

**Lösningar tentan SF1662 DISKRET MATEMATIK, CLGYM1, TSVDK2,
20 augusti 2014**

Tyrrckfel kan förekomma.

1) (3p) Vi skall avgöra om $155 \in \mathbb{Z}_{228}$ är inverterbart och i så fall finna dess invers.

Lösning: Euklides algoritm:

$$\begin{cases} 228 = 1 \cdot 155 + 73, \\ 155 = 2 \cdot 73 + 9, \\ 73 = 8 \cdot 9 + 1 \end{cases} \quad \text{så } \text{sgd}(228, 155) = 1 \text{ och } \begin{cases} 1 = 73 - 8 \cdot 9 = 73 - 8(155 - 2 \cdot 73) = \\ = -8 \cdot 155 + 17 \cdot 73 = \\ = -8 \cdot 155 + 17(228 - 155) = \\ = 17 \cdot 228 - 25 \cdot 155 \end{cases}$$

155 är alltså inverterbart i $\mathbb{Z}_{228}$ och inversen är $-25 = 228 - 25 = 203 \in \mathbb{Z}_{228}$.

Svar: 155 är inverterbart och $155^{-1} = 203$ i $\mathbb{Z}_{228}$.

2) (3p) Vi skall visa att $\sum_{k=1}^n k(3k+1) = n(n+1)^2$ för alla $n = 1, 2, \dots$

Lösning: Vi kallar den önskade likheten P_n och visar den för alla $n \in \mathbb{Z}_+$ med induktion.

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

Steg: Antag (IA) P_r för ett godtyckligt $r \in \mathbb{Z}_+$, dvs att $\sum_{k=1}^r k(3k+1) = r(r+1)^2$.

Då fås $VL_{r+1} = \sum_{k=1}^{r+1} k(3k+1) = VL_r + (r+1)(3(r+1)+1) \stackrel{\text{IA}}{=} r(r+1)^2 + (r+1)(3r+4) = (r+1)(r^2 + r + 3r + 4) = (r+1)(r+2)^2 = HL_{r+1}$, dvs P_{r+1} .

Så P_1 är sant och om P_r är sant är P_{r+1} sant. **Saken är klar (induktionsprincipen).**

3) (3p) Vi söker antalet sätt att ordna 10 (olika) färgade kulor och 50 (identiska) svarta kulor, då varje färgad kula har två svarta grannar och ingen svart kula två färgade grannar.

Lösning: Vi kan låta varje färgad kula "växa ihop" med sina svarta grannar (villkoret på de svarta ger ju att ingen är granne till två olika färgade) och sedan välja platser för de uppkomna 10 storkulorna bland 40 platser, vilket kan ske på $(40)_{10} = \frac{40!}{30!}$ sätt (injektioner från en 10-mängd till en 40-mängd) (på övriga platser hamnar kvarvarande 30 svarta kulor).

Svar: Antalet sådana sätt att ordna kulorna är $\frac{40!}{30!} (= 3\,075\,990\,524\,006\,400)$.

4) $\pi \in S_8$ ges av $\pi(1)=7, \pi(2)=4, \pi(3)=1, \pi(4)=8, \pi(5)=6, \pi(6)=5, \pi(7)=3, \pi(8)=2$.

Vi skall (a, 1p) skriva π i cykelnotation, (b, 1p) ge $\pi^{-1}\tau$ då τ är $(182)(365)(47)$ och (c, 1p) avgöra om $\sigma^3\pi^{-2}\tau\sigma^{-1}\tau$ är jämn eller udda då $\sigma \in S_8$.

Lösning: a. $\pi(1) = 7, \pi(7) = 3, \pi(3) = 1, \pi(2) = 4, \pi(4) = 8, \dots$ ger att

$\pi = (1\,7\,3)(2\,4\,8)(5\,6)$.

b. $\pi^{-1}\tau = (1\,3\,7)(2\,8\,4)(5\,6)(1\,8\,2)(3\,6\,5)(4\,7) = \dots = (1\,4)(2\,3\,5\,7)$ ($1 \mapsto 8 \mapsto 4, 4 \mapsto 7 \mapsto 1$ etc.).

c. $\text{sgn}(\sigma^3\pi^{-2}\tau\sigma^{-1}\tau) = \text{sgn}(\sigma)^3 \text{sgn}(\pi)^{-2} \text{sgn}(\tau) \text{sgn}(\sigma)^{-1} \text{sgn}(\tau) = 1$, ty alla $\text{sgn}(\cdot)$ är ± 1 . Permutationen är alltså jämn.

Svar a: $\pi = (1\,7\,3)(2\,4\,8)(5\,6)$, b: $\pi^{-1}\tau = (1\,4)(2\,3\,5\,7)$, c: Den är jämn.

5) (3p) Vi skall avgöra om det måste finnas en fullständig matchning i en bipartit graf $G = (X \cup Y, E)$ där X -hörnens valenser alla är olika och ≥ 1 .

Lösning: Låt $A \subseteq X$ (och, som vanligt, $P(A) = \{y \in Y \mid \{x, y\} \in E \text{ för något } x \in A\}$). Alla A :s hörn har olika valens, så det finns $x \in A$ med valens $\geq |A|$ (om $A \neq \emptyset$). Alla x :s grannar tillhör $P(A)$, så $|P(A)| \geq |A|$. (Om $A = \emptyset$ är $|P(A)| = 0 = |A|$). Enligt Halls sats har G en fullständig matchning (av X -hörnen).

Svar: Ja, det måste finnas en fullständig matchning i G .

(Alternativt kan man matcha X -hörnen i ordning efter växande valens.)

6) (4p) Vi söker alla $x \in \mathbb{Z}$ sådana att $19 \mid (13x^{57} + 14x^{39} + 11x^3 - 12)$.

Lösning: Eftersom 19 är ett primtal ger Fermats lilla sats att $x^{19} \equiv_{19} x$ för alla $x \in \mathbb{Z}$. Det ger, fortfarande för alla $x \in \mathbb{Z}$, att $13x^{57} + 14x^{39} + 11x^3 - 12 \equiv_{19} 13x^3 + 14x^3 + 11x^3 - 12 \equiv_{19} 38x^3 - 12 \equiv_{19} 0 \cdot x^3 + 7 \equiv_{19} 7 \not\equiv_{19} 0$, så det finns inga sådana x .

Svar: Det finns inga sådana x .

7) Vi skall (a, 1p) finna alla element i U_{21} (de inverterbara elementen i $\mathbb{Z}_{21}$) och (b, 3p) finna ordningarna för 2 och 16 i U_{21} .

Lösning: a. $x \in U_{21}$ om $x \in \mathbb{Z}_{21}$ och $\text{sgd}(x, 21) = 1$, så

$U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

b. Ordningen för elementen i U_{21} är delare till 12 ($= |U_{21}|$), så möjliga värden är 1, 2, 3, 4, 6, 12. $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^6 = 64 = 1$, så $o(2) = 6$. $16^2 = 2^4 \cdot 2^4 = 2^6 \cdot 2^2 = 1 \cdot 4 = 4$, $16^3 = 16^2 \cdot 16 = 4 \cdot 16 = 2^2 \cdot 2^4 = 2^6 = 1$, så $o(16) = 3$

Svar a: $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, **b:** $o(2) = 6$, $o(16) = 3$.

8) $a, m, x \in \mathbb{Z}$. Vi skall avgöra (a, 2p) om $ax \equiv_m 1$ medför att det finns $y \in \mathbb{Z}$ med $my \equiv_a 2$ och (b, 2p) om $ax \equiv_m 2$ medför att det måste finnas $y \in \mathbb{Z}$ med $my \equiv_a 1$.

Lösning: a. $ax \equiv_m 1$ betyder att $ax - 1 = km$ för ett $k \in \mathbb{Z}$, så $m(-2k) - 2 = (-2x)a$ och $y = -2k$ ger $my \equiv_a 2$. Svaret blir alltså ja i a.

b. Motexempel: $a = m = 2$, $x = 1$. De ger ju $ax = 2 \equiv_2 2$, men $my = 2y \not\equiv_2 1$ för alla $y \in \mathbb{Z}$, så svar nej i b. (Sök a med $ax = 2$ i $\mathbb{Z}_m$, m inte inverterbart i $\mathbb{Z}_a$, dvs a inte inverterbart i $\mathbb{Z}_m$)

Svar a: Ja, b: Nej.

9) $S_{\mathbb{Z}}$ är mängden av bijektioner av $\mathbb{Z}$. $(S_{\mathbb{Z}}, \circ)$ är en grupp och vi skall (a, 1p) finna identitets-element och invers till $f \in S_{\mathbb{Z}}$ och (b, 4p) avgöra om $K_A = \{f \in S_{\mathbb{Z}} \mid f(x) \in A \text{ för alla } x \in A\}$ är en delgrupp till $S_{\mathbb{Z}}$ för alla $A \subseteq \mathbb{Z}$.

Lösning: a. $id \in S_{\mathbb{Z}}$, där $id(x) = x$ för alla $x \in \mathbb{Z}$, är identitets-element, ty $(f \circ id)(x) = f(id(x)) = f(x)$ och $(id \circ f)(x) = id(f(x)) = f(x)$ för alla $x \in \mathbb{Z}$, $f \in S_{\mathbb{Z}}$. Inversfunktionen f^{-1} (finns, ty f är en bijektion) är inverselement till $f \in S_{\mathbb{Z}}$: $f \circ f^{-1} = f^{-1} \circ f = id$.

b. Om A är oändlig är K_A inte en delgrupp till $S_{\mathbb{Z}}$.

För $A = \mathbb{N}$ ger t.ex. $f(x) = x + 1$ att $f \in K_{\mathbb{N}}$ (f är ju en bijektion av $\mathbb{Z}$ och $x \in \mathbb{N}$ medför att $x + 1 \in \mathbb{N}$), men dess invers $f^{-1} \notin K_{\mathbb{N}}$, ty $f^{-1}(x) = x - 1$, så $0 \in \mathbb{N}$ men $f^{-1}(0) = -1 \notin \mathbb{N}$.

Svar a: id är identitets-element, funktionsinversen f^{-1} är inverselement till f ,
b: Nej, K_A är inte säkert en delgrupp till $S_{\mathbb{Z}}$.

10) (5p) Vi söker antalet väsentligt olika armband av 5 svarta, 2 röda och 2 vita pärlor uppträdda på en ögla av snöre.

Lösning: Vi använder Burnsidess lemma. Om armbandet placeras med pärlorna i hörnen av en reguljär 9-hörning, ser man att gruppen G som verkar på mängden av konfigurationer består av identitetsavbildningen id , elementen $r, r^2, \dots, r^8$ (där r är rotation $\frac{2\pi}{9}$ kring en axel genom 9-hörningens mittpunkt och vinkelrät mot dess plan) och $s, rs, r^2s, \dots, r^8s$ (där s är rotation kring en axel i 9-hörningens plan, genom dess medelpunkt och en av pärlorna. $|X_g|$, antalet konfigurationer som inte ändras av g , ses vara som i tabellen:

g :s typ	antal sådana g	$ X_g $	
id	1	$\binom{9}{5,2,2} = 756$	alla konfigurationer
$r, r^2, \dots, r^8$	8	0	de två vita kan inte roteras till varandra
$s, rs, \dots, r^8s$	9	$4 \cdot 3 = 12$	8 pärlor paras ihop 2 och 2, ett par skall vara vitt, ett rött

Så antalet väsentligt olika armband = antalet banor under G :s verkan = $\frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{18} (1 \cdot 756 + 8 \cdot 0 + 9 \cdot 12) = \frac{1}{18} 864 = 48$.

Svar: Antalet olika sådana armband är 48.
