Eksamen 2. juni 2015
Eksamenstid 4 timar

IR201712 Diskret Matematikk
Nynorsk

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

Oppgåve 1 ..... *(4%)*

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

Solution:

$$\binom{6}{4} = \frac{6 \cdot 5}{2 \cdot 1} = 15$$

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

Solution:

$$\binom{640}{639} = 640$$

Oppgåve 2 ..... *(7%)*

Rekn ut fylgjande

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

Solution:

$$(5 + 8) \mod 9 = 4$$

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

Solution: $(9 \cdot 6 + 3) \mod 19 = 57 \mod 19 = 0$

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

Solution: $(x^2 + x + 1) \cdot (x + 1) = (x^3 + x^2 + x) + (x^2 + x + 1) = x^3 + 1$

Oppgåve 3 ..... *(5%)*

Løys fylgjande kongruensar (modulære likningar)

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

Solution:

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 2 \cdot 2x &\equiv 2 \cdot 1 \pmod 3 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

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

Solution:

$$\begin{aligned} 3x + 2 &\equiv 1 \pmod 5 \\ 3x &\equiv 4 \pmod 5 \\ 2 \cdot 3x &\equiv 2 \cdot 4 \pmod 5 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Oppgåve 4 ..... *(4%)*

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

Solution: $2\text{C} = 2 \cdot 16 + 12 = 44$

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

Solution:

$$\begin{aligned} \lfloor 20/16 \rfloor &= 1 \\ 20 \mod 16 &= 4 \end{aligned}$$

Thus we write 20 as 14 in hexadecimal.

Oppgåve 5 ..... *(12%)*

Me har eit datasystem med brukarnamn og passord. Forklar korleis me finn talet på unike, moglege passord, når

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

> **Solution:** The password is a list of 6 elements from a set (alphabet) of 29 elements. Using the product principle (or the formula for the number of lists) we have 29^6 different possibilities.

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

> **Solution:** The password is a list of 6, 7, or 8 elements from a set (alphabet) of 29 elements. We use the sum principle to combine the number of 6-, 7-, and 8-character passwords, for a total of
>
> $$29^6 + 29^7 + 29^8$$
>
> options.

(c) ... passordet må bestå av seks til åtte teikn der *det fyrste* er ein stor norsk bokstav, og resten kan vera anten store eller små bokstavar?

> **Solution:** Again we need to split the problem into 6-, 7-, and 8-character passwords. For n-character passwords we note that we choose one character (the first) from a 26-element set, and the remaining $i - 1$ characters from a 46-element set (as in the previous subproblem). Thus we have 29 choices for the first letter and 58^{i-1} for the rest. Using the product principle we have $29 \cdot 58^{i-1}$ possible i-character passwords. Using the sum principle as before, we get a total of
>
> $$29 \cdot 58^5 + 29 \cdot 58^6 + 29 \cdot 58^7$$
>
> passwords.

Det er tilstrekkeleg å setja opp formlar og setja inn tal. Du **treng ikkje** å rekna ut formlane. Forklar kva teljeprinsipp du treng og korleis du kjem fram til formlane i kvart delspørsmål.

Oppgåve 6 ..... *(6%)*

I dette spørsmålet ser me på logiske argument.

(a) Sjå på dei to utsagna

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

Kva slutning kan du trekkja frå desse to premissane ved hjelp av direkte prov (Modus Ponens)?

> **Solution:** Me konkluderer med at «eg tek på regnjakke».

(b) Sjå på argumentet

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

$\therefore \neg s$

Kva utsagn må du setja for spørsmålsteikna for at argumentet skal vera gyldig (Modus Tollens)? (Symbolet $\therefore$ kan lesast som «ergo» eller som «dermed kan me konkludera med at».)

> **Solution:** Den andre premissen er $\neg t$.

Oppgåve 7 ..... *(5%)*

Forklar kva me meiner med ein nulldivisor, og list opp nulldivisorane i $\mathbb{Z}_{12}$.

Solution: Ein nulldivisor er eit element x som løyser likninga $x \cdot y = 0$ slik at $x \neq 0$ og $y \neq 0$. Nulldivisorar førekjem i ein del ringar, men aldri i kroppar.

Me faktoriserer $12 = 3 \cdot 2 \cdot 2$. Nulldivisorane er dermed multiplar av 3 og av 2: 2,3,4,6,8,9,10.

Oppgåve 8 ..... *(4%)*

Krypter meldinga «godmorgen» med Cæsars siffer. Vis fullstendig korleis meldinga kan krypterast ved å bruka modulær aritmetikk over heiltal.

Solution:

Klartekst	g	o	d	m	o	r	g	e	n
Talverdi	6	14	3	12	14	17	6	4	13
$x + 3 \mod 26$	9	17	6	15	17	20	9	7	16
Siffertekst	j	r	g	p	r	u	j	h	q

Oppgåve 9 ..... *(8%)*

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

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

Rekn ut $A \cdot B =$

Solution:

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

(b) Lat C og D vera matrisar over $\mathbb{Z}_5$:

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

Rekn ut $C \cdot D =$.

Solution:

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

Oppgåve 10 ..... *(12%)*

Tenk på relasjonen $<$ (mindre enn)

(a) Kva meiner me (generelt) 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 $b \in B$.

Svar på fylgjande tre spørsmål om $<$-relasjonen og grunngje kvart svar:

(b) Er $<$ symmetrisk?

> **Solution:** $<$ is not symmetric because $x < y$ does not imply $x > y$.

(c) Er $<$ refleksiv?

> **Solution:** $<$ is not reflexive because $x < x$ may well be false.

(d) Er $<$ transitiv?

> **Solution:** $<$ is transitive because $x < y$ and $y < z$ implies $x < z$

Oppgåve 11 ..... *(12%)*

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

> **Solution:**
>
> $$\begin{aligned}\text{hcf}(413, 273) &= \text{hcf}(273, 140)\\ &= \text{hcf}(140, 133)\\ &= \text{hcf}(133, 7) = 7\end{aligned}$$
>
> I.e. $\text{hcf}(413, 273) = 7$.

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 11 modulo 91.

> **Solution:**
>
$a = n \cdot q + r$	x	y
$91 = 11 \cdot 8 + 3$	$-1 - 8 \cdot 4 = -33$	4
$11 = 3 \cdot 3 + 2$	$1 - 3 \cdot (-1) = 4$	-1
$3 = 2 \cdot 1 + 1$	-1	1
>
> Me ser at $11^1 \equiv -33 \equiv 58 \mod 91$.

(c) Gjeve $\text{hcf}(a, b)$, korleis veit me om a hev ein multiplikativ invers modulo b?

> **Solution:** Inversen eksisterer dersom og berre dersom $\text{hcf}(a, b) = 1$.

Oppgåve 12 ..... *(16%)*

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

(a) Vis, steg for steg, korleis du reknar ut $16^{14} \mod 21$ på ein effektiv måte.

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

Solution:

$$\begin{aligned} 16^{14} \mod 21 &= (16^2 \mod 21)^7 \mod 7 = (256 \mod 21)^7 \mod 7 = 4^7 \mod 21 \\ &= (4^2)^3 \cdot 4 \mod 21 = 16^3 \cdot 4 \mod 21 \\ &= (16^2 \mod 21) \cdot 16 \cdot 4 \mod 21 \\ &= 4 \cdot 16 \cdot 4 \mod 21 \\ &= 256 \mod 21 = 4 \end{aligned}$$

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

Solution:

```
1  Algorithm SquareNmultiply(x, e, n)
2  if e = 1, return x mod n
3  y := SquareNmultiply(x, ⌊e/2⌋, n)
4  y := y^2 mod n
5  if e mod 2 = 1,
6  y := y · x mod n
7  return y
```

(c) Prov at algoritmen frå (b) avsluttar i endeleg tid.

Solution: Me føreset at $e \geq 1$ når algoritmen startar. Algoritmen terminerer når $e = 1$. Dersom $e > 1$ vert algoritmen kalt rekursivt med $e \leftarrow \lfloor e/2 \rfloor$. Me ser at $\lfloor e/2 \rfloor < e$, slik at e vert mindre for kvar runde. Me ser òg at $\lfloor e/2 \rfloor \geq 1$ for $e > 1$, slik at e ikkje kan hoppa over grunnfallet $e = 1$. Før eller sidan må dermed e verta lik 1 og algoritmen vil då terminera.

(d) I krypteringsfunksjonen over er (e, n) den offentlege nykkelen. Forklar korleis den løynde (private) nykkelen er definert eller korleis han vert rekna ut.

Solution: Den løynde nykkelen er (d, n) der d er den multiplikative inversen åt e modulo $\phi(n) = (p-1)(q-1)$ når n er produktet av to primtal p og q.

Oppgåve 13 ..... *(5%)*

Sjå på rekurrenslikninga

$$\begin{aligned} T(n) &= 2 \cdot T(n-1) + 1, \\ T(0) &= 1. \end{aligned}$$

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

Solution: We see immediately that $T(0) = 2^1 - 1 = 1$, so the claim is true for the base case $n = 0$.

Assuming that the claim is true for n, we have to prove that it is true for $n + 1$, i.e. that $T(n+1) = 2^{n+2} - 1$. We write $T(n+1) = 2 \cdot T(n) + 1 = 2 \cdot (2^{n+1} - 1) + 1 = 2^{n+2} - 2 + 1 = 2^{n+2} - 1$, q.e.d.