

Inga hjälpmedel tillåtna. Motivering krävs i varje uppgift. Minst 15 poäng krävs för godkänt. Bonuspoäng från 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

1. (a) Hur många inverterbara element finns det i ringen $\mathbb{Z}_{28}$? (1p)
(b) Låt M vara mängden av 2×2 -matriser med reella element och determinant lika med 0. Utrusta M med sedvanlig matrismultiplikation. Definierar detta en grupp? (1p)
(c) Finns det en graf som har fem hörn, fem kanter och kromatiskt tal lika med 3? (1p)

Lösningsförslag: (a) Antalet inverterbara element i $\mathbb{Z}_n$ ges av Eulers ϕ -funktion. Vi påminner oss att $\phi(mn) = \phi(m)\phi(n)$ för m, n relativt prima. Detta ger

$$\varphi(28) = \varphi(2^2 \cdot 7) = \phi(4)\phi(7) = 2 \cdot 6 = 12.$$

(b) Om M vore en grupp med matrismultiplikation skulle det finnas ett entydigt identitetselement.

Vi noterar dock att exempelvis matrisen $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ har egenskapen att $AB = A$ samt $BA = A$ medför att B har ettor på diagonalen, samt en nolla i nedre vänster hörn. Men då gäller det $B \neq 0$ vilket betyder att $B \notin M$. Således är M ej en grupp.

(c) Det existerar sådana grafer. Tag en triangel, välj ett av dess hörn och förbind två hñn med detta. Då fås en graf med fem hörn och fem kanter samt med kromatiskt tal lika med 3 eftersom en triangel kräver tre färger vid färgläggning.

2. (a) Visa att relationen $x^3 \equiv y^3 \pmod{12}$ definierar en ekvivalensrelation på $\mathbb{Z}$. (3p)
(b) Hur många ekvivalensklasser finns det? Ange en representant för varje ekvivalensklass. (2p)

Lösningsförslag:

(a) Vi verifierar villkoren på en ekvivalensrelation en efter en. Till exempel ger definitionen av relationen ovan genast att $x \sim x$ eftersom $x^3 = x^3$, och om $x \sim y$ så gäller även $y \sim x$ på grund av de grundläggande egenskaperna hos modulär aritmetik.

(b) Vi beräknar x^3 modulo 12 för samtliga $x \in \{0, 1, \dots, 11\}$. Detta ger

x	x^3
0	0
1	1
2	8
3	3
4	4
5	5
6	0
7	7
8	8
9	9
10	4
11	11

Vi har alltså representanter 0, 1, 2, 3, 4, 5, 7, 9, 11 för de nio ekvivalensklasserna.

3. (a) Ge definitionerna av (i) cykeltypen samt (ii) tecknet för en permutation. (2p). (b) Skriv permutationerna $\alpha, \beta \in S_8$ som ges av

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

på cykelform. (2p)

(c) Ange typen för α samt för $\alpha\beta$. Ange tecknet för β . (2p)

Lösningsförslag:

(a) Se kursboken för definitionerna av cykeltyp och tecken.

(b) Vi ser att under α har vi $1 \rightarrow 3 \rightarrow 1$ så att α innehåller transpositionen (13). Permutationen α fixerar vidare 2. Vi har vidare $4 \rightarrow 8 \rightarrow 5 \rightarrow 7 \rightarrow 4$ vilket ger oss cykeln (4857). Slutligen fixeras 6. Tillsammans ger detta oss

$$\alpha = (13)(4857).$$

På liknande sätt erhåller vi att

$$\beta = (12)(57)(68).$$

(c) Vi ser från (b) att α har cykeltyp $[1^2 2^1 4^1]$. Vi har vidare $\alpha\beta = (123)(5486)$ vilket ger cykeltypen $[1^1 3^1 4^1]$. Slutligen ser vi att β kan skrivas som en produkt av tre transpositioner, vilket ger $\text{sgn}(\beta) = -1$.

4. (a) Bestäm antalet polynom i $\mathbb{Z}_5[x]$ av grad 4 som uppfyller villkoren $f(0) = 0$ och $f(3) \neq 0$. (3p)
 (b) Är polynomet $x^4 + 1$ irreducibelt i $\mathbb{Z}_5[x]$? (3p)

Lösningsförslag:

(a) Vi observerar att villkoret om grad 4 gör att $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ måste ha $a_4 \in \{1, 2, 3, 4\}$. Vidare medför $f(0) = 0$ att $a_0 = 0$. Det finns alltså totalt $4 \cdot 5 \cdot 5 \cdot 5 \cdot 1 = 500$ polynom av grad 4 som har $f(0) = 0$.

Att $f(3) = 0$ är enligt faktorsatsen ekvivalent med att $f(x) = (x - 3)g(x)$ där g har grad 3 och konstantterm 0. Det finns enligt samma resonemang som ovan $4 \cdot 5 \cdot 5 \cdot 1 = 100$ sådana polynom.

Alltså finns det $500 - 100 = 400$ polynom i $\mathbb{Z}_5[x]$ som har grad 4 och uppfyller $f(0) = 0$ och $f(3) \neq 0$.

(b) Sätt $p(x) = x^4 + 1$. Vi har $p(0) = 1$, $p(1) = 2$, $p(2) = 2$ samt $p(3) = 2$ i $\mathbb{Z}_5$. Enligt en känd sats från kursen saknar p därmed linjära faktorer. Detta ger vid handen att p antingen är irreducibelt eller kan skrivas som en produkt av två andragradspolynom. I $\mathbb{Z}_5[x]$ har vi $x^4 + 1 = x^4 - 4$ och det senare polynomet kan skrivas $(x^2 + 2)(x^2 - 2)$ vilket i sin tur är lika med $(x^2 + 2)(x^2 + 3)$ i $\mathbb{Z}_5[x]$. Alltså gäller

$$x^4 + 1 = (x^2 + 2)(x^2 + 3)$$

i $\mathbb{Z}_5[x]$.

5. (a) Betrakta gruppen D_3 som ges av symmetrier på en liksidig triangel med gruppoperationen sammansättning. Beskriv samtliga grupp-element och bestäm gruppens ordning. (2p).

(b) Är D_3 en abelsk grupp? (1p)

(b) Vilka ordningar är möjliga för en delgrupp till D_3 ? Visa att det för var och en av dessa möjligheter faktiskt finns en delgrupp med denna ordning. (2p)

Lösningsförslag:

(a) Symmetrierna till en liksidig triangel ges av rotationer och speglingar, närmare bestämt rotation med 120, 240 och 360 grader och spegling i tre linjer som går genom ett hörn i triangeln och mittpunkten på den motstående sidan.

Om r betecknar en rotation med 120 grader har vi $r^3 = \text{id}$. Låt s beteckna spegling genom en av linjerna. Vi inser att de två återstående speglingarna nu kan skrivas som sammansättningar av r och s , närmare bestämt ger $\{\text{id}, r, r^2, s, sr, sr^2\}$ en lista över samtliga grupp-element.

Gruppens ordning är 6.

(b) Lagranges sats ger genast att de möjliga ordningarna för en delgrupp till D_3 är 1, 2, 3 och 6. Den triviala delgruppen har ordning 1 och D_3 har ordning 6. Delgruppen som ges av rotationer har ordning 3 enligt ovan. Eftersom en spegling är sin egna invers ger oss $\{\text{id}, s\}$ ett exempel av en delgrupp av ordning 2.

6. (a) Vad menas med en checkmatris hörande till en linjär kod i $(\mathbb{Z}_2)^5$? (1p)

(b) Utgör

$$C = \{(00000), (00101), (11010), (11111)\} \subset (\mathbb{Z}_2)^5$$

en linjär kod? Ange i sådana fall motsvarande checkmatris. (3p)

(c) Beräkna minimiavståndet för C . Kommer C att kunna rätta 1 felaktig bit? (1p)

Lösningsförslag:

(a) Se kursboken för en definition av linjär kod.

(b) Mängden C utgör en delgrupp till $(\mathbb{Z}_2)^5$ och är därmed en linjär kod. Vi observerar att kodorden i C uppfyller $x_1 = x_2 = x_4$ och $x_3 = x_5$. En checkmatris ges till exempel av

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

(c) Vi har $\delta(00000, 00101) = \delta(11010, 11111) = 2$. Koden kan ej rätta en felaktig bit eftersom till exempel $\delta(11110, 11111) = 1$ och $\delta(11110, 11010) = 1$ vilket betyder att 11110 har två närmaste grannar.