G. Nebe, M. Künzer 01.09.2006

Diskrete Strukturen, SS 06

Vordiplomsklausur

Bearbeitungszeit: 120 Minuten.

Zugelassene Hilfsmittel: Ein beliebig beschriebenes Blatt DIN A4 und ein nichtprogrammierbarer Taschenrechner.

Es sind insgesamt 36 Punkte erreichbar.

Ist ein **Kasten** bei der Frage, so bitte die Antwort in den Kasten. Die für diese Antwort benötigten Rechnungen gehen diesenfalls in die Bewertung nicht ein. Eine falsche Antwort gibt 0 Punkte (aber keine negativen Punkte).

Bitte zu jeder Bearbeitung einer Frage **ohne Kasten** deutlich die Aufgabennummer angeben.

Wer mehr Papier benötigt, bitte melden.

Aufgabe 1 **(1+2+2+2 Punkte)**

(1) Auf wieviele Arten kann man 3 Kugeln aus 5 Kugeln ziehen, wenn man jeweils nicht wieder zurücklegt und nicht auf die Reihenfolge achtet? $\boxed{}$

(2) Bestimme die Anzahl der Elemente der Konjugationsklasse von $(1,2)(3,4)(5,6)$ in $\mathcal{S}_8$. $\boxed{}$

(3) Bestimme die Anzahl der surjektiven Abbildungen von $\{1,2,3,4,5\}$ nach $\{1,2,3,4\}$. $\boxed{}$

(4) Bestimme die Anzahl der normierten irreduziblen Polynome von Grad 8 in $\mathbf{F}_3[X]$. $\boxed{}$

Aufgabe 2 **(2+2+1+1 Punkte)**

Sei $G := \langle a := (1,4)(3,5)(2,6),\ b := (1,3)\rangle \leq \mathcal{S}_6$.

(1) Bestimme die Bahnenlänge $|G \cdot 2|$. $\boxed{}$

(2) Bestimme die Bahnenlänge $|\operatorname{Stab}_G(2) \cdot 1|$. $\boxed{}$

(3) Bestimme die Bahnenlänge $|\operatorname{Stab}_G(1,2) \cdot 4|$. $\boxed{}$

(4) Bestimme $|G|$. $\boxed{}$

Aufgabe 3 **(3+1 Punkte)**

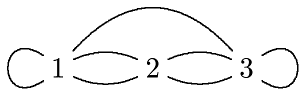
Sei $\mathbf{F}_{32} := \mathbf{F}_2[X]/(X^5 + X^2 + 1)$. Schreibe $\delta := [X]_{X^5+X^2+1}$.

(1) Berechne $(\delta^2 + 1)^{-1}$ als Linearkombination der Standardbasis $(\delta^0, \delta^1, \delta^2, \delta^3, \delta^4)$ von $\mathbf{F}_{32}$ über $\mathbf{F}_2$. $\boxed{}$ (Hinweis: Euklid.)

(2) Entscheide, ob $\delta^2 + 1$ ein Erzeuger von $\mathbf{F}_{32}^*$ ist. Begründe!

Aufgabe 4 **(2 Punkte)**

Betrachte folgenden Graphen.



Bestimme die Anzahl seiner Kantenzüge von Länge 2. $\boxed{}$

Aufgabe 5 **(2+1+1 Punkte)**

Wir wollen das RSA-Verfahren anwenden und verwenden dabei die Standardbezeichnungen.
Seien $p = 7$, $q = 11$ und $v = 7$. (Hinweis: Taschenrechner.)

(1) Bestimme e. $\boxed{}$

(2) Verschlüssele die Ziffer 5. $\boxed{}$

(3) Entschlüssele die Ziffer 2. $\boxed{}$

Aufgabe 6 **(2+2 Punkte)**

Sei C der lineare Code über $\mathbf{F}_4$ mit der Erzeugermatrix $\begin{pmatrix} 1 & 1 & \omega & \omega^2 \\ \omega^2 & 0 & 1 & 1 \end{pmatrix}$.

(1) Bestimme eine Prüfmatrix für C.

(2) Bestimme den Minimalabstand von C.

Aufgabe 7 **(2+1+2+1 Punkte)**

Sei $f(X) = X^3 + X^2 + 1 \in \mathbf{F}_2[X]$. Es ist $g(X) := (X^7 - 1)/f(X) = X^4 + X^3 + X^2 + 1$. Sei C der zyklische Code der Länge 7 mit Erzeugerpolynom $f(X)$.

(1) Bestimme alle Nullstellen von $f(X)$ in $\mathbf{F}_8$. $\boxed{}$

(2) Bestimme den designierten Minimalabstand von C.

(3) Bestimme den Minimalabstand $d(C)$ und vergleiche mit dem designierten Minimalabstand von C.

(4) Vergleiche die Dimension von C mit der Hammingschranke im vorliegenden Fall, d.h. für Länge und Minimalabstand wie C.

Aufgabe 8 **(3 Punkte)**

Zeige oder widerlege folgende Aussage.

Sei G eine endliche Gruppe. Seien U und V Untergruppen in G. Sei $|U|$ teilerfremd zu $|V|$, d.h. sei $\mathrm{ggT}(|U|, |V|) = 1$. Es ist $U \cap V = \{1\}$.