Matematik Chalmers

Tentamen i TMV210 och MAD100 Diskret matematik den 22 oktober 2004, kl. 14.00-18.00

Hjälpmedel: Inga hjälpmedel

Telefonvakt: Tobias Gebäck, tel. 0739-779268

1. (6p) Lös först den diofantiska ekvationen

$$10x + 23y = 7.$$

   Ange sedan inversen till $[10]$ i $\mathbf{Z}_{23}$.

2. (8p) Hur många sjusiffriga tal där alla siffror är 1, 2 eller 3 finns det

   (a) totalt?

   (b) som innehåller exakt två ettor?

   (c) som saknar ettor?

   (d) som innehåller minst fyra ettor?

3. (6p) Avgör vilka av följande två logiska argument som är giltiga.

   (a)
   $$\begin{array}{r} p \vee q \vee r \\ \neg s \rightarrow \neg p \\ p \vee q \rightarrow s \\ p \vee r \rightarrow t \\ \neg t \vee q \\ \hline s \end{array}$$

   (b)
   $$\begin{array}{r} a \text{ är ett heltal} \\ b = 6a \\ \text{Det finns ett heltal } k \text{ sådant att } c = bk + 3 \\ \hline c \text{ är ett udda heltal} \end{array}$$

4. (6p) Visa att det för alla positiva heltal n gäller att

$$n + 3\sum_{i=1}^{n} i(i-1) = n^3.$$

5. (6p) Antag att du är användare i RSA-krypteringssystemet och att din slutna nyckel består av de två primtalen $p = 5$ och $q = 11$ och talet $s = 23$ (som är relativt primt $\Phi(pq)$). Således består din öppna nyckel av talen 55 och 23.

   Antag nu att någon skickar dig ett meddelande som är krypterat för att ingen annan än du ska kunna läsa det. Om meddelandet är 3, vad är då det riktiga meddelandet?

6. (6p) Betrakta ekvationssystemet

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$

Visa, genom att översätta till en diofantisk ekvation, att systemet är lösbart om och endast om $\text{sgd}(m_1, m_2) | a_1 - a_2$.

7. (6p) Vad blir koefficienten framför $x^9y^4z^2$ i utecklingen av $(x + y^2 + 3z)^{13}$?

8. (6p) Antag att $G = (V, E)$ är en sammanhängande graf, där varje kant tillskrivs en "kostnad", dvs till varje kant $e \in E$ tillskrivs ett positivt reellt tal $k(e)$. Antag också att olika kanter alltid har olika kostnad. För varje delgraf till G säger man att kostnaden för delgrafen är summan av vad alla dess kanter kostar. Man definierar sedan det *minimala uppspännande trädet* $T(G)$ till G som den sammanhängande delgraf som innehåller alla G's noder som har lägst kostnad. (Det är uppenbart att $T(G)$ blir ett träd, ty annars skulle man kunna ta bort en kant från $T(G)$ och fortfarande ha en sammanhängande graf på alla G's noder med en lägre kostnad.)

   En algoritm som finner $T(G)$ är den s.k. *giriga algoritmen* där man steg för steg plockar på sig kanter (och tillhörande ändnoder) där man i varje steg plockar den billigaste kanten bland de kanter som man ännu inte tagit och som inte bildar någon cykel tillsammans med tidigare valda kanter. Man avslutar arbetet så fort man på detta sätt fått med alla G's noder. Använd induktion till att visa att denna algoritm verkligen ger det minimala uppspännande trädet.

/Johan Jonasson

Lösningar

1. Eftersom $\text{sgd}(10, 23) = 1$ är ekvationen lösbar. Man ser (till exempel med hjälp av Euklides algoritm) att $10 \cdot 7 + 23 \cdot (-3) = 1$, varför en lösning till ekvationen ges av $(x, y) = (7 \cdot 7, 7 \cdot (-3)) = (49, -21)$. Den allmänna lösningen blir då

$$(x, y) = (49 - 23n, -21 + 10n),\ n \in \mathbf{Z}.$$

   Vi ser också ur ett utrryck ovan att $[10]^{-1} = [7]$ i $\mathbf{Z}_{23}$.

2. I (a) finns det tre val för varje position så enligt multiplikationsprincipen blir det sökta antalet 3^7.

   För del (b) gäller att det finns $\binom{7}{2}$ olika sätt att placera ut de två ettorna och för varje sådant val finns det 2^5 olika sätt att fylla övriga positioner. Svaret är alltså $\binom{7}{2}2^5 = 672$.

   Svaret i del (c) är 2^5 helt i analogi med del (a). I del (d) får man svaret genom att summera antalet tal med exakt fyra ettor med antalet med exakt fem ettor, antalet med exakt sex ettor och antalet tal med exakt sju ettor. Dessa termer räknas ut på samma sätt som del (b) och slutsvaret blir 379.

3. (a) Vi försöker leta upp ett motexempel, dvs en situation där slutsatsen är falsk samtidigt som alla hypoteserna är sanna: Om $s = F$ kräver andra hypotesen att $p = F$ och rad 3 kräver att även $q = F$. Men då kräver hypotes 5 att $t = F$, så fjärde raden kräver vidare att $r = F$. Sammantaget har vi fått att $p = q = r = F$, vilket motsäger den första hypotesen. Argumentet är alltså giltigt.

(b) Argumentet är giltigt ty om a är ett heltal och $b = 6a$ blir $b = 6a$ jämnt och därför blir även bk jämnt, varför $c = bk + 4$ är udda.

4. Vi använder induktionsprincipen: Då $n = 1$ hävdar formeln att $1 = 1^3$ vilket är uppenbart sant. Låt nu m vara ett godtyckligt positivt heltal och antag att formeln gäller då $n = m$, dvs att

$$m + 3\sum_{i=1}^{m} i(i-1) = m^3.$$

Då gäller det att

$$(m+1)+3\sum_{i=1}^{m+1} i(i-1) = 1+m^3+3m(m+1) = 1+3m+3m^2+m^3 = (m+1)^3.$$

Saken är klar.

5. Den del av den slutna nyckeln som inte finns angiven i uppgiften är inversen till s modulo $\Phi(pq)$, dvs inversen till 23 modulo $(p-1)(q-1) = 40$. Denna invers ges av $t = 7$, ty $7 \cdot 23 = 161 \equiv 1 \bmod 40$. Det riktiga meddelandet ges nu av 3^7 modulo 55. Lite räknande ger att $3^7 = 42$ modulo 55, dvs det riktiga meddelandet är 42.

6. Att lösa ekvationsystemet innebär att man ska finna två heltal k_1 och k_2 sådana att $x = a_1 + k_1 m_1 = a_2 + k_2 m_2$. Detta kan skrivas som

$$m_1 k_1 - m_2 k_2 = a_2 - a_1$$

dvs en diofantisk ekvation. Denna är enligt känt resultat lösbar om och endast om $sgd(m_1, m_2) | a_2 - a_1$ som önskat.

7. Enligt binomialsatsen gäller att

$$(x + y^2 + 3z)^{13} = \sum_{k=0}^{13} \binom{13}{k} x^k (y^2 + 3z)^{13-k}.$$

En term som innehåller x^9 uppstår precis då $k = 9$ och denna term blir $\binom{13}{9} x^9 (y^2 + 3z)^4$. För att se vad detta uttryck får för koefficient framför $x^9 y^4 z^2$ använder vi binomialsatsen igen för att utveckla $(y^2 + 3z)^4$. Denna utveckling har en $y^4 z^2$-term med koefficient $\binom{4}{2} 3^2$. Sammantaget blir koefficienten framför $x^9 y^4 z^2$ i utvecklingen av ursprungsuttrycket $\binom{13}{9}\binom{4}{2} 3^2 = 38610$.

8. Algoritmen fungerar uppenbarligen för en graf med två noder, så antag att vi vet för ett visst positivt heltal n fungerar algoritmen för alla grafer med n noder. Betrakta nu en graf G med $n + 1$ noder. Det är uppenbart att det uppspännande trädet på G måste innehålla grafen allra billigaste kant, ty om så inte vore fallet skulle man kunna skapa ett billigare träd genom att lägga till denna kant och ta bort en annan kant. Räkna nu in denna och betrakta därefter dess två grannoder

som en enda nod. Detta skapar möjligen en multigraf med n noder, men skapa då en graf genom att då dubbla kanter förekommer helt enkelt ta bort den dyraste. Vi har då en graf G' med n noder och den giriga algoritmen applicerad på denna graf ger det minimala uppspännande trädet på G'. Tillsammans med den först valda kanten får vi det minimala uppspännande trädet på G och en sekunds eftertanke visar att det är just den giriga algoritmen på hela G som vi använt. Resultatet följer nu av induktionsprincipen.