Eksamen MAT1140 - H2014 - Løsninger

Oppgave 1

Vi setter opp en vanlig sannhetsverditabell. La Φ betegne formelen i oppgaven. Tabellen vil bli som følger:

A	B	C	$A \Rightarrow B$	$\sim A \Rightarrow \sim C$	Φ
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	F	T	T
T	F	F	F	T	T
F	T	T	T	F	T
F	T	F	T	T	T
F	F	T	T	F	T
F	F	F	T	T	T

Konklusjonen blir at utsagnet er en tautologi

Oppgave 2

2a

Vi vet at 25 og 36 er innbyrdes primiske, så 1 kan skrives som en lineærkombinasjon av 25 og 36.
Vi bruker Euklids algoritme for å finne $(36, 25)$, og skriver hver rest vi finner som en lineærkombinasjon av 25 og 36:

36 = 25 + 11

11 = 36 - 25

$25 = 2 \cdot 11 + 3$

$3 = 25 - 2 \cdot 11 = 25 - 2 \cdot (36 - 25) = 3 \cdot 25 - 2 \cdot 36$

$11 = 3 \cdot 3 + 2$

$2 = 11 - 3 \cdot 3 = (36 - 25) - 3 \cdot (3 \cdot 25 - 2 \cdot 36) = 7 \cdot 36 - 10 \cdot 25$

$3 = 2 + 1$

$1 = 3 - 2 = (3 \cdot 25 - 2 \cdot 36) - (7 \cdot 36 - 10 \cdot 25) = 13 \cdot 25 - 9 \cdot 36$

Det gir oss at
$$3 = 39 \cdot 25 - 27 \cdot 36.$$

$\phi(n)$ er antall tall m mellom 0 og n som er innbyrdes primiske med n. For $n = 36$ vil tallene som er innbyrdes primiske med n være

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31 \text{ og } 35.$$

Det gir $\phi(36) = 12$.
Eulers teorem sier at hvis a og n er innbyrdes primiske, så er

$$a^{\phi(n)} \equiv 1 \ (mod\ n).$$

Det betyr at

$$25^{24} \equiv 1 \ (mod\ 36)$$

og at det er tilstrekkelig å finne

$$25^2 \ (mod\ 36).$$

Man kan enten regne direkte fra $25^2 = 625$, dele på 36, og få 13 som rest, eller man kan bruke at 25 og -11 er det samme modulo 36, og ta utgangspunkt i $121 = (-11)^2$. Regner man riktig, får man selvfølgelig 13 da også.

2b

En kvadratisk rest er en restklasse $\bar{a}$ i $\mathbb{Z}/(p)$, hvor p er et primtall, som tillater en løsning av likningen

$$\bar{x}^2 = \bar{a}.$$

Jeg har lært studentene at for å finne alle kvadratiske rester i $\mathbb{Z}/(p)$, er det tilstrekkelig å finne alle $\bar{a}^2$ hvor $1 \leq a \leq \frac{p-1}{2}$. Det gir at de kvadratiske restene i $\mathbb{Z}/(7)$ er $\bar{1}$, $\bar{4}$ og $\bar{2}(=\bar{9})$, og i $\mathbb{Z}/(11)$ er de $\bar{1}$, $\bar{4}$, $\bar{9}$, $\bar{5}(=\overline{16})$ og $\bar{3}(=\overline{25})$.
Utledningen av formelen for løsning av annengradslikninger er gyldig også for $\mathbb{Z}/(p)$ når $p > 2$ (Hvis $p = 2$ har vi problemer med å dele på 2.) Det betyr at løsningen av likningen vil være

$$\bar{x} = \frac{\bar{1} \pm \sqrt{\bar{5}}}{\bar{2}}.$$

I $\mathbb{Z}/(7)$ er ikke $\bar{5}$ en kvadratisk rest, så likningen har ingen løsning.
I $\mathbb{Z}/(11)$ har vi at $\bar{4}^2 = \bar{5}$ og at $(-\bar{4})^2 = \bar{5}$.
$-\bar{4} = \bar{7}$.
De to løsningene er altså $\frac{\bar{5}}{\bar{2}}$ og $\frac{\bar{8}}{\bar{2}}$.
Sistnevnte er $\bar{4}$, mens, for å finne førstnevnte, ser vi på $\bar{5} = \overline{16}$, og får at halvparten er $\bar{8}$.
Riktig svar er $\bar{4}$ og $\bar{8}$. Innsetting i likningen for kontroll gir at

$$4^2 - 4 - 1 = 11 \equiv 0 \ (mod\ 11)$$

og

$$8^2 - 8 - 1 = 55 \equiv 0 \ (mod\ 11).$$

Oppgave 3

3a

Eulers formel sier at summen over alle hjørnene i grafen er to ganger antall kanter, Summerer vi gradene, får vi 20. Det betyr at det er ti kanter.
Tar vi bort navet, og de fem kantene som er knyttet til navet, står vi igjen med 5 hjørner og 5 kanter.
Hvis denne restgrafen ikke er sammenhengende, vil den ha en isolert delgraf med ett eller to hjørner. I grafer med ett hjørne er graden 0, det vil si at hjørnet har grad 1 i den gitte grafen. I en sammenhengende graf med to hjørner har begge hjørnene grad 1, og hvis en slik inngår i restgrafen, må disse hjørnene ha grad 2 i den opprinnelige grafen. Begge deler er mot forutsetningen. Derfor må restgrafen være en sammenhengende graf hvor alle hjørner har grad 2, og 5-sykelen er eneste mulighet.
Merk at denne oppgaven bare kan løses under de forutsetningene som er gitt i læreboka, at ingen graf inneholder løkker (kant fra et hjørne til seg selv) og at det aldri går mer enn én kant mellom to hjørner.

Tegning av graf

3b

En graf er k-fargbar hvis vi kan tilordne hvert hjørne én av k farger $c_1, \ldots, c_k$ slik at nabohjørner ikke får samme farge.
Dette kan formuleres som at det finnes en partisjon av mengden av hjørner i k deler slik at to naboer aldri ligger i samme del.
Grafen i 3a kan ikke være 3-fargbar. Hvis navet har en farge, må alle de andre hjørnene ha en av de to andre fargene. En syklisk graf med et odde antall hjørner er ikke 2-fargbar.

3c

La hjørnene i V være farget med fargene $c_1, \ldots, c_k$. Vi k-farger $V \uplus V$ ved å la $(0, v)$ få samme farge som v har i V. Hvis v har fargen c_i, lar vi $(1, v)$ få fargen c_{i+1} om $i < k$ og fargen c_1 om $i = k$.

Oppgave 4

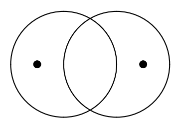
La $g : \mathbb{N} \to A$ være surjektiv.
For hver $a \in A$ finnes en $b \in A$ slik at $a < b$. La $h(a)$ være en slik b (eksempelvis $g(n)$ hvor n er minimal slik at $a < g(n)$).
La $f(1) = g(1)$.
Anta at $f(1) < \ldots < f(n)$ er bestemt.
Hvis $f(n) < g(n)$ lar vi $f(n+1) = g(n)$. Ellers lar vi $f(n+1) = h(f(n))$.
Da er f strengt voksende.

Anta at a er en øvre skranke for $\{f(n)\ ;\ n \in \mathbb{N}\}$. Vi skal se at det gir oss en motsigelse. Det finnes en $m \in \mathbb{N}$ slik at $a = g(m)$. Da vil vi ha at $f(m) < g(m)$, så $a = g(m) = f(m+1)$. Men da var ikke a en øvre skranke for bildet av f likevel.
Altså har ikke bildet av f noen øvre skranke.

Oppgave 5

5a

I dette Venn-diagrammet markerer prikkene hvilke felter det er som utgjør $A \triangle B$.



Vi viser de tre punktene uten bruk av Venn-diagram. Henvisning til Venn-diagram er akseptabelt.

1. Det er ikke mulig for et objekt x å være element i nøyaktig én av A og A, vi kan ikke ha både at $x \in A$ og $x \notin A$. Den symmetriske differensen, som er mengden som markerer forskjellen mellom A og A, vil være tom.

2. Definisjonen av $A \triangle B$ er symmetrisk i A og B, noe vi også kan se av Venn-diagrammet.

3. La $x \in A$ og $x \notin C$
   Hvis $x \in B$ vil $x \in B$ og $x \notin C$, så $x \in B \triangle C$.
   Hvis $x \notin B$, er $x \in A \triangle B$.
   Uansett er $x \in (A \triangle B) \cup (B \triangle C)$.
   Tilfellet hvor $x \in C$ og $x \notin A$ behandles på samme måte.
   Dette viser inklusjonen.
   Her vil også et Venn-diagram kunne godkjennes.

5b

- $\sim$ er refleksiv siden $A \triangle A = \emptyset$ og $\emptyset$ er endelig.
- $\sim$ er symmetrisk siden $A \triangle B = B \triangle A$, så den ene mengden er endelig hvis og bare hvis den andre er det.
- Hvis $A \triangle B$ er endelig og $B \triangle C$ er endelig, er unionen av disse to mengdene også endelig. Siden $A \triangle C$ er inneholdt i denne mengden, må $A \triangle C$ være endelig. Det viser at $\sim$ er transitiv.

5c

Det finnes flere måter å formulere argumentet på. Vi har forelest, og gitt som oppgave, at mengden av endelige delmengder av en tellbar mengde er tellbar, så hvis $A \subseteq X$ og $B \sim A$, så er B bestemt av A og $A \triangle B$. Min formulering er gjengitt under, men det finnes mange måter å formulere samme idé på:

La $A \subseteq X$. Hvis $A \sim B$ finnes det to disjunkte endelige delmengder C og D av X slik at

$$B = (A \cup C) \setminus D.$$

Mengden av endelige delmengder av X er tellbar, så mengden av par (C, D) av disjunkte endelige delmengder vil også være tellbar.
Konstruksjonen av B fra A og (C, D) gir en surjektiv avbildning fra mengden av par av disjunkte endelige delmengder av X til ekvivalensklassen til A. Denne ekvivalensklassen må derfor være tellbar.
Siden potensmengden til X er overtellbar, må vi ha mer enn tellbart mange ekvivalensklasser.