Gruppearbeid

Generelt ved gruppearbeid:

(1) Presentasjon av deltakerne, navn, studieprogram, kull.
(2) Velg en deltaker til å dele "whiteboard".
(3) Husk å spørre om alle er enige/er med, og husk å si i fra om du ikke skjønner noe eller har en annen måte å tenke på. I forelesningene skal vi lære og ikke prestere.

1. Gruppearbeid A i 20F

Husk:

(i) $a \equiv a' \mod n \Leftrightarrow a + n\mathbb{Z} = a' + n\mathbb{Z}$ i $\mathbb{Z}/n\mathbb{Z}$.
(ii) Anta at $a \equiv a' \mod n$ og $b \equiv b' \mod n$, da er

$$a + b \equiv a' + b' \mod n.$$
$$ab \equiv a'b' \mod n.$$

Oppgave 1 (Gammel eksamensoppgave). Finn alle x i $\mathbb{Z}$ slik at

(a) $9x \equiv 7 \mod 12$.
(b) $6x \equiv 9 \mod 15$.

Oppgave 2. Vis følgende korollar av Setning 71.

Korollar 72. *La $n > 1$ være et kvadratfritt heltall, og la $a \in \mathbb{Z}$. For hver $k \geq 1$, så er*

$$a^{k\varphi(n)+1} \equiv a \mod n,$$

der φ betegner Eulers phi-funksjon.

Oppgave 3, RSA. Alice ønsker å sende hemmelige meldinger til Bob. Alle kan lese hva som blir sendt, men likevel ikke klare å finne meldingen.

Vi har følgende antakelser: La p, q være to forskjellige primtall, og la $n = pq$. Da er $\varphi(n) = (p-1)(q-1)$. Velg e med $1 < e < \varphi(n)$ og $\gcd(e, \varphi(n)) = 1$, dvs. $\overline{e}$ har en inverse $\overline{d}$ i $\mathbb{Z}_{\varphi(n)}$ og $\overline{d} \cdot \overline{e} = \overline{1}$ i $\mathbb{Z}_{\varphi(n)}$ og $de - 1 = k\varphi(n)$ for en $k \geq 1$, der $1 < d < \varphi(n)$.

Alice: Hemmelig nøkkel $\{n, d\}$, og offentlig nøkkel $\{n, e\}$.
Bob: Vil sende en melding M, der $0 \leq M < n$, til Alice. Krypterer meldingen:
  (i) Beregner N slik at $M^e \equiv N \mod n$, der $0 \leq N < n$.
  (ii) Sender N til Alice.
Alice: (i) Mottar N.
  (ii) Beregner $D(N)$ med $0 \leq D(N) < n$ slik at

$$N^d \equiv D(N) \mod n.$$

(a) Får Alice tilbake M? Er $M = D(N)$?
(b) Hva avgjør om dette gir en rimelig sikker/hemmelig måte å kommunisere på?

2. Gruppearbeid B i 20F

Oppgave 4. La R være en ring med 1.

(i) Definer et *polynom* $f(x)$ med koeffisienter i R til å være en uendelig formell sum

$$\sum_{i\geq 0} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots ,$$

der $a_i \in R$ og $a_i \neq 0$ for bare et endelig antall i'er. Elementene $\{a_i\}_{i\geq 0}$ er *koeffisientene til polynomet* $f(x)$. Skriver

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

hvis $a_i = 0$ for alle $i > n$.

(ii) *Graden til* $f(x)$ er gitt ved

$$\deg f(x) = \begin{cases} n, & \text{hvis } a_n \neq 0 \text{ og } a_i = 0 \text{ for } i > n. \\ -\infty, & \text{hvis } a_i = 0 \text{ for alle } i \geq 0. \end{cases}$$

(iii) La $f(x) = \sum_{i\geq 0} a_i x^i$ og $g(x) = \sum_{i\geq 0} b_i x^i$ være polynomer med koeffisienter i R. Da er $f(x) = g(x)$ hvis $a_i = b_i$ for alle $i \geq 0$.

La $R[x]$ betegne mengden av alle polynomer med koeffisienter i R. Definer to binære operasjoner på $R[x]$, $+$ og $\cdot$: La

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

og

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n,$$

der $n = \max\{\deg f(x), \deg g(x)\}$. Definer

(i) $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n$.
(ii) $f(x)g(x) = d_0+d_1x+d_2x^2+\cdots+d_nx^n$, der $d_t = \sum_{i=0}^{t} a_i b_{t-i} \in R$.

Vis at $R[x]$ er en ring med 1. Spesielt, finn 1 og 0 i $R[x]$.

Oppgave 5. La $R = \mathbb{R}[x]$ være ringen av alle polynomer med koeffisienter i $\mathbb{R}$. La $f(x) = 2x^2 + 3x + 1$ og $g(x) = 3x^3 + 2$.

(a) Beregn $f(x)g(x)$.
(b) Hva kan vi si om graden til $f(x)g(x)$ for $f(x), g(x) \in R$?

Oppgave 6. La $R = \mathbb{Z}_6[x]$. være ringen av alle polynomer med koeffisienter i $\mathbb{Z}_6$. La $f(x) = \overline{2}x^2 + \overline{3}x + \overline{1}$ og $g(x) = \overline{3}x^3 + \overline{2}$.

(a) Beregn $f(x)g(x)$.
(b) Hva kan vi si om graden til $f(x)g(x)$ for $f(x), g(x) \in R$?
(c) Hvorfor får vi ulik konklusjon i Oppgave 5 og Oppgave 6?

Oppgave 7. Bevis eller gi et moteksempel til følgende utsagn:

(i) $R[x]$ er kommutativ hvis og bare hvis R er kommutativ?
(ii) $R[x]$ er et integritetsområde hvis og bare hvis R er et integritetsområde?
(iii) $R[x]$ er en kropp hvis og bare hvis R er en kropp?

Oppgave 8. La p være et primtall. Betrakt polynomet $f(x) = x^p - x$ i $\mathbb{Z}_p[x]$.

(a) Vis at $f(\overline{a}) = \overline{0}$ for alle $\overline{a}$ i $\mathbb{Z}_p$.
(b) La $p = 3$. Vis at $x(x-\overline{1})(x-\overline{2}) = x^3-x$ og at $(x-\overline{1})(x-\overline{2}) = x^2-\overline{1}$.
(c) Anta at vi har vist at $\prod_{i=0}^{p-1}(x - \overline{i}) = x^p - x$. Vis at

$$\prod_{i=0}^{p-1}(x + \overline{p-i}) = x^p - x.$$

(d) Under samme antakelse som i (c), vis at

$$\prod_{i=1}^{p-1}(x + \overline{p-i}) = x^{p-1} - \overline{1}.$$

(e) **Utfordring:** Vis en implikasjon av Wilsons teorem, nemlig at

$$(p-1)(p-2)\cdots 2 \cdot 1 = (p-1)! \equiv -1 \mod p.$$