TECHNISCHE UNIVERSITÄT BERLIN
Fakultät II – Institut für Mathematik
Martin Skutella

Diskrete MAFI
SoSe 2002

Prüfungsklausur „Diskrete und strukturelle Mathematik für Informatiker“

Name: .....

Vorname: .....

Matr.-Nr.: .....

☐ Informatik ☐ Sonstige:.....

*Mit dem Aushang des Klausurergebnisses nur mit der Matrikelnummer am Anschlagbrett beim Raum **MA 601** bin ich einverstanden.*

Die Klausur ist mit 12 von 24 Punkten bestanden.
Alle Antworten müssen genau begründet werden. Dabei dürfen Ergebnisse aus dem Skript und von den Übungsblättern (mit genauer Quellenangabe) benutzt werden.
Alle Blätter sind mit *Namen und Matrikelnummer* zu versehen. Abzugeben sind die Lösungen in *Reinschrift* mit allen *Nebenrechnungen* auf DIN A4-Blättern, sowie diesem Blatt als Deckblatt.
Bitte jeweils ein neues Blatt für eine neue Aufgabe.
Mit *Bleistift* oder *in rot* geschriebene Klausurteile können nicht gewertet werden.
Die Bearbeitungszeit für die Klausur beträgt 100 Minuten.
Einzige erlaubte Hilfsmittel sind das Vorlesungsskript und die Übungsblätter. Nicht erlaubt sind insbesondere Taschenrechner aller Art.

Aufgabe	Punkte	von
1		5
2		4
3		5
4		5
5		5
Summe		24

Note: .....

.....
(Unterschrift des Korrektors)

Aufgabe 1: **3+2 Punkte**

a) Es sei $G = (V, E)$ ein Baum. Beweise, dass weniger als die Hälfte aller Knoten von G Grad größer oder gleich 3 haben (d. h.: $|\{v \in V \mid d(v) \geqslant 3\}| < |V|/2$).

b) Zeichne einen Baum mit 8 Knoten, von denen mindestens 3 den Grad größer oder gleich 3 haben, oder beweise, dass es keinen solchen Graphen gibt.

Aufgabe 2: **4 Punkte**

a) Berechne eine ganze Zahl $x \in [0, 41]$, die die Kongruenzen

$$x \equiv 2 \pmod 3 \qquad x \equiv 3 \pmod 6 \qquad x \equiv 4 \pmod 7$$

erfüllt oder zeige, dass es keine solche Zahl gibt.

b) Berechne eine ganze Zahl $x \in [0, 41]$, die die Kongruenzen

$$x \equiv 0 \pmod 3 \qquad x \equiv 3 \pmod 6 \qquad x \equiv 4 \pmod 7$$

erfüllt oder zeige, dass es keine solche Zahl gibt.

Hinweis: Zeige, dass aus $x \equiv 3 \pmod 6$ direkt $x \equiv 0 \pmod 3$ folgt.

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

Gegeben sei der RSA-Code mit $m = 187$ und $e = 9$.

a) Verschlüssele $x = 3$.

b) Bestimme $\varphi(m)$.

c) Verwende den euklidischen Algorithmus, um den geheimen Schlüssel d (mit $0 < d < \varphi(m)$) zu bestimmen.

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

Es sei $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$.

a) Zeige, dass $f(x)$ irreduzibel ist.

b) Bestimme das inverse Element von x^3+1 bezüglich der Multiplikation in dem Körper $\mathbb{Z}_2(f)$.

c) Bestimme $g(x) \in \mathbb{Z}_2(f)$, so dass das Produkt von $x^3 + 1$ mit $g(x)$ in $\mathbb{Z}_2(f)$ gleich $x^2 + 1$ ist.

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

Es sei der Code $C := \{b \in B^7 \mid w(b) = 3\} \subseteq B^7$ gegeben.

a) Ist C zyklisch?

b) Bestimme den Hamming-Abstand von C.

c) Gebe drei Elemente $x, y, z \in B^7 \setminus C$ an, so dass $C \cup \{x, y, z\}$ denselben Hamming-Abstand wie C hat (mit Begründung!).