Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Diskret Matematik för F3 och F1spec, 5B1203, onsdagen den 23 augusti.

1. **Lösning** Då $n = 77 = 11 \cdot 7$ så är $m = (11-1)(7-1) = 60$. Vi söker nu, med hjälp av Euklides algoritm, ett tal d sådant att $d \cdot e \equiv 1 \pmod{m}$.

$$60 = 5 \cdot 13 - 5, \quad 13 = 3 \cdot 5 - 2, \quad 5 = 2 \cdot 2 + 1.$$

Ur denna algoritm får vi

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (3 \cdot 5 - 13) = -5 \cdot 5 + 2 \cdot 13 = 5(60 - 5 \cdot 13) + 2 \cdot 13 = 5 \cdot 60 - 23 \cdot 13.$$

Härav sluter vi att

$$-23 \cdot 13 \equiv 1 \pmod{60} \quad \text{eller ekvivalent} \quad 37 \cdot 13 \equiv 1 \pmod{60}.$$

Vårt sökta tal d är alltså lika med 37. Det dechiffrerade meddelandet blir nu

$$2^d \pmod{77} = 2^{37} \pmod{77} = 2^{32} \cdot 2^4 \cdot 2 \pmod{77}.$$

Vi räknar ut att

$$\begin{aligned} &2^4 = 16, \\ &2^8 \equiv_{77} 16^2 \equiv_{77} 256 \equiv_{77} 25, \\ &2^{16} \equiv_{77} 25^2 \equiv_{77} 9, \\ &2^{32} \equiv_{77} 9^2 \equiv_{77} 4. \end{aligned}$$

Vi får alltså att

$$2^{37} \equiv_{77} 4 \cdot 16 \cdot 2 \equiv_{77} 51$$

Svar 51.

2. **Lösning** Om kontrollmatrisen H har full rang och m kolonner och n rader så blir antalet ord i koden 2^{m-n}. Kontrollmatrisens kolonner skall vara olika och ingen kolonn får vara nollkolonnen. Detta leder till att

$$\{\text{antal olika kolonner} \neq 0 \text{ av höjd } n\} = 2^n - 1 \geq m \quad \text{och} \quad m - n = 5.$$

Vi ser att den minsta ordlängd m för vilket detta går att uppfylla är när $m = 9$. Ett exemplel på en sådan kontrollmatris är

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Vi tar ordet $\bar{c} = 110111100$. Det tillhör inte koden då

$$H\bar{c}^T = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Eftersom $H\bar{c}^T$ är lika med den tredje kolonnen i matrisen H så har ett fel uppstått i tredje positionen i ordet. Korrigerat blir ordet alltså lika med ordet 111111100.

3. **Lösning** Svaret är ja. Låt en komponent bestå av en 4-cykel med en extra kant mellan två motstående hörn. Denna komponent har tre stycken olika cykler. En annan komponent består av en 3-cykel. Nu har vi precis fyra stycken cykler och två komponenter till vilka vi använt sammanlagt 8 kanter och 7 noder. Återstår att konstruera en graf med tre komponenter, 28 noder och 25 kanter. Låt två noder vara isolerade och bilda varsina två komponenter. Av resterande 26 noder och 25 kanter ritar vi ett träd, vilket som helst.

4. **Lösning:** Vi bestämmer stavens automorfigrupp G sedan använder vi Burnsides lemma och behöver då talen $|Fix_g(S)|$ där $g \in G$.

   Beteckna stavens ändar med v och h och de sex övriga sidoytorna i ordning med 1, 2, 3, 4, 5 och 6.

   Vi får följande tabell

$g \in G$	$\lvert Fix_g(S)\rvert$
id	p^8
$(v)(h)(1\ 2\ 3\ 4\ 5\ 6)$	p^3
$(v)(h)(1\ 3\ 5)(2\ 4\ 6)$	p^4
$(v)(h)(1\ 4)(2\ 5)(3\ 6)$	p^5
$(v)(h)(1\ 5\ 3)(2\ 6\ 4)$	p^4
$(v)(h)(1\ 6\ 5\ 4\ 3\ 2)$	p^3
$(v\ h)(1)(2\ 6)(3\ 5)(4)$	p^5
$(v\ h)(1\ 2)(3\ 6)(4\ 5)$	p^4
$(v\ h)(1\ 3)(2)(4\ 6)(5)$	p^5
$(v\ h)(1\ 4)(2\ 3)(5\ 6)$	p^4
$(v\ h)(1\ 5)(2\ 4)(3)(6)$	p^5
$(v\ h)(1\ 6)(2\ 5)(3\ 4)$	p^4

   Burnsides lemma ger nu

   Svar: $\frac{1}{12}(p^8 + 4p^5 + 5p^4 + 2p^3)$.

5. (a) **Lösning** Söker först inversen till elementet $3x - 2$ i kroppen F. Euklides algoritm ger direkt

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

   varur vi får att i F så gäller att $2x \cdot (3x - 2) + 1 = 0$. Alltså är

   $$(3x - 2)^{-1} = -2x = 3x.$$

   Därav följer att

   $$z = (3x - 2)^{-1}(x + 2) = 3x(x + 2) = 3x^2 + x = 3(-x - 1) + x = -2x - 3 = 3x + 2.$$

   Svar: $z = 3x + 2$.

(b) **Lösning** Kroppen Z_5 är en delmängd till F och med samma multiplikationsstruktur. Då gäller att $Z_5 \setminus \{0\}$ är en delgrupp till multiplikativa gruppen till F. Eftersom $Z_5 \setminus \{0\}$ består av fyra element ger detta oss vårt

Svar: $\{1, 2, 3, 4\}$.

6. **Lösning** Ringen Z_{72} är isomorf med den direkta produkten $Z_8 \times Z_9$. Så ekvivalent problem är att söka antalet lösningar till ekvationen

$$(a, b)^6 = (1, 1) \quad \text{eller ekvivalent} \quad (a^6, b^6) = (1, 1)$$

i denna direkta produkt.

Vi löser ekvationen $a^6 = 1$ i Z_8 genom systematisk genomgång av alla element.

$$1^6 = 1, \quad 2^6 = 0, \quad 3^6 = 1, \quad 4^6 = 0, \quad 5^6 = 1, \quad 6^6 = 0, \quad 7^6 = 1.$$

Således fyra lösningar till $a^6 = 1$ i Z_8 nämligen 1, 3, 5 och 7.

Vi löser ekvationen $b^6 = 1$ i Z_9 genom systematisk genomgång av alla element.

$$1^6 = 1, \quad 2^6 = 1, \quad 3^6 = 0, \quad 4^6 = 1, \quad 5^6 = 1, \quad 6^6 = 0, \quad 7^6 = 1, \quad 8^6 = 1.$$

Således sex lösningar till $b^6 = 1$ i Z_9 nämligen 1, 2, 4, 5, 7 och 8.

Enligt multiplikationsprincipen har vi alltså totalt $4 \cdot 6 = 24$ olika lösningar till ekvationen $z^6 = 1$ i ringen Z_{72}. Två lösningar är givetvis $z = 1$ och $z = -1$. En tredje får vi räkna ut med hjälp av kinesiska restsatsen. T ex ett z som motsvarar elementet $(3, 1)$ i den direkta produkten $Z_8 \times Z_9$, dvs ett z sådant att

$$\begin{aligned} z &\equiv 3 \pmod 8, \\ z &\equiv 1 \pmod 9. \end{aligned}$$

Ett sådant kan skrivas

$$z = 3 \cdot A \cdot 9 + 1 \cdot B \cdot 8 + n72$$

för tal A och B sådana att $A \cdot 9 \equiv 1 \pmod 8$ och $B \cdot 8 \equiv 1 \pmod 9$. Vi tar t ex $A = 1$ och $B = -1$. Då blir

$$z = 3 \cdot 9 + (-1) \cdot 8 + n72 = 19 + n72.$$

Svar: Det finns totalt 24 olika lösningar varav elementen $1, -1$ och 19 är tre exempel.

7. (a) **Lösning:** Den kanske enklaste lösningen, men måhända inte den elegantaste, är att inse att k stycken av elementen i mängden $\{4, 5, 6, 7, 8\}$ måste placeras i de övriga två lådorna så att ingen av dessa blir tom, detta för $k = 2, 3, 4, 5$, och att resterande $5 - k$ element ur denna mängd helt godtyckligt kan placeras i de tre lådorna med elementen 1, 2 respektive 3.

Op. 1: Välj k element av 5 element:	$n_1 = \binom{5}{k}$.
Op. 2: Placera ut dessa så att ingen av de två lådorna blir tomma:	$n_2 = S(k, 2)$.
Op. 3: Placera ut resterande $5 - k$ element:	$n_3 = 3^{5-k}$

Multiplikationsprincipen ger nu för varje $k = 2, 3, 4, 5$ att antalet möjligheter är

$$\binom{5}{k} \cdot S(k, 2) \cdot 3^{5-k}.$$

De fyra fallen $k = 2, 3, 4, 5$ innehåller inga gemensamma utplaceringar, dvs de är disjunkta. Summerar vi nu för dessa värden på k får vi

Svar: $\sum_{k=2}^{5} \binom{5}{k} \cdot S(k, 2) \cdot 3^{5-k}$.

(b) **Lösning:** Nu har vi faktiskt fyra etiketterade lådor. En med elementet 1, en med elementet 2, en med elementet 3 och en, den fjärde, som inte innehåller något av elementen 1, 2 eller 3.

Antalet sätt att placera ut de övriga fem elementen på, i dessa lådor, om man tillåter den fjärde lådan att vara tom, är 4^5. I 3^5 av dessa fall blir den fjärde lådan tom. Så (b)-uppgiften har svaret $4^5 - 3^5$.

8. **Lösning** Vi tar den direkta produkten $G_1 \times G_2$ där $G_1 = S_4$, gruppen av alla permutationer på en mängd med 4 element, och $G_2 = (Z_3, +)$. Eftersom $|S_4| = 24$ och $|(Z_3, +)| = 3$ så kommer $|G| = 24 \cdot 3 = 72$.

Låt nu $a = (1\ 2\ 3)$ och $b = (1\ 4)$ vara två element i S_4. Då gäller

$$(a, 0)(b, 0) = (ab, 0) = ((1\ 4\ 2\ 3), 0) \neq (b, 0)(a, 0) = (ba, 0) = ((1\ 2\ 3\ 4), 0).$$

Alltså kan gruppen inte vara abelsk.