Ingen hjelpemidler er tillatt.
Ta med **all mellomregning** som er nødvendig for å grunngi svaret.

Oppgave 1 .... *(4%)*

(a) Regn ut $\binom{6}{4}$.

(b) Regn ut $\binom{640}{639}$.

Oppgave 2 .... *(7%)*

Regn ut følgende

(a) $(5+8) \mod 9 =$

(b) $(9 \cdot 6 + 3) \mod 19 =$

(c) $(x^2 + x + 1) \cdot (x + 1)$ over $\mathbb{Z}_2$.

Oppgave 3 .... *(5%)*

Løs følgende kongruenser (modulære ligninger)

(a) $2x \equiv 1 \pmod 3$

(b) $3x + 2 \equiv 1 \pmod 5$

Oppgave 4 .... *(4%)*

(a) Skriv det heksadesimale tallet 2C om på desimalform.

(b) Skriv tallet 20 (desimal) på heksadesimal form.

Oppgave 5 .... *(12%)*

Vi har et datasystem med brukernavn og passord. Forklar hvordan vi finner antall unike, mulige passord, når

(a) ... passordet må bestå av nøyaktig seks små, norske bokstaver?

(b) ... passordet må bestå av seks til åtte små, norske bokstaver?

(c) ... passordet må bestå av seks til åtte teikn der *det første* er en stor norsk bokstav, og resten kan være enten store eller små bokstaver?

Det er tilstrekkelig å sette opp formler og sette inn tall. Du **trenger ikke** å regne ut formlene. Forklar hvilke telleprinsipper du trenger og hvordan du kommer frem til formlene i hvert delspørsmål.

Oppgave 6 .... *(6%)*

I dette spørsmålet ser vi på logiske argumenter.

(a) Se på de to utsagnene

1. Dersom det regnar, tek eg på regnjakke.
2. Det regnar.

Hvilken slutning kan du trekke fra disse to premissene ved hjelp av direkte bevis (Modus Ponens)?

(b) Se på argumentet

1. $s \Rightarrow t$
2. ??

$\therefore \neg s$

Hvilket utsagn må du sette for spørsmålstegnene for at argumentet skal være gyldig (Modus Tollens)? (Symbolet $\therefore$ kan lesesa som «ergo» eller som «dermed kan vi konkludere med at».)

Oppgave 7 .... *(5%)*

Forklar hva vi mener med en nulldivisor, og list opp nulldivisorene i $\mathbb{Z}_{12}$.

Oppgave 8 .... *(4%)*

Krypter meldingen «godmorgen» med Cæsars siffer. Vis fullstendig hvordan meldingen kan krypteres ved å bruke modulær aritmetikk over heltall.

Oppgave 9 .... *(8%)*

(a) La A og B være matriser over $\mathbb{Z}_2$:

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

Regn ut $A \cdot B =$

(b) La C og D være matriser over $\mathbb{Z}_5$:

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

Regn ut $C \cdot D =$.

Oppgave 10 .... *(12%)*

Tenk på relasjonen $<$ (mindre enn)

(a) Hva mener vi (generelt) med en relasjon?

Svar på følgende tre spørsmål om $<$-relasjonen og grunngi hvert svar:

(b) Er $<$ symmetrisk?

(c) Er $<$ refleksiv?

(d) Er $<$ transitiv?

Oppgave 11 .... *(12%)*

(a) Vis steg for steg hvordan du bruker Euklids algoritme for å finne $\text{hcf}(413, 273)$[1]?

(b) Vis hvordan du bruker Euklids utvidede algoritme for å finne den multiplikative inversen til 11 modulo 91.

(c) Gitt $\text{hcf}(a, b)$, hvordan vet vi om a har en multiplikativ invers modulo b?

Oppgave 12 .... *(16%)*

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

(a) Vis, steg for steg, hvordan du regner ut $16^{14} \mod 21$ på en effektiv måte.

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

(c) Bevis at algoritmen fra (b) avslutter i endelig tid.

(d) I krypteringsfunksjonen over er (e, n) den offentlige nøglen. Forklar hvordan den hemmelige (private) nøglen er definert eller hvordan den blir regnet ut.

Oppgave 13 .... *(5%)*

Se på rekurrensligningen

$$T(n) = 2 \cdot T(n-1) + 1,$$
$$T(0) = 1.$$

Bruk matematisk induksjon til å bevise at $T(n) = 2^{n+1} - 1$ for alle $n \geq 0$.

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