Eksamen 2. desember 2014 **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) Rekn ut $\binom{5}{3}$.

Solution:
$$\binom{5}{3} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

(b) Rekn ut $\binom{520}{519}$.

Solution:
$$\binom{520}{519} = 520$$

Oppgåve 2 ..... *(6%)*

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

(a) Forenkl uttrykket $s \vee \neg s =$

Solution: $s \vee \neg s = T$

(b) Forenkl uttrykket $s \wedge T =$

Solution: $s \wedge T = s$

(c) Sett opp ein sanningstabell for uttrykket $p \Rightarrow q$.

Solution:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Oppgåve 3 ..... *(4%)*

Rekn ut fylgjande

(a) $12 + 3 \mod 13$

Solution: $12 + 3 \mod 13 = 2$

(b) $6 \cdot 5 \mod 10$

Solution: $6 \cdot 5 \mod 10 = 0$

Oppgåve 4 ..... *(5%)*

Løys fylgjande kongruensar (modulære likningar)

(a) $2x \equiv 1 \pmod 5$

Solution:

$$2x \equiv 1 \pmod 5 \quad (1)$$
$$3 \cdot 2x \equiv 3 \cdot 1 \pmod 5 \quad (2)$$
$$x \equiv 3 \pmod 5 \quad (3)$$
$$(4)$$

(b) $4x + 2 \equiv 1 \pmod 9$

Solution:

$$4x \equiv -1 \equiv 8 \pmod 9, \quad (5)$$
$$7 \cdot 4x \equiv 7 \cdot 8 \pmod 9 \quad (6)$$
$$x \equiv 56 \equiv 2 \pmod 9 \quad (7)$$
$$(8)$$

Oppgåve 5 ..... *(12%)*

Klasse 5A skal velja elevrepresentantar. Der er tolv jenter og sju gutar i klassa. Svar på fylgjande, og forklar kva teljeprinsipp du bruker for kvart spørsmål.

(a) På kor mange måtar kan dei velja éin representant av kvart kjøn?

Solution: Me har mengdene J av jenter og G av gutar. Me skal velja éin av kvart kjøn, dvs. eit element frå det kartesiske produktet $J \times G$. Produktprinsippet seier at $\#(J \times G) = \#J \cdot \#G = 12 \cdot 7 = 84$. Me har altso 84 måtar å velja på.

(Ein kan bruka ein meir omstendeleg og generell føring med eksplisitt partisjonering, men ovanståande er enklare.)

(b) På kor mange måtar kan dei velja éin representant og éin vara?

Solution: Me har ei klasse $K = J \cup G$ der $\#K = 19$. Me skal velja eit ordna par av element frå K. Lat S vera mengda av slike par.

Me kan partisjonera $S = \bigcup_{x \in K} S_x$ der S_x er mengda av par med x som fyrste element (representant). Uavhengig av kven som er representant er der 18 kandidatar att til vara, so $\#S_x = 18$. Produktprinsippet gjev $\#S = \#K \cdot \#S_x = 19 \cdot 18 = 342$

(c) På kor mange måtar kan dei velja éin representant og éin vara når dei to må ha ulikt kjøn?

Solution: Me skal velja éin person av kvart kjøn som i del a, men me har to alternativ; jenta kan vera (hovud)representant eller guten kan vera det. Me tel kvart fall for seg og bruker sumprinsippet til slutt.

I det fyrste fallet har me 12 alternativ for representant og 7 for vara, og produktprinsippet gjev $12 \cdot 7 = 84$ alternativ totalt (sjå a). I det andre fallet har me 12 alternativ for representant og 7 for vara, og produktprinsippet gjev $7 \cdot 12 = 84$ alternativ totalt.

Sumprinsippet gjev $84 + 84 = 168$ måtar å velja på totalt.

(Merk at ein kan vera litt knappare i argumentet ved å visa til a.)

Oppgåve 6 ..... *(4%)*

(a) Skriv det heksadesimale talet 1E om på desimalform.

Solution: $1\text{E} = 16 + 14 = 30$

(b) Skriv talet 33 (desimal) på heksadesimal form.

Solution:

$$\lfloor 33/16 \rfloor = 2 \tag{9}$$

$$33 \mod 16 = 1 \tag{10}$$

Thus we write 33 as 21 in hexadecimal.

Oppgåve 7 ..... *(8%)*

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

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{11}$$

Rekn ut $A \cdot B =$

Solution:

$$A \cdot B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \tag{12}$$

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

$$C = \begin{bmatrix} 1 & 1 \\ 6 & 1 \\ 2 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 3 & 2 \\ 3 & 0 \end{bmatrix} \tag{13}$$

Rekn ut $C \cdot D =$.

Solution:

$$C \cdot D = \begin{bmatrix} 6 & 2 \\ 0 & 5 \\ 2 & 4 \end{bmatrix} \tag{14}$$

Oppgåve 8 ..... *(8%)*

Sjå på utsagnet

dersom m er eit oddetal, so er m^2 eit oddetal

(a) Formaliser utsagnet ved hjelp av logiske symbol.

Solution: We define the predicate

$$s(m) := \exists m' \in \mathbb{Z} \text{ such that } m = 2m' + 1 \tag{15}$$

and then the statement can be written as

$$t(m) := s(m) \Rightarrow s(m^2)$$

(b) Bevis utsagnet.

Solution: Consider an arbitrary m and assume that $s(m)$ is true. To prove the statement $t(m)$ we have to prove $s(m^2)$.
By the assumption, there is an m' such that $m = 2m' + 1$. We write

$$m^2 = (2m' + 1)^2 = 4m'^2 + 4m' + 1 = 2(2m'^2 + 2m') + 1$$

Now $m'' = 2m'^2 + 2m'$ is the value of m' which proves that $s(m^2)$ is true, so we have proved the statement $t(m)$ by conditional proof.

Oppgåve 9 ..... *(9%)*

Tenk på ekvivalensrelasjonar.

(a) Kva meiner me med ein relasjon?

> **Solution:** Ein relasjon R frå ei mengd A til ei mengd B, er ei delmengd $R \subset A \times B$. Me andre ord, R er ei mengd av par (a, b) der $a \in A$ og $b \in B$.

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

> **Solution:** Ein relasjon R er ein ekvivalensrelasjon dersom han er symmetrisk, refleksiv, og transitiv.
> (Dei tre kriteria bør definerast, men det rekk å visa at definisjonane er forstått i demonstrasjonen i neste delspørsmål.)

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

> **Solution:** Me må visa tre ting
>
> **Refleksivitet** $\forall x, x \equiv x \pmod{n}$
>
> **Symmetri** $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$
>
> **Transitivitet** $x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$
>
> I alle tre tilfella fylgjer eigenskapen trivielt sidan $\equiv$ er definert som ein likhet ($\exists m, x = y + mn$ er det same som $x \equiv y \pmod{n}$).

Oppgåve 10 ..... *(3%)*

List opp nulldivisorane i $\mathbb{Z}_{15}$.

> **Solution:** Me faktoriserer $15 = 3 \cdot 5$. Nulldivisorane er dermed multiplar av 3 og av 5: 3,5,6,9,10,12

Oppgåve 11 ..... *(16%)*

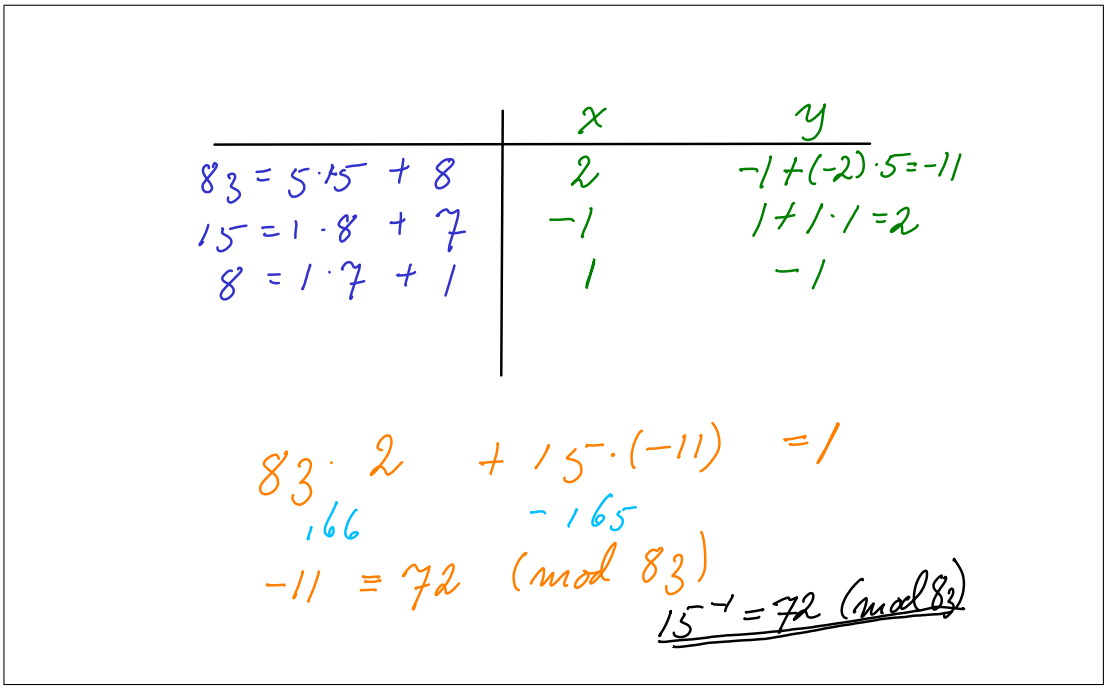
(a) Vis steg for steg korleis du bruker Euklids algoritme for å finna $\text{hcf}(365, 189)$[1]?

> **Solution:**
>
> $$\begin{aligned} \text{hcf}(365, 189) &= \text{hcf}(189, 176) \\ &= \text{hcf}(176, 13) \\ &= \text{hcf}(13, 7) \\ &= \text{hcf}(7, 6) \\ &= \text{hcf}(6, 1) = 1 \end{aligned}$$
>
> I.e. $\text{hcf}(365, 189) = 1$.

(b) Vis korleis du bruker Euklids utvida algoritme for å finna den multiplikative inversen til 15 modulo 83.

> **Solution:**

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



(c) Skriv ned pseudo-kode for Euklids algoritme.

Solution:

```
Euklid(a,b)
if b deler a, return b
else return Euklid(b,a mod b)
```

(d) Forklar korleis me kan vita at Euklids algoritme fullfører i endeleg tid.

Solution: Algoritma terminerer når b deler a. Merk at 1 deler a.
Sjå på $a \mod b$. Dersom $a \mod b = 0$, so har me grunnfallet og algoritma terminerer. Elles har me $a \mod b \in \{1, 2, \ldots, b-1\}$, og me gjer eit rekursivt kall med *ein mindre verdi for* b. I løpet av dei rekursive kalla er altso b monotont minkande og positiv. Innan høgst $b-1$ iterasjonar må me altso koma til grunnfallet $a \mod b = 0$, om ikkje anna ved at $b = 1$.

Oppgåve 12 ..... *(12%)*

(a) Forklar kva me meiner med eit siffer med offentleg nykel (asymmetrisk siffer).

> **Solution:** Offentleg nykel vil seia at krypterings- og krypteringsfunksjonen tek ulike nyklar som argument. Den offentlege nykelen vert brukt til kryptering. Dekryptering krev ein løynnykel som ikkje kan utleidast (i praksis) frå den offentleg nykelen.

(b) Nemn eitt døme på eit siffer som bruker offentleg nykel og som er i vanleg bruk i dag.

> **Solution:** RSA

(c) Kva føremonar har siffer med offentlege nyklar samanlikna med symmetriske siffer?

> **Solution:** Ein er ikkje avhengig av å ha delt ein løynd nykel på førehand. Den offentlege nykelen kan kringkastast.

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

> **Solution:** AES

(e) Kva føremonar har symmetriske siffer samanlikna med offentlege nyklar?

> **Solution:** Fyrst og framst er asymmetriske siffer treigare.
> Der er òg større uvisse om sikkerheita i asymmetriske system i framtida. Teoretiske og teknologiske nyvinningar kan tenkjast å knekka eksisterande asymmetriske siffer. Det er t.d. kjend at kvantemaskiner vil gjera det. Sikkerheita i symmetriske siffer vil heller svekkast jamnt.

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

> **Solution:** Ein bruker eit asymmetrisk siffer i oppstarten av kommunikasjonen, der ein mellom anna vel ein løynd nykel som vert sent kryptert med det asymmetriske sifferet.
> Denne løynde nykelen kan ein so bruka i eit symmetrisk siffer i resten av kommunikasjonen.

Oppgåve 13 ..... *(9%)*

Sjå på uttrykket $3^{69} \mod 19$.

1. Vis korleis du kan bruka Fermats lille teorem for å forenkla utrekninga.

> **Solution:**
> $$3^{69} \mod 19 = 3^{69 \mod 18} \mod 19 = 3^{15} \mod 19$$

2. Forklar kva andre rekneregler du kan bruka for å rekna ut slike uttrykk ($x^y \mod n$) so enkelt som mogleg.

> **Solution:** Me nyttar *square and multiply*, og reduserer modulo n for kvart steg, soleis:

3. Rekn ut $3^{69} \mod 19$. Vis korleis du gjer utrekninga.

Solution:

$$\begin{aligned} 3^{15} \mod 19 &= ((3^2 \cdot 3)^2 \cdot 3)^2 \cdot 3 \mod 19 \\ &= ((27 \mod 19)^2 \cdot 3)^2 \cdot 3 \mod 19 \\ &= ((8^2 \mod 19) \cdot 3)^2 \cdot 3 \mod 19 \\ &= (7 \cdot 3 \mod 19)^2 \cdot 3 \mod 19 \\ &= (2^2 \cdot 3 \mod 19 \\ &= 12 \end{aligned} \tag{16}$$