Eksamensdøme 12. november 2013 **IR201712 Diskret Matematikk**
Eksamenstid 4 timar *Nynorsk*

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

Oppgåve 1 ..... *(12%)*

Sjå for deg ei klasse med 19 gutar og 7 jenter. Dei skal velja tillitsvalde. Svar på fylgjande, og forklar kva teljeprinsipp du brukar for kvart spørsmål.

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

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

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

Oppgåve 2 ..... *(7%)*

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

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

(b) Forenkla uttrykket $s \vee F =$

(c) Lag ein sanningstabell for uttrykka $\neg(s \wedge t)$ og $\neg s \vee \neg t$. Kva fortel sanningstabellen oss om uttrykka?

Oppgåve 3 ..... *(9%)*

Vurder kvart av fylgjande argument, og sei om argumentet er gyldig og evt. kva argumentteknikk som vert brukt.

(a)
- Dersom du forsøv deg i deg, so får du ikkje ta eksamen.
- Du får ta eksamen.
- Ergo forsøv du deg ikkje.

(b)
- Dersom du forsøv deg i deg, so får du ikkje ta eksamen.
- Du får ikkje ta eksamen.
- Ergo forsøv du deg.

(c)
- Dersom du forsøv deg i deg, so får du ikkje ta eksamen.
- Du forsøv deg.
- Ergo får du ikkje ta eksamen.

Oppgåve 4 ..... *(4%)*

Krypter meldinga ‘goddag’ med Cæsars siffer. Vis fullstendig korleis meldinga kan krypterast ved å bruka modulær aritmetikk over heiltal.

Oppgåve 5 ..... *(4%)*

Rekna ut fylgjande

(a) $6 + 7 \mod 9$

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

Oppgåve 6 ..... *(8%)*

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

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

Rekna ut $A \cdot B =$.

(b) Lat C og D vera matrisar over $\mathbb{Z}_5$:

$$C = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 0 \end{bmatrix} \quad D = \begin{bmatrix} 3 & 1 & 4 \\ 0 & 2 & 4 \\ 1 & 1 & 4 \end{bmatrix} \tag{2}$$

Rekna ut $C \cdot D =$.

Oppgåve 7 ..... *(12%)*

(a) Vis korleis du bruker Euclids algoritme for å finna $\text{hcf}(54, 69)$?

(b) Gjeve $\text{hcf}(a, b)$, korleis veit me om a hev ein multiplikativ invers modulo b?

(c) Vis korleis du bruker Euclids utvida algoritme for å finna den multiplikative inversen til 12 modulo 55.

Oppgåve 8 ..... *(12%)*

Ein ring R har to operasjonar $+$ og $\cdot$ som må vera assosiative og kommutative

(a) Kva vil det seia at ein operasjon er assosiativ?

(b) Kva vil det seia at ein operasjon er kommutative?

(c) Kva seier den distributive lova?

(d) Kva ekstra eigenskap krev me for at ein ring R ogso skal vera ein kropp?

Oppgåve 9 ..... *(8%)*

Rekna ut fylgjande over $\mathbb{Z}_3$:

(a) $(x^3 + 2x + 1)(x^4 + 2x^2 + 2)$

(b) $(2x^5 + x^3 + 2x + 1) \mod (x^2 + x + 1)$

Oppgåve 10 ..... *(10%)*

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

(b) Kva fordelar har siffer med offentleg nykel samanlikna med symmetriske siffer?

(c) Kva ulemper har siffer med offentleg nykel samanlikna med symmetriske siffer?

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

Oppgåve 11 ..... *(14%)*

Sjå på fylgjande merge-algoritme som vert brukt som ein subrutine i MergeSort.

```
1       procedure Merge (A,B) (where A and B are sorted arrays)
2       i=1 ; j=1 ; k=0
3       while ( i≤n or j≤m )
4           k = k+1
5           if i>n, C_k = B_j ; j = j+1
6           else if j>m, C_k = A_i ; i = i+1
7           else if A_i ≤ B_j, C_k = A_i ; i = i+1
8           else C_k = B_j ; j = j+1
9       return C
```

(a) Skriv ned pseudokode for MergeSort, der du bruker Merge-algoritmen over som subrutine.

(b) Definér formelt kva me meiner med at tabellen $A_1, A_2, \ldots, A_n$ er sortert.

(c) Bevis formelt at Merge er korrect, dvs. at utdata C er sortert når både A og B er sorterte.