

**Lösningar tentan SF1662 DISKRET MATEMATIK, CL1,
28 maj 2012**

Tryckfel kan förekomma.

1) Vi skall (a, 1p) avgöra om 153, 209 och 216 är inverterbara i $\mathbb{Z}_{323}$ och (b, 2p) finna inversen för ett av dem. ($323 = 17 \cdot 19$)

Lösning: $153 = 9 \cdot 17$ och $209 = 11 \cdot 19$, så $\text{sgd}(153, 323), \text{sgd}(209, 323) \neq 1$ och 153, 209 är inte inverterbara. $17, 19 \nmid 216$, så $\text{sgd}(216, 323) = 1$ och 216 är inverterbart.

Euklides algoritm: $323 = 1 \cdot 216 + 107$ $1 = 107 - 53 \cdot 2 = 107 - 53(216 - 2 \cdot 107) =$
 $216 = 2 \cdot 107 + 2$ $= -53 \cdot 216 + 107 \cdot 107 =$
 $107 = 53 \cdot 2 + 1$ $= -53 \cdot 216 + 107(323 - 216) =$
 $= 107 \cdot 323 - 160 \cdot 216$

Så $216^{-1} = -160 = 163$ i $\mathbb{Z}_{323}$.

Svar a: 153 och 209 är inte inverterbara, men det är 216, b: $216^{-1} = 163$ i $\mathbb{Z}_{323}$.

2) (3p) Vi skall visa att $a_n = 2 \cdot 7^n + 6 \cdot (-2)^n$ för $n \in \mathbb{N}$ om $a_{n+2} = 5a_{n+1} + 14a_n$ för $n \in \mathbb{N}$ och $a_0 = 8, a_1 = 2$.

Lösning: Vi visar med induktion påståendet (P_n) att för alla $n \in \mathbb{N}$ gäller

$a_n = 2 \cdot 7^n + 6 \cdot (-2)^n$ och $a_{n+1} = 2 \cdot 7^{n+1} + 6 \cdot (-2)^{n+1}$.

Bas: P_0 är sant, ty $a_0 = 8 = 2 + 6 = 2 \cdot 7^0 + 6 \cdot (-2)^0$, $a_1 = 2 = 14 - 12 = 2 \cdot 7^1 + 6 \cdot (-2)^1$.

Steg: Antag för $k \in \mathbb{N}$ att P_k är sant.

Enligt P_k gäller $a_{k+1} = 2 \cdot 7^{k+1} + 6 \cdot (-2)^{k+1}$ och $a_{k+2} = 5a_{k+1} + 14a_k \stackrel{\text{IA}}{=} 5(2 \cdot 7^{k+1} + 6 \cdot (-2)^{k+1}) + 14(2 \cdot 7^k + 6 \cdot (-2)^k) = (5 \cdot 2 \cdot 7 + 14 \cdot 2)7^k + (5 \cdot 6 \cdot (-2) + 14 \cdot 6)(-2)^k = 98 \cdot 7^k + 24 \cdot (-2)^k = 2 \cdot 7^{k+2} + 6 \cdot (-2)^{k+2}$, så om P_k är sant är P_{k+1} sant.

Enligt induktionsprincipen är saken klar.

3) Vi har $X = \{f : \{1, 2, \dots, 11\} \rightarrow \{1, 2, \dots, 15\}\}$ och söker (a, 1p) $|A|$, där $A = \{f \in X \mid f \text{ injektiv}\}$, (b, 1p) $|B|$, där $B = \{f \in X \mid f(x) \text{ udda om } x \text{ udda}\}$ och (c, 1p) $|C|$, där $C = \{f \in X \mid \text{precis en av } f \in A \text{ och } f \in B\}$.

Lösning: Antalet injektioner från en 11-mängd till en 15-mängd ($= |A|$) är $(15)_{11} = \frac{15!}{4!}$.

Det finns 8^6 sätt att ta de udda till udda och 7^5 sätt att ta de jämna till jämna. Multiplikationsprincipen ger $|B| = 8^6 \cdot 7^5$.

$|C| = (|A| - |A \cap B|) + (|B| - |A \cap B|) = |A| + |B| - 2 \cdot |A \cap B|$. $|A \cap B| = (8)_6 \cdot (7)_5 = \frac{8!}{2!} \cdot \frac{7!}{2!}$ (injektioner av udda och jämna för sig), så $|C| = \frac{15!}{4!} + 8^6 \cdot 7^5 - \frac{8! \cdot 7!}{2}$.

Svar a: $\frac{15!}{4!} = (54486432000)$ st, b: $8^6 \cdot 7^5 (= 4405854208)$ st,

c: $\frac{15!}{4!} + 8^6 \cdot 7^5 - \frac{8! \cdot 7!}{2} = (58790679808)$ st.

4) $(G, \cdot)$ är en grupp och vi har ekvationerna $x = y^2, y = z^2, z = x^2$ för $x, y, z \in G$. Vi söker (a, 1p) alla lösningar då minst två av x, y, z är lika och skall (b, 2p) visa att det om $|G| = 1000$ inte finns några lösningar med alla x, y, z olika.

Lösning: Låt x, y, z uppfylla ekvationerna och $x = y$ ($y = z$ och $z = x$ ger samma sak). Då är $x = y^2 = x^2$, så $x = 1$, identitets-elementet i G (multiplicera med x^{-1}). Det ger också $y = x = 1$ och $z = x^2 = 1$.

Ekvationerna ger $x = y^2 = (z^2)^2 = z^4 = (x^2)^4 = x^8$ och således $x^7 = 1$. Det betyder att $o(x) \mid 7$, så $o(x) = 1$ eller 7. $o(x) = 1$ ger $x = 1$ och därmed $y = z = 1$ (så de är inte olika), medan $o(x) = 7$ är omöjligt eftersom $o(x) \mid |G|$ och $7 \nmid 1000$. **Saken är klar.**

Svar a: Enda möjligheten är $x = y = z = 1$, b: Visat ovan.

5) (3p) Av ytorna en plan, sammanhängande graf delar in planet i har en 10 kanter, 3 st har 5 kanter, 4 st har 4 kanter och 7 st har 3 kanter. Vi söker antalet hörn i grafen.

Lösning: Antalet ytor är $r = 1+3+4+7 = 15$. Antalet kanter är $e = \frac{1}{2}(10+3\cdot 5+4\cdot 4+7\cdot 3) = 31$ (då man lägger ihop antalen kanter kring ytorna räknas varje kant två gånger). Eulers polyederformel (för en plan sammanhängande graf) ger $2 = v - e + r = v - 31 + 15$, så antalet hörn $v = 2 + 31 - 15 = 18$.

Svar: Grafen har 18 hörn.

6) Vi skall (a, 2p) ange villkoren för e, d i ett RSA-system med $n = 4757 = 67 \cdot 71$ och (b, 2p) finna det minsta fungerande $d \geq 25$.

Lösning: Villkoret för e, d är $e \cdot d \equiv 1 \pmod{m}$, där $m = (p-1)(q-1) = 66 \cdot 70 (= 4620)$. Möjliga d är de som är relativt prima med m , dvs inte delbara med dess primfaktorer 2, 3, 5, 7, 11 (fås från 66 och 70, hellre än 4620!). Det minsta icke-prima $d \geq 25$ är alltså $d = 13^2 = 169$.

Svar: a) Villkoret är $e \cdot d \equiv 1 \pmod{66 \cdot 70 (= 4620)}$,

b: Den minsta möjliga avkrypteringsexponenten är $d = 169$.

7) Med $\pi_1 = (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 4 & 8 & 6 & 3 & 5 & 2 \end{smallmatrix})$, $\pi_2 = (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 6 & 2 & 9 & 8 & 4 & 3 & 1 \end{smallmatrix})$, $\pi_3 = (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 1 & 8 & 7 & 3 & 2 & 4 & 6 \end{smallmatrix})$ skall vi dels (a, 1p) skriva π_1, π_2, π_3 på cykelform och ange deras ordningar och dels (b, 3p) avgöra om det finns $\tau_i \in S_9$ så att $\pi_i = \tau_i^2$ och i så fall ge exempel.

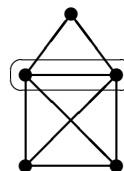
Lösning: Man finner $\pi_1 = (1\ 7\ 3)(2\ 9)(4)(5\ 8)(6)$ (ty $\pi_1(1) = 7, \pi_1(7) = 3$ etc.), $\pi_2 = (1\ 5\ 9)(2\ 7\ 4)(3\ 6\ 8)$, $\pi_3 = (1\ 9\ 6\ 3)(2\ 5\ 7)(4\ 8)$. Ordningen för en permutation är mgm av cykellängderna, så $o(\pi_1) = 6, o(\pi_2) = 3, o(\pi_3) = 12$.

Vid kvadrering ger en cykel av jämn längd två cykler av halva längden, medan en cykel av udda längd ger en cykel av samma längd. Det betyder att π_3 inte kan skrivas som τ_3^2 (udda antal cykler av den jämna längden 4). Men $\pi_1 = \tau_1^2, \pi_2 = \tau_2^2$ med $\tau_1 = (1\ 3\ 7)(2\ 5\ 9\ 8)(4\ 6), \tau_2 = (1\ 9\ 5)(2\ 4\ 7)(3\ 8\ 6)$.

Svar a: π_1, π_2, π_3 enligt ovan, ordningar $o(\pi_1) = 6, o(\pi_2) = 3, o(\pi_3) = 12$,

b: T.ex. $\tau_1 = (1\ 3\ 7)(2\ 5\ 9\ 8)(4\ 6), \tau_2 = (1\ 9\ 5)(2\ 4\ 7)(3\ 8\ 6)$, sådant τ_3 finns inte.

8) Grafen G bildas av K_m och K_n ($m, n \geq 3$) genom att slå ihop en kant ($m = 3, n = 4$ i figuren). Vi skall avgöra (a, 1p) för vilka värden på m, n G har en eulerkrets och (b, 3p) för vilka värden på m, n G har en eulerväg (som inte är en eulerkrets).



Lösning: G innehåller 3 typer av hörn:

K_m :s "egna" hörn ($m - 2$ st) har valens $m - 1$, K_n :s egna ($n - 2$ st) har valens $n - 1$ och de "gemensamma" (2 st) har valens $(m - 1) + (n - 1) - 1 = m + n - 3$. G (som ju är sammanhängande) har en eulerkrets omm alla hörn har jämn valens, men om $m - 1$ och $n - 1$ är jämna, är m, n udda, så $m + n - 3$ udda. G kan alltså inte ha någon eulerkrets.

G har en eulerväg omm exakt två hörn har udda valens. Om m, n båda är udda har de två gemensamma hörnen udda valens, övriga jämn (ok). Om m är udda och n jämn är K_m :s och de gemensamma hörnen av jämn valens och K_n :s egna av udda (ok precis om $n - 2 = 2$, så $n = 4$). Om m jämn och n udda måste p.s.s. $m = 4$. Om m, n båda är jämna blir alla hörn (minst 4 st) udda.

Svar a: G har inte för några (tillåtna) m, n någon eulerkrets,

b: G har en eulerväg omm en av m, n är udda och den andra är udda eller 4.

9) $E_H = \{\pi \in A_n \mid \pi(x) = \tau(x), \text{ alla } x \in \{1, 2, \dots, m\}, \text{ ngt } \tau \in H\}$, där H är en delgrupp till S_m ($1 \leq m < n$). Vi skall (a, 2p) visa att E_H är en delgrupp till A_n och (b, 3p) finna alla möjliga värden för $\frac{|E_H|}{|H|}$ då $n - m = 1, 2, 3$.

Lösning: Eftersom A_n (så E_H) är ändlig räcker det att visa att $E_H \neq \emptyset$ och att E_H är sluten under gruppoperationen. $id \in E_H$ och $\pi_1, \pi_2 \in E_H$ ger $\pi_1\pi_2$ jämn och för $x \in \{1, 2, \dots, m\}$ gäller $(\pi_1\pi_2)(x) = \pi_1(\pi_2(x)) = \pi_1(\tau_2(x)) = \tau_1(\tau_2(x)) = (\tau_1\tau_2)(x)$ (där vi använt att $\tau_2(x) \in \{1, 2, \dots, m\}$) och $\tau_1\tau_2 \in H$. **a-Saken är klar.**

$\pi \in E_H$ verkar som ett $\tau \in H$ på $\{1, 2, \dots, m\}$ och som ett $\sigma \in S_{n-m}$ på $\{m+1, \dots, n\}$. Eftersom $\text{sgn } \pi = 1$ är $\text{sgn } \tau = \text{sgn } \sigma$. Mot varje $\tau \in H$ svarar lika många $\pi \in E_H$ som antalet $\sigma \in S_{n-m}$ med $\text{sgn } \sigma = \text{sgn } \tau$. Om $n - m = 1$ är det 1 om $\text{sgn } \tau = 1$ och 0 om $\text{sgn } \tau = -1$, så $\frac{|E_H|}{|H|} = 1$ (om $H \subseteq A_m$) eller $\frac{1}{2}$ (om något, så hälften, av elementen i H är udda). Om $n - m = 2, 3$ är antalet π svarande mot varje τ 1 respektive 3, oberoende av $\text{sgn } \tau$.

Svar a): Visat ovan, **b):** Om $n - m = 1$ kan $\frac{|E_H|}{|H|}$ vara 1 eller $\frac{1}{2}$, om $n - m = 2$ är $\frac{|E_H|}{|H|} = 1$ och om $n - m = 3$ är $\frac{|E_H|}{|H|} = 3$.

10) Vi har $A \subset \{1, 2, \dots, 1000\}$, $|A| = 681$, och skall visa att det finns $a_1, a_2, a_3 \in A$ med $a_3 = a_2 + 10 = a_1 + 20$.

Lösning: Enligt ledningen låter vi $B = \{a + 10 \mid a \in A\}$ och $C = \{a + 20 \mid a \in A\}$.

Att $x \in A \cap B \cap C$ betyder precis att det finns $a_1, a_2, a_3 \in A$ med $x = a_3$ (ty $x \in A$), $x = a_2 + 10$ (ty $x \in B$), $x = a_1 + 20$ (ty $x \in C$). Det gäller alltså att visa att $A \cap B \cap C \neq \emptyset$.

Antag, för att få en motsägelse, att $A \cap B \cap C = \emptyset$. Då är $A \cup B \cup C \subseteq \{1, 2, \dots, 1020\}$ och (inklusion/exklusion) $|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |B \cap C| + |C \cap A|)$. Men $A \cap B$ och $C \cap A$ är då disjunkta delmängder till A , så $|A| \geq |A \cap B| + |C \cap A|$ och på samma sätt $|B| \geq |A \cap B| + |B \cap C|$ och $|C| \geq |C \cap A| + |B \cap C|$. Genom att addera får man $|A| + |B| + |C| \geq 2(|A \cap B| + |B \cap C| + |C \cap A|)$, dvs $-(|A \cap B| + |B \cap C| + |C \cap A|) \geq -\frac{1}{2}(|A| + |B| + |C|)$ och alltså $1020 \geq |A \cup B \cup C| \geq |A| + |B| + |C| - \frac{1}{2}(|A| + |B| + |C|) = \frac{1}{2} \cdot 3|A| = \frac{3}{2}681 > 1021$. Antagandet ledde till motsägelse, så **saken är klar.**

(En mer detaljerad analys visar att det räcker med färre än 681.)

Kommentar: Ovanstående lösning skulle fungera lika bra om det gällde t.ex. $a_3 = a_2 + 4 = a_1 + 7$. I det aktuella fallet är det nog enklare att dela upp $\{1, \dots, 1000\}$ i 10 delar $\{1, 11, 21, \dots, 991\}$, $\{2, 12, \dots, 992\}$, $\dots$, $\{10, 20, \dots, 1000\}$ och notera att var och en av dem kan rymma högst 67 tal utan "tre i rad". Postfacksprincipen ger att minst en av dem har fler från A (och att det räcker med $|A| = 671$).
