UNIKASSEL
VERSITÄT

FB 17, AG Computational Mathematics
Prof. Dr. Werner M. Seiler
Dipl.-Inform. Marcus Hausdorf

Klausur zu Diskrete Strukturen II (WS 07/08)

06.03.2008

Name:	
Vorname:	
Geburtsdatum:	
Matrikelnummer:	

Bitte verwenden Sie für die Bearbeitung der Aufgaben je ein neues Blatt, auf das Sie die *Nummer der Aufgabe* und *Ihren Namen* schreiben.

Bitte geben Sie bei Rechnungen alle Zwischenschritte an.

1	2	3	4	5	Σ	Note

Aufgabe 1 $(3 + 2 + 3 = 8$ Punkte)

Gegeben sei die Menge $\mathbb{Z}_{14}^* := \{[m] \in \mathbb{Z}_{14} \mid \text{es existiert } [n] \in \mathbb{Z}_{14} \text{ mit } [m] \cdot [n] = [1]\}$ („$\cdot$“ ist die übliche Multiplikation von Restklassen).

a) Bestimmen Sie die Elemente von $\mathbb{Z}_{14}^*$ und zeigen Sie, daß $(\mathbb{Z}_{14}^*, \cdot)$ eine Gruppe ist. Stellen Sie die außerdem die zugehörige Multiplikationstafel auf.

b) Finden Sie eine Menge $U \subseteq \mathbb{Z}_{14}^*$ mit genau drei Elementen, so daß $(U, \cdot)$ eine Untergruppe von $(\mathbb{Z}_{14}^*, \cdot)$ ist.

c) $(G, *)$ sei nun eine *beliebige* Gruppe. Beweisen Sie: $(G, *)$ ist genau dann abelsch, wenn die Abbildung $f : G \to G,\ x \mapsto x * x$, ein Homomorphismus ist.

Aufgabe 2 $(4 + 3 + 5 = 12$ Punkte)

a) Es sei $p \geq 5$ eine Primzahl. Zeigen Sie: $p^2 \equiv 1 \mod 24$.

b) Bestimmen Sie alle Lösungen (in $\mathbb{Z}$) der linearen Kongruenz

$$145x \equiv 87 \mod 377.$$

c) Bestimmen Sie alle Lösungen (in $\mathbb{Z}$) des linearen Kongruenzensystems

$$\begin{aligned} x &\equiv 5 \mod 6, \\ x &\equiv 2 \mod 11, \\ x &\equiv 1 \mod 13. \end{aligned}$$

Aufgabe 3 $(3 + 4 = 7$ Punkte)

Gegeben sei der öffentliche Schlüssel $K := (k = 73, n = 187)$ für das RSA-Kryptoverfahren.

a) Verschlüsseln Sie die Nachricht $N := 25$ mit K. Benutzen Sie dabei modulares Potenzieren („Repeated Squaring“).

b) Bestimmen Sie den zu K gehörigen privaten Schlüssel l.

Aufgabe 4 $(1 + 1 + 1 + 1 + 1 = 5$ Punkte)

$G = (V, E)$ sei der Graph mit $V := \{1, 2, 3, 4, 6, 8, 12, 24\}$ und

$$E := \{\{a, b\} \mid a, b \in V,\ a \neq b,\ (a \text{ teilt } b) \ \vee \ (b \text{ teilt } a)\}\,.$$

a) Geben Sie die Kantenmenge E explizit an. Wie viele Kanten hat G?

b) Bestimmen Sie $\deg(v)$ für alle $v \in V$.

c) Ist G eulersch?

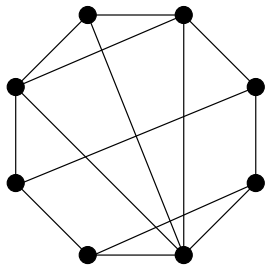
d) Ist G hamiltonsch?

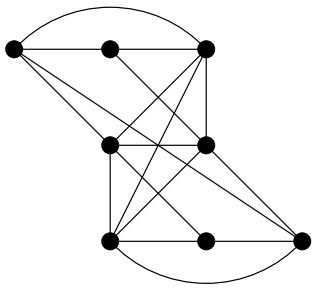
e) Ist G plättbar?

Aufgabe 5 $(4 + 4 = 8$ Punkte)

a) Gibt es Graphen $G = (V, E)$ mit der Knotenmenge $V = \{1, 2, 3, 4, 5, 6\}$ und $\deg(v) = v$ für alle $v \in V \setminus \{6\}$? Falls ja, welche Werte kommen dann für $\deg(6)$ in Frage?

b) Überprüfen Sie, ob die folgenden beiden Graphen plättbar sind:





Viel Erfolg!