Eksamen 1. desember 2015 **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 $\binom{5}{3}$.

Solution:

$$\binom{5}{3} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

(b) Rekn ut $\binom{777}{776}$.

Solution:

$$\binom{777}{776} = 777$$

Oppgåve 2 ..... *(4%)*

(a) Skriv det heksadesimale talet 2D om på desimalform.

Solution: $2\mathrm{D} = 2 \cdot 16 + 13 = 45$

(b) Skriv talet 63 (desimal) på heksadesimal form.

Solution:

$$\lfloor 63/16 \rfloor = 3 \quad (1)$$
$$63 \mod 16 = 15 \quad (2)$$

Thus we write 63 as $3F$ in hexadecimal.

Oppgåve 3 ..... *(4%)*

Rekn ut fylgjande

(a) $(17 + 12) \mod 9 =$

Solution:

$$(17 + 12) \mod 9 = 2$$

(b) $(4 \cdot 12 + 3) \mod 16 =$

Solution: $(4 \cdot 12 + 3) \mod 16 = 3$

Oppgåve 4 ..... *(4%)*

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

Løys fylgjande kongruensar (modulære likningar)

(a) $3x \equiv 2 \pmod 5$

Solution:

$$\begin{aligned} 3x &\equiv 2 \pmod 5 \\ 2 \cdot 3x &\equiv 2 \cdot 2 \pmod 5 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

(b) $4x - 2 \equiv 4 \pmod 9$

Solution:

$$\begin{aligned} 4x - 2 &\equiv 4 \pmod 9 \\ 4x &\equiv 6 \pmod 9 \\ 7 \cdot 4x &\equiv 7 \cdot 6 \pmod 9 \\ x &\equiv 42 \pmod 9 \\ x &\equiv 6 \pmod 9 \end{aligned}$$

Oppgåve 6 ..... *(6%)*

Ei pokerhand er fem tilfeldige kort frå ein vanleg stokk på 52 kort.

(a) Kor mange ulike pokerhender finst?

(b) Kor mange ulike pokerhender innehelde fire kort med same verdi? (Der er tretten moglege verdiar: $2, 3, \ldots, 10$ samt Knekt, Dame, Konge, Ess. Det femte kortet kan vera kva som helst.)

Oppgåve 7 ..... *(8%)*

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

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

Rekn ut $A \cdot B =$

Solution:

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

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

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 3 \\ 0 & 2 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 5 \\ 6 & 2 \end{bmatrix}$$

Rekn ut $C \cdot D =$

Solution:

$$C \cdot D = \begin{bmatrix} 6 & 2 \\ 0 & 0 \\ 5 & 4 \end{bmatrix}$$

Oppgåve 8 ..... *(4%)*

Lat s og t vera to utsegner. Sjå på tre ulike argument:

a) $s \Rightarrow t$, t / $\therefore s$

b) $s \Rightarrow t$, s / $\therefore t$

c) $s \Rightarrow t$, $\neg t$ / $\therefore \neg s$

For kvart av dei tre argumenta, svar på om det er gyldig eller ugyldig.

Oppgåve 9 ..... *(9%)*

Sjå på fylgjande utsegn frå NRKs vevsider:

Må legge ned Aukrustsenteret hvis Caprino vinner rettsaken

Me kaller denne utsegna for u.

(a) Definer to utsegner, s og t, slik at utsegna u kan skrivast som $u = (s \Rightarrow t)$.

(b) Skriv det kontrapositive utsegna til u på symbolsk form (som eit uttrykk i s og t).

(c) Skriv det kontrapositive utsegna til u på i naturleg språk.

Oppgåve 10 ..... *(15%)*

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

(a) Forklar kva me meiner med at RSA er eit *asymmetrisk* siffer.

> **Solution:** Eit asymmetrisk siffer har to nyklar. Den offentlege nykelen vert brukt til kryptering. Dekryptering krev ein løynnykel som ikkje kan utleidast (i praksis) frå den offentleg nykelen.

(b) Kva føremonar har asymmetriske siffer samanlikna med symmetriske siffer?

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

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

> **Solution:** AES

(d) Kva føremonar har symmetriske siffer samanlikna med asymmetriske?

> **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.

(e) 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 ..... *(12%)*

Denne oppgåva ser på relasjonar mellom to mengder.

(a) Kva meiner me (generelt i matematikken) med ein relasjon?

> **Solution:** Ein relasjon R frå ei mengd A til ei mengd B, er ei delmengd $R \subset A \times B$. Med andre ord, R er ei mengd av par (a, b) der $a \in A$ og $b \in B$.

(b) Ein ekvivalens er ein relasjon som har tre spesielle eigenskapar. Gje namn og definisjon for kvar av desse eigenskapane.

(c) Hugs at me skriv $x \equiv y \pmod n$ om $x \mod n = y \mod n$. Dette er ein relasjon som me kaller kongruens modulo n. Er kongruens modulo n ein ekvivalens? Grunngje svaret ditt.

> **Solution:** Congruence is an eqivalence because it satisfies the necessary properties. This is easy to see if we remember that $x \equiv y \pmod n$ is equivalent to $x \mod n = y \mod n$.
>
> 1. $\equiv \pmod n$ is symmetric because $=$ is symmetric.
> 2. $\equiv \pmod n$ is reflexive because $=$ is reflexive.
> 3. $\equiv \pmod n$ is transitive because $=$ is transitive.

Oppgåve 12 ..... *(4%)*

Krypter meldinga «godaften» med eit transposisjonssiffer. Nykelen er permutasjonen $(4, 2, 1, 3)$.

Solution:

Klartekst	g	o	d	a	f	t	e	n
Siffertekst	a	o	g	d	n	t	f	e

Oppgåve 13 ..... *(6%)*

Me skal vurdera køyretida på fire ulike sorteringsalgoritmar ved sortering av svært store tabellar.Lat n vera talet på element som skal sorterast. Fylgjande tabell viser kor mange gongar kvar algoritme treng å byta om to element i tabellen i verste fall, og me reknar med at det er den mest tidkrevjande operasjonen.

Algoritme 1	$\frac{n(n-1)}{2}$
Algoritme 2	n^2
Algoritme 3	$n(1 + \log n)$
Algoritme 4	$2^n - n^{20} + n^{10}$

(a) Gje eit enklast mogleg Big-Θ-uttrykk (best mogleg Big-O-uttrykk) for kor mange ombytingar kvar algoritme treng.

Solution:

Algoritme 1	$\frac{n(n-1)}{2} \in \Theta(n^2)$
Algoritme 2	$n^2 \in \Theta(n^2)$
Algoritme 3	$n(1 + \log n) \in \Theta(n \log n)$
Algoritme 4	$2^n - n^{20} + n^{10} \in \Theta(2^n)$

(b) Sorter dei fire algoritmane frå raskast til treigast basert på køyretida for store tabellar (når n går mot uendeleg). Dersom du finn to eller fleire algoritmar som er like raske skal det markerast.

Solution:

1. Algoritme 3
2. Algoritme 1 og 2
3. Algoritme 4

Oppgåve 14 ..... *(8%)*

(a) Vis steg for steg korleis du bruker Euklids algoritme for å finna hcf$(525, 1295)$[1]?

Solution:

$$\text{hcf}(525, 1295) = \text{hcf}(245, 525) = \text{hcf}(35, 245) = 35.$$

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 13 modulo 81.

Solution:

$a = n \cdot q + r$	x	y
$81 = 13 \cdot 6 + 3$	-4	$1 - (-4) \cdot 6 = 25$
$13 = 3 \cdot 4 + 1$	1	-4
$3 = 1 \cdot 3 + 0$	0	1

Me ser at $13^{-1} \equiv 25 \mod 81$.

Oppgåve 15 ..... *(8%)*

Ta to polynom over $\mathbb{Z}_2$:

$$f(x) = x^4 + x^3 + x^2 + 1,$$
$$g(x) = x^3 + 1.$$

Rekn ut fylgjande

(a) $f(x) \mod g(x) =$

Solution:

$(x^4 + x^3 + x^2 + 1) / (x^3 + 1) = x + 1$

$x^4 + x$

$x^3 + x^2 + x + 1$

$x^3 + 1$

REST $= x^2 + x$

$f(x) \mod g(x) == x^2 + x.$

(b) $\text{hcf}(f(x), g(x)) =$

Solution:

$$\begin{aligned} \text{hcf}(f(x), g(x)) &= \text{hcf}(g(x), x^2 + x) \\ &= \text{hcf}(x^2 + x, x + 1) = x + 1 \end{aligned} \tag{3}$$

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