STOCKHOLMS UNIVERSITET
MATEMATISKA INSTITUTIONEN
Avd. Matematik,
Examinator: P. Alexandersson

Tentamen i
Algebra och kombinatorik
11 augusti 2022 kl $08^{00} - 13^{00}$

Inga hjälpmedel tillåtna. Alla svar ska motiveras noga.

Uppgift 1. Svara på följande frågor.

a) Hitta en lösning till ekvationen $6x + 18 = 12$ i $\mathbb{Z}_{42}$.

b) Ge exempel på en delgrupp till $(\mathbb{Z}_{20}, +)$ med exakt 5 element.

c) Vilken rest får man då $x^7 + x^6 + x + 1 \in \mathbb{Z}_5[x]$ delas med $(x + 4)$?

d) Om man har genererat primtalen $p = 7$, $q = 3$, ge exempel på en publika RSA-nyckel tillhörande dessa primtal.

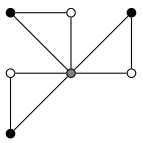
e) Rita en graf med kromatiskt tal 3, minst ett hörn med grad 6, och med en Eulerkrets.

Lösning. (a) Ekvationen blir ekvivalent med att lösa den diofantiska ekvationen $6x+42y = -6$. Division med 6 ger $x + 7y = -1$. En lösning är $x = 6$, $y = -1$, så $x = 6$ är en lösning. (b) Mängden $\{0, 4, 8, 12, 16\}$ är en sådan delgrupp.

(c) Vi har att $x^7 + x^6 + x + 1 = q(x)(x + 4) + r$, där $r \in \mathbb{Z}_5$ är resten. Sätter vi in $x = 1$, får vi $1^7 + 1^6 + 1 + 1 = q(1)5 + r$. Eftersom $5 \equiv 0$ i $\mathbb{Z}_5$, ger detta att $4 = r$, och vi har hittat resten.

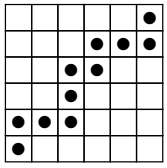
(d) Vi beräknar $m = (p-1)(q-1) = 6 \cdot 2 = 12$. Vi måste nu välja $e > 1$, så att $\text{sgd}(e, 12) = 1$. Dessa e är $\{3, 5, 7, 11\}$, och tillsammans med $pq = 21$ bildar de 4 möjliga publika nycklar.

(e) Tag tre trianglar, som delar ett hörn.



Tre färger behövs pga. triangeln, och det är lätt att se att tre färger räcker. Mittenhörnet har grad 6, och vi ser att det finns en Eulerkrets då graden för varje hörn är jämnt, och grafen är sammanhängande.

Uppgift 2. I ett 6×6-rutnät kan man bilda stigar som börjar i det nedre vänstra hörnet och slutar i det övre högra hörnet. I varje steg så går man antingen uppåt, eller höger (se figur).



a) Beräkna det totala antalet sådana stigar—svara med ett heltal.

b) Antag att varje ruta innehåller ett heltal mellan 0 och 22. *Värdet* på en stig ges av summan talen i alla rutor den besöker. Visa att det finns två olika stigar med samma värde.

Lösning. a) I en stig måste man göra totalt 5 uppsteg samt 5 högersteg. Alla möjliga permutationer av 10 sådana steg ger en giltig stig. Således finns det

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 2 \cdot 9 \cdot 2 \cdot 7 = 63 \cdot 4 = 252$$

sådana stigar.

b) Varje stig besöker exakt 11 rutor, så det maximala värdet på en stig är $11 \times 22 = 242$. Det finns alltså 243 olika värden som en stig kan anta, men hela 252 olika stigar. Lådprincipen ger då att det finns (minst) två olika stigar med samma värde.

Uppgift 3. Betrakta heltalsekvationen

$$x_1 + x_2 + \cdots + x_8 + x_9 = 7, \qquad x_1, x_2, \ldots, x_9 \geq 0. \tag{1}$$

(a) Bestäm totala antalet heltalslösningar till ekvationen.

(b) Hur många lösningar till (1) uppfyller att $x_1 + x_2 + x_3 = 2$?

(c) Bestäm antalet lösningar till (1) som uppfyller de tre villkoren

$$x_1 + x_2 + x_3 \neq 2, \quad x_4 + x_5 + x_6 \neq 2, \quad x_7 + x_8 + x_9 \neq 2.$$

Svaren får innehålla kombinatoriska kvantiteter—binomialtal, fakulteter, etc.

Lösning. (a) Det finns $\binom{7+8}{8}$ lösningar.

(b) Ekvationen $x_1 + x_2 + x_3 = 2$ har $\binom{2+2}{2} = 6$ lösningar, och vi måste kombinera dessa med de $\binom{5+5}{5} = 252$ lösningarna till $x_4 + \cdots + x_9 = 7 - 2$. Totalt alltså $\binom{4}{2}\binom{10}{5}$ lösningar.

(c) Vi använder inklusion-exklusion. Låt

- A_1 vara mängden lösningar som uppfyller att $x_1 + x_2 + x_3 = 2$,
- A_2 vara mängden lösningar som uppfyller att $x_4 + x_5 + x_6 = 2$,
- A_3 vara mängden lösningar som uppfyller att $x_7 + x_8 + x_9 = 2$.

Vi måste räkna ut storleken på snitt av sådana mängder.

- $|A_i| = \binom{4}{2}\binom{10}{5}$ enligt (b)-delen (och symmetri).

- $|A_1 \cap A_2|$ kräver

$$x_1 + x_2 + x_3 = 2, \quad x_4 + x_5 + x_6 = 2, \quad x_7 + x_8 + x_9 = 3.$$

  Dessa kan räknas oberoende av varandra, och vi får $\binom{4}{2}\binom{4}{2}\binom{5}{2}$ lösningar.

- $A_1 \cap A_2 \cap A_3 = \emptyset$ eftersom vänsterledets summa är 6, och det kan då inte vara 7.

Det finns nu flera "varianter" av varje snitt, där man väljer vilka mängder som ingår. Till exempel, det finns $\binom{3}{2}$ olika snitt av två olika A_i.
Sätter vi nu samman allt enligt inklusion-exklusionsformeln, får vi

$$\binom{3}{0}\binom{15}{8} - \binom{3}{1}\binom{4}{2}\binom{10}{5} + \binom{3}{2}\binom{4}{2}\binom{4}{2}\binom{5}{2} - 0 = 2979.$$

Uppgift 4. En graf $\Gamma = (V, E)$ definieras enligt följande. Vi har $V = \{S : S \subseteq \{1, 2, \ldots, 8\}\}$, dvs. hörnen utgörs av alla möjliga delmängder till $\{1, 2, \ldots, 8\}$. Två hörn S_1, S_2 är sammanbundna med en kant om mängden S_1 kan fås från mängden S_2 genom att lägga till eller ta bort exakt ett tal. Till exempel så är $\{1, 2, 5, 7\}$ och $\{1, 2, 4, 5, 7\}$ sammanbundna med en kant.

a) Bestäm alla granner till hörnet $\{1, 2, 5, 7\}$.

b) Visa att Γ har en Eulerkrets.

Lösning. a) Grannarna är $\{2, 5, 7\}$, $\{1, 5, 7\}$, $\{1, 2, 3, 5, 7\}$, $\{1, 2, 4, 5, 7\}$, $\{1, 2, 7\}$, $\{1, 2, 5, 6, 7\}$, $\{1, 2, 5\}$ samt $\{1, 2, 5, 7, 8\}$.
b) Vi kan nå alla hörn från $\emptyset$, genom att succesivt lägga till ett tal i taget. Detta visar att Γ är sammanhängande. Vidare, om vi har ett hörn, S, så har det exakt 8 grannar, varje tal i $\{1, 2, \ldots, 8\}$ kan antingen läggas till eller tas bort från S för att ge en granne till S. Eftersom graden för varje hörn är 8, så garanterar detta en Eulerkrets.

Uppgift 5. En *paritets-alternerande permutation* $\pi \in \mathrm{S}_n$, uppfyller att

$$\pi(j) \equiv j \mod 2 \quad \text{för alla } j = 1, 2, \ldots, n.$$

Till exempel är

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 5 & 6 & 1 & 4 & 7 \end{bmatrix}$$

en paritetsalternerande permutation i S_9. Låt P_n vara mängden paritets-alternerande permutationer av talen $\{1, \ldots, n\}$.

a) Skriv ned alla paritetsalternerande permutationer i P_4.

b) Visa att P_n är en delgrupp till S_n.

c) Argumentera för att det finns en grupp-isomorfi mellan P_7 och $\mathrm{S}_4 \times \mathrm{S}_3$. *En mening eller två räcker.*

Lösning. a) Från definitionen kan man utläsa att en paritetsalternerande permutation skickar udda tal på udda tal, och jämna tal på jämna tal. Vi får då de fyra permutationerna

$$(1)(2)(3)(4), \quad (1)(24)(3), \quad (13)(2)(4), \quad (13)(24).$$

b) Om $\pi, \sigma \in P_n$, så kommer π^{-1} också skicka udda på udda och jämna tal på jämna. Vidare, $\pi(\sigma(k))$ är udda precis då k är udda, så P_n är sluten under grupp-operationen. Detta räcker för att konstatera att P_n är en delgrupp.

c) Vi har att $P_7 \cong \mathrm{S}_4 \times \mathrm{S}_3$, eftersom vi redan konstaterat att en permutation i P_7 kan delas upp i en permutation av de udda talen för sig, och de jämna talen för sig. Ska man vara petig, så ges en isomofi av

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \pi_1 & \pi_2 & \pi_3 & \pi_4 & \pi_5 & \pi_6 & \pi_7 \end{bmatrix} \quad \mapsto \quad \left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \frac{\pi_1+1}{2} & \frac{\pi_3+1}{2} & \frac{\pi_5+1}{2} & \frac{\pi_7+1}{2} \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ \frac{\pi_2}{2} & \frac{\pi_4}{2} & \frac{\pi_6}{2} \end{bmatrix} \right)$$

och som exempel, så skickas $\pi = (1\,5\,3)(2)(4\,6)(7) \in P_7$ till paret $((1\,3\,2)(4),\ (1)(2\,3)) \in \mathrm{S}_4 \times \mathrm{S}_3$.

Uppgift 6. Låt X vara mängden av ord av längd 6 med bokstäverna $\{\mathtt{x}, \mathtt{y}, \mathtt{z}\}$, och varje bokstav måste förekomma minst en gång. Till exempel, $\mathtt{xyzzyz} \in X$, men $\mathtt{xyyyyy} \notin X$.

Gruppen $\mathbb{Z}_6$ verkar på X genom att $k \in \mathbb{Z}_6$ roterar ordet cykliskt k steg till vänster. Till exempel,

$$2 \cdot \mathtt{xyzzyz} = \mathtt{zzyzxy}.$$

a) Visa att storleken på X ges av $3! \cdot S(6,3)$, där $S(6,3) = 90$ är ett Stirlingtal.

b) Ge exempel på ett element i X som fixeras av $3 \in \mathbb{Z}_6$.

c) Bestäm antalet banor i X under gruppverkan av $\mathbb{Z}_6$, *svara med heltal.*

Lösning. a) Ett ord $(w_1, \ldots, w_6) \in X$ kan tolkas som en surjektion från $1, 2, \ldots, 6$ till mängden $\{\mathtt{x}, \mathtt{y}, \mathtt{z}\}$. Antalet sådana surjektioner ges av $3! \cdot S(6,3)$.

b) Ordet $\mathtt{xyzxyz}$ fixeras av 3, då cykliskt skift tre steg åt vänster inte ändrar ordet.

c) Vi använder Burnsides lemma. Inget ord fixeras av 1 eller 5, då detta skulle tvinga $w_1 = w_2 = \cdots = w_6$ men detta kan då ej innehålla alla tre bokstäver. På samma sätt, element som fixas av 2 eller 4, skulle tvinga $w_1 = w_3 = w_5$ och $w_2 = w_4 = w_6$, och då kan det inte heller innehålla alla tre bokstäver. Ett ord som fixeras av 3 bestäms unikt av w_1, w_2, w_3, och dessa värden måste vara en permutation av $\{\mathtt{x}, \mathtt{y}, \mathtt{z}\}$. Det finns alltså 3! fixpunkter. Burnsides lemma ger då slutligen att antalet banor blir

$$\tfrac{1}{6}\left(3! \cdot S(6,3) + 3!\right) = S(6,3) + 1 = 91.$$