Matematiska Institutionen
KTH

Lösning till tentamensskrivning på kursen Diskret Matematik för F3 och F1spec, 5B1203, fredagen den 14 januari.

1. En faktorisering ger att $n = 77 = 7 \cdot 11$ så $m = (7-1)(11-1) = 60$. Dekrypteringsnycklen d satisfierar
$$d \cdot e \equiv 1 \pmod{60}.$$
Vi minns att $11^2 = 121 \equiv 1 \pmod{60}$ (eller så använder vi på sedvanligt sätt Euklides algoritm för att få fram att) således är $d = 11$. Vi vet nu att $D(2) = 2^{11} \pmod{77}$. Då $2^{11} = 2^8 \cdot 2^2 \cdot 2$. Då $2^8 = 256 = 3 \cdot 77 + 25$ får vi att
$$2^{11} = 2^8 \cdot 2^2 \cdot 2 \equiv_{77} 25 \cdot 4 \cdot 2 \equiv_{77} 46.$$
SVAR: 46.

2. Vi beräknar först antal möjligheter då vi kan tänka oss att A och B ingår i samma komitee. Det finns $\binom{12}{3} = \frac{12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3} = 220$ olika sätt att välja ut pojkar och $\binom{8}{2} = \frac{8 \cdot 7}{1 \cdot 2} = 28$ olika sätt att välja ut flickorna i så fall. Vart och ett av de 220 valen av pojkar kan kombineras med vart och ett av de 28 valen av flickor. Så vi får då $220 \cdot 28 = 6160$ olika möjligheter.
Vi beräknar nu antal möjligheter då A och B ingår i samma komitee. Välj A och B. Återstår att välja två pojkar och en flicka. Antal möjligheter blir för pojkarnas del $\binom{11}{2} = 55$ och för flickornas del 7. Totalt under dessa omständigheter $7 \cdot 55 = 385$. Så vi har
SVAR: $6160 - 385 = 5775$.

3. Vi gör substitutionen $y_1 = x_1$, $y_2 = x_2 - 2$, $y_3 = x_3 + 1$ och $y_4 = x_4$. Antalet lösningar till givna ekvationen är samma som antalet lösningar till
$$y_1 + (y_2 + 2) + (y_3 - 1) + y_4 < 20, \quad \text{dvs} \quad y_1 + y_2 + y_3 + y_4 < 19$$
som uppfyller $y_1 \geq 0$, $y_2 \geq 0$, $y_3 \geq 0$ och $x_4 \geq 0$. Vi inför en variabel y_5 och får att antal lösningar till ovanstående är samma som antalet lösningar till
$$y_1 + y_2 + y_3 + y_4 + y_5 = 19,$$
där $y_i \geq 0$ för $i = 1, 2, 3, 4, 5$. Detta antal är, enligt välkänd formel,
SVAR: $\binom{19+(5-1)}{5-1} = \binom{23}{4}$.

4. Antag G är bipartit. Vi visar att då får vi en motsägelse.
Antag vi har x stycken noder i den ena delen V_1 av grafen och $v - x$ i den andra delen V_2. Vi har alltså inga kanter mellan noderna i nodmängden V_1 och inga kanter mellan noderna i nodmängden V_2. Totala antalet kanter blir då som mest när vi har en kant från varje nod i V_1 till varje nod i V_2. Antal kanter i den bipartita grafen är högst $x(v-x)$. Men
$$x(v-x) \leq (\frac{v}{2})^2$$
eftersom
$$(\frac{v}{2})^2 - x(v-x) = x^2 - vx + (\frac{v}{2})^2 = (x - \frac{v}{2})^2 \geq 0$$
för alla värden på x. Antal kanter i en bipartit graf kan alltså aldrig vara större än $(\frac{v}{2})^2$.

5. Vi söker permutationer γ, φ och τ sådana att $\gamma^3 = (1\ 2\ 3\ 4)$, $\varphi^3 = (5\ 6)$ och $\tau^3 = (7)(8)(9)$. Då permutationen $(5\ 6)$ har ordning två gäller att om vi låter $\varphi = (5\ 6)$ så har vi $\varphi^3 = (5\ 6)$. Permutationerna $(7\ 8\ 9)$ och $(7\ 9\ 8)$ har bägge ordningarna tre så med $\tau_1 = (7\ 8\ 9)$ och $\tau_2 = (7\ 9\ 8)$ så har vi att $\tau_i^3 = (7)(8)(9)$ för både $i = 1$ och $i = 2$. Vidare om vi låter $\tau_3 = (7)(8)(9)$ så gäller också givetvis att $\tau_3^3 = (7)(8)(9)$. Med $\gamma = (4\ 3\ 2\ 1)$ har vi en permutation av ordning fyra $\gamma^4 = id$ och därmed $\gamma^3\gamma = id$ varur $\gamma^{-1} = \gamma^3$ erhålles. Men vi ser att $\gamma^3 = (1\ 2\ 3\ 4)$. Eftersom cyklernma är disjunkta gäller nu att

$$(\gamma\varphi\tau_i)^3 = \gamma^3\varphi^3\tau_i^3 = (1\ 2\ 3\ 4)(5\ 6)(7)(8)(9)$$

för $i = 1, 2$ och 3. Vi fann tre olika permutationer med den sökta egenskapen.

6. Givna ringen är, i enlighet med t ex stencilen om kinesiska restsatsen, isomorf med den direkta produkten $Z_7 \times Z_{13}$. Vi löser ekvationen i repektive ring:

   I ringen Z_7 kan ekvationen skrivas $(5x + 2)(2x + 3) = 0$, dvs $3x^2 - 2x - 1 = 0$ och efter multiplicering med 5, $x^2 + 4x + 2 = 0$. En kvadratkomplettering ger $(x + 2)^2 = 2$. Detta ger $x + 2 = \pm 3$ dvs $x = 3$ eller 4.

   I ringen Z_{13} får vi ekvationen $6x^2+7x+6 = 0$. Inverst element till 6 i ringen Z_{13} är elementet 11 och vi multiplicerar med detta, i syfte att förenkla, och får ekvationen $x^2 + 12x + 1 = 0$ som efter en kvadratkomplettering övergår i ekvationen $(x+6)^2 = 9$ som ju har lösningarna $x + 6 = \pm 3$. Så vi har alltså att $x = -3$ eller -9 dvs 10 eller 4.

   Vi söker alltså x som satisfierar $x \equiv_7 a$ och $x \equiv_{13} b$ där $a = 3$ eller 4 och $b = 10$ eller 4. Vi ansätter, i enlighet med ovan angivna stencil,

   $$x = 13A + 7B + n \cdot 91$$

   och får

   $$13A \equiv_7 a \quad \text{och} \quad 7B \equiv_{13} b$$

   som ger $-A \equiv_7 a$ eller $A \equiv -a$ respektive $B \equiv_{13} 2b$. Vi får således $x \equiv 13(-a)+2b \pmod{91}$ dvs i ringen Z_{91} elementen i vårt

   SVAR: $x = 72$, 59, 60, 47.

7. a) Antag att $G = H_1 \cup H_2$, där $H_i \neq G$ för $i = 1, 2$. Då finns $g \in H_1 \setminus H_2$ och $h \in H_2 \setminus H_1$. Men elementet $gh \notin H_1$ och $gh \notin H_2$ ty om t ex $gh \in H_1$ skulle $gh = g_1 \in H_1$ och därmed $h = g^{-1}g_1 \in H_1$ vilket strider mot antagandet om h. Elementet gh tillhör gruppen G eftersom G är sluten med avseende på operationen i G, men gh tillhör varken H_1 eller H_2 vilket strider mot antagandet att G är unionen av H_1 och H_2.

   b) Låt $G = Z_2^2$ och $H_1 = \{(0,0),(1,0)\}$, $H_1 = \{(0,0),(1,0)\}$ och $H_3 = \{(0,0),(1,1)\}$.

8. Elementet x är primitivt i kroppen, eftersom räkningar ger att $x^2 = x + 3$, $x^3 = x^2 + 3x = (x+3)+3x = -x+3$, $x^4 = -x^2+3x = -(x+3)+3x = 2x+2$, $x^6 = (3-x)^2 = 4-x+x^2 = -1 - x + (x + 3) = 2$, $x^8 = (2x + 2)^2 = -x^2 + 3x + 4 = -(x + 3) + 3x + 4 = 2x + 1$ och $x^{12} = 2^2 = -1$. Inga potenser x^d där d delar antalet element i kroppens multiplikativa grupp, blir lika med 1. Detta bevisar att elemente x är primitivt.

   Vi söker nu element z i kroppen sådana att $z^4 = -1$. Det finns fyra lösningar till denna ekvationen i kroppen F. Följande potenser av x satisfierar denna ekvation: x^3, $x^3 \cdot x^6$, $x^3 \cdot (x^6)^2$ och $x^3 \cdot (x^6)^3$, detta eftersom $(x^3)^4 = x^{12} = -1$ och $((x^6)^k)^4 = (x^{24})^k = 1^k = 1$ i denna kropp. Emendan x är primitivt i kroppen är de fyra elementen är olika och vi får

   SVAR: x^3, x^9, x^{15} och x^{21}.