Eksamen 2. desember 2014 **IR201712 Diskret Matematikk**
Eksamenstid 4 timar *Nynorsk*

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

Oppgåve 1 .... *(4%)*

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

(b) Rekn ut $\binom{520}{519}$.

Oppgåve 2 .... *(6%)*

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

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

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

(c) Sett opp ein sanningstabell for uttrykket $p \Rightarrow q$.

Oppgåve 3 .... *(4%)*

Rekn ut fylgjande

(a) $12 + 3 \mod 13$

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

Oppgåve 4 .... *(5%)*

Løys fylgjande kongruensar (modulære likningar)

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

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

Oppgåve 5 .... *(12%)*

Klasse 5A skal velja elevrepresentantar. Der er tolv jenter og sju gutar i klassa. Svar på fylgjande, og forklar kva teljeprinsipp du bruker for kvart spørsmål.

(a) På kor mange måtar kan dei velja éin representant av kvart kjøn?

(b) På kor mange måtar kan dei velja éin representant og éin vara?

(c) På kor mange måtar kan dei velja éin representant og éin vara når dei to må ha ulikt kjøn?

Oppgåve 6 .... *(4%)*

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

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

Oppgåve 7 .... *(8%)*

(a) Lat A og B vera matrisar over $\mathbb{Z}_2$:

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

Rekn ut $A \cdot B =$

(b) Lat C og D vera matrisar over $\mathbb{Z}_7$:

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

Rekn ut $C \cdot D =$.

Oppgåve 8 .... *(8%)*

Sjå på utsagnet

dersom m er eit oddetal, so er m^2 eit oddetal

(a) Formaliser utsagnet ved hjelp av logiske symbol.

(b) Bevis utsagnet.

Oppgåve 9 .... *(9%)*

Tenk på ekvivalensrelasjonar.

(a) Kva meiner me med ein relasjon?

(b) Kva vil det seia at ein relasjon er ein ekvivalensrelasjon?

(c) Vis at $a \equiv b \pmod{n}$ er ein ekvivalensrelasjon. (Hugs at $a \equiv b \pmod{n}$ er det same som at $a \mod n = b \mod n$.)

Oppgåve 10 .... *(3%)*

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

Oppgåve 11 .... *(16%)*

(a) Vis steg for steg korleis du bruker Euklids algoritme for å finna hcf(365, 189)[1]?

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 15 modulo 83.

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

(d) Forklar korleis me kan vita at Euklids algoritme fullfører i endeleg tid.

Oppgåve 12 .... *(12%)*

(a) Forklar kva me meiner med eit siffer med offentleg nykel (asymmetrisk siffer).

(b) Nemn eitt døme på eit siffer som bruker offentleg nykel og som er i vanleg bruk i dag.

(c) Kva føremonar har siffer med offentlege nyklar samanlikna med symmetriske siffer?

(d) Nemna eitt døme på eit symmetrisk siffer som er i vanleg bruk i dag.

(e) Kva føremonar har symmetriske siffer samanlikna med offentlege nyklar?

(f) Kva gjer ein i praktiske system (t.d. SSL) for å få det beste ut av symmetriske og asymmetriske siffer?

Oppgåve 13 .... *(9%)*

Sjå på uttrykket $3^{69} \mod 19$.

1. Vis korleis du kan bruka Fermats lille teorem for å forenkla utrekninga.
2. Forklar kva andre rekneregler du kan bruka for å rekna ut slike uttrykk ($x^y \mod n$) so enkelt som mogleg.
3. Rekn ut $3^{69} \mod 19$. Vis korleis du gjer utrekninga.

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