

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

16 januari 2014

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 $x \circ x^{-1} = x^{-1} \circ x = e$ (inverseelement).
 (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) Banan för $x \in X$ då G verkar på X är $Gx = \{gx \mid g \in G\}$ (gx fås då g verkar på x).
 b) (1p) Om $x \in X$ har banan Gx och stabilisatorn G_x gäller $|G| = |Gx| \cdot |G_x|$.
 c) (1p) Om $(R, +, \cdot)$ är en ring är $(R, +)$ en abelsk grupp (= en kommutativ grupp).

- 3a) (1p) Karakteristiken för en kropp är det minsta $p > 0$ sådant att $\underbrace{1 + 1 + \dots + 1}_{p \text{ st}} = 0$ (om ett sådant p finns, annars är karakteristiken 0).
 b) (1p) $f(x) \in F[x]$ är irreducibelt omm $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$, medför att precis en av $g(x)$ och $h(x)$ är konstant (dvs av grad 0).
 c) (1p) Entydig faktorisering i $F[x]$ innebär att varje $f(x) \in F[x]$ är en produkt av irreducibla polynom och om $f(x) = g_1(x) \dots g_m(x) = h_1(x) \dots h_n(x)$, alla $g_i(x), h_j(x) \in F[x]$ irreducibla, så är $m = n$ och för ett $\pi \in S_n$ gäller $g_i(x) = a_i h_{\pi(i)}(x)$, $a_i \in F$ (för $i = 1, \dots, n$).

- 4a) (1p) Kodet $\mathcal{C}$ rättar e fel omm minimiavståndet $\delta \geq 2e + 1$.
 b) (1p) Om $n = p \cdot q$ (p, q primtal) bestäms d av $e \cdot d \equiv_m 1$, där $m = (p-1)(q-1)$.
 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 vet att g i gruppen G har ordning 10 och söker ordningen för g^6 .

Lösning:

Ordningen för g^6 är det minsta $k > 0$ med $(g^6)^k = g^{6k} = 1$, identitetsselementet i G .
 Enligt en känd sats är $g^n = 1$ omm $10 \mid n$ (eftersom g 's ordning är 10). $10 \mid 6k \Leftrightarrow 5 \mid k$, så det minsta $k > 0$ som uppfyller $g^{6k} = 1$ är 5. Det betyder att g^6 har ordning 5.

Svar: g^6 har ordning 5.

- 6) (3p) Givet delgruppen $G = \{id, \pi, \sigma, \pi\sigma, \sigma\pi, \pi\sigma\pi, \sigma\pi\sigma, \pi\sigma\pi\sigma\}$ till S_6 , $\pi = (12)(34)(56)$ och $\sigma = (23)$, söker vi banor och stabilisatorer för 1 och 5 då G verkar på $\{1, 2, 3, 4, 5, 6\}$.

Lösning:

$id(1) = 1$, $\pi(1) = 2$, $\sigma(1) = 1$, $\pi\sigma(1) = \pi(1) = 2$, $\sigma\pi(1) = \sigma(2) = 3$, $\pi\sigma\pi(1) = \pi(3) = 4$,
 $\sigma\pi\sigma(1) = \sigma(2) = 3$, $\pi\sigma\pi\sigma(1) = \pi(3) = 4$, så $G1 = \{1, 2, 3, 4\}$, $G_1 = \{id, \sigma\}$.
 $id(5) = 5$, $\pi(5) = 6$, $\sigma(5) = 5$, $\pi\sigma(5) = \pi(5) = 6$, $\sigma\pi(5) = \sigma(6) = 5$, $\pi\sigma\pi(5) = \pi(6) = 5$,
 $\sigma\pi\sigma(5) = \sigma(6) = 5$, $\pi\sigma\pi\sigma(5) = \pi(6) = 5$, så $G5 = \{5, 6\}$, $G_5 = \{id, \sigma, \pi\sigma\pi, \pi\sigma\pi\sigma\}$.

Svar: 1:s bana är $G1 = \{1, 2, 3, 4\}$ och dess stabilisator är $G_1 = \{id, \sigma\}$,
 5:s bana är $G5 = \{5, 6\}$ och dess stabilisator är $G_5 = \{id, \sigma, \pi\sigma\pi, \pi\sigma\pi\sigma\}$.

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

Lösning:

Vi undersöker först om (det är så lyckligt att) $f(x)$ har någon förstgradsfaktor, dvs om det har något nollställe i $\mathbb{Z}_3$. Vi finner $f(0) = 2$, $f(1) = 1 + 1 + 1 + 2 = 2$, $f(2) = 1 + 2 + 1 + 2 = 0$, så $f(x)$ har enligt faktorsatsen en faktor $x - 2 = x + 1$. Polynomdivision ger $f(x) = (x+1)(x^3 + x + 2) = (x+1)g(x)$. $x+1$ är irreducibelt. Om $g(x)$ är reducibelt har det en förstgradsfaktor. $g(0), g(1) \neq 0$ (ty $f(0), f(1) \neq 0$), $g(2) = 2 + 2 + 2 = 0$, så $g(x)$ har en faktor $x + 1$. Polynomdivision ger $g(x) = (x+1)(x^2 + 2x + 2) = (x+1)h(x)$. $h(0), h(1) \neq 0$ och $h(2) = 1 + 1 + 2 = 1$, så $h(x)$ saknar nollställe och är irreducibelt (ty av andra graden).

Svar: $f(x) = (x+1)^2(x^2 + 2x + 2)$, där faktorerna är irreducibla.

8) Vi har en linjär, binär kod med kontrollmatrisen $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ och de mottagna orden 110100, 101001, 010100. Vi söker de sända kodorden, då högst ett fel har uppstått i varje.

Lösning:

Matrismultiplikation ger $H(110100)^T = (110)^T$, H 's tredje kolonn. $H(101001)^T = (000)^T$. $H(010100)^T = (001)^T$, H 's sista kolonn. Det har alltså blivit fel i tredje, ingen respektive sista positionen.

Svar De sända kodorden var **111100, 101001 respektive 010101.**

9) (4p) Vi skall avgöra om $(H, +) = (\{\ln x \mid x \in \mathbb{Q}, x > 0\}, +)$ är en delgrupp till $(\mathbb{R}, +)$.

Lösning:

Enligt en känd sats räcker det att visa följande fyra påståenden:

1. $H \neq \emptyset$, 2. $H \subseteq \mathbb{R}$, 3. $a, b \in H \Rightarrow (a + b) \in H$ och 4. $a \in H \Rightarrow (-a) \in H$.

Vi tar dem ett i taget:

1. $0 = \ln 1 \in H$, så $H \neq \emptyset$.

2. $x \in \mathbb{Q}_+ \Rightarrow \ln x \in \mathbb{R}$, så $H \subseteq \mathbb{R}$. ($\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x > 0\}$.)

3. $\ln x + \ln y = \ln(x \cdot y)$ och $x, y \in \mathbb{Q}_+ \Rightarrow x \cdot y \in \mathbb{Q}_+$, så $a, b \in H \Rightarrow (a + b) \in H$.

4. $-\ln x = \ln \frac{1}{x}$ och $x \in \mathbb{Q}_+ \Rightarrow \frac{1}{x} \in \mathbb{Q}_+$, så $a \in H \Rightarrow (-a) \in H$.

Svar: Ja, det är en delgrupp.

10) Vi söker (a, 1p) inversen och (b, 3p) ordningen för elementet 2 i gruppen $(U_{99}, \cdot)$, där U_{99} är mängden av inverterbara element i ringen $(\mathbb{Z}_{99}, +, \cdot)$.

Lösning:

a. $2 \cdot 50 = 99 + 1 \equiv_{99} 1$, så $2 \cdot 50 = 1$ i $\mathbb{Z}_{99}$ och $2^{-1} = 50$ i U_{99} .

b. $99 = 3^2 \cdot 11$, så $|U_{99}| = \phi(99) = 3^{2-1}(3-1) \cdot 11^{1-1}(11-1) = 60$, så ordningen för 2, $o(2)$, är en delare till 60, dvs någon av 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 och 60.

Direkt ser vi att $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$.

Sedan får vi $2^{10} = 1024 = 10 \cdot 99 + 34 = 34$, $2^{12} = 2^2 \cdot 2^{10} = 4 \cdot 34 = 136 = 99 + 37 = 37$, $2^{15} = 8 \cdot 37 = 296 = 3 \cdot 99 - 1 = -1$. Då är $2^{30} = (2^{15})^2 = (-1)^2 = 1$ och enligt känd sats $o(2) \mid 30$ och alltså (eftersom $2^1, 2^2, 2^3, 2^5, 2^6, 2^{10}, 2^{15} \neq 1$) $o(2) = 30$.

Svar a: $2^{-1} = 50$, b: 2:s ordning i U_{99} är 30.

11) Vi har ringen $R = \mathbb{Z}_7[x]/(f(x))$, där $f(x) = x^3 + 5x^2 + 4x + 4$.

Vi kallar x 's ekvivalensklass för α och skall (a, 2p) uttrycka α^4 som en linjärkombination av 1, α , α^2 och (b, 2p) finna nolldelare i R .

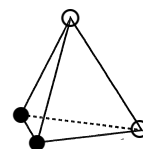
Lösning:

a. Eftersom $x^3 + 5x^2 + 4x + 4 \equiv_{(f(x))} 0$ är $\alpha^3 + 5\alpha^2 + 4\alpha + 4 = 0$, så $\alpha^3 = -2\alpha^2 - 4\alpha - 4 = 2\alpha^2 + 3\alpha + 3$ i R . Det ger $\alpha^4 = \alpha \cdot \alpha^3 = \alpha(2\alpha^2 + 3\alpha + 3) = 2\alpha^3 + 3\alpha^2 + 3\alpha = 2(2\alpha^2 + 3\alpha + 3) + 3\alpha^2 + 3\alpha = (4+3)\alpha^2 + (6+3)\alpha + 6 = 2\alpha + 6$.

b. $r \cdot s = 0$, $r, s \neq 0$ i R , betyder precis att r och s svarar mot polynom $g(x), h(x) \in \mathbb{Z}_7[x]$ 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 om $f(x)$ är reducibelt. Man finner $f(0) = 4$, $f(1) = 1 + 5 + 4 + 4 = 0$, så $(x-1) = (x+6) \mid f(x)$. Polynomdivision ger $f(x) = (x+6)(x^2 + 6x + 3)$ i $\mathbb{Z}_7[x]$, så $(\alpha+6)(\alpha^2 + 6\alpha + 3) = 0$ i R .

Svar a: $\alpha^4 = 2\alpha + 6$, b: Nolldelare är (t.ex.) $\alpha + 6$ och $\alpha^2 + 6\alpha + 3$.

12) Vi söker (a, 1p) antalet rotationssymmetrier för en regelbunden tetraeder och (b, 4p) antalet väsentligt olika maskotar i form av regelbundna tetraedrar man kan skapa genom att foga samman svarta och vita pinnar och svarta och vita kulor, då båda färgerna skall vara med på både pinnar och kulor.



Lösning:

a. Kalla gruppen av rotationssymmetrier för G och betrakta ett hörn x i tetraedern. x kan med element i G roteras till vilket som helst av de andra hörnen och inte till några andra punkter, så $|Gx| = 4$. Det finns precis tre element i G som inte flyttar x (rotationer (inklusive id) kring axeln genom x och tetraederns tyngdpunkt), så $|G_x| = 3$. Det ger $|G| = |Gx| \cdot |G_x| = 12$.

b. Vi använder Burnsidess lemma (Thm 21.4 i Biggs).

Symmetrigruppen G 's 12 element är av tre typer:

- identitetens "rotation", id ,
- 8 rotationer $\pm \frac{2\pi}{3}$ kring axlar genom ett hörn och motstående sidas tyngdpunkt, rot_{hs} ,
- 3 rotationer π kring axlar genom mittpunkter av motsatta kanter, rot_{kk} .

$|F(g)|$, antalet konfigurationer som inte ändras av g , ges av $(2^m - 2)(2^n - 2)$, där m är antalet banor för kanterna under $\langle g \rangle$'s verkan ($\langle g \rangle$ är som vanligt den cykliska delgrupp till G som genereras av g) och n motsvarande för hörnen (alla i samma bana måste ha samma färg och banornas färger kan väljas på 2^m , 2^n sätt; -2 för de otillåtna med alla banor av samma färg).

För de olika $g \in G$ blir det:

g	antal g	$ F(g) $
id	1	$(2^6 - 2)(2^4 - 2) = 62 \cdot 14$ (var och en sin egen bana, $m = 6$, $n = 4$)
rot_{hs}	8	$(2^2 - 2)(2^2 - 2) = 4$ ($m = n = 2$)
rot_{kk}	3	$(2^4 - 2)(2^2 - 2) = 14 \cdot 2$ ($m = 4$, $n = 2$)

Så antalet olika maskotar = antalet banor under G 's verkan på hela färgningarna = $= \frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{12} (62 \cdot 14 + 8 \cdot 4 + 3 \cdot 14 \cdot 2) = \frac{1}{3} (31 \cdot 7 + 8 + 3 \cdot 7) = 82$.

Svar a: 12 rotationssymmetrier, b: Det finns 82 olika sådana maskotar.

(Utan begränsningen om att använda båda färgerna blir antalet $\frac{1}{12} (64 \cdot 16 + 8 \cdot 4 \cdot 4 + 3 \cdot 16 \cdot 4) = 112$.)

13) Vi har ett RSA-system med $n = 1147 (= 31 \cdot 37)$, $e = 271$. Vi söker (a, 1p) motsvarande d och (b, 4p) antalet heltal x , $0 \leq x \leq 1146$, med $E(x) = x$.

Lösning:

a. d uppfyller $e \cdot d \equiv_m 1$, där $m = (31 - 1)(37 - 1) = 30 \cdot 36 = 1080$.

Med Euklides algoritm: $1080 = 4 \cdot 271 - 4$, $271 = 68 \cdot 4 - 1$, så $1 = -271 + 68 \cdot 4 = -271 + 68(-1080 + 4 \cdot 271) = -68 \cdot 1080 + 271 \cdot 271$.

Vi får alltså $d = e = 271$.

b. Vi söker antalet lösningar $0 \leq x \leq 1146$ till ekvationen $x^{271} \equiv x \pmod{1147}$, dvs antalet $x \in \mathbb{Z}_{1147}$ med $x^{271} = x$. Eftersom $1147 = 31 \cdot 37$ och 31 och 37 är relativt prima, är $\mathbb{Z}_{1147} \approx \mathbb{Z}_{31} \times \mathbb{Z}_{37}$ och det sökta antalet är antalet par $(y, z) \in \mathbb{Z}_{31} \times \mathbb{Z}_{37}$ där $y^{271} = y$ och $z^{271} = z$ (dvs $y(y^{270} - 1) = 0$ och $z(z^{270} - 1) = 0$).

Eftersom $\phi(31) = 30$ är $y^{270} = (y^{30})^9 = 1$ för alla $y \neq 0$ i $\mathbb{Z}_{31}$ och $y^{271} = y$ för **alla** $y \in \mathbb{Z}_{31}$. $\phi(37) = 36$ och $z^{270} = (z^{36})^7 z^{18} = z^{18}$ för alla $z \neq 0$ i $\mathbb{Z}_{37}$, så lösningar till z -ekvationen är dels 0, dels alla lösningar till $z^{18} = 1$ i $\mathbb{Z}_{37}$. Eftersom $\mathbb{Z}_{37}$ är en ändlig kropp (37 är ju ett primtal) är $\mathbb{Z}_{37} \setminus \{0\}$ en cyklisk grupp med 36 element. Eftersom $18|36$ finns precis 18 olika lösningar till $z^{18} = 1$ (Biggs 20.9). Antalet $z \in \mathbb{Z}_{37}$ med $z(z^{270} - 1) = 0$ är alltså $1 + 18 = 19$. Det sökta antalet par är då $31 \cdot 19 = 589$,

Svar a: $d = 271$, b: Det finns 589 sådana x .