Chalmers Tekniska Högskola

Lösningsförslag till omtentamen på kursen TMV211: Inledande diskret matematik

Den 5 Januari 2021 kl 08:30-12:30
Examinator: Jonathan Nilsson

---

1. Hitta alla heltal x som löser följande ekvationssystem: [7p]

$$\begin{cases} x \equiv 7 \mod 11 \\ x \equiv 3 \mod 13 \end{cases}$$

Lösningsförslag

Den övre ekvationen kan skrivas $x = 7 + 11y$ där $y \in \mathbb{Z}$. Insättning i den nedre ger $7 + 11y + 13z = 3$ som kan skrivas $11y + 13z = -4$. Denna diofantiska ekvation kan t.ex. lösas med Euklides algoritm.

Vi har $13 = 11 + 2$, men redan här ser vi att $2| - 4$ så vi kan skriva $13 - 11 = 2$ och därför har vi $2 \cdot 11 + (-2 \cdot 13) = -4$ så en lösning till $11y + 13z = -4$ är $(y, z) = (2, -2)$. Denna ger $x = 7 + 11 \cdot 2 = 29$. Enligt Kinesiska restsatsen har systemet en unik lösning modulo $11 \cdot 13$ så mängden av alla heltal x som uppfyller systemet är $\{29 + 143k \mid k \in \mathbb{Z}\}$.

2. Fyra syskon i olika åldrar ska fördela tio identiska pepparkakor mellan sig. På hur många olika sätt kan fördelningen göras... [8p]

   (a) ...utan några övriga villkor?

   (b) ...om de två yngsta syskonen ska få minst en pepparkaka var?

   (c) ...om alla ska få ett udda antal pepparkakor?

   (d) ...om alla ska få olika många pepparkakor?

Lösningsförslag

(a) Vi använder tankesättet med "bollar och väggar". Vi formar alltså sekvenser med 10 pepparkakssymboler ♡ och 3 väggar | som avskiljer pepparkakor till de 4 syskonen. Till exempel motsvarar sekvensen ♡♡♡|♡♡||♡♡♡♡♡ att det första syskonet får tre, andra syskonet får två, tredje syskonet får noll, och fjärde syskonet får fem pepparkakor. Vi har alltså totalt 13 symboler varav tre ska väljas till att vara väggar. Alltså kan fördelningen göras på $\binom{13}{3} = 286$ sätt.

(b) Ge de två yngsta syskonen varsin pepparkaka. Då har vi kvar 8 pepparkakor som ska fördelas. Precis som i (a) går detta att göra på $\binom{11}{3} = 165$ sätt.

(c) Ge alla syskon 1 pepparkaka, och para ihop resterande 6 pepparkakar i tre högar med två i varje. För att alla ska få ett udda antal ska nu dessa tre högar fördelas godtyckligt mellan syskonen, så precis som i (a) går detta att göra på $\binom{6}{3} = 20$ sätt.

(d) Först kan man tänka på vilka antal pepparkakor som ska delas ut till de fyra syskonen. Vi söker alltså alla sätt att skriva talet 10 som en summa av fyra olika tal ≥ 0. Går man igenom de olika fallen ser man att detta kan göras på 5 sätt: $(0+1+2+7), (0+1+3+6), (0+1+4+5), (0+2+3+5), (1+2+3+4)$. För var och en av dessa kan man också välja vilket syskon som ska få vilket antal, så vi får multiplicera med antalet permutationer av syskonen, alltså $4!$. Totala antalet sätt blir $5 \cdot 4! = 5! = 120$.

3. Vi definierar en logisk operator $\heartsuit$ med följande sanningstabell, där 1 betyder sant och 0 betyder falskt. [8p]

p	q	$p \heartsuit q$
1	1	1
1	0	1
0	1	0
0	0	1

Avgör om var och en av följande utsagor är tautologier, kontradiktioner, eller ingetdera. Motivera dina svar.

(a) $(p \vee q) \heartsuit (p \wedge q)$

(b) $(p \wedge r) \vee (q \heartsuit r)$

(c) $(p \heartsuit q) \heartsuit p$

(d) $p \heartsuit (q \heartsuit p)$

Lösningsförslag

(a) **Tautologi**. Antag att uttrycket är falskt. Då måste enligt tabellen $(p \vee q)$ vara falskt och $(p \wedge q)$ vara sant vilket är omöjligt. Alltså kan uttrycket inte vara falskt och därför är det en tautologi.

(b) **Ingetdera**. För $(p, q, r) = (1, 1, 1)$ blir uttrycket sant, och för $(p, q, r) = (0, 0, 1)$ blir uttrycket falskt. Därför är uttrycket varken en tautologi eller en kontradiktion.

(c) **Tautologi**. Uttrycket är sant då $(p, q) = (1, 1)$ så vi undersöker om det kan vara falskt. I sådant fall måste p vara sant, och $(p \heartsuit q)$ falskt vilket inte är möjligt när $p = 1$. Alltså är uttrycket aldig falskt.

(d) **Ingetdera**. Uttrycket är sant då $(p, q) = (1, 1)$ och falskt då $(p, q) = (0, 0)$.

En alternativ lösning kan vara att först notera att $p \heartsuit q \Leftrightarrow p \vee \neg q \Leftrightarrow p \leftarrow q$ och sedan förenkla de vanliga logiska operatorerna.

4. Använd induktion för att visa att för varje heltal $n \geq 1$ så gäller [8p]

$$\sum_{k=1}^{n} \frac{n+1}{k(k+1)} = n.$$

Lösningsförslag

Vi dividerar båda sidor med $(n+1)$ och inför predikatet

$$S(n) : \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

Vi bevisar nu att $S(n)$ är sann för alla $n \geq 1$ med induktion.
Bassteg: Vi har $S(1) : \sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{1+1}$ vilket är ekvivalent med $\frac{1}{1(1+1)} = \frac{1}{1+1}$. Alltså är $S(1)$ sann.

Induktionssteg. Antag nu att $S(p)$ är sann för något $p \geq 1$. Vi ska bevisa att det följer att $S(p+1)$ också är sann. Vänsterledet i $S(p+1)$ kan förenklas:

$$\sum_{k=1}^{p+1} \frac{1}{k(k+1)} = \sum_{k=1}^{p} \frac{1}{k(k+1)} + \frac{1}{(p+1)(p+2)} = \frac{p}{p+1} + \frac{1}{(p+1)(p+2)} = \frac{p(p+2)+1}{(p+1)(p+2)}$$

$= \frac{(p+1)^2}{(p+1)(p+2)} = \frac{p+1}{p+2} = \frac{p+1}{(p+1)+1}$, vilket är högerledet i $S(p+1)$. (I andra likheten ovan använde vi induktionsantagandet $S(p)$). Vi har nu visat att $S(1)$ är sann och att $S(p) \Rightarrow S(p+1)$. Enligt induktionsprincipen är påståendet sant för alla heltal $n \geq 1$.

5. Rita för varje deluppgift en graf som uppfyller villkoren, eller motivera varför en sådan graf inte existerar. [9p]

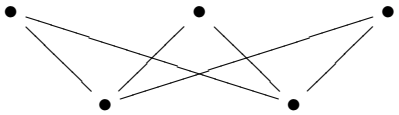
   (a) En sammanhängande bipartit graf med 5 noder, som inte är ett träd.

   (b) En sammanhängande graf med 5 noder som har en Eulerväg men saknar Hamiltonstigar.

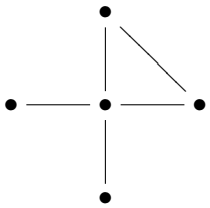
   (c) En multigraf med 3 noder som är sammanhängande men saknar Eulervägar.

Lösningsförslag

(a) Tag exempelvis den fullständiga bipartita grafen $K_{3,2}$:



(b)



(c) **En sådan graf existerar ej**. Bevis: Enligt Eulers sats finns det en Eulerväg i en sammanhängande graf om och endast om max två noder har udda gradtal. För att Eulervägar inte ska existera måste därför alla tre noderna ha udda gradtal. Men då blir summan av alla gradtal i grafen udda vilket är omöjligt - varje kant i grafen adderar ju två till det totala gradtalet, så detta tal är jämnt i alla grafer.

6. Vi definierar en binär operation $\star$ på heltalen $\mathbb{Z}$ enligt följande: [10p]

$$a \star b = 5a + 3b$$

(a) Beräkna $(3 \star 1) \star 10$ och $3 \star (1 \star 10)$. Är operationen $\star$ associativ?

(b) Finns det ett identitetselement? Finns det ett nollelement?

(c) Hitta alla heltal x som uppfyller $(x - 3) \star (x + 1) = x^2$

(d) Är påståendet $\forall z : \big(\exists x, y : (x \star y = z)\big)$ sant eller falskt? Ge ett bevis eller ett motexempel! (universum är heltalen)

Lösningsförslag

(a) $(3 \star 1) \star 10 = 18 \star 10 = 120$ och $3 \star (1 \star 10) = 3 \star 35 = 120$. För att operationen ska vara associativ måste dock $a \star (b \star c) = (a \star b) \star c$ för alla a, b, c vilket inte är sant - ta t.ex. $a = b = c = 1$. Operationen är alltså **inte associativ**.

(b) Om e är identitetselement och n är nollelement ska det bland annat gälla för alla x att $e \star x = x$ och $n \star x = n$, vilket är ekvivalent med $5e + 3x = x$ och $5n + 3x = n$. Men några sådana heltal n eller e som uppfyller detta för alla x samtidigt finns ej. Alltså **saknas både identitetselement och nollelement för** $\star$.

(c) Enligt definitionen får vi

$$(x-3)\star(x+1) = x^2 \Leftrightarrow 5(x-3)+3(x+1) = x^2 \Leftrightarrow x^2-8x+12 = 0 \Leftrightarrow (x-6)(x-2) = 0.$$

Ekvationen har alltså två lösningar, $x = 6$ respektive $x = 2$.

(d) Frågan är om den diofantiska ekvationen $5x + 3y = z$ är lösbar för varje fixt z. Eftersom $gcd(5, 3) = 1$ har ekvationen $5x + 3y = 1$ lösningar. Multiplicerar man sådana x, y med z får man därför en lösning till $5x + 3y = z$ för vilket z som helst. Påståendet är därför sant. Mer explicit kan man se att för varje fixt z kan man t.ex. välja $(x, y) = (-z, 2z)$, då blir $x \star y = z$.

7. Boole ska skicka ett RSA-krypterat meddelande till Arkimedes. Booles ursprungliga meddelande är ett tal $0 \leq M \leq 200$. Han använder Arkimedes offentliga nyckel $(n, e) = (221, 77)$ för krypteringen och får fram ett krypterat meddelande $C \equiv M^e \pmod{221}$ som han skickar till Arkimedes. Euler får tag på det krypterade meddelandet och ser att $C = 186$. Hjälp honom att knäcka koden och hitta det ursprungliga meddelandet M! Redovisa tydligt de olika stegen i din lösning. [10p]
Tips: Börja med att primtalsfaktorisera talet n.

Lösningsförslag

Vi söker M så att $M^{77} \equiv 186 \pmod{221}$.

För att hitta primfaktorer till $n = 221$ behöver man bara testa primfaktorer under $\sqrt{221}$ alltså upp till 14. Man finner då att $221 = 13 \cdot 17$. Vi skriver $p = 13$ och $q = 17$.

Vi beräknar nu $\varphi(n) = (p-1)(q-1) = 12 \cdot 16 = 192$. Vi söker nu ett positivt tal d som är invers till $e = 77$ modulo $\varphi(n)$. Vi ska alltså lösa $d \cdot 77 + k \cdot 192 = 1$. Med Euklides algoritm får vi $192 = 2 \cdot 77 + 38$ och $77 = 2 \cdot 38 + 1$. Därför blir $1 = 77 - 2 \cdot 38 = 77 - 2(192 - 2 \cdot 77) = (-2) \cdot 192 + 5 \cdot 77$. Alltså gäller $d \cdot 77 + k \cdot 192 = 1$ då $d = 5$ och $k = -2$, så $d = 5$ är den sökta inversen till e. Vi upphöjer båda sidor av kongruensen $186 = M^e$ med $d = 5$, då får vi modulo 221:

$$186^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+2 \cdot \varphi(n)} \equiv M \cdot (M^{\varphi(n)})^2 \equiv M \cdot 1^2 \equiv M$$

där den näst sista likheten följer av Eulers sats. Vi har alltså $M \equiv 186^5 \equiv 101 \pmod{221}$. Det ursprungliga meddelandet är alltså $M = 101$.

Kommentar: Enda anledningen att vi kunde knäcka koden var att talet $n = 221$ var så litet att vi kunde hitta dess faktorer. Datorer använder samma algoritm fast med hundratals siffror i n - det finns därför inget snabbt sätt att hitta faktorerna!