Eksamen 6. desember 2013 **IR201712 Diskret Matematikk**
Eksamenstid 4 timar *Nynorsk*

Ingen hjelpemiddel er tillatne.
Ta med **all mellomrekning** som trengst for å grunngje svaret.

Oppgåve 1 ..... *(7%)*

Skriv F og T for hhv. *sann* og *usann*.

(a) Forenkl uttrykket $s \wedge \neg s =$

(b) Forenkl uttrykket $s \vee T =$

(c) Lat $a \oplus b$ stå for XOR av a og b. Bruk sanningstabell for å visa at $a \oplus b$ er ekvivalent med $(a \wedge \neg b) \vee (\neg a \wedge b)$. (Hugs at $a \oplus b$ er usann dersom a og b har same sanningsverdi og sann når a og b har ulik sanningsverdi.)

Oppgåve 2 ..... *(12%)*

Sjå på kvart av fylgjande argument. Definer predikatsymbol og set opp argumentet systematisk på symbolsk form. Vurder om argumentet er gyldig og evt. kva argumentteknikk som vert brukt.

(a)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Jula vert kvit og fin.
- Ergo er eg opplagd og inspirert når neste semester startar.

(b)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Det regnar heile jula.
- Ergo er eg sur og gretten når neste semester startar.

(c)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Eg er sur og gretten når neste semester startar.
- Ergo hadde me ikkje snø i jula.

Oppgåve 3 ..... *(7%)*

Rekn ut fylgjande

(a) $6 + 7 \mod 9 =$

(b) $4 \cdot 7 \mod 17 =$

(c) $(x^3 + x + 2) \cdot (x^4 + 2x^3 + 1)$ over $\mathbb{Z}_3$.

Oppgåve 4 ..... *(12%)*

Me har eit datasystem med brukarnamn og passord. Forklar korleis me finn talet på unike, moglege brukarnamn, når

(a) ... brukarnamnet må bestå av nøyaktig seks teikn som er anten små, engelske bokstavar eller siffer?

(b) ... brukarnamnet må bestå av seks til åtte teikn som er anten små, engelske bokstavar eller siffer?

(c) ... brukarnamnet må bestå av seks til åtte teikn der *det fyrste* er ein liten engelsk bokstav og dei resterande kan vera anten små, engelske bokstavar, siffer, eller eit av dei ti teikna `.,-+:;_%$"`?

Det er tilstrekkeleg å setja opp formlar og setja inn tal. Du **treng ikkje** å rekna ut formlane. Forklar kva teljeprinsipp du treng og korleis du kjem fram til formlane i kvart delspørsmål.

Oppgåve 5 ..... *(8%)*

(a) Rekn ut $A \cdot B$ over $\mathbb{Z}_2$ der:

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

(b) Rekn ut $C \cdot D$ over $\mathbb{Z}_3$ der:

$$C = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 0 \end{bmatrix} \quad D = \begin{bmatrix} 2 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Oppgåve 6 ..... *(4%)*

Lat E vera ei matrise over $\mathbb{Z}_2$:

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{1}$$

Rekn ut E^{-1}.

Oppgåve 7 ..... *(12%)*

(a) Skriv opp formelen (definisjon) for binomialkoeffisienten $\binom{n}{m}$

(b) Rekn ut $\binom{7}{3}$

(c) Forklar korleis eit prov ved matematisk induksjon er bygd opp.

(d) Bruk matematisk induksjon for å bevisa formelen som du fann i del a. Du kan bruka den fylgjande rekursive likninga som er velkjend:

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}, \quad \text{når } n > m. \tag{2}$$

Oppgåve 8 ..... *(6%)*

Kor mange løysingar med $0 \leq x \leq 14$ har fylgjande likningar:

(a) $3x \mod 15 = 3$?

(b) $3x \mod 15 = 1$?

Grunngje svara.

Oppgåve 9 ..... *(10%)*

(a) Vis korleis du bruker Euklids algoritme for å finna $\text{hcf}(90, 462)$[1]?

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 13 modulo 73.

Oppgåve 10 ..... *(12%)*

RSA har krypteringsfunksjonen $e_{e,n}(x) = x^e \mod n$.

(a) Vis, steg for steg, korleis du reknar ut $11^{17} \mod 21$ på ein effektiv måte.

(b) Skriv pseudo-kode for ein effektiv algoritme for å rekna ut $x^e \mod n$.

(c) Kor mange multiplikasjonar trengst for å rekna ut $x^e \mod n$?

Oppgåve 11 ..... *(10%)*

Sjå på fylgjande recurrence og gå ut frå at n er en potens av to,

$$\begin{aligned} T(n) &= 2(T(n/2)) + n, \quad \text{når } n > 1, \\ T(1) &= 1. \end{aligned} \tag{3}$$

(a) Teikn eit recurrence-tre for $T(n)$.

(b) Bruk recurrence-treet for å finna ei eksakt løysing for $T(n)$.

(c) Gje ei Big-Θ-grense (beste moglege Big-O-grense) for $T(n)$.

[1] hcf står for *Highest Common Factor* eller største felles divisor (ogso kjend som gcd).