Institutionen för matematik
KTH

Lösningar till Tentamensskrivning på kursen Diskret matematik för IT1, 5B1118, fredagen den 14 januari 2005.

DEL A

1. Euklides Algoritm ger:

   $513 = 1 \cdot 314 + 199$, $314 = 1 \cdot 199 + 115$, $199 = 2 \cdot 115 - 31$, $115 = 4 \cdot 31 - 9$, $31 = 3 \cdot 9 + 4$, $9 = 2 \cdot 4 + 1$.

   Alltså är den största gemensamma delaren lika med 1.

2. Formeln är sann för $n = 1$ ty då är formelns vänstra led lika med 1 och dess högra led också lika med 1.

   Vi viasr nu att om formeln är sann för det naturliga talet n så är formeln också sann för det efterföljande naturliga talet $n+1$. Vi arbetar med formelns vänstra led och finner med gängse beteckningar att om $VL_n = HL_n$ så

   $$VL_{n+1} = 1 + 4 + 7 + \ldots + (3n-2) + (3(n+1)-2) = HL_n + (3(n+1)-2) =$$
   $$\frac{1}{2}[n(3n-1) + (6n+2)] = \frac{1}{2}[3n^2 + 5n + 2].$$

   Då
   $$HL_{n+1} = \frac{1}{2}(n+1)(3(n+1)-1) = \frac{1}{2}(n+1)(3n+2) = \frac{1}{2}(3n^2 + 5n + 2).$$

   Beviset är nu klart enligt induktionsaxiomet eftersom vi visat $VL_1 = HL_1$ och att för alla naturliga tal n gäller att $VL_n = HL_n$ medför att $VL_{n+1} = HL_{n+1}$.

3. Det finns $\binom{12}{3} = \frac{12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3} = 220$ olika sätt att välja ut pojkar och $\binom{8}{2} = \frac{8 \cdot 7/1}{cdot2} = 28$ olika sätt att välja ut flickorna. Vart och ett av de 220 valen av pojkar kan kombineras med vart och ett av de 28 valen av flickor. Så

   SVAR: $220 \cdot 28 = 6160$ olika möjligheter.

4. Vi tar tex $(Z_5, +)$. Den har tabellen

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

5. Vi betraktar delgruppen $H = \{a^3, a^6, a^9, a^{12} = e\}$. Den är sidoklass till sig själv $H = He$ om man så vill. Övriga sidoklasser är $Ha = \{a^4, a^7, a^{10}, a^{13} = a\}$ och $Ha^2 = \{a^5, a^8, a^{11}, a^{14} = a^2\}$.

6. 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.

DEL B

7. Addition av de bägge ekvationerna ger ekvationen $6x + 11y = 8$, dvs eftersom vi räknar modulo 11 att $6x = 8$. Då $2 \cdot 6 = 1$ i ringen Z_{11} får vi att $2 \cdot 6x = 2 \cdot 8$ dvs $x = 5$. Då $x + y = 5$ så måste $y = 0$. Enda möjligheten för en lösning är att $(x, y) = (5, 0)$. Dessa värden på x och y visar sig också efter en kontroll satisfierar vårt system så de är verkligen lösningar
SVAR: $x = 5$ och $y = 0$.

8. Totala antalet sätt att dela in mängden i fyra icketomma delmängder ges av Stirlingtalet $S(7, 4)$ och antalet sätt att dela in denna mängd i fyra delar där 1 och 2 hamnar i samma mängd blir då $S(6, 4)$ eftersom vi då kan betrakta 1 och 2 som en enhet. Svaret ges alltså av skillnaden $S(7, 4) - S(6, 4)$.

9.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.

10. Vi skall visa att mellan varje par av noder finns minst en stig. Betrakta två godtyckliga noder w och u. Det finns $n - 2$ övriga noder. Om det saknas kant mellan w och u går samtliga kanter från w och u till dessa $n - 2$ noder. Det finns $n - 1$ sådana kanter enligt uppgiften. Alltså måste, enligt pigeon hole principen, minst en av dessa $n - 2$ noder, noden x, träffas av minst två kanter e_1 och e_2 från w och u. Eftersom grafen saknar multipla kanter så måste en av kanterna e_1 och e_2 komma från w och den andra från u. Vi fann nu en stig $w - x - u$.