**Matematik, KTH**
B.Ek

**Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3 m.fl.**
**12 april 2017**
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 $x \in G$ (identitetselement) 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 $\circ : G \times G \to G$.)
**b)** (1p) Gruppen $(G, \circ)$ är abelsk omm $a \circ b = b \circ a$ för alla $a, b \in G$.
**c)** (1p) $105 \mid 3150$, så det sökta antalet är (Biggs sats 20.9) $\phi(105) = \phi(3 \cdot 5 \cdot 7) = 2 \cdot 4 \cdot 6 = 48$.

---

**2a)** (1p) Stabilisatorn för $x \in X$ är $G_x = \{g \in G \mid gx = x\}$ (med $gx$ 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) Operationen $\cdot$ skall vara kommutativ och alla $x \in R$ utom 0 skall ha en multiplikativ invers $x^{-1} \in R$ (dvs $x \cdot x^{-1} = 1$). $R$ skall förstås ha en etta.

---

**3a)** (1p) Möjliga värden för karakteristiken är alla primtal och 0.
**b)** (1p) $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp.
**c)** (1p) Om $f(x) \in F[x]$ och $\alpha \in F$ är $x - \alpha$ en delare till $f(x)$ omm $f(\alpha) = 0$ i $F$.

---

**4a)** (1p) $H$:s kolonner skall alla vara olika och inte **0**-kolonnen.
**b)** (1p) Om $p, q$ är primtal och $k \equiv_{(p-1)(q-1)} 1$ är $x^k \equiv_{p \cdot q} x$ för alla $x \in \mathbb{Z}$.
**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 $|\langle 276, 672 \rangle|$ (då $\langle 276, 672 \rangle$ är den minsta delgruppen till $(\mathbb{Z}_{1440}, +)$ med $276, 672$ i).

**Lösning:**
Om $d$ är en gemensam delare till 276 och 672, är $\langle d \rangle$ en delgrupp som innehåller båda talen.
$12 = \text{sgd}(276, 672)$ (Euklides algoritm: $672 = 276 \cdot 2 + 120$, $276 = 120 \cdot 2 + 36$, $120 = 36 \cdot 3 + 12$, $36 = 12 \cdot 3 + 0$) ingår i $\langle 276, 672 \rangle$ (ty $= 276a + 672b$), så $\langle 276, 672 \rangle = \langle 12 \rangle$, med $|\langle 12 \rangle| = \frac{1440}{12} = 120$ (ty $12 \mid 1440$).

**Svar: Den betraktade delgruppen har 120 element.**

---

**6)** (3p) Vi söker banan $Gx$ och stabilisatorn $G_x$ då $G = \{(1), (1\,2\,3), (1\,3\,2)\} \subset S_3$ verkar med elementvis multiplikation på $X =$ mängden av $H$:s ($H = \{(1), (1\,2)\}$) vänstersidoklasser i $S_3$ och $(1\,2\,3) \in x \in X$.

**Lösning:**
$(1)H = \{(1), (12)\} = (12)H$, $(13)H = \{(13), (123)\} = (123)H$, $(23)H = \{(23), (132)\} = (132)H$, så $X = \{H, \{(1\,3), (1\,2\,3)\}, \{(2\,3), (1\,3\,2)\}\}$, $x = \{(1\,3), (1\,2\,3)\}$ och $(1)x = x$, $(1\,2\,3)x = \{(2\,3), (1\,3\,2)\}$, $(1\,3\,2)x = \{(1\,2), (1)\} = H$. Vi ser att $Gx = \{gx \mid g \in G\} = X$ och $G_x = \{g \in G \mid gx = x\} = \{(1)\}$. **Svar: $Gx = X$, $G_x = \{(1)\}$.**

---

**7)** (3p) Vi söker den moniska $\text{sgd}(f(x), g(x))$ i $\mathbb{Z}_5[x]$, då $f(x) = x^5 + 3x^3 + 3x^2 + 4$ och $g(x) = x^4 + x^3 + 2x^2 + 4x + 1$.

**Lösning:**
Vi använder Euklides algoritm. Polynomdivision ger
$f(x) = g(x)(x + 4) + r_1(x)$, där $r_1(x) = 2x^3 + x^2 + 3x$,
$g(x) = r_1(x)(3x + 4) + r_2(x)$, där $r_2(x) = 4x^2 + 2x + 1$ och
$r_1(x) = 3x \cdot r_2(x) + 0$, så $r_2(x)$ är en $\text{sgd}(f(x), g(x))$.
Den moniska fås (eftersom $4 \cdot 4 = 1$ i $\mathbb{Z}_5$) som $4 \cdot r_2(x) = x^2 + 3x + 4$.

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

---

**8)** (3p) Vi söker $x \in \mathbb{Z}_{299}$ med $E(x) = 55$ för ett RSA-system med $(n, e) = (299, 53)$.

**Lösning:**
$n = 299 = 13 \cdot 23$, så $m = (13-1)(23-1) = 12 \cdot 22 = 264$. $e = 53$, så det räcker om $d$ uppfyller $53d \equiv_{264} 1$. Använd Euklides algoritm: $264 = 53 \cdot 5 - 1$, så $1 = 53 \cdot 5 - 1 \cdot 264$ och vi kan ta $d = 5$. Vi beräknar $D(55) \equiv_{299} 55^5$, $0 \leq D(55) < 299$: $55^2 = 3025 \equiv_{299} 35$, $55^4 \equiv_{299} 35^2 = 1225 \equiv_{299} 29$, $55^5 \equiv_{299} 55 \cdot 29 = 1595 \equiv_{299} 100$, så

**Svar: Meddelandet var '100'.**

---

**9)** $R$ är ringen $\mathbb{Z}_5[x]/(k(x))$, där $k(x) = x^3 + 2x^2 + x + 3$ och $x$:s ekvivalensklass kallas $\alpha$. Vi söker (a, 2p) $(\alpha^2 + 2\alpha + 3)(2\alpha^2 + 3\alpha + 4)$ och (b, 2p) antalet inverterbara element i $R$.

**Lösning:**
a. $(x^2 + 2x + 3)(2x^2 + 3x + 4) = 2x^4 + 2x^3 + x^2 + 2x + 2$ och polynomdivision ger att det är $(2x + 3)k(x) + 3x^2 + 3x + 3$, så $(\alpha^2 + 2\alpha + 3)(2\alpha^2 + 3\alpha + 4) = 3\alpha^2 + 3\alpha + 3$ i $R$.
(Alt. $k(\alpha) = 0$, så $\alpha^3 = 3\alpha^2 + 4\alpha + 2$, vilket ger $\alpha^4 = 3\alpha^3 + 4\alpha^2 + 2\alpha = 3(3\alpha^2 + 4\alpha + 2) + 4\alpha^2 + 2\alpha = 3\alpha^2 + 4\alpha + 1$, sätt in i $(\alpha^2 + 2\alpha + 3)(2\alpha^2 + 3\alpha + 4) = 2\alpha^4 + 2\alpha^3 + \alpha^2 + 2\alpha + 2$.)
b. För att se vilka av $R$:s element som är inverterbara faktoriserar vi $k(x)$.
$k(x)$ är av grad 3, så om det är reducibelt har det minst ett nollställe (faktorsatsen). $k(0) = 3$, $k(1) = 2$, $k(2) = 1$, $k(3) = 1$, $k(4) = k(-1) = 3$, så $k(x)$ saknar nollställe och är irreducibelt. Så $R$ är en kropp och alla dess element utom 0, $|R| - 1 = 5^3 - 1 = 124$ st, är inverterbara.

**Svar a: $3\alpha^2 + 3\alpha + 3$, b: $R$ har 124 inverterbara element.**

---

**10a)** (2p) Vi söker (a, 2p) antalet väsentligt olika armband med 6 färgade ($k$ färger möjliga) pärlor på en ögla och (b, 2p) hur många av dem som har minst en vardera röd och blå pärla.

**Lösning:**
a. Vi använder Burnsides lemma. Om armbandet placeras med pärlorna i hörnen av en regelbunden sexhörning, ser man att gruppen $G$ som verkar på mängden av konfigurationer beskrivs av identitetsavbildningen $id$, elementen $r, r^2, \ldots, r^5$ (där $r$ är rotation $\frac{2\pi}{6} = \frac{\pi}{3}$ kring en axel genom sexhörningens mittpunkt och vinkelrät mot dess plan) och tre olika rotationer $\pi$ vardera av typ $s_1$, $s_2$ (där $s_1$ är rotation kring en axel i sexhörningens plan, genom mittpunkter av två av motstående sidor och $s_2$ kring en axel genom två motstående hörn). $|F(g)|$, antalet konfigurationer som inte ändras av $g$, ses vara som i tabellen:

| $g$:s typ | antal sådana $g$ | $g$:s permutation av pärlorna | $\lvert F(g)\rvert$ |
|---|---|---|---|
| $id$ | 1 | $[1^6]$ | $k^6$ |
| $r, r^5$ | 2 | $[6]$ | $k$ |
| $r^2, r^4$ | 2 | $[3^2]$ | $k^2$ |
| $r^3$ | 1 | $[2^3]$ | $k^3$ |
| $s_1$ | 3 | $[2^3]$ | $k^3$ |
| $s_2$ | 3 | $[1^2 2^2]$ | $k^4$ |

Så antalet väsentligt olika armband = antalet banor under $G$:s verkan $= \frac{1}{|G|} \sum_{g \in G} |F(g)| =$
$= \frac{1}{12}(1 \cdot k^6 + 2k + 2k^2 + k^3 + 3k^3 + 3k^4) = \frac{1}{12}(k^6 + 3k^4 + 4k^3 + 2k^2 + 2k)$.
b. Låt $X$ vara alla färgningar i a) och $B$ de **utan** någon blå pärla, $R$ de utan någon röd pärla. Då söker vi nu $|X \setminus (B \cup R)| = |X| - |B| - |R| + |B \cap R| = f(k) - 2 \cdot f(k-1) + f(k-2)$, där $f(k)$ är svaret i a). Det blir $\frac{1}{2}(5k^4 - 20k^3 + 41k^2 - 38k + 14)$.

**Svar a: Antalet olika sådana armband är $f(k) = \frac{1}{12}(k^6 + 3k^4 + 4k^3 + 2k^2 + 2k)$,**
**b: Antalet är nu $\frac{1}{2}(5k^4 - 20k^3 + 41k^2 - 38k + 14)$.**
(Det går också bra att svara i b) utan att utveckla, så svaret kan börja $\frac{1}{12}(k^6 - 2(k-1)^6 + (k-2)^6 + \ldots)$)

**11)** $H$, $K$ är delgrupper till gruppen $G$. Vi skall visa (a, 1p) att $H \cap K$ är en delgrupp till $G$ och (b, 3p) att om $H \cup K$ är en delgrupp till $G$, så är $H \subseteq K$ eller $K \subseteq H$.

**Lösning:**

a. Enligt känd sats (Thm 20.7 i Biggs) är $D \subseteq G$ en delgrupp till $G$ omm

S0: $D \neq \varnothing$, S1: $x, y \in D \Rightarrow xy \in D$, S2: $x \in D \Rightarrow x^{-1} \in D$.

Här: Eftersom $1 \in H, K$ gäller $1 \in H \cap K$ (1 identitetselementet i $G$), så S0

$x, y \in H \cap K \Rightarrow x, y \in H, K \Rightarrow xy \in H, K \Rightarrow xy \in H \cap K$, så S1,

$x \in H \cap K \Rightarrow x \in H, K \Rightarrow x^{-1} \in H, K \Rightarrow x^{-1} \in H \cap K$, så S2. **a-Saken är klar.**

b. Antag att $H \not\subseteq K$ och $K \not\subseteq H$. Påståendet följer om vi visar att $H \cup K$ inte är en grupp. Låt $h \in H \setminus K$, $k \in K \setminus H$.

Då $hk \notin H$, ty om $hk = h_1 \in H$ skulle $k = h^{-1}h_1 \in H$, och $hk \notin K$, ty om $hk = k_1 \in K$ skulle $h = k_1 k^{-1} \in K$. $H \cup K$ är alltså inte sluten under produkten ($h, k \in H \cup K$, $hk \notin H \cup K$) och därmed inte en grupp. **b-Saken är klar.**

---

**12)** $(G, *)$ och $(A, \circ)$ med identitetselement $I$ respektive $e$ är grupper ($A$ abelsk). $G$ verkar på mängden $A$ med $g(a \circ b) = g(a) \circ g(b)$ (för $g \in G$, $a, b \in A$). Vi skall (a, 3p) visa att $(K, \odot)$ är en grupp, där $K = G \times A$ och $\odot$ ges av $(g_1, a_1) \odot (g_2, a_2) = (g_1 * g_2, g_1(a_2) \circ a_1)$ och (b, 2p) avgöra om $H_1 = G \times \{e\}$, $H_2 = \{I\} \times A$ är delgrupper och normala delgrupper till $(K, \odot)$.

**Lösning:**

a. Att $(K, \odot)$ är en grupp följer av att axiomen för en grupp (G1–G4) är uppfyllda.

G1 (slutenhet): $g_1 * g_2 \in G$ och $g_1(a_2) \circ a_1 \in A$ för alla $g_1, g_2 \in G$, $a_1, a_2 \in A$ ($G, A$ slutna under $*$, $\circ$ och $g_1(a_2) \in A$). G1 klart.

G2 (associativitet): $\big((g_1, a_1) \odot (g_2, a_2)\big) \odot (g_3, a_3) = (g_1 * g_2, g_1(a_2) \circ a_1) \odot (g_3, a_3) =$
$= ((g_1 * g_2) * g_3, (g_1 * g_2)(a_3) \circ (g_1(a_2) \circ a_1))$ skall vara lika med $(g_1, a_1) \odot \big((g_2, a_2) \odot (g_3, a_3)\big) =$
$= (g_1, a_1) \odot (g_2 * g_3, g_2(a_3) \circ a_2) = (g_1 * (g_2 * g_3), g_1(g_2(a_3) \circ a_2) \circ a_1)$.

$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ ($*$ associativ),

$(g_1 * g_2)(a_3) \circ (g_1(a_2) \circ a_1) = \big(g_1(g_2(a_3)) \circ g_1(a_2)\big) \circ a_1$ ($G$ verkar på $A$, $\circ$ associativ) och

$g_1(g_2(a_3) \circ a_2) \circ a_1 = \big(g_1(g_2(a_3)) \circ g_1(a_2)\big) \circ a_1$ (givna egenskapen hos $G$:s verkan) G2 klart.

G3 (identitetselement): $(I, e) \odot (g, a) = (I * g, I(a) \circ e) = (g, a \circ e) = (g, a)$ och $(g, a) \odot (I, e) =$
$= (g * I, g(e) \circ a) = (g, e \circ a) = (g, a)$ ($I, e$ identitetselement, $I(a) = a$ (alla $a \in A$), $g(e) = e$ (alla $g \in G$) (ty $e \circ g(e) = g(e) = g(e \circ e) = g(e) \circ g(e)$)), så $(I, e)$ är ett identitetselement. G3 klart.

G4 (invers): $(g, a) \odot (g^{-1}, g^{-1}(a^{-1})) = (g * g^{-1}, g(g^{-1}(a^{-1})) \circ a) = (I, (g * g^{-1})(a^{-1}) \circ a) =$
$= (I, I(a^{-1}) \circ a) = (I, a^{-1} \circ a) = (I, e)$ ($^{-1}$ invers i $G$ eller i $A$, $G$ verkar på $A$, $I(b) = b$, alla $b \in A$),
$(g^{-1}, g^{-1}(a^{-1})) \odot (g, a) = (g^{-1} * g, g^{-1}(a) \circ g^{-1}(a^{-1})) = (I, g^{-1}(a \circ a^{-1})) = (I, g^{-1}(e)) =$
$= (I, e)$, så $(g^{-1}, g^{-1}(a^{-1}))$ är inverselement till $(g, a)$. G4 klart. **Så $(K, \odot)$ är en grupp.**

b. $H_1$ och $H_2$ är delgrupper till $K$ (bijektionerna $\phi_1((g, e)) = g$, $\phi_2((I, a)) = a$ är isomorfier med $G$ respektive $A$, ty $(g_1, e) \odot (g_2, e) = (g_1 * g_2, g_1(e) \circ e) = (g_1 * g_2, e)$ och $(I, a_1) \odot (I, a_2) = (I * I, I(a_2) \circ a_1) = (I, a_1 \circ a_2)$.
$(I, a) \odot H_1 = \{(g, a) \mid g \in G\}$ och $H_1 \odot (I, a) = \{(g, g(a)) \mid g \in G\}$ är inte lika om $g(a) \neq a$ för något $g \in G$, så $H_1$ behöver inte vara en normal delgrupp.

$(g, a) \odot H_2 = \{(g, g(a') \circ a) \mid a' \in A\}$ och $H_2 \odot (g, a) = \{(g, a \circ a') \mid a' \in A\}$. Båda är $\{g\} \times A$ ($g$ verkar som en bijektion på $A$), så $H_2$ är normal.

**Svar b: $H_1$ och $H_2$ är delgrupper. $H_2$ är normal, men det är $H_1$ inte säkert.**

($K$ kallas en halvdirekt produkt av grupperna $G$ och $A$. Villkoret att $A$ är abelsk behövs inte (se lösningen). Mer naturligt är att definiera $(g_1, a_1) \odot (g_2, a_2) = (g_1 * g_2, a_1 \circ g_1(a_2))$.)

---

**13)** (5p) $f(x) = x^3 + 6x, h(x) = x^3 + 3x^2 + 4x + 5 \in \mathbb{Z}_7[x]$ och vi söker alla $k \in \mathbb{Z}_+$ sådana att $f(x)^k \equiv 1 \pmod{h(x)}$.

**Lösning:**

Vi faktoriserar $h(x)$ i irreducibla faktorer och finner $h(x) = (x+3)(x^2+4)$ ($h(4) = 0$ och $x^2 + 4$ saknar nollställen i $\mathbb{Z}_7$). Eftersom entydig faktorisering gäller i $\mathbb{Z}_7$, innebär det att
$h(x) \mid (f(x)^k - 1) \Leftrightarrow \big((x+3) \mid (f(x)^k - 1)$ och $(x^2+4) \mid (f(x)^k - 1)\big)$

$f(x) \equiv_{x+3} 4$, $f(x)^2 \equiv_{x+3} 4^2 = 2$, $f(x)^3 \equiv_{x+3} 1$ och för $k \in \mathbb{Z}_+$: $(x+3) \mid (f(x)^k - 1) \Leftrightarrow 3 \mid k$.

$f(x) \equiv_{x^2+4} 2x$, $f(x)^2 \equiv_{x^2+4} (2x)^2 = 4 \cdot 3 = 5$. Udda $k \in \mathbb{Z}_+$ ger $f(x)^k \equiv_{x^2+4} ax$, $a \in \mathbb{Z}_7$ och $f(x)^{4,6,8,10,12} \equiv_{x^2+4} 4, 6, 2, 3, 1$ så för $k \in \mathbb{Z}_+$: $(x^2+4) \mid (f(x)^k - 1) \Leftrightarrow 12 \mid k$.

Båda villkoren är alltså för $k \in \mathbb{Z}_+$ uppfyllda omm $12 \mid k$. Enligt ovan ger det vårt svar.

**Svar: Alla $k = 12\,n$, $n \in \mathbb{Z}_+$.**