Eksamensdøme 14. november 2013 **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) Rekna ut $\binom{5}{2}$.

(b) Rekna ut $\binom{720}{719}$.

Oppgåve 2 ..... *(4%)*

Seks venar skal halda ein privat sjakkturnerning 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 sanningstabell for å visa at $p \Rightarrow q$ er ekvivalent med $\neg p \vee (p \wedge q)$.

Oppgåve 4 ..... *(4%)*

Rekna ut fylgjande

(a) $5 + 7 \mod 8$

(b) $5 \cdot 7 \mod 21$

Oppgåve 5 ..... *(5%)*

Solve the equations

(a) $2x \mod 3 = 1$

(b) $3x \mod 5 = 2$

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 $\mathbb{Z}_3$: $(x^5 + x^4 + 2x + 1) \mod (x^2 + 2x + 1)$

Oppgåve 8 ..... *(8%)*

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

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

Rekna ut $A \cdot B =$.

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

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

Rekna ut $C \cdot D =$.

Oppgåve 9 ..... *(5%)*

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

$$E = \begin{bmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{bmatrix} \tag{3}$$

Rekna ut E^{-1}.

Solution:

$$\left[\begin{array}{ccc:ccc} 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{array}\right] \tag{4}$$

Multiply first row by 2.

$$\left[\begin{array}{ccc:ccc} 1 & 2 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{array}\right] \tag{5}$$

Subtract first row from last

$$\left[\begin{array}{ccc:ccc} 1 & 2 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right] \tag{6}$$

Subtract second row from last

$$\left[\begin{array}{ccc:ccc} 1 & 2 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 2 & 1 \end{array}\right] \tag{7}$$

Multiply last row by 2.

$$\left[\begin{array}{ccc:ccc} 1 & 2 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right] \tag{8}$$

Subtract twice Row 2 from Row 1.

$$\left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right] \tag{9}$$

Subtract last row from middle row.

$$\left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{array}\right] \tag{10}$$

Thus we get the answer

$$E^{-1} = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 2 \end{bmatrix} \tag{11}$$

Oppgåve 10 ..... *(8%)*

Consider the statement

if m is even, then m^2 is even

(a) Formalise the statement using logical symbols.

(b) Prove the statement.

Oppgåve 11 ..... *(12%)*

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

(a) Kva meiner me med ein nulldivisor?

(b) Kva er nulldivisorane i $\mathbb{Z}_{28}$?

(c) Kor mange val har me for k_1 i det affine sifferet dersom me krev éintydig dekryptering?

(d) Kva er dekrypteringsfunksjonen som svarer til $e_{k_1,k_2}(x)$?

Oppgåve 12 ..... *(6%)*

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

(a) Krypter meldinga «transposisjon er ein permutasjon».

Solution:

```
trans posis joner einpe rmuta sjon.
ratsn ospsi onjre ineep murat jos.n
```

(b) Kva er dekrypteringsnykelen som svarer til k?

Solution:

$$k = (2, 3, 1, 5, 4) \tag{12}$$

$$k^{-1} = (3, 1, 2, 5, 4) \tag{13}$$

(*Merknad.* For å sjå at løysinga er rett, prøv å permutera (kryptera) k vha. k^{-1} eller omvendt. Du skal da stå at med identiteten $\iota = (1, 2, 3, 4, 5)$.)

Oppgåve 13 ..... *(9%)*

Tenk på ekvivalensrelasjonar.

(a) Kva meiner me med ein relasjon?

(b) Kva vil det seia at ein relasjon er ein ekvivalensrelasjon?

(c) Vis at $a \equiv b \pmod{n}$ er ein ekvivalensrelasjon. (Hugs at $a \equiv b \pmod{n}$ er det same som at $a \mod n = b \mod n$.)

Oppgåve 14 ..... *(6%)*

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

(a) Korleis vert n generert?

(b) Kva er krypteringsfunksjonen for RSA?

(c) Forklar korleis du finn dekrypteringsnykelen (d, n) som svarer til (e, n).

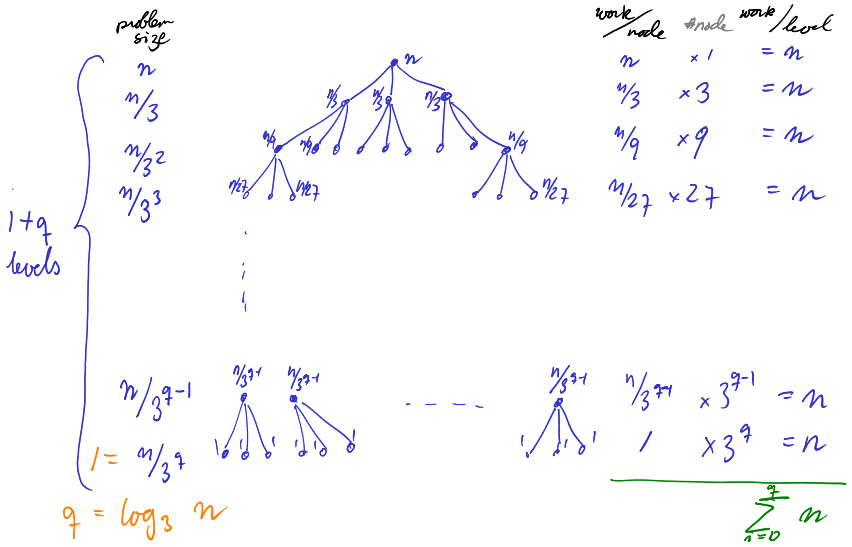
Oppgåve 15 ..... *(10%)*

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

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

(a) Teikn eit recurrence-tre.

Solution:



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

Solution: Me ser $1+\log_3 n$ nivå med n einingar per nivå. Altso får me $T(n) = n(1+\log_3 n)$.

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

Solution: Me har

$$T(n) = n(1 + \log_3 n) = n + n \log_3 n$$

Når me stryk den mindre lekken, har me

$$T(n) \in \Theta(n \log n)$$