

**Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3 m.fl.
14 januari 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 $x \in G$ (identitetsselement) och
3. För varje $x \in G$ finns $x^{-1} \in G$ med $x \circ x^{-1} = x^{-1} \circ x = e$ (inverseelement).
(Villkoret om slutenhet behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)
b) (1p) Grupperna $(G_1, *)$ och $(G_2, \circ)$ är isomorfa omm det finns en bijektion $\beta : G_1 \rightarrow G_2$ sådan att $\beta(g * h) = \beta(g) \circ \beta(h)$ för alla $g, h \in G_1$.
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 $G_x = \{g \in G \mid gx = x\}$ (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) Ja, varje kropp är en ring och eftersom t.ex. $(\mathbb{Z}_2, +, \cdot)$ och $(\mathbb{Q}, +, \cdot)$ är kroppar, är de ringar som också är kroppar.

- 3a)** (1p) För varje $k \in \{10, 11, 12, \dots, 30\}$ finns en ring med k element, t.ex. $(\mathbb{Z}_k, +, \cdot)$.
b) (1p) Om $(F, +, \cdot)$ är en ändlig kropp är $(F \setminus \{0\}, \cdot)$ en cyklisk grupp.
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) Koden $\mathcal{C} \subseteq (\mathbb{Z}_2)^n$ är linjär omm $\mathbf{a} + \mathbf{b} \in \mathcal{C}$ för alla $\mathbf{a}, \mathbf{b} \in \mathcal{C}$ (komponentvis addition).
b) (1p) Kontrollmatrisen H ger en linjär kod som rättar minst ett fel omm alla H 's kolonner är olika och skilda från $\mathbf{0}$ (kolonnen med alla element 0).
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 möjliga värden för ordningen $o(g)$ då $g \in H \cap K$ och H, K är delgrupper med $|H| = 21$ och $|K| = 91$ till en grupp G .

Lösning:

Ordningen för ett element i en grupp delar gruppens ordning, så $o(g) \mid |H|, |K|$, således $o(g) \mid \text{sgd}(|H|, |K|) = \text{sgd}(21, 91) = 7$. $o(g)$ måste alltså vara en av 1 och 7.
Om G är cyklisk med $\text{mgm}(21, 91) = 273$ element, säg $(\mathbb{Z}_{273}, +)$, blir $H = \langle 13 \rangle$, $K = \langle 3 \rangle$ och $H \cap K = \langle 39 \rangle$, en cyklisk grupp med 7 element, så både 1 och 7 är möjliga.

Svar: De möjliga värdena för $o(g)$ är 1 och 7.

- 6)** Vi söker dels alla banor och dels stabilisatorerna G_6 och G_7 , då gruppen $G = \{1, 3, 5, 7\}$ (med operationen multiplikation mod 8) verkar på $X = \mathbb{Z}_{15}$ enligt $g(x) = x^g$.

Lösning:

Man finner

$G_0 = \{0^1, 0^3, 0^5, 0^7\} = \{0\}$, $G_1 = \{1^1, 1^3, 1^5, 1^7\} = \{1\}$, $G_2 = \{2^1, 2^3, 2^5, 2^7\} = \{2, 8\} = G_8$ och p.s.s. $G_3 = \{3, 12\} = G_{12}$, $G_4 = \{4\}$, $G_5 = \{5\}$, $G_6 = \{6\}$, $G_7 = \{7, 13\} = G_{13}$, $G_9 = \{9\}$, $G_{10} = \{10\}$, $G_{11} = \{11\}$, $G_{14} = \{14\}$.

Eftersom $G_6 = \{6\}$ är $G_6 = G$ (ty $g(6) = 6$ för alla $g \in G$).

$1(7) = 7^1 = 7$, $3(7) = 13$, $5(7) = 7$, $7(7) = 13$, så $G_7 = \{1, 5\}$.

Svar: Banorna är $\{0\}, \{1\}, \{2, 8\}, \{3, 12\}, \{4\}, \{5\}, \{6\}, \{7, 13\}, \{9\}, \{10\}, \{11\}$ och $\{14\}$. De sökta stabilisatorerna är $G_6 = G$ och $G_7 = \{1, 5\}$.

- 7)** (3p) Vi söker den moniska största gemensamma delaren till $f(x) = x^5 + 2x^3 + x^2 + x + 3$ och $g(x) = x^6 + x^5 + x^2 + 3x + 2$ i $\mathbb{Z}_5[x]$.

Lösning:

Vi använder Euklides algoritm och finner med polynomdivision

$g(x) = (x+1)f(x) + r_1(x)$, där $r_1(x) = 3x^4 + 2x^3 + 4x^2 + 4x + 4$; $f(x) = (2x+2)r_1(x) + 0$.
 $r_1(x)$ är alltså en största gemensam delare till $f(x)$ och $g(x)$.

Den moniska fås (eftersom $2 \cdot 3 = 1$ i $\mathbb{Z}_5$) som $2 \cdot r_1(x) = x^4 + 4x^3 + 3x^2 + 3x + 3$.

Svar: Den moniska största gemensamma delaren är $x^4 + 4x^3 + 3x^2 + 3x + 3$.

8) Ett RSA-system har offentliga (n, e) , där $n = 4331 [= 61 \cdot 71]$. Vi söker (a, 1p) de av 205, ..., 209 som är möjliga för e och (b, 2p) ett motsvarande d -värde för något av de e :na.

Lösning:

Villkoret på e är att $\text{sgd}(m, e) = 1$, där (om $n = p \cdot q$ med p, q primtal)

$$m = (p-1)(q-1) = 60 \cdot 70 = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Eftersom $2 \mid 206, 208$ och $3 \mid 207$ och $5 \mid 205$ och $2, 3, 5, 7 \nmid 209$ är det enda möjliga $e = 209$.

Motsvarande d bestäms av $e \cdot d \equiv_m 1$.

Euklides algoritm: $4200 = 20 \cdot 209 + 20$, $209 = 10 \cdot 20 + 9$, $20 = 2 \cdot 9 + 2$, $9 = 4 \cdot 2 + 1$, så
 $1 = 9 - 4 \cdot 2 = 9 - 4(20 - 2 \cdot 9) = -4 \cdot 20 + 9 \cdot 9 = -4 \cdot 20 + 9(209 - 10 \cdot 20) = 9 \cdot 209 - 94 \cdot 20 =$
 $= 9 \cdot 209 - 94(4200 - 20 \cdot 209) = -94 \cdot 4200 + 1889 \cdot 209$ och vi kan ta $d = 1889$.

Svar a: Det enda möjliga $e = 209$, b: Motsvarande $d = 1889$.

9) $(G, \cdot)$ är gruppen $(U(\mathbb{Z}_{36}), \cdot)$ och H är den minsta delgruppen till G med $5 \in H$. Vi skall (a, 2p) finna alla G :s element och (b, 2p) finna alla H :s element och sidoklasser.

Lösning:

Eftersom $U(\mathbb{Z}_{36})$ består av alla $x \in \mathbb{Z}_{36}$ som uppfyller $\text{sgd}(x, 36) = 1$ och $36 = 2^2 \cdot 3^2$, är
 $G = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

H består av alla potenser av 5 (de bildar en delgrupp och måste alla ingå i H). Man finner
 $5^2 = 25$, $5^3 = 5 \cdot 25 = 17$, ... och $H = \{5, 25, 17, 13, 29, 1\}$. $|G \setminus H| = 6 = |H|$, så H har
bara en ytterligare (dvs utöver H själv) sidoklass, $G \setminus H = \{7, 11, 19, 23, 31, 35\}$.

Svar a: $G = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$,

b: $H = \{1, 5, 13, 17, 25, 29\}$, dess sidoklasser är H och $\{7, 11, 19, 23, 31, 35\}$.

10) (2p) Vi skall (a, 2p) beskriva en kropp $(F, +, \cdot)$ med $|F| = 49$ med nollställe α till
 $x^2 + 3x + 5$ och (b, 2p) finna ett $k \in F$ med $k^2 + 1 = 0$.

Lösning:

Vi skall ha $|F| = 49 = 7^2$, så F skall ha karakteristik 7.

Polynomet $f(x) = x^2 + 3x + 5 \in \mathbb{Z}_7[x]$ saknar nollställen ($f(0) = f(4) = 5$, $f(1) = f(3) = 2$, $f(2) = 1$, $f(5) = f(6) = 3$), så det är irreducibelt (andragradspolynom utan nollställe) och vi kan ta
 $F = \mathbb{Z}_7[x]/(f(x))$ och kalla x :s klass för α (det är ju en kropp med $7^2 = 49$ element och $f(\alpha) = 0$).

Då är $F = \{r + s\alpha \mid r, s \in \mathbb{Z}_7\}$ och man räknar i F "som vanligt" i en kropp och
 $\alpha^2 = 4\alpha + 2$ (eftersom $f(\alpha) = 0$ i F). Så $(r_1 + s_1\alpha) + (r_2 + s_2\alpha) = (r_1 + r_2) + (s_1 + s_2)\alpha$
och $(r_1 + s_1\alpha)(r_2 + s_2\alpha) = (r_1r_2 + 2s_1s_2) + (r_1s_2 + s_1r_2 + 4s_1s_2)\alpha$.

Eftersom $\alpha^2 + 3\alpha + 5 = \alpha^2 + 10\alpha + 5 = (\alpha + 5)^2 + 1$ uppfyller $k = 5 + \alpha \in F$ att $k^2 + 1 = 0$.

(Man kan också sätta $k = r + s\alpha$, $k^2 + 1 = (r^2 + 2s^2 + 1) + (2rs + 4s^2)\alpha$ och lösa $r^2 + 2s^2 + 1 = 2rs + 4s^2 = 0$ i $\mathbb{Z}_7$. Det ger $k = \pm(5 + \alpha)$.)

Svar a: $F = \{r + s\alpha \mid r, s \in \mathbb{Z}_7\}$, $a + b$, $a \cdot b$ ovan, b: $k = 5 + \alpha$ (eller $k = 2 + 6\alpha$).

(Alla kroppar med p^k element är isomorfa, så $k \in F$ med $k^2 + 1 = 0$ finns. Vi sökte lösningarna uttryckta i α .)

11) Vi har gruppen $(\mathbb{Z}_{9431} \setminus \{0\}, \cdot)$ och söker antalet element i den som har ordning (a, 2p) 114 och (b, 2p) 115.

Lösning:

Gruppen har ordning $9431 - 1 = 9430$ och $114 \nmid 9430$, så inget element har ordning 114.

Eftersom 9431 är ett primtal är $(\mathbb{Z}_{9431}, +, \cdot)$ en ändlig kropp, så $(\mathbb{Z}_{9431} \setminus \{0\}, \cdot)$ är en cyklisk grupp. $115 \mid 9430$, så enligt känd sats (Biggs Thm 20.9) har precis $\phi(115) = \phi(5 \cdot 23) = (5-1)(23-1) = 88$ element i gruppen ordning 115.

Svar a: Inget element har ordning 114, b: Precis 88 element har ordning 115.

12) Ett ideal i en ring $(R, +, \cdot)$ är ett $J \subseteq R$ med $(J, +)$ en delgrupp till $(R, +)$ och $a \cdot r, r \cdot a \in J$ för alla $r \in R, a \in J$. Vi skall visa (a, 2p) att om $m \in \mathbb{Z}$ är $J_m = \{k \cdot m \mid k \in \mathbb{Z}\}$ ett ideal i ringen $(\mathbb{Z}, +, \cdot)$ och (b, 3p) att om $\sim$ är en ekvivalensrelation i en ring R sådan att $\sim$ respekterar $+$ och $\cdot$ så är $J_\sim = \{x \in R \mid x \sim 0\}$ ett ideal i R .

Lösning:

a. $(J_m, +)$ är en delgrupp till $(\mathbb{Z}, +)$, ty (känd sats) 1. $J_m \neq \emptyset$ (ty $0 = 0 \cdot m \in J_m$),

2. $a, b \in J_m \Rightarrow a + b \in J_m$ om $a, b \in \mathbb{Z}$ (ty $a = k \cdot m, b = k' \cdot m \Rightarrow a + b = (k + k') \cdot m$),

3. $a \in J_m \Rightarrow -a \in J_m$ om $a \in \mathbb{Z}$ (ty $a = k \cdot m \Rightarrow -a = (-k) \cdot m$).

Om $r \in \mathbb{Z}, a \in J_m$ gäller $a \cdot r, r \cdot a \in J_m$ (ty $a = k \cdot m$ ger $a \cdot r = r \cdot a = (kr) \cdot m$).

Eftersom $J_m \subseteq \mathbb{Z}$ är J_m alltså ett ideal i $\mathbb{Z}$, **a-saken är klar**.

b. $(J_\sim, +)$ är p.s.s. en delgrupp till $(R, +)$, ty 1. $J_\sim \neq \emptyset$ (ty $0 \sim 0$ ($\sim$ reflexiv)),

2. $a, b \in J_\sim \Rightarrow a + b \in J_\sim$ om $a, b \in R$ (ty $a \sim 0, b \sim 0 \Rightarrow a + b \sim a + 0 = 0 + a \sim 0 + 0 = 0$, $\sim$ transitiv),

3. $a \in J_\sim \Rightarrow -a \in J_\sim$ om $a \in R$ (ty $a \sim 0 \Rightarrow 0 = -a + a \sim -a + 0 = -a$, så $-a \sim 0$ ($\sim$ symmetrisk)).

Om $r \in R, a \in J_\sim$ gäller $a \cdot r, r \cdot a \in J_\sim$ (ty $a \sim 0 \Rightarrow a \cdot r \sim 0 \cdot r = 0, r \cdot a \sim r \cdot 0 = 0$).

Eftersom $J_\sim \subseteq R$ är $J_\sim$ alltså ett ideal i R , **också b-saken är klar**.

(a. följer också från b. (med $\equiv_m$ som $\sim$), om man visar att $\equiv_m$ är en ekvivalensrelation som respekterar $+$ och $\cdot$)

13) 120 identiska kulor placeras i 4 lådor, med $n_i > 0$ st i låda $i = 1, 2, 3, 4$. Vi söker (a, 2p) $a_4, a_{31}, a_{22}, a_{211}, a_{1111}$, antalet fördelningar med $n_1 = n_2 = n_3 = n_4$, antalet med $n_1 = n_2 = n_3$, antalet med $n_1 = n_2$ och $n_3 = n_4$, antalet med $n_1 = n_2$ resp. det totala antalet och (b, 3p) $p_4(120)$, antalet partitioner av 120 i precis 4 delar.

Lösning:

a. Det finns bara ett sätt att lägga lika många (30 st) i varje låda, så **$a_4 = 1$** .

Om det är lika många i tre av lådorna, kan det antalet vara $1, 2, \dots, 39$ (ingen tom), så **$a_{31} = 39$** .

Fördelningar med lika många i lådorna parvis motsvarar precis uppdelningar av 120 i två positiva jämna tal, så **$a_{22} = 59$** .

Om det är lika många i två av lådorna kan det antalet vara $1, 2, \dots, 59$ och med k st var i dem kan övriga $120 - 2k$ kulor fördelas på $119 - 2k$ sätt i de återstående lådorna. $117 + 115 + \dots + 1 = \frac{59 \cdot (117 + 1)}{2} = 59^2$ (aritmetisk serie), så **$a_{211} = 59^2$** .

Det totala antalet sätt att fördela kulorna ges av $\binom{(120-4)+3}{3} = \frac{119 \cdot 118 \cdot 117}{3 \cdot 2}$ (först en kula i varje, så ordnat val med upprepning bland återstående kulor), så **$a_{1111} = 119 \cdot 59 \cdot 39$** .

b. Att betrakta lådorna som identiska innebär precis att se det som samma fördelning då lådorna kastas om, så det sökta antalet är antalet banor bland fördelningarna i a. då gruppen S_4 verkar med omkastning av lådorna.

Vi använder Burnsidess lemma (Thm 21.4 i Biggs).

S_4 :s 24 element är av fem typer, med cykelstrukturer $[1^4], [2^1 2^1], [2^2], [3^1], [4]$.

Antalen element av dem är respektive 1, 6 ($\binom{4}{2}$), 3 (vilken med låda 1?), 8 (vilken ensam?, två olika 3-cykler av resten) och 6 (6 möjliga ordningar bland dem låda 1 tas till).

$|F(\pi)|$, antalet konfigurationer som inte ändras av $\pi \in S_4$, ges av respektive

$a_{1111}, a_{211}, a_{22}, a_{31}$ och a_4 (konfigurationen bevaras precis om lådor i samma π -cykel innehåller lika många kulor).

Så antalet partitioner $p_4(120) =$ antalet banor under S_4 :s verkan på fördelningarna $= \frac{1}{|S_4|} \sum_{\pi \in S_4} |F(\pi)| = \frac{1}{24} (1 \cdot a_{1111} + 6 \cdot a_{211} + 3 \cdot a_{22} + 8 \cdot a_{31} + 6 \cdot a_4)$.

Svar a: $a_4 = 1, a_{31} = 39, a_{22} = 59, a_{211} = 59^2 (= 3481)$,

$a_{1111} = 119 \cdot 59 \cdot 39 (= 273819)$,

b: $p_4(120) = \frac{1}{24} (1 \cdot a_{1111} + 6 \cdot a_{211} + 3 \cdot a_{22} + 8 \cdot a_{31} + 6 \cdot a_4) (= 12300)$.