

**Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3 m.fl.
9 april 2015**

- 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 $x \in G$ (identitets-element) 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) $g^s = 1$ omm $m \mid s$, där $m = o(g)$, g :s ordning.
c) (1p) Centrum för gruppen G är $Z(G) = \{z \in G \mid zg = gz \text{ för alla } g \in G\}$.

- 2a)** (1p) Stabilisatorn för $x \in X$ är $G_x = \{g \in G \mid gx = x\}$ (gx är resultatet av g :s verkan på x).
b) (1p) Antalet banor är $\frac{1}{|G|} \sum_{g \in G} |F(g)|$, där $F(g) = \{x \in X \mid gx = x\} (= X_g)$.
c) (1p) Operationen $\cdot$ skall vara kommutativ och alla $x \in R$ utom 0 skall ha en invers $x^{-1} \in R$ (dvs $x \cdot x^{-1} = 1$). R skall förstås ha en etta.

- 3a)** (1p) Ändliga kroppar finns av ordning p^n , primtal och $n \in \mathbb{Z}_+$ och inga andra, så bland de föreslagna för 11, 13, 16, 17, 19, 23, 25, 27, 29.
b) (1p) Om $(F, +, \cdot)$ är en ändlig kropp är $(F \setminus \{0\}, \cdot)$ en cyklisk grupp.
c) (1p) Möjliga värden för karakteristiken är alla primtal och 0.

- 4a)** (1p) Kodet $\mathcal{C}$ rättar e fel omm minimiavståndet $\delta \geq 2e + 1$.
b) (1p) $x \in \mathbb{Z}_n$ krypteras som $E(x) = x^e \in \mathbb{Z}_n$.
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 minsta möjliga $|G|$ då G har en delgrupp H med $|H| = 51$ och ett $g \in G$ med $o(g) = 39$. Vi söker också exempel på sådana minimerande G, H, g .

Lösning:

Ordningen för en delgrupp och för ett element i en ändlig grupp är delare till gruppens ordning, så det måste gälla att $51 \mid |G|$ och $39 \mid |G|$. $|G|$ (som ju är ≥ 1) måste alltså vara minst $\text{mgm}(51, 39) = \text{mgm}(3 \cdot 17, 3 \cdot 13) = 3 \cdot 13 \cdot 17 = 663$.
Exemplet $(G, *) = (\mathbb{Z}_{663}, +)$, $H = \langle 13 \rangle = \{0, 13, 26, \dots, 650\}$ och $g = 17 (= \frac{663}{39})$ visar att 663 också är ett möjligt värde.

Svar: $(G, *) = (\mathbb{Z}_{663}, +)$, $H = \langle 13 \rangle$, $g = 17$ ger det minimala värdet $|G| = 663$.

- 6)** (3p) Vi söker banan Gx och stabilisatorn G_x i X , mängden av färgningar av $\{1, 2, 3, 4\}$ med två färger, då $G = S_4$ och $x \in X$ gör 1 och 3 röda och 2 och 4 blå.

Lösning:

Eftersom S_4 innehåller alla permutationer av $\{1, 2, 3, 4\}$ kan gx vara alla färgningar med 2 röda och 2 blå element, så Gx är mängden av sådana färgningar.
Stabilisatorn G_x består av alla $g \in G$ som tar x till sig själv, dvs de som bara tar element till sådana med samma färg i x . Tydligt $G_x = \{(1), (13), (24), (13)(24)\}$.

Svar: Banan Gx består av alla färgningar med 2 röda och 2 blå element.
Stabilisatorn $G_x = \{(1), (13), (24), (13)(24)\}$.

- 7)** (3p) Vi skall faktorisera $p(x) = x^5 + x^4 + 2x^3 + 2 \in \mathbb{Z}_3[x]$ i irreducibla faktorer.

Lösning:

Vi börjar med att söka förstgradsfaktorer, vilket enligt faktorsatsen är ekvivalent med att finna nollställan till p . Man finner att $p(1) = 0$, så $x - 1 = x + 2$ är en faktor i $p(x)$. Polynomdivision ger att $p(x) = (x + 2)q(x)$, där $q(x) = x^4 + 2x^3 + x^2 + x + 1$. Det gäller nu att faktorisera $q(x)$. Man finner att också $q(1) = 0$ och polynomdivision ger $q(x) = (x + 2)r(x)$, där $r(x) = x^3 + x + 2$. Vidare $r(2) = 0$, så $r(x)$ är delbart med $x - 2 = x + 1$. Polynomdivision igen ger $r(x) = (x + 1)s(x)$, där $s(x) = x^2 + 2x + 2$. Eftersom andragradspolynomet $s(x)$ saknar nollställan i $\mathbb{Z}_3$ saknar det förstgradsfaktorer och är alltså irreducibelt.

Svar: Den sökta faktoriseringen är : $p(x) = (x + 2)^2(x + 1)(x^2 + 2x + 2)$.

8) En binär kod har kontrollmatrisen $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ och vi söker (a, 2p) de sända kodorden (med högst ett fel i varje) då (01010), (10101), (11011) har mottagits och (b, 1p) ett ord som inte kan fås med högst ett fel i ett kodord.

Lösning:

a. $H[01010]^T = [111]^T$, $H[10101]^T = [000]^T$ och $H[11011]^T = [011]^T$. $[111]^T$ och $[011]^T$ är H 's första och sista kolonner, så fel har uppstått i första, ingen och sista positionerna. De sända orden var alltså (11010), (10101) och (11010).

b. Lösningar till $Hc = [101]^T$ är $c = [01100]^T$, $[11001]^T$, $[10110]^T$, $[00011]^T$. De ger ord som inte kan rättas med högst ett fel, eftersom $[101]^T$ inte är (0 eller) en kolonn i H . (Det går lika bra med $[010]^T$ som HL.)

Alt.: finn koden $\{(00000), (10101), (11010), (01111)\}$ och "för hand" ord med avstånd mer än 1 till dem alla.

Svar a: De sända kodorden var (11010), (10101) och (11010), b: T.ex. (01100).

9) Vi söker antalet kvadrater i dels (a, 1p) $\mathbb{Z}_{13}$ och dels (b, 3p) $\mathbb{Z}_p$, då p är ett udda primtal.

Lösning:

I $\mathbb{Z}_{13}$ finner vi $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 3$, $5^2 = 12$, $6^2 = 10$, $7^2 = 10$, $8^2 = 12$, $9^2 = 3$, $10^2 = 9$, $11^2 = 4$, $12^2 = 1$, så kvadraterna är 0, 1, 3, 4, 9, 10, 12, dvs 7 stycken. I $\mathbb{Z}_p$, p udda primtal, gäller att $x^2 = y^2$ precis om $p \mid x^2 - y^2 = (x+y)(x-y)$, så (p primtal) precis om minst en av $p \mid x+y$ och $p \mid x-y$, så precis om $(0 \leq x, y \leq p-1)$ $x+y = 0$, $x+y = p$ eller $x-y = 0$. Enda möjligheterna är alltså $y = p-x$ och $y = x$, så alla $x = 0, 1, \dots, \frac{p-1}{2}$ ger olika kvadrater, men övriga ger upprepningar (som för $\mathbb{Z}_{13}$). Det sökta antalet är alltså $1 + \frac{p-1}{2} = \frac{p+1}{2}$.

Svar a: $\mathbb{Z}_{13}$ har 7 kvadrater, b: $\mathbb{Z}_p$, p udda primtal, har $\frac{p+1}{2}$ stycken.

10) Vi söker (a, 1p) en icke-trivial abelsk delgrupp till S_3 och skall (b, 3p) visa att varje icke-abelsk grupp G har minst två olika abelska icke-triviala delgrupper.

Lösning:

a. $\{(1), (12)\} \subset S_3$ är en delgrupp (ändlig, $\neq \emptyset$ och sluten) och den är abelsk.

b. Att G är icke-abelsk betyder precis att det finns $g, h \in G$ med $gh \neq hg$.

De cykliska delgrupper till G som genereras av g och h , $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ och p.s.s. $\langle h \rangle$ är abelska ($g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$). $\langle g \rangle \neq \langle h \rangle$, ty $g \in \langle g \rangle$, $g \notin \langle h \rangle$ (ty $h \in \langle h \rangle$ och $\langle h \rangle$ är abelsk). Varken $\langle g \rangle$ eller $\langle h \rangle$ är trivial (inte $\{1\}$, ty $g, h \neq 1$ (eftersom $gh \neq hg$) och inte G (eftersom G inte är abelsk)), så **saken är klar**.

Svar a: T.ex. $\{(1), (12)\}$, b: Visat ovan.

11) Vi har ringen $R = \mathbb{Z}_5[x]/(f(x))$, där $f(x) = x^3 + 3x^2 + 3$.

Vi kallar x 's ekvivalensklass för α och skall (a, 1p) finna antalet element i R , (b, 2p) beräkna $(\alpha^2 + 3\alpha + 2)(3\alpha^2 + 4)$ i R och (c, 1p) finna nolldelare i R .

Lösning:

a. I varje ekvivalensklass (mod $f(x)$) finns precis ett polynom av grad ≤ 2 . Det kan representera sin klass, dvs sitt element i R , och varje element i R kan då skrivas som $c_2\alpha^2 + c_1\alpha + c_0$, alla $c_i \in \mathbb{Z}_5$. Det totala antalet element, $|R|$, är antalet sätt att välja c_i :na, dvs $5^3 = 125$.

b. Eftersom $x^3 + 3x^2 + 3 \equiv_{(f(x))} 0$ är $\alpha^3 + 3\alpha^2 + 3 = 0$, så $\alpha^3 = 2\alpha^2 + 2$ i R .

Det ger $(\alpha^2 + 3\alpha + 2)(3\alpha^2 + 4) = 3\alpha^4 + 4\alpha^3 + 2\alpha + 3 = 3\alpha \cdot (2\alpha^2 + 2) + 4\alpha^3 + 2\alpha + 3 = 3\alpha + 3$.

c. $r \cdot s = 0$, $r, s \neq 0$ i R , betyder precis att r och s svarar mot polynom $g(x), h(x) \in \mathbb{Z}_5[x]$ med $f(x) \mid g(x) \cdot h(x)$, $f(x) \nmid g(x)$, $f(x) \nmid h(x)$. Sådana $g(x), h(x)$ finns omm $f(x)$ är reducibelt. Man finner $f(0) = 3$, $f(1) = 2$, $f(2) = 3$, $f(3) = 2$, $f(4) = 0$, så $(x-4) = (x+1) \mid f(x)$. Polynomdivision ger $f(x) = (x+1)(x^2 + 2x + 3)$ i $\mathbb{Z}_5[x]$, så $(\alpha+1)(\alpha^2 + 2\alpha + 3) = 0$ i R .

Svar a: $|R| = 125$, b: $3\alpha + 3$, c: Nolldelare är (t.ex.) $\alpha + 1$ och $\alpha^2 + 2\alpha + 3$.

12) (5p) En kub skall få en enfärgad kula i varje hörn. Vi söker antalet väsentligt olika sätt det kan ske om man skall använda precis två röda och två blå kulor och godtyckliga antal kulor med k andra färger.

Lösning:

Vi använder Burnsidess lemma (Thm 21.4 i Biggs). Symmetrigruppen G har 24 element ($|Gx| = 8 \cdot 3 = 24$ om x är ett av kubens hörn):

identitetens "rotationen" id ,

8 rotationer $\frac{2\pi}{3}$ kring axlar genom motsatta hörn rot_{hh} ,

6 rotationer π kring axlar genom mittpunkter av motsatta kanter rot_{kk} ,

3 rotationer π kring axlar genom mittpunkter av motsatta sidor $rot_{ss\pi}$ och

6 rotationer $\frac{\pi}{2}$ kring axlar genom mittpunkter av motsatta sidor $rot_{ss\frac{\pi}{2}}$.

$|F(g)|$, antalet konfigurationer som inte ändras av g för de olika $g \in G$ blir:

g	antal element	$ F(g) $
id	1	$\binom{8}{2} \binom{6}{2} k^4 = 28 \cdot 15 \cdot k^4$ (vilka röda? vilka blå? övriga: k^4)
rot_{hh}	8	0 (kulorna samma färg 1,3,3,1, går inte)
rot_{kk}	6	$4 \cdot 3 \cdot k^2$ (kulorna samma färg parvis, vilket par rött? vilket blått?)
$rot_{ss\pi}$	3	$4 \cdot 3 \cdot k^2$ (kulorna samma färg parvis, som förra)
$rot_{ss\frac{\pi}{2}}$	6	0 (kulorna samma färg 4 och 4, går inte)

Så antalet olika utsmyckningar = antalet banor under G 's verkan på färgningarna =
 $= \frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24} (1 \cdot 28 \cdot 15 \cdot k^4 + 8 \cdot 0 + 6 \cdot 4 \cdot 3 \cdot k^2 + 3 \cdot 4 \cdot 3 \cdot k^2 + 6 \cdot 0) = \frac{1}{2} (35k^4 + 9k^2)$.

Svar: Det finns $\frac{1}{2}(35k^4 + 9k^2)$ olika sådana utsmyckningar.

13) $(G, \cdot) = (U(\mathbb{Z}_{589}), \cdot)$ och vi söker (a, 1p) G 's ordning, (b, 2p) den maximala ordningen för element i G och (c, 2p) antalet element i G som har den maximala ordningen.

Lösning:

a. $|G| =$ antalet inverterbara element i $\mathbb{Z}_{589} = \phi(589) = \phi(19 \cdot 31) = (19 - 1)(31 - 1) = 540$ (känd sats, nästan definitionen av Eulers funktion ϕ).

b. Enligt kinesiska restsatsen är $(\mathbb{Z}_{589}, \cdot) \approx (\mathbb{Z}_{19}, \cdot) \times (\mathbb{Z}_{31}, \cdot)$ (ty $\text{sgd}(19, 31) = 1$). Ett element i HL är inverterbart omm båda dess komponenter är det, så $(G, \cdot) \approx (U(\mathbb{Z}_{19}), \cdot) \times (U(\mathbb{Z}_{31}), \cdot)$. Eftersom 19 och 31 är primtal är grupperna i HL de multiplikativa grupperna i ändliga kroppar, så cykliska, av ordning 18 och 30. Om (x, y) är ett element i HL är $(x, y)^k = (1, 1)$ (identitetselementet i HL) omm $o(x) \mid k$ och $o(y) \mid k$, så $o((x, y)) = \text{mgm}(o(x), o(y))$. Dess största värde fås (bl.a.) då $o(x), o(y)$ är maximala, så den sökta maximala ordningen är $\text{mgm}(18, 30) = \text{mgm}(2 \cdot 3^2, 2 \cdot 3 \cdot 5) = 2 \cdot 3^2 \cdot 5 = 90$.

c. Enligt en känd sats finns det i en cyklisk grupp av ordning n precis $\phi(d)$ element av ordning d om $d \mid n$ och inga för andra d .

Enligt ovan är $o((x, y)) = \text{mgm}(o(x), o(y))$, så för $o((x, y)) = 90$ kan antingen $o(x) = 18$ och $o(y)$ vara en av 5, 10, 15, 30 eller $o(x) = 9$ och $o(y)$ vara 10 eller 30. Det ger det totala antalet element av ordning 90: $\phi(18) \cdot (\phi(5) + \phi(10) + \phi(15) + \phi(30)) + \phi(9) \cdot (\phi(10) + \phi(30)) = 6 \cdot (4 + 4 + 8 + 8) + 6 \cdot (4 + 8) = 216$.

Svar a: G 's ordning är 540, b: Elementens maximala ordning är 90, c: 216 element har ordning 90.