

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

24 oktober 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 $x \in G$ (identitetsselement) 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 $m \mid s$ (känd sats).
 c) (1p) Antalet delgrupper av ordning m är 1 om $m \mid n$, annars 0.
-

- 2a) (1p) Banan Gx består av de $y \in X$ som något $g \in G$ tar x till, $Gx = \{gx \mid g \in G\}$.
 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) $f(x) \in F[x]$ 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).
 b) (1p) Om n är en (positiv) potens av ett primtal finns precis en kropp av ordning n , för övriga n finns ingen, så svaret: 1, 1, 1, 0, 0, 0, 1.
 c) (1p) Då $k(x)$ är irreducibelt är $F[x]/(k(x))$ en kropp.
-

- 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) 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) H och K är delgrupper till G och $|H| = |K| = p$, ett primtal. Vi skall visa att $H = K$ eller $H \cap K = \{1\}$.
-

Lösning:

$H \cap K$ är en delgrupp till H (ty $H \cap K \subseteq H$, $1 \in H \cap K$, så $H \cap K \neq \emptyset$, och $x, y \in H \cap K \Rightarrow (x, y \in H$ och $x, y \in K) \Rightarrow (xy \in H$ och $xy \in K) \Rightarrow xy \in H \cap K$). Det ger att $|H \cap K|$ delar $|H| = p$, dvs $|H \cap K| = 1$ eller p (p primtal). I det förra fallet är $H \cap K = \{1\}$ (ty $1 \in H \cap K$) och i det andra fallet är $H \cap K = H$ och eftersom $|H| = |K|$ är då $H = K$. **Saken är klar.**

- 6) (3p) $G = U_{15}$, de inverterbara elementen i ringen $(\mathbb{Z}_{15}, +, \cdot)$, verkar på mängden $X = \mathbb{Z}_{15}$ med ringens multiplikation. Vi söker bana och stabilisator för elementen 3 och 5 i X .
-

Lösning:

$G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (alla $x \in \mathbb{Z}$, $1 \leq 15$ med $\text{sgd}(x, 15) = 1$) och multiplikation i $\mathbb{Z}_{15}$ ger $G3 = \{3, 6, 12, 6, 9, 3, 9, 12\} = \{3, 6, 9, 12\}$ och $G3 = \{1, 11\}$ ($g \in G$ med $g \cdot 3 = 3$ i $\mathbb{Z}_{15}$). På samma sätt fås $G5 = \{5, 10, 5, 5, 10, 10, 5, 10\} = \{5, 10\}$ och $G5 = \{1, 4, 7, 13\}$.

Svar: Banorna är $G3 = \{3, 6, 9, 12\}$, $G5 = \{5, 10\}$ och stabilisatorerna är $G_3 = \{1, 11\}$, $G_5 = \{1, 4, 7, 13\}$.

7) (3p) Vi vill faktorisera $f(x) = x^5 + 3x^4 + x^3 + x^2 + 6x + 1 \in \mathbb{Z}_7[x]$ i irreducibla faktorer.

Lösning:

Vi undersöker först om (det är så lyckligt att) $f(x)$ har någon förstgradsfaktor, dvs om det har något nollställe i $\mathbb{Z}_7$. Vi finner $f(0) = 1$, $f(1) = 1 + 3 + 1 + 1 + 6 + 1 = 6$, men

$f(2) = 4 + 6 + 1 + 4 + 5 + 1 = 0$, så $f(x)$ har enligt faktorsatsen en faktor $x - 2 = x + 5$.

Polynomdivision ger $f(x) = (x + 5)(x^4 + 5x^3 + 4x^2 + 2x + 3) = (x + 5)g(x)$.

Vi söker nollställena hos $g(x)$. $g(0), g(1) \neq 0$ (ty $f(0), f(1) \neq 0$), $g(2) = 2 + 5 + 2 + 4 + 3 = 2$, $g(3) = 4 + 2 + 1 + 6 + 3 = 2$, $g(4) = g(-3) = 4 - 2 + 1 - 6 + 3 = 0$, så $g(x)$ har en faktor $x - 4 = x + 3$. Polynomdivision ger $g(x) = (x + 3)(x^3 + 2x^2 + 5x + 1) = (x + 3)h(x)$. $h(0), \dots, h(3) \neq 0$, $h(4) = h(-3) = -6 + 4 - 1 + 1 = 5$, $h(5) = h(-2) = -1 + 1 - 3 + 1 = 5$, $h(6) = h(-1) = -1 + 2 - 5 + 1 = 4$, så $h(x)$ saknar nollställena och är, liksom faktorerna $x + 3$ och $x + 5$, irreducibelt (ty det är av grad ≤ 3).

Svar: $f(x) = (x + 3)(x + 5)(x^3 + 2x^2 + 5x + 1)$, där faktorerna är irreducibla.

8) (3p) Vi söker ett $x \in \mathbb{Z}_+$ sådant att för alla $a, b \in \mathbb{Z}$ gäller att $b \equiv_{447} a^{143} \Leftrightarrow a \equiv_{447} b^x$.

Lösning:

Vi känner igen ett RSA-system med $n = 447$, $e = 143$ och söker d (med gängse beteckningar). $447 = 3 \cdot 149$ (båda primtal), så $m = 2 \cdot 148 = 2^3 \cdot 37 = 296$. Vi söker x med $143x \equiv_{296} 1$:

Euklides algoritmen, $296 = 143 \cdot 2 + 10$, $143 = 10 \cdot 14 + 3$, $10 = 3 \cdot 3 + 1$ (så $e = 143$ fungerar) och $1 = 10 - 3 \cdot (143 - 14 \cdot 10) = -3 \cdot 143 + 43 \cdot (296 - 2 \cdot 143) = 43 \cdot 296 - 89 \cdot 143 = (43 - 143) \cdot 296 + (296 - 89) \cdot 143 = -100 \cdot 296 + 207 \cdot 143$, så vi kan ta $(d =) x = 207$.

Svar: Ett möjligt värde är $x = 207$.

(Det räcker att $143x \equiv_{148} 1$ ($148 = \text{mcm}(2, 148)$). Det ger en annan möjlighet, $x = 59$.)

9) (4p) Vi skall visa att 1 är det enda inverterbara elementet i en ring $(R, +, \cdot)$ med egenskapen att $a^2 = a$ för alla $a \in R$ (en boolesk ring).

Lösning:

Om a är inverterbart ger $a^2 = a$ (som ju gäller för alla $a \in R$) att $a = a^{-1}a^2 = a^{-1}a = 1$.

$1 \in R$ är också inverterbart, $1^{-1} = 1$, ty $1 \cdot 1 = 1$.

Saken är klar.

10) $k(x) = x^3 + 2x^2 + 4x + 4 \in \mathbb{Z}_5[x]$ och $F = \mathbb{Z}_5[x]/(k(x))$. Vi skall (a, 2p) finna $|F|$ och visa att $(F, +, \cdot)$ är en kropp och (b, 2p) finna ett $t \in F$ med $(\alpha^2 + 2\alpha + 2) \cdot t = 3\alpha^2 + 2\alpha + 1$, där α är restklassen med polynomet x .

Lösning:

a. Elementen i F består av alla polynom i $\mathbb{Z}_5[x]$ som ger samma rest av grad ≤ 2 vid division med $k(x)$. Restklasserna motsvarar entydigt dessa rester, så de är $5^3 = 125$ st.

$(F, +, \cdot)$ är en kropp omm $k(x)$ är irreducibelt (känd sats), vilket det är omm det saknar nollställe i $\mathbb{Z}_5$ (eftersom dess grad är 3). Man finner $k(0) = 4$, $k(1) = 1 + 2 + 4 + 4 = 1$, $k(2) = 3 + 3 + 3 + 4 = 3$, $k(3) = k(-2) = -3 + 3 - 3 + 4 = 1$, $k(4) = k(-1) = -1 + 2 - 4 + 4 = 1$, alla $\neq 0$. F är alltså en kropp.

b. För att finna t söker vi först $(\alpha^2 + 2\alpha + 2)^{-1}$ med hjälp av Euklides algoritmen:

Polynomdivision ger $k(x) = f(x) \cdot x + (2x + 4)$ ($f(x) = x^2 + 2x + 2$) och $f(x) = (2x + 4) \cdot 3x + 2$, så $2 = f(x) - 3x \cdot (k(x) - x \cdot f(x)) = (3x^2 + 1) \cdot f(x) - 3x \cdot k(x)$ och $(3\alpha^2 + 1) \cdot f(\alpha) = 2$ i F .

Multiplikation med 3 ger att $(\alpha^2 + 2\alpha + 2)^{-1} = 4\alpha^2 + 3$, så $t = (4\alpha^2 + 3)(3\alpha^2 + 2\alpha + 1) = 2\alpha^4 + 3\alpha^3 + 3\alpha^2 + \alpha + 3 = 2 \cdot (4\alpha + 3) + 3 \cdot (3\alpha^2 + \alpha + 1) + 3\alpha^2 + \alpha + 3 = 2\alpha^2 + 2\alpha + 2$ (där vi använt att $k(\alpha) = 0 \Rightarrow \alpha^3 = 3\alpha^2 + \alpha + 1$, så $\alpha^4 = 3\alpha^3 + \alpha^2 + \alpha = 3 \cdot (3\alpha^2 + \alpha + 1) + \alpha^2 + \alpha = 4\alpha + 3$).

Svar a: $|F| = 5^3 = 125$, F är enligt ovan en kropp, **b:** $t = 2\alpha^2 + 2\alpha + 2$.

11) Då H är en delgrupp till gruppen G låter vi $K = \{g \in G \mid gxg^{-1} \in H \Leftrightarrow x \in H\}$ och skall (a, 2p) visa att K är en delgrupp till G och (b, 2p) finna K_1, K_2 svarande mot delgrupperna $H_1 = \{(1), (13)\}$ och $H_2 = \{(1), (12)(34), (13)(24), (14)(23)\}$ till gruppen $G = \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\} \subset S_4$.

Lösning:

a. Räcker att visa: 1. $K \neq \emptyset$, 2. $k, k' \in K \Rightarrow kk' \in K$ och 3. $k \in K \Rightarrow k^{-1} \in K$ (känd sats).

1. $1 \in K$, ty $1x1^{-1} = x$ för alla $x \in G$. Alltså $K \neq \emptyset$,

2. Om $k, k' \in K$: $x \in H \Rightarrow k'xk'^{-1} \in H \Rightarrow (kk')x(kk')^{-1} = k(k'xk'^{-1})k^{-1} \in H$
och $(kk')x(kk')^{-1} = k(k'xk'^{-1})k^{-1} \in H \Rightarrow k'xk'^{-1} \in H \Rightarrow x \in H$, så $kk' \in K$,

3. Om $k \in K$: $k(k^{-1}x(k^{-1})^{-1})k^{-1} = x \in H \Leftrightarrow k^{-1}x(k^{-1})^{-1} \in H$, så $k^{-1} \in K$.

(I 3. användes villkoret för $k \in K$ med $k^{-1}x(k^{-1})^{-1}$ i stället för x)

Saken är klar.

b. Tabellen visar gxg^{-1} med rad g , kolumn x .

	x							
	(1)	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(13)	(24)
(1)	(1)	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(13)	(24)
(1234)	(1)	(1234)	(13)(24)	(1432)	(14)(23)	(12)(34)	(24)	(13)
(13)(24)	(1)	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(13)	(24)
g (1432)	(1)	(1234)	(13)(24)	(1432)	(14)(23)	(12)(34)	(24)	(13)
(12)(34)	(1)	(1432)	(13)(24)	(1234)	(12)(34)	(14)(23)	(24)	(13)
(14)(23)	(1)	(1432)	(13)(24)	(1234)	(12)(34)	(14)(23)	(24)	(13)
(13)	(1)	(1432)	(13)(24)	(1234)	(14)(23)	(12)(34)	(13)	(24)
(24)	(1)	(1432)	(13)(24)	(1234)	(14)(23)	(12)(34)	(13)	(24)

(Konjugering av permutationer, så elementen i tabellen är enkla att finna. $\pi(a_1 a_2 \dots) \pi^{-1} = (\pi(a_1) \pi(a_2) \dots)$.)

K_1 innehåller de $g \in G$ vars rad har (1) och (13) (H_1 :s element) i deras kolumner och bara i dem. Tydligt $K_1 = \{(1), (13)(24), (13), (24)\}$.

På samma sätt ses att $K_2 = G$ (K_2 är en union av hela konjugatklasser från G).

Svar a: Visat ovan, b: $K_1 = \{(1), (13)(24), (13), (24)\}$ och $K_2 = G$.

12) (5p) Ett (misslyckat försök till) RSA-system använder parametrarna $n = 899 (= 29 \cdot 31)$ och $e = 484$. Vi söker antalet $x \in \mathbb{Z}_n$ som krypteras som sig själva (dvs uppfyller $E(x) = x$).

Obs! De givna n och e är inte tillåtna som parametrar i ett RSA-system, eftersom $\text{sgd}(e, m)$ inte blir 1. Uppgiften går ändå att lösa med $E(x) = x^{484}$ i $\mathbb{Z}_{899}$.

Lösning:

Det gäller antalet $x \in \mathbb{Z}_{899}$ som uppfyller $x^{484} = x$, dvs $x(x^{483} - 1) = 0$.

Enligt Kinesiska restsatsen är $x^{484} = x$ i $\mathbb{Z}_{899}$ omm $x^{484} = x$ i både $\mathbb{Z}_{29}$ och $\mathbb{Z}_{31}$ ($899 = 29 \cdot 31$).

I $\mathbb{Z}_{29}$: $x(x^{483} - 1) = 0$ omm $x = 0$ eller $x^{483} = 1$ (ty 29 är ett primtal). Om $x \neq 0$ är $x^{28} = 1$ i $\mathbb{Z}_{29}$ (ty $(\mathbb{Z}_{29} \setminus \{0\}, \cdot)$ är en grupp av ordning 28). $483 = 17 \cdot 28 + 7$, så $x^{483} = x^7$ och det finns 8 olika $x \in \mathbb{Z}_{29}$ med $x^{484} = x$ ($x = 0$ och de 7 (enligt känd sats, $7 \mid 28$) i den cykliska $(\mathbb{Z}_{29} \setminus \{0\}, \cdot)$ med $x^7 = 1$).

I $\mathbb{Z}_{31}$ fås på samma sätt 4 olika x med $x(x^{483} - 1) = 0$ ($x = 0$ och 3 olika lösningar till $x^3 = 1$ ($483 = 16 \cdot 30 + 3$, $3 \mid 30$)).

Lösningar i $\mathbb{Z}_{899}$ svarar bijectivt mot par av lösningar i $\mathbb{Z}_{29}$ och $\mathbb{Z}_{31}$, så de är $8 \cdot 4 = 32$ st.

Svar: 32 st $x \in \mathbb{Z}_{899}$ krypteras som sig själva.

(Nämigen 0, 1, 25, 36, 87, 94, 248, 284, 310, 315, 335, 342, 372, 373, 377, 397, 435, 459, 465, 552, 558, 625, 645, 683, 687, 745, 749, 806, 807, 837, 842 och 893.)

(Att de givna (n, e) inte var tillåtna RSA-parametrar berodde på slarv, flera x med $E(x) = x$ blir det t.ex. också med (de tillåtna) $n = 899$, $e = 127$ (105 st sådana x).)

13) Vi söker antalet väsentligt olika färgningar av en kubs hörn, med högst k färger och utan likfärgade grannhörn. Vi har fått reda på att det kromatiska polynomet för kubgrafen är $P_{\text{kub}}(k) = k(k-1)(k^6 - 11k^5 + 55k^4 - 159k^3 + 282k^2 - 290k + 133)$.

Lösning:

Vi använder Burnsidess lemma och behöver $|F(g)|$ för varje (typ av) symmetrirotation g .

typ av g	g :s permutation av kubens hörn	antal g	$ F(g) $
id	$[1^8]$	1	$P_{\text{kub}}(k)$
rot $hh \pm \frac{2\pi}{3}$	$[1^2 3^2]$	8	$k(k-1)^3$
rot $kk \pi$	$[2^4]$	6	0
rot $ss \pm \frac{\pi}{2}$	$[4^2]$	6	0
rot $ss \pi$	$[2^4]$	3	$k(k-1)(k^2 - 3k + 3)$

("rot xxv ": rotation vinkeln v kring en axel genom kubens och sidors(s), kanters(k) eller hörns(h) medelpunkter.)

$|F(g)|$: antalet g -invarianta (dvs samma färg på alla hörn i samma cykel i g :s permutation) färgningar.

$F(id)$ är alla graffärgningar av kubgrafen, $P_{\text{kub}}(k)$ st.

Andra raden: inga grannar i samma hörncykel, så vi kan betrakta det som att vi hörnfärgar grafen av g :s cykler, med kanter mellan dem som har några grannar. Här ett träd.

Tredje och fjärde raderna: minst en cykel innehåller grannar, så ingen tillåten färgning.

Sista raden: g :s cykler innehåller inte grannar och grafen av dem (som ovan) är en C_4 , med kromatiskt polynom $k(k-1)(k^2 - 3k + 3)$ (med rekursionsformeln, fall-för-fall-analys eller uttrycket från föreläsningen).

Lemmat ger antalet färgningar: $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24} (P_{\text{kub}}(k) + 8k(k-1)^3 + 3k(k-1)(k^2 - 3k + 3)) = \frac{1}{24} k(k-1)(k^6 - 11k^5 + 55k^4 - 159k^3 + 293k^2 - 315k + 150)$

Svar: Det sökta antalet är $\frac{1}{24} k(k-1)(k^6 - 11k^5 + 55k^4 - 159k^3 + 293k^2 - 315k + 150)$.

($k = 0, 1, 2, 3, 4, 5$ ger 0, 0, 1, 15, 157, 1375 väsentligt olika färgningar.)