

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

Oppgåve 1 (4%)

- (a) Rekna ut $\binom{5}{2}$.
- (b) Rekna ut $\binom{720}{719}$.

Oppgåve 2 (4%)

Seks venar skal halda ein privat sjakkturnering der alle skal spela éin gong mot kvar av dei andre. Kor mange parti trengst? Kva teljeprinsipp bruker du?

Oppgåve 3 (7%)

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

- (a) Forenkla uttrykket $s \vee \neg s =$
- (b) Forenkla uttrykket $s \wedge F =$
- (c) Bruk ein sanningsstabell for å visa at $p \Rightarrow q$ er ekvivalent med $\neg p \vee (p \wedge q)$.

Oppgåve 4 (4%)

Rekna ut fylgjande

- (a) $5 + 7 \pmod{8}$
- (b) $5 \cdot 7 \pmod{21}$

Oppgåve 5 (5%)

Solve the equations

- (a) $2x \pmod{3} = 1$
- (b) $3x \pmod{5} = 2$

Oppgåve 6 (4%)

- (a) Skriv talet 17 (desimal) på hexadesimal form.
- (b) Skriv det hexadesimale talet 2F om på desimalform.

Oppgåve 7 (8%)

Rekna ut fylgjande

- (a) Over \mathbb{Z}_2 : $(x^3 + x + 1)(x^2 + 1)$
- (b) Over \mathbb{Z}_3 : $(x^5 + x^4 + 2x + 1) \pmod{(x^2 + 2x + 1)}$

Oppgåve 8 (8%)

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

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

Rekna ut $A \cdot B =$.

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

$$C = \begin{bmatrix} 2 & 1 \\ 6 & 1 \\ 3 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 2 & 3 \\ 4 & 0 \end{bmatrix} \quad (2)$$

Rekna ut $C \cdot D =$.

Oppgåve 9..... (5%)

Lat E vera ei matrise over \mathbb{Z}_3 :

$$E = \begin{bmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{bmatrix} \quad (3)$$

Rekna ut E^{-1} .

Oppgåve 10..... (8%)

Consider the statement

if m is even, then m^2 is even

- Formalise the statement using logical symbols.
- Prove the statement.

Oppgåve 11..... (12%)

Sjå på det affine sifferet $e_{k_1, k_2}(x) = k_1 \cdot x + k_2 \pmod{28}$.

- Kva meiner me med ein nulldivisor?
- Kva er nulldivisorane i \mathbb{Z}_{28} ?
- Kor mange val har me for k_1 i det affine sifferet dersom me krev éintydig dekryptering?
- Kva er dekrypteringsfunksjonen som svarer til $e_{k_1, k_2}(x)$?

Oppgåve 12..... (6%)

Sjå på transposisjonssifferet med krypteringsnykel $k = (2, 3, 1, 5, 4)$

- Krypter meldinga «transposisjon er ein permutasjon».
- Kva er dekrypteringsnykelen som svarer til k ?

Oppgåve 13..... (9%)

Tenk på ekvivalensrelasjonar.

- Kva meiner me med ein relasjon?
- Kva vil det seia at ein relasjon er ein ekvivalensrelasjon?
- Vis at $a \equiv b \pmod{n}$ er ein ekvivalensrelasjon. (Hugs at $a \equiv b \pmod{n}$ er det same som at $a \pmod{n} = b \pmod{n}$.)

Oppgåve 14..... (6%)

Sjå på RSA med ein krypteringsnykel (e, n) .

- Korleis vert n generert?
- Kva er krypteringsfunksjonen for RSA?
- Forklar korleis du finn dekrypteringsnykelen (d, n) som svarer til (e, n) .

Oppgåve 15..... (10%)

Sjå på fylgjande recurrence og gå ut frå at n er ein potens av tre,

$$\begin{aligned} T(n) &= 3(T(n/3)) + n, \quad \text{når } n \geq 1, \\ T(0) &= 1. \end{aligned}$$

- Teikn eit recurrence-tre.
- Bruk recurrence-treet for å finna ei eksakt løysing for $T(n)$.
- Gje ei Big- Θ -grense (beste moglege Big- O -grense) for $T(n)$.