Inledande diskret matematik D, HT2014
Lösningar till tentan 2013-01-19

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. Här har r inget med saken att göra. Hypotesen säger att $p \to q$ samt att $\neg q$, dvs att q är falsk. Men då måste även p vara falsk, så slutsatsen $\neg p$ är sann.

   (b) En tautologi. Antag att slutsatsen är falsk. Då är p sann och minst en av $q,\ r$ är falska. Men om q vore falsk så vore då även $p \to q$ falsk, så minst en av $p \to q$ och r måste vara falsk, dvs hypotesen är falsk.

   (c) En tautologi. Hypotesen är sann endast då $p,\ q,\ r$ är alla sanna. Men då är det också sann att p implicerar både q och r.

2. Eftersom 5 är ett primtal så är $a^4 \equiv 1 \pmod 5$ då SGD$(a,\ 5) = 1$. Detta gäller för både $a = 2$ och $a = 3$ så vi kan räkna enligt

$$2^{18} = (2^4)^4 \cdot 2^2 \equiv 1^4 \cdot 4 \equiv 4 \pmod 5,$$
$$3^{18} = (3^4)^4 \cdot 3^2 \equiv 1^4 \cdot 9 \equiv 4 \pmod 5.$$

   Så $2^{18} + 3^{18} \equiv 4 + 4 \equiv 3 \pmod 5$.

3. Vi kan dela med två och få ekvationen $17x + 14y = 4$. Euklides framåt ger

$$17 = 14 + 3, \quad 14 = 4 \cdot 3 + 2, \quad 3 = 2 + 1,$$

   och sedan bakåt

$$1 = 3 - 2 = 3 - (14 - 4 \cdot 3) = 5 \cdot 3 - 14 = 5(17 - 14) - 14 = 5 \cdot 17 - 6 \cdot 14.$$

   Multiplicera igenom med 4 för att få $4 = 20 \cdot 17 - 24 \cdot 14$. Så en lösning till vår Diof. ekv. är $x_0 = 20$, $y_0 = -24$. Den allmänna lösningen blir

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

Här är $a = 17$, $b = 14$, $d = 1$ så den allmänna lösningen är

$$x = 20 + 14n, \quad y = -24 - 17n, \quad n \in \mathbb{Z}.$$

4. Enligt den Kinesiska Restsatsen så finns det en unik lösning modulo $17 \cdot 10 = 170$, som ges av

$$x \equiv 3(10b_1) + 2(17b_2) \pmod{170}, \tag{1}$$

där $10b_1 \equiv 1 \pmod{17}$ och $17b_2 \equiv 1 \pmod{10}$. Vi hittar $b_1,\, b_2$ enligt

$$\begin{aligned} 1 \equiv 10b_1 \equiv -7b_1 \Rightarrow b_1 \equiv -5 \pmod{17}, \\ 1 \equiv 17b_2 \equiv -3b_2 \Rightarrow b_2 \equiv 3 \pmod{10}. \end{aligned}$$

Insättning in i (1) ger $x \equiv -3 \cdot 5 \cdot 10 + 2 \cdot 3 \cdot 17 \equiv -48 \equiv 122 \pmod{170}$.

5. (a) *Reflexiv:* $f \mathcal{R} f$ är uppenbart, ty $f(0) = f(0)$ och $f(1) = f(1)$, det spelar ju ingen roll vad f är.
Symmetrisk: Om $f(0) = g(0)$ så är även $g(0) = f(0)$. Samma sak för $x = 1$.
Transitiv: Om $f(0) = g(0)$ och $g(0) = h(0)$ så är även $f(0) = h(0)$. Samma sak för $x = 1$.

(b) En ekvivalensklass bestäms av värdena $f(0)$ och $f(1)$, som annars kan vara vilka två reella tal som helst. M.a.o. finns det en naturlig bijektion mellan ekvivalensklasserna och punkterna $(u,\, v) \in \mathbb{R}^2$. För en linjär funktion $f(x) = ax + b$ gäller att $f(0) = b$ och $f(1) = a + b$. Linjen bestäms också entydigt av dessa två y-värden $(b,\, a + b)$, så det finns en unik linjär funktion i varje ekvivalensklass och en bijektion $(u,\, v) \leftrightarrow (b,\, a + b)$, given av $b = u$, $a = v - u$. Så en bijektion mellan ekvivalensklasserna och linjära funktioner ges explicit av

$$(u,\, v) \leftrightarrow f(x) = (v - u)x + u.$$

6. Om man ska få en udda summa så måste den ena kulan ha ett jämnt nummer och den andra ett udda nummer. Så den ena bollen dras från $\{2,\, 4,\, 6,\, 8,\, 10\}$ och den andra från $\{1,\, 3,\, 5,\, 7,\, 9\}$. Det finns 5 val för varje boll och därmed, enligt multiplikationsprincipen, $5 \cdot 5 = 25$ möjligheter för paret.

7. För att vara konkret, sätt $\mathbb{Z}_3 = \{0,\, 1,\, 2\}$ och $\mathbb{Z}_4 = \{0,\, 1,\, 2,\, 3\}$.

(a) Det finns 4 val för vart 0 ska skickas, sedan 3 val för 1 och sedan 2 val för 2. Så antalet injektiva funktioner är $4 \cdot 3 \cdot 2 = 24$.

(b) Låt unviersum U bestå av alla möjliga funktioner från $\mathbb{Z}_4$ till $\mathbb{Z}_3$. Då är $|U| = 3^4 = 81$, ty det finns 3 val per element och 4 element i definitionsmängden (multiplikationsprincipen). Vi kan räkna bort de funktioner som inte är surjektiva m.h.a. sållprincipen. Definiera följande delmängder till U:

$$A = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{0,\, 1\}\},$$
$$B = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{0,\, 2\}\},$$
$$C = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{1,\, 2\}\}.$$

Poängen är att de icke-surjektiva funktionerna är precis de som tillhör $A \cup B \cup C$. Enligt sållprincipen så är

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \quad (2)$$

Notera dessutom att

$$A \cap B = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{0\}\},$$
$$A \cap C = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{1\}\},$$
$$B \cap C = \{f : \mathbb{Z}_4 \to \mathbb{Z}_3 : f(\mathbb{Z}_4) \subseteq \{2\}\},$$
$$A \cap B \cap C = \phi, \quad \text{ty } \{0,\, 1\} \cap \{0,\, 2\} \cap \{1,\, 2\} = \phi.$$

Så $|A \cap B| = |A \cap C| = |B \cap C| = 1$ ty alla tre mängder består av endast en konstant funktion, medan att $|A \cap B \cap C| = 0$. Multiplikationsprincipen ger också att $|A| = |B| = |C| = 2^4 = 16$. Insättning av allting in i (2) ger att $|A \cup B \cup C| = 3 \cdot 16 - 3 \cdot 1 = 45$.
Så antalet surjektiva fuktioner är $|U| - |A \cap B \cap C| = 81 - 45 = 36$.

8. Vi kan räkna fram följande tabell:

$x \pmod 8$	$x^2 \pmod 8$
0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

Så varje heltalskvadrat är kongruent till $0,\ 1$ eller $4 \pmod 8$. Så en summa av tre heltakskvadrater är kongruent till

$$(0 \vee 1 \vee 4) + (0 \vee 1 \vee 4) + (0 \vee 1 \vee 4) \pmod 8.$$

Sedan är det bara att kolla att denna summa kan aldrig bli $7 \pmod 8$, v.s.v.