Eksamen 6. desember 2013 **IR201712 Diskret Matematikk**
Eksamenstid 4 timer *Bokmål*

Ingen hjelpemidler er tillatt.
Ta med **all mellomregning** som er nødvendig for å grunngi svaret.

Oppgave 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) La $a \oplus b$ stå for XOR av a og b. Bruk sanhetstabell for å vise at $a \oplus b$ er ekvivalent med $(a \wedge \neg b) \vee (\neg a \wedge b)$. (Husk at $a \oplus b$ er usann dersom a og b har samme sannhetsverdi og sann når a og b har forskjellig sannhetsverdi.)

Oppgave 2 .... *(12%)*

Se på hvert av følgende argument. Definer predikatsymbol og sett opp argumentet systematisk på symbolsk form. Vurder om argumentet er gyldig og evt. hvilken argumentteknikk som blir 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.

Oppgave 3 .... *(7%)*

Regn ut følgende

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

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

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

Oppgave 4 .... *(12%)*

Vi har et datasystem med brukernavn og passord. Forklar hvordan vi finner antall unike, mulige brukernavn, når

(a) ... brukernavnet må bestå av nøyaktig seks tegn som er enten små, engelske bokstaver eller siffer?

(b) ... brukernavnet må bestå av seks til åtte tegn som er enten små, engelske bokstaver eller siffer?

(c) ... brukernavnet må bestå av seks til åtte tegn der *det første* er en liten engelsk bokstav og resten kan være enten små, engelske bokstaver, siffer, eller et av de ti tegnene `.,-+:;_%$"`?

Det er tilstrekkelig å sette opp formler og sette inn tall. Du **trenger ikke** å regne ut formlene. Forklar hvikle telleprinsipper du trenger og hvordan du kommer frem til formlene i hvert delspørsmål.

Oppgave 5 .... *(8%)*

(a) Regn 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) Regn ut $C \cdot B$ over $\mathbb{Z}_3$ der:

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

Oppgave 6 .... *(4%)*

La E være en matrise over $\mathbb{Z}_2$:

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

Regn ut E^{-1}.

Oppgave 7 .... *(12%)*

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

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

(c) Forklar hvordan et matematisk induksjonsbevis er bygd opp.

(d) Bruk matematisk induksjon for å bevise formelen som du fant i del a. Du kan bruke følgende ligning som er velkjent:

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

Oppgave 8 .... *(6%)*

Hvor mange løsninger med $0 \leq x \leq 14$ har følgende ligninger:

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

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

Grunngi svarene.

Oppgave 9 .... *(10%)*

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

(b) Vis hvordan du bruker Euklids utvidede algoritme for å finne den multiplikative inversen til 13 modulo 73.

Oppgave 10 .... *(12%)*

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

(a) Vis, steg for steg, hvordan du regner ut $11^{17} \mod 21$ på en effektiv måte.

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

(c) Hvor mange multiplikasjoner trengs for å regne ut $x^e \mod n$?

Oppgave 11 .... *(10%)*

Ta følgende recurrence og anta 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) Tegn et recurrence-tre for $T(n)$.

(b) Bruk recurrence-treet for å finne en eksakt løsning for $T(n)$.

(c) Gi en Big-Θ-grense (beste mulige Big-O-grense) for $T(n)$.

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