

Lösningsskiss tenta 2025-05-23, Algebra och kombinatorik

- Vi har $300 = 3 \cdot 2^2 \cdot 5^2$, så $\phi(300) = \phi(3)\phi(2^2)\phi(5^2) = (3-1) \cdot (2-1)2 \cdot (5-1)5 = 80$.
 - Vi vill lösa kongruensen $17x \equiv 1 \pmod{127}$, vilket är ekvivalent med att lösa den diofantiska ekvationen $17x + 127y = 1$. Euklides algoritm blir

$$127 = 7 \cdot 17 + 8$$

$$17 = 2 \cdot 8 + 1$$

vilket ger $1 = 17 - 2 \cdot 8 = 17 - 2(127 - 7 \cdot 17) = 15 \cdot 17 - 2 \cdot 127$, så en lösning är $(x, y) = (15, -2)$. Inversen till 17 är därmed 15.

- En fixpunktsfri permutation saknar 1-cykler, så σ måste ha cykelstrukturen $(***)$ eller $(**)(**)$. I de första fallet är permutationen udda, i det andra fallet jämn. Alla element ges därmed av $(12)(34)$, $(13)(24)$ och $(14)(23)$.
- Gausseliminering ger

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[\begin{smallmatrix} \leftarrow \\ \leftarrow \\ \leftarrow \end{smallmatrix}]{+} \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim$$

så kodorden ges av $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ där

$$x_1 = x_2 + x_5 + x_7$$

$$x_3 = x_2 + x_5$$

$$x_4 = x_2 + x_7$$

$$x_6 = x_2 + x_5 + x_7$$

så vi har $2^3 = 8$ kodord och dimensionen 3.

- Eftersom H saknar nollkolonn och inte har två kolonner som är lika, rättar koden minst ett fel, enligt känd sats, så minimiavståndet $\delta \geq 3$. Men ordet 0101100, som har vikt 3, ingår i koden så $\delta = 3$ och koden rättar precis 1 fel.
 - Utför vi multiplikationen av H med kolonnen för första ordet med blir resultatet lika med kolonn 6 i H , så ordet rättas till 1010110. Gör vi samma sak med de andra ordet får vi varken 0 eller någon kolonn i H , så ordet har mer än 1 fel och går inte att rätta.
- Enligt faktorsatsen behöver vi bara hitta ett nollställe till $f(x)$. Man ser direkt att $f(1) = 0$, så $p(x) = x - 1 = x + 4$.
 - Vi får $g(x) = f(x) - x^2 = ((x-1)^2 - x)((x-1)^2 + x) = (x^2 + 2x + 1)(x^2 + 4x + 1) = (x+1)^2(x^2 + 4x + 1)$. Genom prövning ser man att faktorn $x^2 + 4x + 1$ saknar nollställe i $\mathbb{Z}_5$, så den är irreducibel.
 - Vi söker a så att $f(x) + a$ saknar nollställe. Med Fermats lilla sats (eller direkt uträkning) får man att $f(x) = (x-1)^4$ bara kan anta värdena 0 och 1, så vi behöver $a \neq 0$ och $a + 1 \neq 0$, så de möjliga värdena på a är 1, 2 och 3.

4. (a) Om Y är alla möjliga ord av bokstäverna i SOMMARLOV ges $|Y|$ av multinomialkoefficienten $\binom{9}{2,2,1,1,1,1,1} = \frac{9!}{(2!)^2}$. Om Y_1 är alla ord som innehåller SOM, Y_2 alla som innehåller MAL, och X alla tillåtna ord är $X = Y \setminus (Y_1 \cup Y_2)$ så inklusion-exklusion ger $|X| = |Y| - |Y_1| - |Y_2| + |Y_1 \cap Y_2|$. Om vi betraktar SOM som en enda bokstav är $|Y_1| = 7!$ och på motsvarande sätt fås av $|Y_2| = \binom{7}{2,1,1,1,1} = \frac{7!}{2!}$. Orden i $Y_1 \cap Y_2$ är dels de som innehåller bokstäverna SOM, MAL, O, R, V, dels de som innehåller bokstäverna SOMAL, M, O, R, V, så $|Y_1 \cap Y_2| = 5! + 5!$. Sammanfattningsvis får vi att antalet tillåtna ord är

$$|X| = \frac{9!}{4} - 7! - \frac{7!}{2} + 2 \cdot 5!.$$

- (b) Antalet surjektioner från en mängd med n till en med k element är $k!S(n, k)$, så vi får $3!S(5, 3)$ surjektioner. Genom upprepad användning av rekursionsformeln $S(n, k) = S(n-1, k-1) + kS(n-1, k)$ får vi $S(5, 3) = 25$, så antalet surjektioner är 150.
5. Triangelns symmetrigrupp är $G_\Delta = \{e, r, r^2, s_1, s_2, s_3\}$, där r är en rotation 120° , och elementen s_i är speglingar. Vi vill beräkna fixpunkterna $F(g)$ till alla element i G_Δ . Fixpunkterna till e är alla arrangemang, och det finns $\binom{10}{3} = 120$ sådana. Fixpunkterna till en icke trivial rotation kan inte ha en svart kula i mitten, så vi får 3 möjliga arrangemang av svarta kulor längs kanten. Fixpunkterna av en spegling måste ha precis en svart av de två kulorna längs speglingsaxeln, samt ett symmetriskt par av svarta vilket ger $2 \cdot 4 = 8$ fixpunkter. Med Burnsidess lemma får vi därmed att antalet banor är

$$\frac{1}{|G_\Delta|} \sum_{g \in G_\Delta} |F(g)| = \frac{1}{6} (120 + 2 \cdot 3 + 3 \cdot 8) = 25.$$

6. (a) Eftersom vi har två möjliga värden på a och tre möjliga på b har gruppen $2 \cdot 3 = 6$ element. Gruppens identitets-element är $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Betrakta elementet $g = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Ordningen av ett element måste dela gruppens ordning, så det kan vara 1, 2, 3 eller 6. Nu får vi $g^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq e$ och $g^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq e$, så ordningen av g är 6, så $G = \langle g \rangle$ är cyklisk.
- (b) En delgrupp H som inte är trivial eller hela G måste pga Lagranges sats ha ordning 2 eller 3. Eftersom dessa ordningar är primtal måste en sådan grupp vara cyklisk, och vi får därmed utöver delgrupperna $\{e\}$ och G de två delgrupperna

$$H_2 = \langle g^3 \rangle = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_3, a \neq 0 \right\}$$

och

$$H_3 = \langle g^2 \rangle = \langle g^4 \rangle = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_3 \right\},$$

så totalt 4 delgrupper.