Eksamen 2. desember 2014
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 $\binom{520}{519}$.

Oppgave 2 .... *(6%)*

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

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

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

(c) Sett opp en sannhetstabell for uttrykket $p \Rightarrow q$.

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

Regn ut følgende

(a) $12 + 3 \mod 13$

(b) $6 \cdot 5 \mod 10$

Oppgave 4 .... *(5%)*

Løs følgende kongruenser (modulære ligninger)

(a) $2x \equiv 1 \pmod 5$

(b) $4x + 2 \equiv 1 \pmod 9$

Oppgave 5 .... *(12%)*

Klasse 5A skal velge elevrepresentanter. Der er tolv piker og syv gutter i klassen. Svar på følgende, og forklar hvilke(t) telleprinsipp(er) du bruker for hvert spørsmål.

(a) På hvor mange måter kan de velge én representant av hvert kjønn?

(b) På hvor mange måter kan de velge én representant og én vara?

(c) På hvor mange måter kan de velge én representant og én vara når de to må ha forskjellig kjønn?

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

(a) Skriv det heksadesimale tallet 1E om på desimalform.

(b) Skriv tallet 33 (desimal) på heksadesimal form.

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

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

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{11}$$

Regn ut $A \cdot B =$

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

$$C = \begin{bmatrix} 1 & 1 \\ 6 & 1 \\ 2 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 3 & 2 \\ 3 & 0 \end{bmatrix} \tag{13}$$

Regn ut $C \cdot D =$.

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

Se på utsagnet

hvis m er et oddetall, så er m^2 et oddetall

(a) Formaliser utsagnet ved hjelp av logiske symboler.

(b) Bevis utsagnet.

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

Tenk på ekvivalensrelasjoner.

(a) Hva mener vi med en relasjon?

(b) Hva vil det si at en relasjon er en ekvivalensrelasjon?

(c) Vis at $a \equiv b \pmod{n}$ er en ekvivalensrelasjon. (Husk at $a \equiv b \pmod{n}$ er det samme som at $a \mod n = b \mod n$.)

Oppgave 10 .... *(3%)*

List opp nulldivisorene i $\mathbb{Z}_{15}$.

Oppgave 11 .... *(16%)*

(a) Vis steg for steg hvordan du bruker Euklids algoritme for å finne $\mathrm{hcf}(365, 189)$[1]?

(b) Vis hvordan du bruker Euklids utvidede algoritme for å finne den multiplikative inversen til 15 modulo 83.

(c) Skriv ned pseudo-kode for Euklids algoritme.

(d) Forklar hvordan vi kan vite at Euklids algoritme fullfører i endelig tid.

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

(a) Forklar hva vi mener med et siffer med offentlig nøgle (asymmetrisk siffer).

(b) Nevn ett eksempel på et siffer som bruker offentlig nøgle og som er i vanlig bruk i dag.

(c) Hvilke fordeler har sifre offentlige nøgler sammenlignet med symmetriske sifre?

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

(e) Hvilke fordeler har symmetriske sifre sammenlignet med offentlige nøgler?

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

Oppgave 13 .... *(9%)*

Se på uttrykket $3^{69} \mod 19$.

1. Vis hvordan du kan bruke Fermats lille teorem for å forenkle utregningen.
2. Forklar hvilke andre regneregler du kan bruke for å regne ut slike uttrykk ($x^y \mod n$) så enkelt som mulig.
3. Regn ut $3^{69} \mod 19$. Vis hvordan du gjør utregningen.

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