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?

Solution: Me har mengdene J av jenter og G av gutar. Me skal velja éin av kvart kjøn, dvs. eit element frå det kartesiske produktet $J \times G$. Produktprinsippet seier at $\#(J \times G) = \#J \cdot \#G = 7 \cdot 19 = 133$. Me har altso 133 måtar å velja på.

(Ein kan bruka ein meir omstendeleg og generell føring med eksplisitt partisjonering, men ovanståande er enklare.)

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

Solution: Me har ei klasse $K = J \cup G$ der $\#K = 26$. Me skal velja eit ordna par av element frå K. Lat S vera mengda av slike par.

Me kan partisjonera $S = \bigcup_{x \in K} S_x$ der S_x er mengda av par med x som fyrste element (tillitsvald). Uavhengig av kven som er tillitsvald er der 25 kandidatar att til vara, so $\#S_x = 25$. Produktprinsippet gjev $\#S = \#K \cdot \#S_x = 26 \cdot 25 = 650$

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

Solution: Me skal velja éin person av kvart kjøn som i del a, men me har to alternativ; jenta kan vera (hovud)tillitsvald eller guten kan vera det. Me tel kvart fall for seg og bruker sumprinsippet til slutt.

I det fyrste fallet har me 7 alternativ for tillitsvald og 19 for vara, og produktprinsippet gjev $7 \cdot 19 = 133$ alternativ totalt (sjå a). I det andre fallet har me 19 alternativ for tillitsvald og 7 for vara, og produktprinsippet gjev $19 \cdot 7 = 133$ alternativ totalt.

Sumprinsippet gjev $133 + 133 = 266$ måtar å velja på totalt.

(Merk at ein kan vera litt knappare i argumentet ved å visa til a.)

Oppgåve 2 . . . . *(7%)*

Skriv T og F 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, so får du ikkje ta eksamen.
- Du får ta eksamen.
- Ergo forsøv du deg ikkje.

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

(c)
- Dersom du forsøv 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 $\text{hcf}(54, 69)$?

> **Solution:**
>
> $$\begin{aligned} \text{hcf}(54,69) &= \text{hcf}(15,54) \\ &= \text{hcf}(9,15) \\ &= \text{hcf}(6,9) \\ &= \text{hcf}(3,6) = 3. \end{aligned}$$
>
> I.e. $\text{hcf}(54, 69) = 3$.

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

> **Solution:** Inversen eksisterer dersom og berre dersom $\text{hcf}(a, b) = 1$.

(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?

> **Solution:** Ein operasjon $\circ$ er assosisativ dersom
>
> $$(a \circ b) \circ c = a \circ (b \circ c)$$

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

> **Solution:** Ein operasjon $\circ$ er kommutativ dersom
>
> $$a \circ b = b \circ a$$

(c) Kva seier den distributive lova?

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

> **Solution:** Ein ring R er ein kropp dersom ein kvar $a \in R$, $a \neq 0$, hev ein multiplikativ invers a^{-1}.

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?

> **Solution:** Ein er ikkje avhengig av å ha delt ein løynd nykel på førehand. Den offentlege nykelen kan kringkastast.

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

> **Solution:** Fyrst og framst er asymmetriske siffer treigare.
>
> Der er òg større uvisse om sikkerheita i asymmetriske system i framtida. Teoretiske og teknologiske nyvinningar kan tenkjast å knekka eksisterande asymmetriske siffer. Det er t.d. kjend at kvantemaskiner vil gjera det. Sikkerheita i symmetriske siffer vil heller svekkast jamnt.

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

> **Solution:** Ein bruker eit asymmetrisk siffer i oppstarten av kommunikasjonen, der ein mellom anna vel ein løynd nykel som vert sent kryptert med det asymmetriske sifferet.
>
> Denne løynde nykelen kan ein so bruka i eit symmetrisk siffer i resten av kommunikasjonen.

Oppgåve 11 . . . . *(14%)*

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

```
procedure Merge (A, B)  (where A and B are sorted arrays)
i = 1 ; j = 1 ; k = 0
while ( i ≤ n or j ≤ m )
    k = k+1
    if i > n , C_k = B_j ; j = j+1
    else if j > m , C_k = A_i ; i = i+1
    else if A_i ≤ B_j , C_k = A_i ; i = i+1
    else C_k = B_j ; j = j+1
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.