

Inga hjälpmedel tillåtna. Motivering krävs i varje uppgift. Minst 15 poäng krävs för godkänt. Bonuspoäng från terminens kontrollskrivningar kan användas för att tillgodoräkna deluppgifter från Uppgift 1 enligt följande. Du får själv välja vilka deluppgifter du vill tillgodoräkna: ange i förekommande fall dessa.

24-30 p 3 deluppgifter
16-23 p 2 deluppgifter
8-15 p 1 deluppgift

- (a) Hur många inverterbara element finns det i ringen $\mathbb{Z}_{64}$? (1p)
(b) Ange två grupper av ordning 4 som inte är isomorfa som grupper. (1p)
(c) Finns det en graf som har fyra hörn, sex kanter och kromatiskt tal lika med 3? (1p)
- (a) Ge definitionen av tecknet för en permutation. Ge definitionen av den alternerande gruppen av ordning n . (2p).
(b) Skriv permutationerna $\alpha, \beta \in S_8$ som ges av

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 7 & 8 & 6 & 5 \end{pmatrix}$$

- på cykelform. (2p)
- (c) Beräkna tecknet för α och β . Tillhör α och β den alternerande gruppen A_8 ? (2p)
- (a) Låt p vara ett primtal. Visa att villkoret $f(0) - g(0) = 0$ definierar en ekvivalensrelation på polynomringen $\mathbb{Z}_p[x]$. (2p)
(b) Hur många ekvivalensklasser finns det? (1p)
(c) Visa att mängden av ekvivalensklasser kan ges strukturen av en kropp. (2p)
 - (a) Bestäm antalet polynom i $\mathbb{Z}_5[x]$ av grad 4 som uppfyller villkoren $f(2) \neq 0$ och $f(3) \neq 0$. (3p)
(b) För vilka $a \in \mathbb{Z}_5$ är polynomet $x^3 + 2x + a$ irreducibelt i $\mathbb{Z}_5[x]$? (3p)
 - (a) Betrakta gruppen D_4 som ges av symmetrier på en kvadrat med gruppoperationen sammansättning. Beskriv samtliga gruppelment och bestäm gruppens ordning. (2p).
(b) Är D_4 en abelsk grupp? (1p)
(c) Innehåller D_4 någon delgrupp av ordning 2? Innehåller D_4 någon delgrupp av ordning 4? (2p)
 - (a) Vad menas med en checkmatris hörande till en linjär kod C i $(\mathbb{Z}_2)^5$? (1p)
(b) Hur definieras minimiavståndet för en linjär kod C ? Finns det en linjär kod i $(\mathbb{Z}_2)^5$ som har minimiavstånd 5? (2p)
(c) Utgör
$$C = \{(00000), (10101), (11010), (11110), (11111)\} \subset (\mathbb{Z}_2)^5$$
en linjär kod? (2p)