Litt repetisjon

$\mathbb{Z} = \{\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\}$
$\mathbb{N} = \{0,\ 1,\ 2,\ 3, \ldots\}$
$\mathbb{Z}_+ = \{1,\ 2,\ 3, \ldots\}$
$\mathbb{Z}_n = \{0,\ 1,\ 2,\ 3, \ldots,\ n-2,\ n-1\}$

Divisjonsalgoritmen: $n \in \mathbb{Z}$ og $d \in \mathbb{Z}_+$.
$n = qd + r, \qquad q \in \mathbb{Z},\ r \in \mathbb{N},\ 0 \leq r < d.$

$d|n$ "d deler n" eller "n er delelig/delbar med d"

$a, b \in \mathbb{Z}$ største felles divisor:
$(a, b) = \gcd(a, b) = \text{mfm}(a, b)$

$a_1, a_2, \ldots, a_n$ er parvis relativt primiske hvis $(a_i, a_j) = 1$ når $i \neq j$.

Modulo begrepet

$m \in \mathbb{Z}_+$ et "referansetall"

Divisjonsalgoritmen: $a = qm + r$, $0 \leq r < m$.
Skriver: a **div** $m = q$ og a **mod** $m = r$

En del utsagn som er ekvivalente:
$a \equiv b \pmod{m}$
$b \equiv a \pmod{m}$
$m|a - b$
$m|b - a$
$a - b = km$ for et tall $k \in \mathbb{Z}$
$b - a = km$ for et tall $k \in \mathbb{Z}$
a **mod** $m = b$ **mod** m

Noen ganger kan det være en ide å "tenke":
"For $a \in \mathbb{Z}$ har vi en $b \in \mathbb{Z}_m$ slik at $a \equiv b \pmod{m}$." eller
"For $b \in \mathbb{Z}_m$ har vi en mengde med tall a slik at $a \equiv b \pmod{m}$; $\{b + km | \ k \in \mathbb{Z}\}$."

Modulær aritmetikk

Nyttig redskap: **Euklids algoritme**
brukes til å finne største felles multiplum av to tall
er videre nyttig for å finne *heltalls* løsninger for ligninger av typen $4s + 7t = 1$.
Hvordan utfører vi den? Bruk divisjonsalgoritmen.

Vi kan addere, subtrahere og multiplisere "som vanlig".
I en subtraksjon, addisjon, eller multiplikasjon kan vi bytte ut tallene med "tilsvarende tall" og få samme svar.

Vi kan derimot generelt **ikke dividere**.
Men, *i en del tilfeller* kan vi "i stedet" finne *inverser.*
For å finne inverser er det nyttig å kunne løse ligninger av typen $4s + 7t = 1$.
Dermed er *Euklids algoritme* et nyttig verktøy for å finne inverser.

Noen nyttige resultater

Den kinesiske restsetningen: Løsninger til ligningssett av typen

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Fermats lille setning: p et primtall, a et heltall. Da har vi
$a^p \equiv a \pmod{p}$.
Hvis i tillegg $p \not| a$ så har vi
$a^{p-1} \equiv 1 \pmod{p}$.