

Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3 m.fl.

16 mars 2016

Tryckfel kan förekomma.

- 1a) (1p) $(G, \circ)$ är en grupp omm 1. $(x \circ y) \circ z = x \circ (y \circ z)$ för alla $x, y, z \in G$ (associativitet),
 2. Det finns $e \in G$ sådant att $e \circ x = x \circ e = x$ för alla $x \in G$ (identitetsselement) och
 3. För varje $x \in G$ finns $x^{-1} \in G$ med $x \circ x^{-1} = x^{-1} \circ x = e$ (inverselement).
 (Villkoret om slutenhet behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)
 b) (1p) Om H är en delgrupp till den ändliga gruppen G , är $|H|$ en delare till $|G|$.
 c) (1p) En grupp G är cyklisk omm det finns ett $x \in G$ sådant att för varje $g \in G$ finns (minst) ett $n \in \mathbb{Z}$ med $g = x^n$ (om $n < 0$ är $x^n = (x^{-1})^{-n}$).

- 2a) (1p) Stabilisatorn för $x \in X$ är $G_x = \{g \in G \mid gx = x\}$ (då gx är resultatet av g 's verkan på x).
 b) (1p) Om $x \in X$ har banan Gx och stabilisatorn G_x gäller $|G| = |Gx| \cdot |G_x|$.
 c) (1p) Jadå. $(\mathbb{Z}_m, +, \cdot)$ är en ring för varje $m \in \mathbb{Z}_+$.

- 3a) (1p) Om $(F, +, \cdot)$ är en ändlig kropp är $(F \setminus \{0\}, \cdot)$ en cyklisk grupp.
 b) (1p) Karakteristiken för $(F, +, \cdot)$ är ordningen för den additiva delgruppen $\langle 1 \rangle$ som genereras av 1 (om, i oändlig F , $|\langle 1 \rangle| = \infty$, sägs karakteristiken vara 0).
 c) (1p) Faktorsatsen: Om $f(x) \in F[x]$ är $x - \alpha$ en delare till $f(x)$ omm $f(\alpha) = 0$ i F .

- 4a) (1p) En binär kod med minimala avståndet δ rättar upp till $\lfloor \frac{\delta-1}{2} \rfloor$ fel (heltalsdelen av $\frac{\delta-1}{2}$).
 b) (1p) I ett RSA-system med offentliga parametrar (n, e) är $E(x) = x^e$ i $\mathbb{Z}_n$.
 c) (1p) Fermattestet med bas b ($b \in \mathbb{Z}_+$, $b < N$) för att avgöra om $N \in \mathbb{Z}_+$ är ett primtal: Är $b^{N-1} \equiv 1 \pmod{N}$? Om svaret är "nej" är N inte ett primtal.

- 5) (3p) Vi söker alla möjliga värden bland 1, 2, ..., 10 för $|G|$, då gruppen G har ett $g \in G$ med $g \neq 1$ och $g^{12} = 1$ (G 's identitetsselement).

Lösning:

$g^{12} = 1$, så $o(g) = 2, 3, 4, 6$ eller 12 (ty $o(g) \mid 12$ och $g \neq 1$). Eftersom $o(g) \mid |G|$ är $|G| = 1, 5, 7$ omöjliga. Övriga värden är möjliga, vilket t.ex. ses genom att ta G cyklisk.

Svar: Värdena 1, 5, 7 är omöjliga, 2, 3, 4, 6, 8, 9, 10 är möjliga.

- 6) $G = U_{20}$, gruppen av inverterbara element i ringen $(\mathbb{Z}_{20}, +, \cdot)$. Vi (a, 2p) söker alla banor då G verkar på $X = \mathbb{Z}_{20}$ med multiplikation och (b, 1p) ska verifiera vår formel för antalet banor i detta fall.

Lösning:

- a. $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$, vilken också är en bana, $G = G1 = G3 = \dots = G19$ (för $a, b \in G$ fås $ba^{-1} \in G$ och $(ba^{-1})a = b$). Vidare fås banorna:

$G0 = \{0\}$, $G2 = \{2, 6, 14, 18\}$, $G4 = \{4, 8, 12, 16\}$, $G5 = \{5, 15\}$, $G10 = \{10\}$.

- b. För $g \in G$, $x \in \mathbb{Z}_{20}$ fås $gx = x$ omm $(g-1)x = 0$ (i $\mathbb{Z}_{20}$). $|F(g)|$ är antalet x som uppfyller detta. Man finner
- | | | | | | | | | |
|----------|----|---|---|---|----|----|----|----|
| g | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 |
| $ F(g) $ | 20 | 2 | 2 | 4 | 10 | 4 | 4 | 2 |

av $\frac{m}{\text{sgd}(g-1, m)}$ i $\mathbb{Z}_m$, här $m = 20$) och Burnsides lemma ger antalet banor som

$$\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{8} (20 + 2 + 2 + 4 + 10 + 4 + 4 + 2) = \frac{48}{8} = 6, \text{ vilket stämmer!}$$

Svar a: Banorna är $\{0\}$, G , $\{2, 6, 14, 18\}$, $\{4, 8, 12, 16\}$, $\{5, 15\}$, $\{10\}$, b: Se ovan.

7) (3p) Vi söker alla moniska irreducibla polynom i $\mathbb{Z}_3[x]$ som delar både $f(x) = x^5 + x^3 + x^2 + x + 2$ och $g(x) = x^6 + x^5 + x^3 + 1$.

Lösning:

Gemensamma faktorer är precis faktorer i den största gemensamma delaren till $f(x)$ och $g(x)$.

Vi använder Euklides algoritm:

Polynomdivision ger $g(x) = (x+1)f(x) + 2h(x)$, där $h(x) = x^4 + x^3 + 2x^2 + 1$.

P.s.s. $f(x) = (x+2)h(x) + 0$, så $\text{sgd}(f(x), g(x)) = h(x)$ och vi ska finna $h(x)$:s moniska irreducibla faktorer.

Vi söker först linjära faktorer. Enligt faktorsatsen motsvarar de precis nollställena till $h(x)$.

Man finner $h(0) = 1$, $h(1) = 2$, men $h(2) = 0$, så $x - 2 = x + 1$ är en faktor i $h(x)$

Division ger $h(x) = (x+1)k(x)$, där $k(x) = x^3 + 2x + 1$ (båda faktorerna moniska).

$x + 1$ är irreducibelt, men vi försöker faktorisera $k(x)$. $k(0) = k(1) = k(2) = 1 \neq 0$, så $k(x)$ är irreducibelt (deg $k(x) = 3$, så varje icke-trivial faktorisering måste ha en förstgradsfaktor).

Svar: De sökta faktorerna är $x + 1$ och $x^3 + 2x + 1$.

8) (3p) Vi vet att $1234^{503} \equiv_{6767} 4083$ och söker ett $k \in \mathbb{Z}_+$ med $4083^k \equiv_{6767} 1234$.

Lösning:

Vi känner igen ett RSA-system med $n = 6767$ och $e = 503$ och söker d , här kallat k .

$6767 = 67 \cdot 101$, båda primtal, så $m = 66 \cdot 100 = 6600$ och d fungerar om $e \cdot d \equiv_{6600} 1$.

Euklides algoritm: $6600 = 503 \cdot 13 + 61$ så $1 = 61 - 4(503 - 8 \cdot 61) =$
 $503 = 61 \cdot 8 + 15$ $= -4 \cdot 503 + 33(6600 - 13 \cdot 503) =$
 $61 = 15 \cdot 4 + 1$ $= 33 \cdot 6600 - 433 \cdot 503 =$
 $= (33 - 503) \cdot 6600 + (6600 - 433) \cdot 503 =$
 $= -470 \cdot 6600 + 6167 \cdot 503$

Så vi kan ta $d = 6167 (= k)$.

Svar: Ett sådant k är 6167.

(Ett annat är 2867 (det räcker att $e \cdot d \equiv_{\text{mgm}(66,100)} 1$).)

9) (4p) $SL(2, \mathbb{Z}_2)$ är mängden av 2×2 -matriser med element i $\mathbb{Z}_2$ och determinant 1.

Vi ska visa att $SL(2, \mathbb{Z}_2)$ är en grupp och bestämma ordningarna för dess element.

Lösning:

Eftersom $\det(AB) = \det(A) \cdot \det(B)$ är $SL(2, \mathbb{Z}_2)$ sluten under multiplikation.

Matrismultiplikation är associativ, enhetsmatrisen $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ är identitets-element,

$\det(A) \neq 0 \Rightarrow A^{-1}$ existerar (och är A :s invers), så **$SL(2, \mathbb{Z}_2)$ är en grupp.** (Isomorf med S_3 .)

Matrismultiplikation ger ordningarna ($o(A) = \text{minsta } n \in \mathbb{Z}_+ \text{ med } A^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$). De blir:

Svar:	element	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
	ordning	1	2	2	3	3	2

10) Vi skall visa att om p är ett primtal är (a, 2p) $x^{p-1} - 1 = (x-1)(x-2) \dots (x-(p-1))$ i $\mathbb{Z}_p[x]$ och (b, 2p) $(p-1)! \equiv_p -1$.

Lösning:

Enligt Fermats lilla sats är varje $a \neq 0$ i $\mathbb{Z}_p$ ett nollställe till polynomet, så enligt faktorsatsen är $x^{p-1} - 1$ delbart med dessa $x - a$ i $\mathbb{Z}_p[x]$.

De irreducibla (grad 1, ju) polynomen $x - 1, x - 2, \dots, x - (p-1)$ är olika och delar alla det givna polynomet. Således gäller att $x^{p-1} - 1 = (x-1)(x-2) \dots (x-(p-1)) \cdot g(x)$ för något polynom $g(x)$. Men graden för båda leden är lika, så $g(x)$ är en konstant och genom att jämföra höstgradstema ser man att $g(x) = 1$. **a-saken är klar.**

Genom att sätta in $x = p$ i resultatet nyss fås $p^{p-1} - 1 = 0 - 1 = (p-1)(p-2) \dots (p-(p-1)) = (-1)^{p-1} 1 \cdot 2 \cdot \dots \cdot (p-1)$ i $\mathbb{Z}_p$, dvs $(p-1)! \equiv -1 \pmod{p}$. (Om p är udda är $(-1)^{p-1} = 1$, liksom då $p = 2$, då $-1 = 1$) **b-saken är också klar.**

11) (4p) $\mathcal{S}_G$ är gruppen av permutationer av G , själv en grupp.
Vi söker en isomorfi mellan G och en delgrupp till $\mathcal{S}_G$.

Lösning:

Detta är ett klassiskt resultat som kallas Cayleys sats. Det innebär tydligen att varje grupp av ordning n är isomorf med en delgrupp till S_n .

Den sökta isomorfin ges av $\pi : G \rightarrow \pi(G)$, $\pi : g \mapsto \pi_g$, där $\pi_g(h) = gh$ och $\pi(G)$ är bilden av G under π 's verkan, $\{\pi_g \mid g \in G\} \subseteq \mathcal{S}_G$.

Vi ska visa att π är bijektiv (dvs injektiv och surjektiv) och bevarar struktur (dvs att $\pi_{gh} = \pi_g \pi_h$ för alla $g, h \in G$).

$\pi_g = \pi_h \Rightarrow \pi_g(1) = \pi_h(1) \Rightarrow g1 = h1$, för alla $g, h \in G$. Det visar att π är injektiv.

π är (förstås) surjektiv (enligt definitionen av $\pi(G)$).

För godtyckliga $g, h, k \in G$ gäller $\pi_g(\pi_h(k)) = \pi_g(hk) = g(hk) = (gh)k = \pi_{gh}(k)$, så $\pi_g \pi_h = \pi_{gh}$ och π bevarar struktur. Detta visar också att $\pi(G)$ är en delgrupp till $\mathcal{S}_G$.

Svar: En sådan isomorfi ges av $\pi : G \rightarrow \pi(G)$, $\pi : g \mapsto \pi_g$,
där $\pi_g(h) = gh$ och $\pi(G) = \{\pi_g \mid g \in G\} \subseteq \mathcal{S}_G$.

12) (5p) Vi söker $g(x) \in \mathbb{Z}_5[x]$ sådant att $F = \{b_1\alpha + b_0 \mid b_0, b_1 \in \mathbb{Z}_5\}$ med $g(\alpha) = 0$ blir en kropp och $f(x) = x^4 + 2x^3 + x + 2 \in \mathbb{Z}_5[x]$ faktoriseras i förstagsgradsfaktorer i $F[x]$. Vi söker också en sådan faktorisering.

Lösning:

Vi faktorerar först $f(x)$ i $\mathbb{Z}_5[x]$. $f(x)$ har nollställena 3 och 4, så faktorerna $x+2$ och $x+1$. Polynomdivision ger $f(x) = (x+1)(x+2)(x^2+4x+1)$.

Den sista faktorn saknar nollställena i $\mathbb{Z}_5$ och är därför irreducibel (ty av grad ≤ 3). För att kunna faktorisera den i F väljer vi $g(x) = x^2 + 4x + 1$, så $\alpha^2 + 4\alpha + 1 = 0$, dvs $\alpha^2 = -4\alpha - 1 = \alpha + 4$. Från den allmänna teorin följer att F enligt lydelsen är en kropp och polynomdivision med $x - \alpha = x + 4\alpha$ i $F[x]$ ger att $g(x) = (x + 4\alpha)(x + \alpha + 4)$.

Svar: $g(x) = x^2 + 4x + 1$ ger $f(x) = (x+1)(x+2)(x+4\alpha)(x+\alpha+4)$.

13) Vi söker (a, 1p) ordningen $|G|$ för hela symmetrigruppen för en kub, (b, 1p) antalet udda permutationer i S_8 som ges av G 's verkan på kubens hörn och (c, 3p) antalet kirala (dvs väsentligt olika sina spegelbilder) färgningar med högst k färger av kanterna i en tetraeder.

Lösning:

a. Om x är ett av kubens hörn består dess bana av alla hörnen, så $|Gx| = 8$. Stabilisatorn ges av alla permutationer av x 's tre grannhörn (som motsvarar tre rotationer (däribland id) och tre speglingar i plan genom x och en av dess kanter), så $|G_x| = |S_3| = 6$. Det ger att $|G| = |Gx| \cdot |G_x| = 48$.

b. G innehåller 24 rotationer. Deras cykelstrukturer som element i S_8 är $[1^8]$ (id), $[1^2 3^2]$ (axel genom hörn), $[4^2]$, $[2^4]$ (axel genom sidors mittpunkter, $\frac{\pi}{2}$ resp. π), $[2^4]$ (axel genom kanters mittpunkter), alla med ett jämnt antal cykler av jämn längd, så de är alla jämna permutationer. Spegling i ett plan parallellt med två sidor ger cykelstruktur $[2^4]$, så en jämn permutation. Denna spegling går genom rotationerna ger alla icke-rotationer (olika och precis 24 stycken i G), så alla permutationerna i S_8 är produkter av jämna, så inga udda.

c. Kalla tetraederns rotationssymmetrigrupp G_r och dess hela symmetrigrupp G_h . Kirala färgningar är då precis de vilkas banor under G_h är unionen av två banor under G_r . Antalet kirala färgningar är alltså 2·(skillnaden i antalen banor för G_r och G_h).

Vi använder Burnsides lemma (Thm 21.4 i Biggs) och behöver $|F(g)|$ för alla $g \in G_r, G_h$.

$|G_r| = 12$ (för ett hörn x är $|G_{r,x}| = 4$ ($G_{r,x} = \{\text{hörn}\}$) och $|(G_r)_x| = 3$ ($(G_r)_x$ rotationer, axel genom x)).

typ g	antal	typ för kanternas permutation	$ F(g) = k^{\text{antalet cykler}}$
id	1	$[1^6]$	k^6
axel kant-kant	3	$[1^2 2^2]$	k^4
axel hörn-sida	8	$[3^2]$	k^2

För G_h tillkommer lika många icke-rotationer (som i b.). $|G_h| = 24$, svarande mot alla permutationer av de fyra hörnen. Vi finner för de "nya" elementen (de i $G_h \setminus G_r$):

typ för hörnens permutation	antal	typ för kanternas permutation	$ F(g) = k^{\text{antalet cykler}}$
$[1^2 2]$	6	$1^2 2^2$	k^4
$[4]$	6	$[24]$	k^2

Burnside ger antalet banor för G_r : $\frac{1}{12}(k^6 + 3k^4 + 8k^2)$ och

antalet banor för G_h : $\frac{1}{24}(k^6 + 3k^4 + 8k^2 + 6k^4 + 6k^2) = \frac{1}{24}(k^6 + 9k^4 + 14k^2)$.

Enligt ovan blir antalet kirala färgningar: $2 \cdot (\frac{1}{12}(k^6 + 3k^4 + 8k^2) - \frac{1}{24}(k^6 + 9k^4 + 14k^2)) = 2 \cdot \frac{1}{24}(k^6 - 3k^4 + 2k^2) = \frac{1}{12}k^2(k^2 - 1)(k^2 - 2)$.

Svar a: $|G| = 48$, **b:** inga av permutationerna är udda,

c: antalet kirala färgningar är $\frac{1}{12}k^2(k^2 - 1)(k^2 - 2)$ st.