

## Lösningar tentan SF1662 DISKRET MATEMATIK, 2 juni 2016

Tryckfel kan förekomma.

1) (3p) Vi ska avgöra om  $189 \in \mathbb{Z}_{817}$  är inverterbart och i så fall finna inversen.

**Lösning:** Euklides algoritim:

$$\begin{cases} 817 = 189 \cdot 4 + 61, \\ 189 = 61 \cdot 3 + 6, \\ 61 = 6 \cdot 10 + 1 \end{cases} \quad \text{så } \text{sgd}(817, 189) = 1 \text{ och } \begin{cases} 1 = 61 - 10(189 - 3 \cdot 61) = \\ = -10 \cdot 189 + 31(817 - 4 \cdot 189) = \\ = 31 \cdot 817 - 134 \cdot 189. \end{cases}$$

$189 \in \mathbb{Z}_{817}$  är alltså inverterbart och  $189^{-1} = -134 = 683 \in \mathbb{Z}_{817}$ .

**Svar:**  $189 \in \mathbb{Z}_{817}$  är inverterbart.  $189^{-1} = 683$  i  $\mathbb{Z}_{817}$ .

2) (3p) Vi ska visa att  $1 \cdot 4 + 2 \cdot 7 + \dots + n(3n+1) = n(n+1)^2$  för alla  $n \in \mathbb{Z}_+$ .

**Lösning:** Låt  $P_n$  vara det givna påståendet. Vi visar  $P_n$  för alla  $n \in \mathbb{Z}_+$  med induktion.

**Bas:**  $P_1$  är sant, ty  $VL_1 = 1 \cdot 4 = 4$ ,  $HL_1 = 1(1+1)^2 = 4$ .

**Steg:** Antag  $P_k$  för ett godtyckligt  $k \in \mathbb{Z}_+$ , dvs  $1 \cdot 4 + 2 \cdot 7 + \dots + k(3k+1) = k(k+1)^2$ .

Då är  $VL_{k+1} = VL_k + (k+1)(3(k+1)+1) \stackrel{!}{=} k(k+1)^2 + (k+1)(3k+4) =$   
 $= (k+1)(k(k+1) + (3k+4)) = (k+1)(k^2 + 4k + 4) = (k+1)((k+2)^2) = HL_{k+1}.$

Så  $P_1$  är sant och  $P_k \Rightarrow P_{k+1}$  för alla  $k \in \mathbb{Z}_+$ . **Saken är klar** (enligt induktionsprincipen).

3) (3p) Vi söker antalet funktioner  $f : \{a, b, c, d, e\} \rightarrow \{1, 2, 3, \dots, 9\}$  som antar precis 4 olika värden, varav minst ett är ett jämnt tal.

**Lösning:** Precis två av  $a, b, \dots, e$  ska tas till samma värde. Dessa två kan väljas på  $\binom{5}{2} = 10$  sätt (alternativt:  $S(5, 4) = 10$ ). Paret och de övriga tre ska ges olika värden bland  $1, 2, \dots, 9$ . Det kan ske på  $(9)_4 = \frac{9!}{(9-4)!}$  sätt, men från dem skall  $(5)_4 = \frac{5!}{(5-4)!} = 5!$  (antalet fall då bara udda värden tas) dras (additionsprincipen).

Det sökta antalet funktioner blir  $10 \cdot (\frac{9!}{5!} - 5!)$  (multiplikationsprincipen).

**Svar:** Antalet sådana funktioner är  $10 \cdot (\frac{9!}{5!} - 5!) = 29\,040$ .

4) (3p) Ett RSA-system har  $n = 247 (= 13 \cdot 19)$ .

Vi söker vad meddelandet 3 krypteras som, då 10 krypteras som 212 och 25 som 233.

**Lösning:**  $E(10) = 212$ , dvs  $10^e \equiv 212 \pmod{247}$  och  $E(25) = 233 \equiv 25^e \pmod{247}$ .

Eftersom  $10 \cdot 25 \equiv 3 \pmod{247}$  är

$E(3) \equiv 3^e \equiv 10^e 25^e \equiv 212 \cdot 233 \equiv (-35)(-14) = 490 \equiv 243 \pmod{247}$ .

$0 \leq 243 < 247$ , så  $E(3) = 243$ .

**Svar:** 3 krypteras som 243.

5) (3p)  $G = (V, E)$  är en graf,  $\chi(G)$  dess kromatiska tal. Vi ska visa att  $|E| \geq \binom{\chi(G)}{2}$ .

**Lösning:** Betrakta en minimal färgning av grafen(s hörn), dvs en med precis  $\chi(G)$  färger. För varje par av dem måste det finnas en kant mellan ett par av hörn med de färgerna, annars kunde alla hörn med någon av dem ges samma färg. Det innebure en färgning med färre än  $\chi(G)$  färger, men sådana finns inte. Antalet kanter måste alltså vara minst antalet par av färger bland de  $\chi(G)$  st,  $\binom{\chi(G)}{2}$ . **Saken är klar.**

**6)**  $\pi \in S_{11}$  ges av att  $\pi(1) = 3, \pi(2) = 10, \pi(3) = 7, \pi(4) = 1, \pi(5) = 11, \pi(6) = 8, \pi(7) = 4, \pi(8) = 6, \pi(9) = 9, \pi(10) = 2, \pi(11) = 5$ . Vi skall (a, 1p) ge  $\pi$  i cykelnotation och finna  $\pi$ 's ordning,  $o(\pi)$ , (b, 1p) avgöra om  $\pi$  är jämn eller udda och (c, 2p) finna antalet olika  $\sigma \in S_{11}$  sådana att  $\pi$  och  $\sigma\pi$  är konjugerade.

**Lösning:** a.  $\pi(1) = 3, \pi(3) = 7, \pi(7) = 4, \pi(4) = 1, \dots$  ger  $\pi = (1\ 3\ 7\ 4)(2\ 10)(5\ 11)(6\ 8)$ .

Dess ordning är mgm av cykellängderna,  $o(\pi) = \text{mgm}(4, 2, 2, 2, 1) = 4$ .

b.  $\pi$  har ett jämnt antal (4) av cykler av jämn längd, så  $\pi$  är jämn.

c. Antalet sådana  $\sigma$  är lika med antalet  $\tau \in S_{11}$  som är konjugerade med  $\pi$ , dvs som har cykelstruktur  $[12^3 4]$  (ty för varje  $\pi, \tau \in S_{11}$  finns precis ett  $\sigma \in S_{11}$  med  $\tau = \sigma\pi$  (nämligen  $\sigma = \tau\pi^{-1}$ )). Det antalet är  $\binom{11}{4, 2, 2, 2, 1} \cdot 3! \cdot \frac{1}{3!} = \frac{11!}{4! \cdot 2^3} = \frac{11!}{192}$  (Dela upp på cyklerna,  $k$  element kan bilda  $(k-1)!$  st olika  $k$ -cykler och de tre 2-cyklerna är inte "särskiljbara", alternativt kan man använda att antalet permutationer i  $S_n$  av typ  $[1^{\alpha_1} 2^{\alpha_2} \dots]$  är  $\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots \alpha_1! \alpha_2! \dots}$ .)

**Svar a:**  $\pi = (1\ 3\ 7\ 4)(2\ 10)(5\ 11)(6\ 8)$  och  $o(\pi) = 4$ , **b:**  $\pi$  är en jämn permutation, **c:** Antalet sådana  $\sigma$  är  $\frac{11!}{4 \cdot 2^3 \cdot 3!} = \frac{11!}{192} (= 207\ 900)$ .

**7)** (4p)  $\mathcal{R}$  är en binär relation på mängden  $X$ , och 1. för varje  $x \in X$  finns ett  $y \in X$  med  $x\mathcal{R}y$ , 2. för alla  $x, y, z \in X$  gäller  $(x\mathcal{R}y \text{ och } z\mathcal{R}y) \Rightarrow z\mathcal{R}x$ . Vi ska avgöra vilka av reflexivitet, symmetri och transitivitet som  $\mathcal{R}$  kan och vilka  $\mathcal{R}$  måste ha.

**Lösning:**

**Reflexivitet:** Låt  $x \in X$ . Enligt 1. finns  $y \in X$  med  $x\mathcal{R}y$ . 2. (med  $z = x$ ) ger  $x\mathcal{R}x$ .

1. och 2. ger alltså att  $x\mathcal{R}x$  för alla  $x \in X$ , så  $\mathcal{R}$  måste vara reflexiv.

**Symmetri:** Låt  $x, y \in X$  och  $x\mathcal{R}y$ . Reflexivitet ger  $y\mathcal{R}y$ , så 2. (med  $z = y$ ) ger  $y\mathcal{R}x$ .

1. och 2. ger alltså att  $x\mathcal{R}y \Rightarrow y\mathcal{R}x$  för alla  $x, y \in X$ , så  $\mathcal{R}$  måste vara symmetrisk.

**Transitivitet:** Låt  $x, y, z \in X$  och  $x\mathcal{R}y, y\mathcal{R}z$ . Symmetri ger  $z\mathcal{R}y$ , så 2. ger  $x\mathcal{R}z$ .

1. och 2. ger att  $(x\mathcal{R}y \text{ och } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$  för alla  $x, y, z \in X$ , så  $\mathcal{R}$  måste vara transitiv.

För godtyckligt  $X$  uppfyller den ständigt sanna relationen ( $x\mathcal{R}y$  för alla  $x, y \in X$ ) både 1. och

2. Det finns alltså  $\mathcal{R}$  som uppfyller dem, så  $\mathcal{R}$  kan ha alla egenskaperna.

**Svar:**  $\mathcal{R}$  både kan och måste ha alla tre egenskaperna.

**8)** (4p) I sex par (en kvinna, en man i varje) ska alla ha varsin av sex olika sorters hattar, två av varje sort. Alla män ska ha olika sorters hattar och likaså alla kvinnor. Vi söker (a, 1p) antalet sätt att fördela hattarna och (b, 3p) antalet sätt om dessutom de i samma par måste ha olika sorters hattar.

**Lösning:** a. 6 olika sorters hattar kan fördelas bland 6 kvinnor (bijektion 6-mängd  $\rightarrow$  6-mängd) på  $6!$  sätt, likaså för männen. Totalt (multiplikationsprincipen)  $6!^2$  sätt.

b. Fortfarande kan kvinnornas hattar fördelas på  $6!$  sätt.

Om vi för  $\pi \in S_6$  låter  $\pi(i) = j$  betyda att mannen i par  $i$  har samma sorts hatt som kvinnan i par  $j$ , är antalet sätt att sedan fördela männens hattar lika med antalet av de  $\pi \in S_6$  (permutation, ty alla män ska ha olika sorters hattar) som uppfyller  $\pi(i) \neq i$  för  $i = 1, 2, \dots, 6$ . Vi bestämmer det antalet med principen om inklusion/exklusion.

Låt  $A_i = \{\pi \in S_6 \mid \pi(i) = i\}$ . Då söker vi  $|S_6 \setminus (A_1 \cup A_2 \cup \dots \cup A_6)|$ , som enligt principen är  $\sum_{k=0}^6 (-1)^k \alpha_k$ , där  $\alpha_0 = |S_6|$  och  $\alpha_k = \sum_{1 \leq i_1 < \dots < i_k \leq 6} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|$  för  $k = 1, 2, \dots, 6$ . Så  $\alpha_0 = 6!$  och  $\alpha_k = \binom{6}{k} \cdot (6-k)! = \frac{6!}{k!}$  för  $k = 1, 2, \dots, 6$  (antalet termer  $\cdot$  varje terms storlek). Det ger  $\sum_{k=0}^6 (-1)^k \alpha_k = 720 - 720 + 360 - 120 + 30 - 6 + 1 = 265$ .

(Alternativt, antalen i  $S_6$  utan 1-cykler,  $[2^3] : 15, [3^2] : 40, [24] : 90, [6] : 120$ , och  $15 + 40 + 90 + 120 = 265$ .)

Antalet fördelningar är alltså (multiplikationsprincipen)  $6! \cdot 265$ .

**Svar a:** På  $6!^2 (= 518\ 400)$  sätt, **b:** På  $6! \cdot 265 (= 190\ 800)$  sätt.

(Detta med den avsedda tolkningen, att hattar av samma sort betraktas som identiska.

Eftersom texten kunde förstås annorlunda godtas även den motsatta tolkningen, med svaren  $2^6 \cdot$  dem ovan.)

9) Vi ska visa att (a, 2p)  $2^r - 1 \mid 2^{rs} - 1$  för alla  $r, s \in \mathbb{N}$  och (b, 3p) om  $m \in \mathbb{N}$  är udda gäller  $m \mid 2^n - 1$  för något  $n = 1, 2, \dots, m$ .

---

**Lösning:** a.  $2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \dots + 2^r + 1)$ .

(Jfr.  $x^s - 1 = (x - 1)(x^{s-1} + x^{s-2} + \dots + 1)$ , alt. använd induktion över  $s$ .)

**a-saken är klar.**

b.  $2 \in U_m$ , de inverterbara elementen i  $\mathbb{Z}_m$  (ty  $m$  är udda). Det betyder att  $2^{|U_m|} = 1$  i  $\mathbb{Z}_m$ , dvs att  $m \mid 2^{|U_m|} - 1$ .  $1 \leq |U_m| < |\mathbb{Z}_m| = m$  ( $0 \in \mathbb{Z}_m \setminus U_m$ ) ger påståendet (t.o.m. det lite starkare att det räcker med  $n = 1, 2, \dots, m - 1$ ).

**b-saken är klar.**

(Alt. med postfacksprincipen. Antag motsatsen, att division av  $2^n - 1$  med  $m$  ger rest  $\neq 0$  för alla  $n = 1, 2, 3, \dots, m$ .

Då finns två lika rester, säg för  $2^s - 1$  och  $2^t - 1$ , där  $1 \leq s < t \leq m$ , så  $m \mid (2^t - 1) - (2^s - 1) = 2^t - 2^s = 2^s(2^{t-s} - 1)$ , så ( $m$  är udda)  $m \mid 2^{t-s} - 1$ . Men  $1 \leq t - s < m$ , så det motsäger antagandet.)

---

10)  $G$  är en grupp och  $H, K, L$  är ändliga delgrupper till  $G$ . Vi ska visa att (a, 1p)  $H \cap K$  är en delgrupp till  $G$ , (b, 1p)  $H \cup K$  inte behöver vara en delgrupp till  $G$  och (c, 3p)  $|H \cup K \cup L|$  är delbart med  $|H \cap K \cap L|$ .

---

**Lösning:** a.  $H \cap K \neq \emptyset$ , ty identiteten 1 tillhör båda.  $x, y \in H \cap K \Rightarrow (x, y \in H \text{ och } x, y \in K) \Rightarrow (xy \in H \text{ och } xy \in K) \Rightarrow xy \in H \cap K$ . Eftersom  $H, K$ , och därmed  $H \cap K$ , är ändliga, ger en känd sats att  $H \cap K$  är en delgrupp till  $G$ .

**a-Saken är klar.**

b. Med  $G = (\mathbb{Z}_6, +)$  och  $H = \{0, 2, 4\}$ ,  $K = \{0, 3\}$  är  $H, K$  delgrupper till  $G$ , men inte  $H \cup K = \{0, 2, 3, 4\}$  ( $|H \cup K| = 4 \nmid 6 = |G|$ , alt  $2, 3 \in H \cup K$ , men  $2 + 3 = 5 \notin H \cup K$ ).

**b-Saken är klar.**

c. Enligt a. är  $H \cap K$  och  $L$  delgrupper till  $G$ , så enligt a. igen är  $H \cap K \cap L$  också det. Den är alltså delgrupp till alla grupperna  $H, K, L, H \cap K, H \cap L, K \cap L$ . Enligt Lagranges sats är  $H \cap K \cap L$ s ordning en delare till alla dessa gruppers ordningar.

Enligt satsen om inklusion och exklusion är  $|H \cup K \cup L| = |H| + |K| + |L| - (|H \cap K| + |H \cap L| + |K \cap L|) + |H \cap K \cap L|$  och eftersom alla termer i HL är delbara med  $|H \cap K \cap L|$ , är också  $|H \cup K \cup L|$  det.

**c-Saken är klar.**

---