Eksamen 6. desember 2013 **IR201712 Diskret Matematikk**

Eksamenstid 4 timar *Nynorsk*

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

Oppgåve 1 .... *(7%)*

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

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

Solution:

$$s \wedge \neg s = F$$

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

Solution:

$$s \vee T = T$$

(c) Lat $a \oplus b$ stå for XOR av a og b. Bruk sanningstabell for å visa at $a \oplus b$ er ekvivalent med $(a \wedge \neg b) \vee (\neg a \wedge b)$. (Hugs at $a \oplus b$ er usann dersom a og b har same sanningsverdi og sann når a og b har ulik sanningsverdi.)

Solution:

a	b	$a \oplus b$	$\neg a$	$\neg b$	$(a \wedge \neg b)$	$(\neg a \wedge b)$	$(a \wedge \neg b) \vee (\neg a \wedge b)$
T	T	F	F	F	F	F	F
T	F	T	F	T	T	F	T
F	T	T	T	F	F	T	T
F	F	F	T	T	F	F	F

We can see that both expressions have the same truth value for each combination of truth values for a and b. Hence they are equivalent.

Oppgåve 2 .... *(12%)*

Sjå på kvart av fylgjande argument. Definer predikatsymbol og set opp argumentet systematisk på symbolsk form. Vurder om argumentet er gyldig og evt. kva argumentteknikk som vert brukt.

(a)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Jula vert kvit og fin.
- Ergo er eg opplagd og inspirert når neste semester startar.

Solution:

$$s := \text{me får kvit jul,}$$
$$t := \text{eg vert opplagd og inspirert til neste semester.}$$

Argumentet seiar at fordi $s \Rightarrow t$ og s, so kan me konkludera med t. Dette er eit døme på Modus Ponens og er eit gyldig argument.

(b)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Det regnar heile jula.

- Ergo er eg sur og gretten når neste semester startar.

> **Solution:** Med s og t definert som før, seiar argumentet at fordi $s \Rightarrow t$ og $\neg s$, so kan me konkludera med $\neg t$. Dette er eit ugyldig argumentet. Premissane gjev ingen informasjon om kva som skjer når $\neg s$ er sann.

(c)
- Dersom me får kvit jul, so vert eg opplagd og inspirert til neste semester.
- Eg er sur og gretten når neste semester startar.
- Ergo hadde me ikkje snø i jula.

> **Solution:** Med s og t definert som før, seiar argumentet at fordi $s \Rightarrow t$ og $\neg t$, so kan me konkludera med $\neg s$. Dette heiter Modus Tollens og er eit gyldig argument.

Oppgåve 3 .... *(7%)*

Rekn ut fylgjande

(a) $6 + 7 \mod 9 =$

> **Solution:**
> $$6 + 7 \mod 9 = 4$$

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

> **Solution:**
> $$4 \cdot 7 \mod 17 = 11$$

(c) $(x^3 + x + 2) \cdot (x^4 + 2x^3 + 1)$ over $\mathbb{Z}_3$.

> **Solution:**
> $$(x^4 + 2x^3 + 0 + 0 + 1) \cdot (x^3 + 0 + x + 2)$$
> $$\begin{array}{r}
2x^4 + x^3 + 0 + 0 + 2 \\
x^5 + 2x^4 + 0 + 0 + x \\
\underline{x^7 + 2x^6 + 0 + 0 + x^3} \\
\underline{\underline{x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x + 2}}
\end{array}$$

Oppgåve 4 .... *(12%)*

Me har eit datasystem med brukarnamn og passord. Forklar korleis me finn talet på unike, moglege brukarnamn, når

(a) ... brukarnamnet må bestå av nøyaktig seks teikn som er anten små, engelske bokstavar eller siffer?

> **Solution:** The password is a list of 6 elements from a set (alphabet) of 36 elements. Using the product principle (or the formula for the number of lists) we have 36^6 different possibilities.

(b) ... brukarnamnet må bestå av seks til åtte teikn som er anten små, engelske bokstavar eller siffer?

Solution: The password is a list of 6, 7, or 8 elements from a set (alphabet) of 36 elements. We use the sum principle to combine the number of 6-, 7-, and 8-character user names, for a total of

$$36^6 + 36^7 + 36^8$$

options.

(c) ... brukarnamnet må bestå av seks til åtte teikn der *det fyrste* er ein liten engelsk bokstav og dei resterande kan vera anten små, engelske bokstavar, siffer, eller eit av dei ti teikna `.,-+:;_%$"`?

Solution: Again we need to split the problem into 6-, 7-, and 8-character usernames. For n-character usernames we note that we choose one character (the first) from a 26-element set, and the remaining $i-1$ characters from a 46-element set (as in the previous subproblem). Thus we have 26 choices for the first letter and 46^{i-1} for the rest. Using the product principle we have $26 \cdot 46^{i-1}$ possible i-character usernames. Using the sum principle as before, we get a total of

$$26 \cdot 46^5 + 26 \cdot 46^6 + 26 \cdot 46^7$$

usernames.

Det er tilstrekkeleg å setja opp formlar og setja inn tal. Du **treng ikkje** å rekna ut formlane. Forklar kva teljeprinsipp du treng og korleis du kjem fram til formlane i kvart delspørsmål.

Oppgåve 5 . . . . *(8%)*

(a) Rekn ut $A \cdot B$ over $\mathbb{Z}_2$ der:

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

Solution:

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

(b) Rekn ut $C \cdot D$ over $\mathbb{Z}_3$ der:

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

Solution:

$$\begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \end{bmatrix}$$

Oppgåve 6 .... *(4%)*

Lat E vera ei matrise over $\mathbb{Z}_2$:

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{1}$$

Rekn ut E^{-1}.

Solution:

$$\left[\begin{array}{cc:cc} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right]$$

Adding Row 2 to Row 1 we get

$$\left[\begin{array}{cc:cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right]$$

Thus, $E^{-1} = E$.

Oppgåve 7 .... *(12%)*

(a) Skriv opp formelen (definisjon) for binomialkoeffisienten $\binom{n}{m}$

Solution:

$$\frac{n!}{m!(n-m)!}$$

(b) Rekn ut $\binom{7}{3}$

Solution:

$$\frac{7!}{3!(7-3)!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 7 \cdot 5 = 35.$$

(c) Forklar korleis eit prov ved matematisk induksjon er bygd opp.

Solution: Matematisk induksjon tek utgangspunkt i eit predikat $P(n)$ der n er eit heiltal og me ynskjer å bevisa $\forall n \geq n_0, P(n)$.
Ein må bevisa to fall: grunnfallet, at $P(n_0)$ er sann, og induksjonsfallet at $P(n-1) \Rightarrow P(n)$ for $n > n_0$. (Dette er den enklaste variasjonen, og det er bra nok.)
Når ein har vist både grunn- og induksjonsfallet kan ein konkludera at $\forall n \geq n_0, P(n)$ fylgjer ved (svak) matematisk induksjon.

(d) Bruk matematisk induksjon for å bevisa formelen som du fann i del a. Du kan bruka den fylgjande rekursive likninga som er velkjend:

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}, \quad \text{når } n > m. \tag{2}$$

Solution: Grunnfallet er $n = m$ som gjev talet på måtar å velja ei n-mengd frå ei n-mengd. Den einaste måten er å velja heile mengda, altso $\binom{n}{n} = 1$. Me har

$$\frac{n!}{(n-n)!n!} = 1,$$

som formelen stemmer her.

I induksjonsfallet går me ut frå at

$$\binom{n'}{m} = \frac{n'!}{(n'-m)!m!},$$

for $n' = n - 1$, og me kan bruka (2) for å få

$$\begin{aligned}\binom{n}{m} &= \binom{n-1}{m} + \binom{n-1}{m-1} \\ &= \frac{(n-1)!}{(n-1-m)!m!} + \frac{(n-1)!}{(n-m)!(m-1)!} \\ &= \frac{(n-m)(n-1)! + m(n-1)!}{(n-m)!(m-1)!} \\ &= \frac{n!}{(n-m)!m!}\end{aligned}$$

som viser formelen i det induktive fallet.

Me kan konkludera med at formelen held for alle $n \geq m$ ved matematisk induksjon.

Oppgåve 8 .... *(6%)*

Kor mange løysingar med $0 \leq x \leq 14$ har fylgjande likningar:

(a) $3x \mod 15 = 3$?

Solution:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$3x \mod 15$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12

The table shows that we have three solutions.

(Analytical solutions are great, but the table is the time efficient and practical solution.)

(b) $3x \mod 15 = 1$?

Solution: Because $\mathrm{hcf}(3, 15) > 1$, 3 has no inverse and the equation has no solution.

Grunngje svara.

Oppgåve 9 . . . . *(10%)*

(a) Vis korleis du bruker Euklids algoritme for å finna $\text{hcf}(90, 462)$[1]?

Solution:

$$\begin{aligned} \text{hcf}(90, 462) &= \text{hcf}(462, 90) \\ &= \text{hcf}(90, 12) \\ &= \text{hcf}(12, 6) = 6 \end{aligned}$$

I.e. $\text{hcf}(90, 462) = 6$.

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 13 modulo 73.

Solution:

	x	y
$73 = 5 \cdot 13 + 8$	5	$-3 - 5 \cdot 5 = -28$
$13 = 1 \cdot 8 + 5$	-3	$2 + 3 \cdot 1 = 5$
$8 = 1 \cdot 5 + 3$	2	$-1 - 2 \cdot 1 = -3$
$5 = 1 \cdot 3 + 2$	-1	$1 + 1 \cdot 1 = 2$
$3 = 1 \cdot 2 + 1$	1	-1

$$5 \cdot 73 - 28 \cdot 13 = 365 - 364 = 1$$

$$13^{-1} \bmod 73 = -28 \bmod 73 = \underline{\underline{45}}$$

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

Oppgåve 10 .... *(12%)*

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

(a) Vis, steg for steg, korleis du reknar ut $11^{17} \mod 21$ på ein effektiv måte.

Solution:

$$\begin{aligned}
11^{17} \mod 27 &= (11^2 \mod 21)^8 \cdot 11 \mod 21 \\
&= 16^8 \cdot 11 \mod 21 \\
&= (16^2 \mod 21)^4 \cdot 11 \mod 21 \\
&= 4^4 \cdot 11 \mod 21 \\
&= (4^2)^2 \cdot 11 \mod 21 \\
&= (16^2 \mod 21) \cdot 11 \mod 21 \\
&= 4 \cdot 11 \mod 21 \\
&= 44 \mod 21 \\
&= 2
\end{aligned}$$

(b) Skriv pseudo-kode for ein effektiv algoritme for å rekna ut $x^e \mod n$.

Solution:

```
Algorithm SquareNmultiply(x, e, n)
if e = 1, return x mod n
y := SquareNmultiply(x, ⌊e/2⌋, n)
y := y^2 mod n
if e mod 2 = 1,
y := y · x mod n
return y
```

(c) Kor mange multiplikasjonar trengst for å rekna ut $x^e \mod n$?

Solution: At most $2\lfloor \log_2 e \rfloor$ multiplications.
(It is most important to identify the logarithmic relationship, so $\log e$ should give points. Full score assumes the factor of 2 as well.)

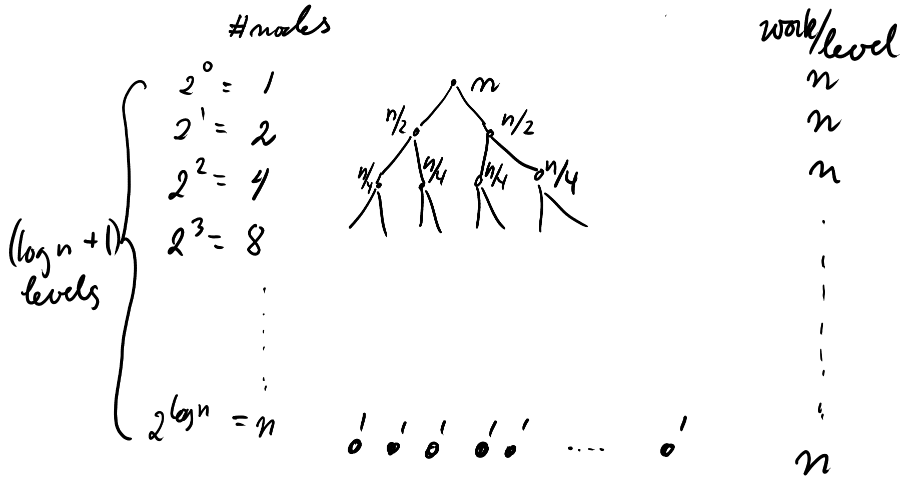
Oppgåve 11 . . . . *(10%)*

Sjå på fylgjande recurrence og gå ut frå at n er en potens av to,

$$\begin{aligned} T(n) &= 2(T(n/2)) + n, \quad \text{når } n > 1, \\ T(1) &= 1. \end{aligned} \tag{3}$$

(a) Teikn eit recurrence-tre for $T(n)$.

Solution:



(b) Bruk recurrence-treet for å finna ei eksakt løysing for $T(n)$.

Solution: Me ser $1 + \log n$ nivå med n einingar per nivå. Altso får me $T(n) = n(1 + \log n)$.

(c) Gje ei Big-Θ-grense (beste moglege Big-O-grense) for $T(n)$.

Solution: $\Theta(n \log n)$