Matematik, KTH
B.Ek

Lösningar tentan TENB SF1630, SF1631 DISKRET MATEMATIK, F, D, 8 juni 2012

Tryckfel kan förekomma.

1) Vad är $8^{6^{2012}}$ i $\mathbb{Z}_{17}$? ($8^{6^{2012}}$ betyder förstås $8^{(6^{2012})}$.)

Lösning:
$(\mathbb{Z}_{17} \setminus \{0\}, \cdot)$ är en grupp av ordning 16, så $x^{16} = 1$ för alla $x \in \mathbb{Z}_{17} \setminus \{0\}$ (Fermats lilla sats). Eftersom $16 \mid 6^4$ är $6^{2012} = 16k$ för något $k \in \mathbb{Z}$ och $8^{6^{2012}} = (8^{16})^k = 1^k = 1$ i $\mathbb{Z}_{17}$.
Svar: $8^{6^{2012}} = 1$ i $\mathbb{Z}_{17}$.

---

2) Låt $G = \{x \in \mathbb{R} \mid -1 < x < 1\}$ och $x * y = \frac{x+y}{xy+1}$ för $x, y \in G$.
a) (1p) Visa att $x * y \in G$ för alla $x, y \in G$.
b) (2p) Visa att $(G, *)$ är en grupp (resultatet i a) får användas).

Lösning:
a) $1 \pm \frac{x+y}{xy+1} = \frac{(x\pm1)(y\pm1)}{xy+1} > 0$ (ty $x+1, y+1 > 0, x-1, y-1 < 0, xy > -1$), så $-1 < \frac{x+y}{xy+1} < 1$.
b) Vi skall verifiera gruppaxiomen i $(G, *)$ (Biggs 20.1).
$(x * y) * z = \frac{\frac{x+y}{xy+1}+z}{\frac{x+y}{xy+1}z+1} = \frac{x+y+z+xyz}{xy+xz+yz+1} = x * (y * z)$ för alla $x, y, z \in G$, så $*$ är associativ i G.
$x * 0 = \frac{x+0}{x\cdot0+1} = x = 0 * x$ för alla $x \in G$, så 0 är identitetselement i G.
$x * (-x) = \frac{x+(-x)}{x(-x)+1} = 0 = (-x) * x$ för alla $x \in G$, så $-x$ är invers till x i G.
Saken är klar. ($(G, *)$ är isomorf med $(\mathbb{R}, +)$. En isomorfi $\mathbb{R} \to G$ ges av $\beta(a) = \tanh(a)$ för $a \in \mathbb{R}$.)

---

3) (3p) Man söker en linjär, binär kod $\mathcal{C}$ som innehåller ordet (011101100), men inte (110011001).
Finn en möjlig kontrollmatris (eng. check matrix) H för $\mathcal{C}$ om den skall rätta (minst) ett fel och innehålla så många ord som möjligt.
Hur många ord innehåller koden?

Lösning:
H skall ha 9 olika och nollskilda kolonner (för att kunna rätta ett fel), så det minimala (ger maximalt antal ord) antalet rader är 4. Kodens dimension blir $9 - 4 = 5$, så den innehåller $2^5 = 32$ ord.
Eftersom (011101100) skall vara ett ord i $\mathcal{C}$ skall summan av kolonnerna 2, 3, 4, 6 och 7 vara $(0000)^T$ och eftersom (110011001) inte skall vara det skall summan av kolonnerna 1, 2, 5, 6, 9 inte vara $(0000)^T$.
Man kan t.ex. ta $\boldsymbol{H} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{bmatrix}$.
Svar: Ett möjligt $\boldsymbol{H}$ är som ovan.

---

4) En bricka har formen av en regelbunden femhörning. Man vill smycka den med glada färger på kulor i de fem hörnen, enfärgade lister längs de fem kanterna och färger på de två ytorna. Hur många väsentligt olika (dvs så att de inte blir lika hur man än vrider brickan i rummet) färgningar finns det, om antalet tillgängliga färger är a för hörnen, b för kanterna och c för ytorna?

Lösning:
Vi använder Burnsides lemma (Thm 21.4 i Biggs).
Brickans grupp av symmetrirotationer har 10 element ($|G_x| = 2, |Gx| = 5$ för alla hörn x): Identitetselementet (bevarar alla konfigurationer, $|F(id)| = a^5b^5c^2$), fyra (andra) rotationer $\pm\frac{2\pi}{5}$, $\pm\frac{4\pi}{5}$ kring axeln vinkelrätt mot brickan genom dess mittpunkt (bevarar konfigurationer med samma färg på alla kulor och alla lister, $|F(g)| = abc^2$) och fem rotationer π kring axlar genom hörnen, i brickans plan (bevarar konfigurationer med två par av hörn, två par av kanter och ytorna likfärgade, $|F(g)| = a^3b^3c$).
Lemmat ger antalet väsentligt olika färgningar, $\frac{1}{|G|}\sum_{g\in G}|F(g)|$.
Svar: Det sökta antalet färgningar är $\frac{1}{10}(\boldsymbol{a^5b^5c^2 + 5a^3b^3c + 4abc^2})$.

---

5) (3p) Faktorisera polynomet $x^4 + 3x^3 + 4x^2 + x + 2$ i $\mathbb{Z}_5[x]$ i irreducibla faktorer.

Lösning:
Vi börjar med att söka förstagradsfaktorer, vilket enligt faktorsatsen är ekvivalent med att finna nollställen till $p(x)$. Man finner att $p(2) = 0$, så $x-2 = x+3$ är en faktor i $p(x)$. Polynomdivision ger att $p(x) = (x+3)q(x)$, där $q(x) = x^3 + 4x + 4$. Det gäller nu att faktorisera $q(x)$. Man finner att $q(2) = 0$, så $x - 2 = x + 3$ är också en faktor i $q(x)$. Polynomdivision ger $q(x) = (x+3)r(x)$, där $r(x) = x^2 + 2x + 3$. Eftersom $r(x)$ saknar nollställen i $\mathbb{Z}_5$, saknar det förstagradsfaktorer och är alltså (eftersom det är ett andragradspolynom) irreducibelt.

Svar: Den sökta faktoriseringen är $(x+3)^2(x^2+2x+3)$.

---

6) Man vill skapa ett RSA-system för kryptering med de "stora" primtalen $p = 71$ och $q = 79$, dvs parametern $n = 71 \cdot 79 = 5609$.
a) (2p) Kan man använda $e = 2723$ som krypteringsexponent? Ange i så fall motsvarande avkrypteringsexponent d.
b) (2p) Man vill ha ett litet d, men ett som innehåller minst två olika primfaktorer. Finn minsta möjliga d (du behöver inte beräkna motsvarande e).

Lösning:
a) e och d skall uppfylla $e \cdot d \equiv 1 \pmod{m}$, där $m = (p-1)(q-1) = 70 \cdot 78 = 5460$, så kravet på e är att $\text{sgd}(m, e) = 1$. Vi prövar $e = 2723$ med Euklides algoritm:
$5460 = 2 \cdot 2723 + 14,\ 2723 = 194 \cdot 14 + 7,\ 14 = 2 \cdot 7 + 0$, så $\text{sgd}(m, e) = 7$, det fungerar inte.
b) d kan användas precis om $\text{sgd}(m, d) = 1$. $m = 70 \cdot 78 = 2 \cdot 5 \cdot 7 \cdot 2 \cdot 3 \cdot 13$, så möjliga primfaktorer i d är 11, 17, 19, ... Minsta möjliga d är alltså $11 \cdot 17 = 187$.

Svar a: Nej, $e = 2723$ kan inte användas, b: Minsta möjliga $d = 187$.

---

7) Låt G vara en delgrupp till S_m, gruppen av permutationer av $\{1, 2, \ldots, m\}$, och $A_G = \{\pi \in A_n \mid \text{för något } \tau \in G : \pi(x) = \tau(x) \text{ för alla } x \in \{1, 2, \ldots, m\}\}$, där A_n är gruppen av alla jämna permutationer i S_n ($n \geq m$).
a) (2p) Visa att A_G är en delgrupp till S_n.
b) (2p) Finn alla värden $|A_G|$, A_G:s ordning, kan anta (uttryckt i $|G|$, m och n).

Lösning:
a) A_G är ändlig ($\subseteq S_n$), så den är en delgrupp till S_n om $A_G \neq \varnothing$ och $\pi, \sigma \in A_G \Rightarrow \pi\sigma \in A_G$.
Eftersom $id_m \in G$ och $id_n \in A_n$ gäller $id_n \in A_G$, så $A_G \neq \varnothing$.
Om π verkar som τ_π på $\{1, 2, \ldots, m\}$ och σ som τ_σ verkar $\pi\sigma$ som $\tau_\pi\tau_\sigma \in G$ där.
$\pi, \sigma \in A_n \Rightarrow \pi\sigma \in A_n$. Så $\pi, \sigma \in A_G \Rightarrow \pi\sigma \in A_G$. **Saken är klar**.
b) Om $\pi \in A_G$, låt den verka som $\pi_m (\in G)$ på $\{1, 2, \ldots, m\}$ och som π_{n-m} på $\{m+1, \ldots, n\}$.
Eftersom π är en jämn permutation är π_m och π_{n-m} antingen båda jämna eller båda udda (produkt, eller räkna cykler av jämn längd i vardera). Permutationerna i G är antingen alla eller precis hälften jämna (om $\tau \in G$ är udda ger $\tau\cdot$ en bijektion mellan udda och jämna i G). Om $n - m \geq 2$ finns för varje $\pi_m \in G$ precis $\frac{1}{2}(n-m)!$ möjliga val av π_{n-m} (udda eller jämna, beroende på π_m:s paritet), så $|A_G| = \frac{1}{2}(n-m)! \cdot |G|$. Om $n = m$ eller $n = m + 1$ måste π_m vara jämn, så $|A_G| = \frac{1}{2}|G|$ eller $= |G|$ (beroende på om G innehåller udda permutationer eller ej).

Svar a: Visat ovan, b: $|A_G| = \begin{cases} \frac{1}{2}(n-m)! \cdot |G| & \text{om } n \geq m+2, \\ \frac{1}{2}|G| \text{ eller } |G| & \text{om } n = m,\ m+1. \end{cases}$

---

8) (4p) Visa att för alla $n \in \mathbb{Z}$ är $69n^{81} - 123n^{23} + 54n$ delbart med 943. [$943 = 23 \cdot 41$.]

Lösning:
Det följer ur Fermats lilla sats (som i RSA-algoritmen) att för alla primtal p och alla $n, k \in \mathbb{Z}$ är $n^{k(p-1)+1} \equiv n \pmod{p}$, så $69n^{81} - 123n^{23} + 54n \equiv 0 \cdot n^{81} - 123n + 54n \equiv -69n \equiv 0 \pmod{23}$ och $69n^{81} - 123n^{23} + 54n \equiv 69n - 0 \cdot n^{23} + 54n \equiv 123n \equiv 0 \pmod{41}$. För varje $n \in \mathbb{Z}$ är alltså talet delbart med primtalen 23 och 41, därmed med deras produkt.
Saken är klar.

---

9) (5p) Visa att $f(x) = x^2 + 1$ är irreducibelt i $\mathbb{Z}_3[x]$ och finn ett primitivt element i den ändliga kropp som kan konstrueras med $\mathbb{Z}_3[x]$ och $f(x)$.

Lösning:
$f(x)$ är irreducibelt, ty om det vore reducibelt skulle det ha en linjär faktor och därmed ett nollställe i $\mathbb{Z}_3$, men $f(0) = 1, f(1) = f(2) = 2$.
Låt $F = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$ vara motsvarande kropp. I F gäller $x^2 = x^2 + 1 + 2 = 2, x^3 = x^2x = 2x, x^4 = x^3x = 2x^2 = 2 \cdot 2 = 1$, så x är inte ett primitivt element i F. Eftersom $F \setminus \{0\}$ har $8 = 2^3$ element, har vart och ett av dess element multiplikativ ordning 1,2,4 eller 8. Elementen $a = x, 2, 2x, 1$ uppfyller $a^4 = 1$, vilken har exakt 4 lösningar i F. Övriga nollskilda element i F har alltså ordning 8 och är därmed primitiva element, t.ex. $x + 1$.

Svar: $x + 1$ är ett primitivt element.

---

10) Låt $*$ vara en binär operation på mängden G sådan att
(i) $\boldsymbol{x * y \in G}$ för alla $x, y \in G$,
(ii) $\boldsymbol{(x * y) * z = x * (y * z)}$ för alla $x, y, z \in G$,
(iii) det finns ett $e \in G$ så att $\boldsymbol{e * x = x}$ för alla $x \in G$,
(iv) för varje $x \in G$ finns ett $x' \in G$ så att $\boldsymbol{x' * x = e}$ (samma e som i (iii)).
a) (1p) Vad fattas i $(i) - (iv)$ för att $(G, *)$ skall uppfylla den vanliga definitionen (som i boken) av en grupp?
b) (4p) Visa att $(G, *)$ faktiskt är en grupp, dvs att de "saknade" egenskaperna följer från $(i) - (iv)$. (Ledning: Utgå t.ex. från $e * e = e$ och $e * x' = x'$.)

Lösning:
a) Det ingår i den vanliga definitionen (Biggs 20.1) att $\boldsymbol{x * e = x}$ **och** $\boldsymbol{x * x' = e}$.
b) För godtyckligt $x \in G$ fås med $(i) - (iv)$ att $x' * (x * e) = (x' * x) * e = e * e = e = x' * x$. $(x')'*$ på båda led ger $(x')' * (x' * (x * e)) = ((x')' * x') * (x * e) = e * (x * e) = x * e$ respektive $(x')' * (x' * x) = ((x')' * x') * x = e * x = x$, så $\boldsymbol{x * e = x}$.
P.s.s. fås $x' * (x * x') = (x' * x) * x' = e * x' = x'$. $(x')'*$ på båda led ger $(x')' * (x' * (x * x')) = ((x')' * x') * (x * x') = e * (x * x') = x * x'$ respektive $(x')' * x' = e$, så $\boldsymbol{x * x' = e}$.
