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 $\binom{777}{776}$.

Oppgåve 2 .... *(4%)*

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

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

Oppgåve 3 .... *(4%)*

Rekn ut fylgjande

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

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

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.)

Oppgåve 5 .... *(4%)*

Løys fylgjande kongruensar (modulære likningar)

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

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

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 $A \cdot B =$

(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 $C \cdot D =$

Oppgåve 8 .... *(4%)*

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

a) $$\begin{array}{c} s \Rightarrow t \\ t \\ \hline \therefore s \\ \hline \end{array}$$

b) $$\begin{array}{c} s \Rightarrow t \\ s \\ \hline \therefore t \\ \hline \end{array}$$

c) $$\begin{array}{c} s \Rightarrow t \\ \neg t \\ \hline \therefore \neg s \\ \hline \end{array}$$

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.

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

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

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

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

Oppgåve 11 .... *(12%)*

Denne oppgåva ser på relasjonar mellom to mengder.

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

(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.

Oppgåve 12 .... *(4%)*

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

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.

(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.

Oppgåve 14 .... *(8%)*

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

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 13 modulo 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) $f(x) \mod g(x) =$

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

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