KONGRUENSREGNING

For $n \in \mathbb{N}$ så danner vi en ekvivalens-relasjon $\sim$ ved

$$a \sim b \iff a - b = K \cdot n, \quad K \in \mathbb{Z}.$$

Hvis vi nå skriver $a = z_1 n + r_1$, $b = z_2 n + r_2$, $r_1, r_2 < n$, har vi at

$$a - b = (z_1 - z_2)n + r_1 - r_2 = \ell n + r$$

med $-n < r < n$.

så $a \sim b$ hvis $r_1 = r_2$.

Vi har sett tidligere at $\sim$ er kompatibel med ringoperasjonene på $\mathbb{Z}$, så vi kan danne kvotientringen $\mathbb{Z}_n = \mathbb{Z}/_{\sim}$

Prop 35. Dersom $\bar{x} + \bar{a} = \bar{x} + \bar{b}$ så har vi $\bar{a} = \bar{b}$.

Bevis: Alle elementer i $\mathbb{Z}_n$ har additive inverser, fordi

$$\bar{x} + \overline{(-x)} = \overline{x - x} = \bar{0}$$

∎

Advarsel: Tilsvarende kanselering holder ikke alltid for multiplikasjon i $\mathbb{Z}_n$.

Eks1 $\bar{4} \cdot \bar{1} = \bar{4} \cdot \bar{4}$ i $\mathbb{Z}_{12}$

men det er ikke tilfelle at $\bar{1} = \bar{4}$.

Eks2 $\bar{4}\,\bar{3} = \overline{12} = \bar{0}$,

Selv om hverken $\bar{3}$ eller $\bar{4}$ er $\bar{0}$.

DEF For $\bar{a} \in \mathbb{Z}_n$, $\bar{a} \neq 0$, sier vi at $\bar{a}$ er en nulldivisor dersom $\bar{a} \cdot \bar{b} = 0$, $\bar{b} \neq 0$.

Vi sier at $\bar{a}$ har kanseleringsegenskapen dersom

$\bar{a}\bar{b} = \bar{a}\bar{c} \Rightarrow \bar{b} = \bar{c}$ for alle $\bar{b}, \bar{c} \in \mathbb{Z}_n$.

Lemma: Vi har at $\bar{a}$ har kanseringsegenskapen hvis og bare hvis $\bar{a}$ ikke er en nulldivisor.

Bevis: Anta kanselering, la $\bar{b} \neq 0$. Da kan ikke $\bar{a}\bar{b} = 0 = \bar{a}\,0$

Anta at $\bar{a}$ ikke er nulldivisor, $\bar{a}\bar{b} = \bar{a}\bar{c}$. $\bar{a}\bar{b} - \bar{a}\bar{c} = 0$

$\bar{a}(\bar{b} - \bar{c}) = 0$. ∎

Prop 36 Vi har at $(a,n)=1$ er ekvivalent med at $\bar{a}$ ikke er en nulldivisor.

Dette er igjen ekvivalent med at $\bar{a}$ multiplikativt er inverterbar.

Bevis. Anta at $(a,n)=1$.

Da har vi $pa+qn=1$

Anta at $\bar{a}\bar{b}=\bar{0}$. Det vi si $ab=kn$.

Da får vi at

$$pab+qnb=b \Rightarrow pkn+qnb=b \Rightarrow n(kn+qb)=b, \text{ så } \bar{b}=\bar{0}.$$

På den annen side, anta $(a,n)=d>1$.

Da har vi $a=pd$, $n=qd$, $q<n$.

Da har vi $aq=\frac{pdn}{d}=pn$, så $\bar{a}\bar{q}=\bar{0}$. ∎

Lineære ligninger i $\mathbb{Z}_n$

Vi ønsker å studere ligninger

(*) $\bar{a}\bar{x} = \bar{b}$.

Å løse (*) er det samme

Som å løse

$$ax - b = -ny \iff ax + ny = b,$$

i $\mathbb{Z}$

Denne ligningen kan løses hvis og bare hvis

$(a,n) \mid b$.

Teorem 38/39. Ligningen $\bar{a}\bar{x} = \bar{b}$ kan løses hvis og bare hvis $d = (a,n) \mid b$. I så fall fins d distinkte løsninger.

Bevis. Må sjekke antall løsninger.

Husk å se på $ax + ny = d$

Hvis sett at hvis x, y er en løsning,

så er $x + \frac{n}{d}k$, $y - \frac{a}{d}k$ løsninger, for $k \in \mathbb{Z}$

EKS 1 Vi vil løse $\overline{3}\bar{x} = \overline{11}$ i $\mathbb{Z}_{19}$. (1 løsning)

Siden 19 er et primtall finns det bare en løsning. Vi har at $(3,19)=1$.

$(*)$ $3x + 19y = 1$

$3 \cdot (-6) + 19 = 1$

Så $(-6, 1)$ løser $(*)$.

Da løser -6 [illegible] løsningen, og $-66 \sim 10 \mod(19)$.

Så To løser $(**)$.