstand 2 an. Welche Rolle spielt das zusätzliche Bit? Was kann man mit solch einem Code machen? Unter welchen Bedingungen ist der Einsatz eines solchen Codes sinnvoll?

(c) Geben Sie einen $(n, 2)$-Code mit Hammingabstand 21 an. Welche Rolle spielen die zusätzlichen Bits? Was kann man mit solch einem Code machen? Unter welchen Bedingungen ist der Einsatz eines solchen Codes sinnvoll?

(d) Sie empfangen die folgende Bitfolge:
10101111111000011010101011.
Diese würde vor der Übertragung mit dem (7,4)-Hamming-Code aus der Vorlesung codiert. Stellen Sie fest, wieviele Fehler mindestens aufgetreten sind, erläutern Sie die daraus resultierende Fehlerkorrektur, und bestimmen Sie die decodierte Bitfolge.

Hinweis: Einige der Fragen aus (b) und (c) kann man auch dann beantworten, wenn man keine Code mit den geforderten Eigenschaften findet.