

Tenta B i 5B1204 DISKRET MATEMATIK för D och 5B1203 DISKRET MATEMATIK för F3 och F1spec den 21 maj 2007, klockan 08.00-13.00.

Hjälpmedel: Inga hjälpmedel tillåtna.

Gränser: Man får en trea för minst 10 poäng, en fyra för minst 14 poäng och en femma för minst 18 poäng.
OBS: Godkänt, dvs minst 4 poäng, på lappskrivningen ger 2 bonuspoäng.

Motivera dina lösningar!!!

1. (3p) Formulera och bevisa Faktorsatsen för polynomringen över en ändlig kropp.
2. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 33$ och $e = 7$. Dekryptera meddelandet 5.
3. (3p) Gruppen $(Z_{19} \setminus \{0\}, \cdot)$ är cyklisk. Bestäm ett element α som genererar denna grupp.
4. (3p) Undersök om polynomet $x^3 + x + 1$ är irreducibelt i polynomringen $Z_7[x]$.
5. (3p) Kroppen F med 25 element består av polynom av grad högst 1, med koefficienter i Z_5 , och man räknar i F som om $x^2 + 2 = 0$. Dvs

$$F = \{ax + b \mid a, b \in Z_5\} \quad \text{och} \quad x^2 = 3.$$

Bestäm ett element z i denna kropp sådant att $(2x + 1)z = x$.

6. (3p) Visa att nedanstående, ej färdigt ifyllda tabell, aldrig kan kompletteras till en grupptabell:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	e			
b					
c					
d					

7. (3p) Tyvärr råkade någon välja en oäkta kontrollmatris (paritycheck-matrix) för att skapa en 1-felsrättande kod, enligt nedan:

$$C = \{\bar{c} = (c_1, c_2, \dots, c_7) \mid H\bar{c}^T = (0 \ 0 \ 0)^T\} \quad \text{där} \quad H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Det är för sent att ändra så vissa ord i koden går inte att använda. Man måste därför utesluta ord ur C och skapa en ny 1-felsrättande kod C' , dvs

$$C' \subseteq C, \quad \text{och} \quad C' \quad \text{är 1-felsrättande.}$$

Hur många ord kan C' ha maximalt, givet kontrollmatrisen H ovan. (Denna kontrollmatris skall vid felrättning användas på sedvanligt sätt.)

8. (3p) Låt H och K vara två delgrupper till en grupp G . Räcker nedanstående information för att bestämma antalet element i $H \cap K$.
 - 1) Gruppen G är cyklisk.
 - 2) Antalet element i H är n .
 - 3) Antalet element i K är m .