Inledande diskret matematik D, HT2014
Lösningar till tentan 2014-08-20

1. En logisk formel sägs vara en *tautologi* om den är sann oavsett sanningsvärdena på de ingående Booleska variablerna. Här har vi tre variabler p, q, r så det finns totalt 8 möjliga kombinationer av sanningsvärden. Det är lite opraktisk att testa alla möjligheter i varje deluppgift (totalt 32 fall), så vi försöker förenkla arbetet först. Alla fyra formlerna är implikationer, och en implikation är alltid sann då hypotesen är falsk. Så det enda intressanta fallet är då hypotesen är sann. Formeln är alltså en tautologi om och endast om slutsatsen är sann när som helst hypotesen är det eller, ekvivalent, om hypotesen är falsk när som helst slutsatsen är det. Sett omvänt, för att bevisa att en av formlerna inte är en tautologi så räcker det att hita en instans då slutsatsen är falsk trots att hypotesen är sann.

   (a) En tautologi. Hypotesen och slutsatsen säger både två att r är sann så snart minst en av p och q är det.

   (b) En tautologi. Hur kan hypotesen vara sann ? Till att börja med så måste $\neg q$ vara sann, alltså q vara falsk. Men då måste p vara sann för att göra $p \vee q$ sann. Och om $p \to r$ är sann, då blir r, som är slutsatsen, också sann.

   (c) En ej tautologi. Om både p och q är falska så är hypoteserna sanna men slutsatsen falsk.

2. Eftersom 7 är ett primtal så är $a^6 \equiv 1 \pmod 7$ då a inte är delbart med 7, enligt Fermats sats. Varken 2 eller 3 är delbara med 7 så vi kan räkna modulo 7 enligt:

$$2^{12} = (2^6)^2 \equiv 1^2 \equiv 1,$$
$$3^{11} = (3^6)^2 \cdot 3^{-1} \equiv (1)^2 \cdot 5 \equiv 5.$$

   Så $2^{12} + 3^{11} \equiv 1 + 5 \equiv 6 \pmod 7$.

3. Vi kan dela igenom med 2 utan att ändra ekvationen och i stället lösa $17x - 13y = 5$. Vi vet att det kommer att finnas lösningar ty SGD$(17, 13) = 1$. Euklides framåt ger

$$17 = 13 + 4, \quad 13 = 3 \cdot 4 + 1,$$

   och sedan bakåt

$$1 = 13 - 3 \cdot 4 = 13 - 3(17 - 13) = 4 \cdot 13 - 3 \cdot 17.$$

Multiplicera igenom med 5 för att få $5 = 20 \cdot 13 - 15 \cdot 17$, så en lösning till vår Diof. ekv. är $x_0 = -15$, $y_0 = -20$. Den allmänna lösningen ges av

$$x = x_0 + \left(\frac{b}{d}\right) n, \quad y = y_0 + \left(\frac{a}{d}\right) n, \quad n \in \mathbb{Z}.$$

Här är $a = 17$, $b = 13$, $d = 1$ så den allmänna lösningen blir

$$x = -15 + 13n, \quad y = -20 + 17n, \quad n \in \mathbb{Z}.$$

4. Tanken är att man ska bevisa det med induktion.

   Steg 1: Kolla basfallet $n = 1$. VL $= 1 \cdot 0 = 0$ och HL $= \frac{1 \cdot 2 \cdot 0}{3} = 0$.

   Steg 2: Antag att
$$\sum_{k=1}^{p} k(k-1) = \frac{p(p+1)(p-1)}{3}. \tag{1}$$
   Vi vill deducera att
$$\sum_{k=1}^{p+1} k(k-1) = \frac{(p+1)(p+2)p}{3}. \tag{2}$$
   Vi kör med det vanliga tricket och delar upp summan i VL av (2) s.a. (1) kan användas:
$$\sum_{k=1}^{p+1} k(k-1) = \left[\sum_{k=1}^{p} k(k-1)\right] + (p+1)p =$$
$$= \frac{p(p+1)(p-1)}{3} + p(p+1) = \frac{p(p+1)}{3}\left[(p-1)+3\right] = \frac{p(p+1)(p+2)}{3}, \quad \text{v.s.v.}$$

5. Den "vanliga" formeln för lösningarna till en kvadratisk ekvation gäller så länge allting maker sense i sammanhanget. Dvs det finns följande sats:

   Sats. *Låt n vara ett positivt heltal och a, b, c heltal sådana att SGD$(a, n) = 1$. Den kvadratiska kongruensen*
$$ax^2 + bx + c \equiv 0 \ (\textit{mod}\ n)$$
   är lösbar om och endast om $b^2 - 4ac$ är en kvadrat i $\mathbb{Z}_n$. I så fall ges lösningen/arna av
$$x \equiv (2a)^{-1} \cdot \left(-b \pm \sqrt{b^2 - 4ac}\right) \ (\textit{mod}\ n).$$

Här är $n = 7$, $a = 1$, $b = -2$, $c = -1$. Så $b^2 - 4ac = 8 \equiv 1 = (\pm 1)^2$. Så kongruensen är lösbar och lösningen är

$$x \equiv 2^{-1} \cdot (2 \pm 1) \equiv 4 \cdot (2 \pm 1) \Rightarrow$$
$$\Rightarrow x_1 \equiv 4(2+1) = 12 \equiv 5, \quad x_2 \equiv 4(2-1) \equiv 4.$$

SVAR: Två lösningar: $x_1 \equiv 5 \pmod 7$, $x_2 \equiv 4 \pmod 7$.

6. Det finns $\binom{17}{2}$ sätt att välja de två kvinnliga talrollerna och $\binom{13}{3}$ sätt att välja de manliga talrollerna. Enligt multiplikationsprincipen finns det $\binom{17}{2}\binom{13}{3}$ sätt att tillsätta talrollerna.

   När talrollerna är tillsatta kommer det att finnas 15 flickor och 10 pojkar kvar.

   (a) Om alla 7 statister ska vara manliga så finns det $\binom{10}{7}$ sätt att välja dem.

   (b) Om bland de 7 statisterna det måste finnas minst två av varje kön, så har vi följande fyra möjligheter:

   i. 2 flickor och 5 pojkar.
   ii. 3 flickor och 4 pojkar.
   iii. 4 flickor och 3 pojkar.
   iv. 5 flickor och 2 pojkar.

   Enligt samma slags resonemang som tidigare så finns det följande antal alternativ i var och ett av dessa fyra fall:

   i. $\binom{15}{2}\binom{10}{5}$,
   ii. $\binom{15}{3}\binom{10}{4}$,
   iii. $\binom{15}{4}\binom{10}{3}$,
   iv. $\binom{15}{5}\binom{10}{2}$.

   Det totala antalet alternativ i (b) är alltså summan av dessa, dvs

$$\binom{15}{2}\binom{10}{5} + \binom{15}{3}\binom{10}{4} + \binom{15}{4}\binom{10}{3} + \binom{15}{5}\binom{10}{2}.$$

7. (a) Antag att $g \circ f$ är bijektiv, på en mängd S säg. Speciellt är den surjektiv så för varje $s \in S$ finns det s' sådan att $(g \circ f)(s') = s$. Om vi sätter $s'' = f(s')$ då har vi $g(s'') = s$, så g är surjektiv.

   När det gäller f, antag motsatsen till det som påstås och att f inte är injektiv. Då måste det finnas $s_1 \neq s_2$ sådana att $f(s_1) = f(s_2)$. Men då är också $(g \circ f)(s_1) = g(f(s_1)) = g(f(s_2)) = (g \circ f)(s_2)$, så $g \circ f$ är inte heller injektiv, en motsägelse.

(b) Låt $S = \mathbb{N}$ och definiera $f,\ g : S \to S$ enligt $f(s) = 2s$, $g(s) = \lfloor s/2 \rfloor$. Då är $g \circ f = \mathrm{id}_S$ så den är bijektiv. Men f är inte surjektiv, ty $f(S)$ innehåller inga udda tal, och g är inte injektiv ty $g(2s) = g(2s+1) = s$ för alla $s \in S$.

8. Vi söker en lösning till den Diofantiska ekvationen $x^2 - y^2 = 2z^2$, där z är udda. Det finns dock ingen lösning, något som kan ses lättast genom att tänka modulo 4. Eftersom z är udda så måste $z^2 \equiv 1 \pmod 4$ och således är HL $\equiv 2 \pmod 4$. Men varje heltalskvadrat är kongruent till $0 \vee 1 \pmod 4$ och VL är således kongruent till $(0-0) \vee (0-1) \vee (1-0) \vee (1-1) \pmod 4 = 0 \vee 3 \vee 1 \pmod 4$. Så VL kan inte vara kongruent till HL modulo 4.