Eksamen 1. desember 2015
Eksamenstid 4 timer

IR201712 Diskret Matematikk
Bokmål

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

Oppgave 1 .... *(4%)*

(a) Regn ut $\binom{5}{3}$.

(b) Regn ut $\binom{777}{776}$.

Oppgave 2 .... *(4%)*

(a) Skriv det heksadesimale tallet 2D om på desimalform.

(b) Skriv tallet 63 (desimal) på heksadesimal form.

Oppgave 3 .... *(4%)*

Regn ut følgende

(a) $(17 + 12) \mod 9 =$

(b) $(4 \cdot 12 + 3) \mod 16 =$

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

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 5 .... *(4%)*

Løs følgende kongruenser (modulære ligninger)

(a) $3x \equiv 2 \pmod 5$

(b) $4x - 2 \equiv 4 \pmod 9$

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

En pokerhånd er fem tilfeldige kort fra en vanlig stokk på 52 kort.

(a) Hvor mange forskjellige pokerhender fins?

(b) Hvor mange forskjellige pokerhender inneholder fire kort med samme verdi? (Der er tretten mulige verdier: $2, 3, \ldots, 10$ samt Knekt, Dame, Konge, Ess. Det femte kortet kan være hva som helst.)

Oppgave 7 .... *(8%)*

(a) La A og B være matriser over $\mathbb{Z}_2$:

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

Regn ut $A \cdot B =$

(b) La C og D være matriser over $\mathbb{Z}_7$:

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 3 \\ 0 & 2 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 5 \\ 6 & 2 \end{bmatrix}$$

Regn ut $C \cdot D =$

Oppgave 8 .... *(4%)*

La s og t være to utsagn. Se på tre forskjellige argumenter:

a) $s \Rightarrow t$, t ———— $\therefore s$

b) $s \Rightarrow t$, s ———— $\therefore t$

c) $s \Rightarrow t$, $\neg t$ ———— $\therefore \neg s$

For hvert av de tre argumentene, svar på om det er gyldig eller ugyldig.

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

Se på følgende utsagn fra NRKs vevsider:

Må legge ned Aukrustsenteret hvis Caprino vinner rettsaken

Vi kaller dette utsagnet for u.

(a) Definer to utsagn, s og t, slik at utsagnet u kan skrives som $u = (s \Rightarrow t)$.

(b) Skriv det kontrapositive utsagnet til u på symbolsk form (som et uttrykk i s og t).

(c) Skriv det kontrapositive utsagnet til u på i naturleg sprog.

Oppgave 10 .... *(15%)*

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

(a) Forklar hva vi mener med at RSA er et *asymmetrisk* siffer.

(b) Hvilke fordeler har asymetriske sifre sammenlignet med symmetriske sifre?

(c) Nevn ett eksempel på et symmetrisk siffer som er i vanlig bruk i dag.

(d) Hvilke fordeler har symmetriske sifre sammenlignet med asymmetriske?

(e) Hva gjør man i praktiske systemer (t.eks. SSL) for å få det beste ut av symmetriske og asymmetriske sifre?

Oppgave 11 .... *(12%)*

Denne oppgaven ser på relasjoner mellom to mengder.

(a) Hva mener vi (generelt i matematikken) med med en relasjon?

(b) En ekvivalens er en relasjon som har tre bestemte egenskaper. Gi navn og definisjon for hver av disse egenskapene.

(c) Husk at vi skriver $x \equiv y \pmod{n}$ hvis $x \mod n = y \mod n$. Dette er en relasjon som vi kaller kongruens modulo n. Er kongruens modulo n en ekvivalens? Begrunn svaret.

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

Krypter meldingen «godaften» med et transposisjonssiffer. Nøglen er permutasjonen $(4, 2, 1, 3)$.

Oppgave 13 .... *(6%)*

Vi skal vurdere kjøretiden på fire ulike sorteringsalgoritmar ved sortering av svært store tabeller.La n være antall elementer som skal sorteres. Følgende tabell viser hvor mange ganger hver algoritme må bytte om to elementer i tabellen i verste fall, og vi regner med at det er den mest tidkrevende operasjonen.

Algoritme 1	$\frac{n(n-1)}{2}$
Algoritme 2	n^2
Algoritme 3	$n(1 + \log n)$
Algoritme 4	$2^n - n^{20} + n^{10}$

(a) Gi et enklest mulig Big-Θ-uttrykk (beste mulige Big-O-uttrykk) for hvor mange ombyttinger hver algoritme trenger.

(b) Sorter de fire algoritmene fra raskest til tregest basert på kjøretiden for store tabeller (når n går mot uendelig). Hvis du finner to eller flere algoritmer som er like raske skal det markeres.

Oppgave 14 .... *(8%)*

(a) Vis steg for steg hvordan du bruker Euklids algoritme for å finne $\text{hcf}(525, 1295)$[1]?

(b) Vis hvordan du bruker Euklids utvidede algoritme for å finne den multiplikative inversen til 13 modulo 81.

Oppgave 15 .... *(8%)*

Ta to polynomer over $\mathbb{Z}_2$:

$$f(x) = x^4 + x^3 + x^2 + 1,$$
$$g(x) = x^3 + 1.$$

Regn ut følgende

(a) $f(x) \mod g(x) =$

(b) $\text{hcf}(f(x), g(x)) =$

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