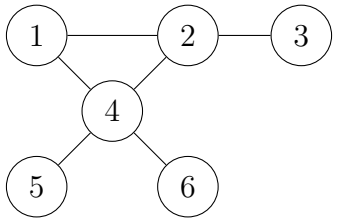
**Lösningsskiss tenta 2026-01-13, Algebra och kombinatorik.**

(1) (a) Eftersom $30 = 2 \cdot 3 \cdot 5$ har vi att antalet invertebara element ges av $\phi(30) = \phi(2) \cdot \phi(3) \cdot \phi(5) = 1 \cdot 2 \cdot 4 = 8$ där $\phi$ är Eulers phi-funktion.

(b) Ordet FALAFELFEST innehåller tre stycken F, två stycken A, E och L samt ett S och ett T. Utan restriktioner ges antalet ord därmed av multinomialkoefficienten $\binom{11}{3,2,2,2,1,1}$. Om vi ser [FEST] som en symbol har vi kvar två A, F och L samt ett E. Det är därför $\binom{8}{2,2,2,1,1}$ ord som innehåller ordet FEST. Antalet ord som inte innehåller ordet FEST är därför

$$\binom{11}{3,2,2,2,1,1} - \binom{8}{2,2,2,1,1}.$$

(c) Grafen nedan är sammanhängande med sex hörn och har inte kromatiskt tal 2 eftersom hörnen $1, 2$ och $4$ alla måste ha olika färger i en färgläggning. Hörnet 4 har valens 4 eftersom det har fyra grannar.




(2) (a) Från sats i kursen vet vi att matrisen blir en checkmatris för en kod som rättar åtminstone ett fel om alla kolonner är nollskilda och unika. Genom att jämföra kolonn 2 och 7 ser vi därför att $a = 1$. Kalla den erhålla matrisen för $H$. Vi har då att

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

vilket inte är en kolonn i $H$ och vi därmed inte kan rätta. Vi ser sedan att

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

är den första kolonnen av $H$ och därmed kan rättas till 1010011.

(b) Vi har att $n = 119 = 17 \cdot 7$ och $\phi(n) = 16 \cdot 6 = 96$. Dekrypteringsnyckeln $d$ kan nu hittas som inversen till $e = 29$ i $\mathbb{Z}_{96}$. Denna finner vi genom att ställa upp den diofantiska ekvationen

$$29d + 96k = 1,$$

vilket vi kan lösa med hjälp av Euklides algoritm. Den ger att

$$\begin{aligned} 96 &= 29 \cdot 3 + 9 \\ 29 &= 9 \cdot 3 + 2 \\ 9 &= 2 \cdot 4 + 1. \end{aligned}$$

Genom att gå igenom den baklänges får vi att $1 = 13 \cdot 96 - 43 \cdot 29$. Alltså finner vi att $d = -43 = 53$ i $\mathbb{Z}_{96}$. Det dekrypterade meddelatet är därmed

$$b^d = 4^{53} = 2^{106} \text{ i } \mathbb{Z}_{119}.$$

Eftersom 2 är inverterbar i $\mathbb{Z}_{119}$ ger Eulers sats oss att $2^{\phi(119)} = 2^{96} = 1 \pmod{119}$. Vi kan då förenkla meddelandet till

$$2^{106} = 2^{96} \cdot 2^{10} \equiv 2^{10} = 2^7 \cdot 2^3 = 128 \cdot 8 \equiv 9 \cdot 8 = 72 \pmod{119}.$$

Meddelandet är därmed 72.

(3) (a) Ett polynom i $\mathbb{Z}_7[x]$ av grad fyra är ett uttryck på formen

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

där alla $a_i \in \mathbb{Z}_7$ och $a_4 \neq 0$. Det finns alltså 7 val var för $a_0, a_1, a_2$ och $a_3$ samt 6 val för $a_4$, vilket ger att det finns $6 \cdot 7^4$ polynom i $\mathbb{Z}_7[x]$ av grad fyra. För att finna hur många av dem som uppfyllar att $f(1) \neq 0$ och $f(2) \neq 0$ använder vi oss av principen av inklusion och exklusion. Enligt faktorsatsen är $f(1) = 0$ ekvivalent med att $f(x) = (x-1) \cdot g(x)$ för något polynom $g(x)$. Eftersom $f$ har grad 4 har då $g$ grad 3 och antalet sådana polynom $g$ är, på samma sätt som ovan, givet av $6 \cdot 7^3$. Det finns alltså $6 \cdot 7^3$ polynom $f$ i $\mathbb{Z}_7[x]$ av grad fyra som uppfyllar att $f(1) = 0$. På samma sätt finns det lika många, alltså $6 \cdot 7^3$ stycken, som uppfyller att $f(2) = 0$.
De polynom $f$ av grad fyra som uppfyller att $f(1) = f(2) = 0$ kan nu enligt faktorsatsen skrivas som $f(x) = (x-1) \cdot (x-2) \cdot h(x)$ där $h(x)$ är ett polynom av grad 2. Eftersom $h(x)$ måste ha formen $h(x) = b_2x^2 + b_1x + b_0$ där $b_2 \neq 0$ finns det därför $6 \cdot 7^2$ möjligheter för vad $h$ kan vara och därmed lika många polynom $f$ av grad 4 som uppfyller att $f(1) = f(2) = 0$.
Principen av inklusion och exklusion ger oss därmed att antalet polynom i $\mathbb{Z}_7[x]$ av grad fyra som uppfyller att $f(1) \neq 0$ och $f(2) \neq 0$ är

$$6 \cdot 7^4 - 2 \cdot 6 \cdot 7^3 + 6 \cdot 7^2 = 6 \cdot 7^2 \cdot (7^2 - 14 + 1) = 6^3 \cdot 7^2.$$

(b) Vi använder oss av Euklides algoritm. Polynomdivision ger först att

$$x^3 + x + 1 = (x^2 + 2) \cdot x + (2x + 1).$$

Eftersom $(2x+1) \cdot (2x+2) = 4x^2 + 6x + 2 = x^2 + 2$ i $\mathbb{Z}_3[x]$ är $2x+1$ den sista icke-försvinnande resten och därmed en största gemensam delare

till $f(x)$ och $g(x)$. För att få den monisk multipliserar vi med $2^{-1} = 2$ i $\mathbb{Z}_3$ och får $2 \cdot (2x + 1) = x + 2$. Den moniska största gemensamma delaren är alltså $x + 2$.

(4) Betrakta permutationerna $\alpha = (7\ 3\ 5)(2\ 4\ 1)(6\ 8)$ och $\beta = (1\ 5\ 3\ 2)(4\ 8)$ i $S_8$.

(a) Vi har att

$$\gamma = \alpha^{-1} \cdot \beta^2 = (5\ 3\ 7)(1\ 4\ 2)(6\ 8)(1\ 3)(5\ 2) = (1\ 7\ 5)(2\ 3\ 4)(6\ 8).$$

Eftersom 3-cylker är jämna är $\gamma$ udda.

(b) Vi vet att $\operatorname{sgn}(\sigma^2) = \operatorname{sgn}(\sigma)^2 = 1$, så $\sigma^2$ är jämn. Men vi vet från (a) att om $\sigma$ uppfyller ekvationen, då måste $\sigma^2$ vara udda. Alltså finns ingen permutation $\sigma$ som uppfyller ekvationen.

(c) Mängden består av alla permutationer i $S_8$ som är konjugerade till $\beta$. Enligt sats är detta detsamma som alla permutationer med samma cykeltyp som $\beta$. Eftersom $\beta$ har cykeltyp $[4^1 2^1 1^2]$ finns det enligt känd formel

$$\frac{8!}{4^1 \cdot 2^1 \cdot 2!} = \frac{8!}{16} = \frac{7!}{2}$$

permutationer med denna cykeltyp i $S_8$.

(5) Betrakta mängden $G = \{(a, b, c) \mid a, b, c \in (\mathbb{Z}_3 \setminus \{0\})\}$.

(a) Vi vet att $(\mathbb{Z}_3 \setminus \{0\}) = U_3$ är de inverterbara elementen i $\mathbb{Z}_3$ och är därmed en grupp under multiplikation. Att $G$ är sluten och associativ följer då direkt från samma egenskaper i $U_3$. Identiteten i $G$ är $(1, 1, 1)$ och inversen av $(a, b, c)$ är $(a^{-1}, b^{-1}, c^{-1})$, vilket finns eftersom alla element har inverser i $U_3$. Därmed är $G$ en grupp. Ordningen på $G$ är $|U_3|^3 = 2^3 = 8$.

(b) Enligt Lagrange måste storleken på en delgrupp till $G$ dela storleken på $G$, vilket är 8. De möjliga storlekarna på delgrupper är därför $1, 2, 4$ och 8. Delgrupper av alla dessa storlekar finns också, och som exempel kan vi ta $\{(1, 1, 1)\}$, $\{(1, 1, 1), (2, 1, 1)\}$, $\{(1, 1, 1), (2, 1, 1), (1, 2, 1), (2, 2, 1)\}$ och $G$.

(6) Tänk på pärlorna som utplaserade i hörnen av en regelbunden åttahörning och låt $G$ vara gruppen av symmetrier av en sådan åttahörning. Om $X$ är mängden av alla sådanna utplaseringar av pärlorna vill vi veta hur många banor som $G$ har på $X$. Dessa banor räknar vi med hjälp av Burnsides lemma.

För $g = \mathrm{id}$ som identitetselementet är ges dess fixpunktmängd av hela $X$. Så

$$|F(g)| = |X| = \binom{8}{3, 3, 2}$$

eftersom det finns 8 pärlor totalt och positionen på kulorna i samma färg spelar ingen roll.

För $g = r$, en rotation med en åttondels varv, gäller att $|F(g)| = 0$. Detta eftersom att det finns ett udda antal svarta pärlor, men eftersom det finns 8 antal pärlor totalt så täcker en pärla upp ett jämt antal platser vid repeterad användning av rotationen. Samma argument ger att $|F(g)| = 0$ även för $g = r^2, r^3, \ldots, r^7$, de resterande rotationerna.

För $g = s_1$, en spegling i en linje som går genom motsatta sidor, har vi att $|F(g)| = 0$ eftersom det måste vara lika många svarta pärlor på vardera sida av speglingslinjen, men eftersom det finns ett udda antal svarta pärlor är det ej möjligt. Det finns 4 av dessa speglingar.

Slutligen, för $g = s_2$, en spegling i en linje som går genom två motsatta hörn, då är $|F(g)| \neq 0$. För att få lika många svarta och vita pärlor på vardera sida av speglingslinjen behöver vi ha att det är en svart och en vit pärla på linjen, samt en pärla av varje färg på vardera sida av linjen. Om man har plaserat ut var pärlorna på ena sidan av linjen är, då är det bestämt var de på andra sidan ligger. Detta ger att $|F(g)| = 2 \cdot 3! = 12$ där 2 kommer från att välja vilken pärla på linjen som är svart och vilken som är vit, medan 3! kommer från att orda pärlorna på ena sidan av linjen. Det finns 4 av dessa tyen av speglingar.

Enligt Burnsides lemma finns det därmed

$$\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{16} \left( \binom{8}{3, 3, 2} + 12 \cdot 4 \right) = 38$$

olika halsband som kan skapas.