

## Lösningsskiss tenta 2025-08-15, Algebra och kombinatorik

1. (a) Vi får  $\tau = (1\ 4\ 2)(3\ 5\ 6\ 7)$  och  $\sigma^{-1} = (1\ 4\ 3)(2\ 7)$ . Eftersom  $\tau$  är en produkt av disjunkta cykler av ordning 3 och 4 har  $\tau$  ordningen  $\text{MGM}(3, 4) = 12$ .
  - (b) Ett element av ordning 3 måste ha cykelstrukturen  $(***)$ , och det finns 8 sådana element.
  - (c) Enligt Lagranges sats måste ordningen av en delgrupp dela  $|S_4| = 24$ , och de enda udda delarna till 24 är 1 och 3. Det finns bara 1 delgrupp av ordning 1. Eftersom 3 är ett primtal måste delgrupper  $H$  av ordning 3 vara cykliska, och därmed genereras av något av de 8 elementen av ordning 3. Men i varje delgrupp finns det precis två möjliga generatorer, så antalet grupper blir  $8/2 = 4$ . Totalt har vi alltså  $1 + 4 = 5$  delgrupper av udda ordning.
2. (a) Vi har  $n = p \cdot q = 13 \cdot 11$ . Krypteringsnyckeln  $d$  fås genom att lösa kongruensen  $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$ , så vi behöver lösa

$$103d \equiv 1 \pmod{120},$$

vilket är ekvivalent med att lösa den diofantiska ekvationen  $103d + 120y = 1$ . Euklides algoritm blir

$$120 = 1 \cdot 103 + 17$$

$$103 = 6 \cdot 17 + 1$$

vilket ger  $1 = 104 - 6 \cdot 17 = 103 - 6(120 - 103) = 7 \cdot 103 - 6 \cdot 120$ , så en lösning är  $(d, y) = (7, -6)$ . Dekrypteringsnyckeln är därmed  $d = 7$  så det dekryperade meddelandet är

$$3^d = 3^5 3^2 = 243 \cdot 9 \equiv 100 \cdot 9 = 900 \equiv 42 \pmod{143}.$$

- (b) Kodorden  $(x_1, x_2, x_3, x_4, x_5)$  uppfyller  $x_2 = x_4 = 0$  och  $x_1 = x_3 = x_5$ , vilket ger (t ex) checkmatrisen

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

3. (a) Man får att  $p(1) = 0$  så  $x - 1$  är en faktor, och med polynomdivision får vi att  $p(x) = (x - 1)q(x)$  där  $q(x) = x^4 + x^3 + x^2 + x + 2$ . Nu är  $x = 1$  ett nollställe även till  $q(x)$ , så en ny polynomdivision ger  $q(x) = (x - 1)r(x)$  där  $r(x) = x^3 + 2x^2 + 1$ . Ett reducibelt tredjegradspolynom måste ha minst en linjär faktor, och därmed ett nollställe, men man kontrollerar enkelt att  $r(x)$  saknar nollställe i  $\mathbb{Z}_3$  och därmed är irreducibelt. Den sökta faktoriseringen är alltså

$$p(x) = (x + 2)^2(x^3 + 2x^2 + 1).$$

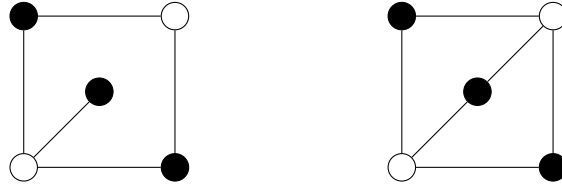
- (b) Man behöver att  $f(0) = b$ ,  $f(1) = 1 + a + b$  och  $f(-1) = 1 - a + b$  alla är nollskilda, speciellt är  $b$  inte 0. Om  $b = 1$  måste  $a = 0$ , om  $b = -1$  funkar  $a = \pm 1$ , så vi får de tre irreducibla polynomen

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2.$$

4. (a) Man kontrollerar enkelt  $U(\mathbb{Z}_5) = \{1, 2, 3, 4\} = \langle 2 \rangle$  och  $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\} = \langle 3 \rangle$ , så båda är cykliska och därmed isomorfa.

I gruppen  $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$  däremot får vi  $1^2 = 3^2 = 5^2 = 7^2 = 1$ , så den gruppen är inte cyklisk och därmed inte isomorf med de två andra.

- (b) De två graferna



har kromatiskt tal 2. De är inte träd eftersom de innehåller cykler, och slutligen är de inte isomorfa med varandra eftersom de har olika antal kanter.

5. (a) Om vi sätter  $x_i = y_i + i$  för  $i = 1, 2, 3, 4$  får vi ekvationen

$$y_1 + y_2 + y_3 + y_4 = 2015$$

där vi söker antalet icke-negativa heltalslösningar. Med stars-and-bars-metoden är antalet lösningar till den  $\binom{2018}{3}$ .

- (b) Den aktuella symmetrigruppen är  $G = \{e, r, r^2, r^3\}$ , där  $r$  är en rotation  $90^\circ$ . Vi vill beräkna fixpunkterna  $F(g)$  till alla element i  $G$ . Fixpunkterna till  $e$  är alla möjliga sätt att måla de 4 delrutorna, och det finns  $n^4$  sådana. Fixpunkterna för rotationerna  $r$  och  $r^3$  innebär att alla 4 delrutor har samma färg, så det finns  $n$  stycken. Fixpunkterna till  $r^2$  har samma färg på rutor som ligger på samma diagonal, så antalet fixpunkter blir  $n^2$ . Med Burnsidess lemma får vi därmed att antalet banor är

$$\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{4} (n^4 + n^2 + 2n).$$

6. (a) Genom att leta efter lämpliga exempel på matriser med determinant 0 ser vi att exempelvis elementet  $s = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R_0$  är  $\neq 0$ , men  $s^2 = 0$  vilket visar

att  $R_0$  inte är en kropp. I  $R_4$  kan vi observera att  $\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix} = 0$ .

- (b) Det vi behöver visa är att alla nollskilda element i  $R_3$  har en multiplikativ invers. Om  $t = \begin{pmatrix} x & ay \\ y & x \end{pmatrix} \neq 0$  är minst en av  $x, y$  nollskild. Därmed är  $\det(t) = x^2 - 3y^2 \neq 0$ , eftersom  $\sqrt{3}$  är irrationellt. Därmed får vi

$$t^{-1} = \frac{1}{x^2 - 3y^2} \begin{pmatrix} x & -3y \\ -y & x \end{pmatrix} \in R_3,$$

vilket skulle visas.