17/10 - 2013

MAT 1140

Kongruensregning

Anta at t er et naturlig tall større enn 1. Definér en relasjon $\equiv \pmod t$ på $\mathbb{Z}$ ved

$$a \equiv b \pmod t \iff t \mid b-a$$

Lemma: $\equiv \pmod t$ er en ekvivalensrelasjon

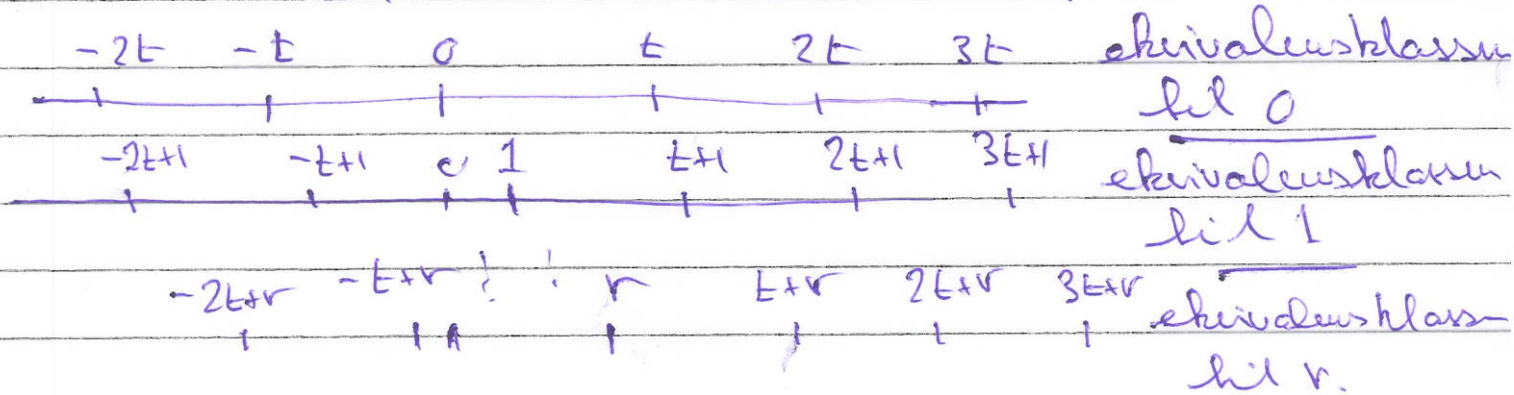
Bevis: Vi må sjekke de tre betingelsene

(i) **Refleksiv** $a \equiv a \pmod t$ siden $t \mid a-a$.

(ii) **Symmetri:** Anta $a \equiv b \pmod t$. Da er $b-a$ delelig med t, og følgelig er $a-b$ delelig med t; dvs $b \equiv a \pmod t$

(iii) **Transitivitet:** Anta $a \equiv b \pmod t$ og $b \equiv c \pmod t$, da $b-a = nt$ og $c-b = mt$ siden både $b-a$ og $c-b$ er delelig med t. Dermed er $c-a = c-b+b-a = mt+nt = (m+n)t$, som viser at $a \equiv c \pmod t$.

Hvordan ser ekvivalensklassene ut:

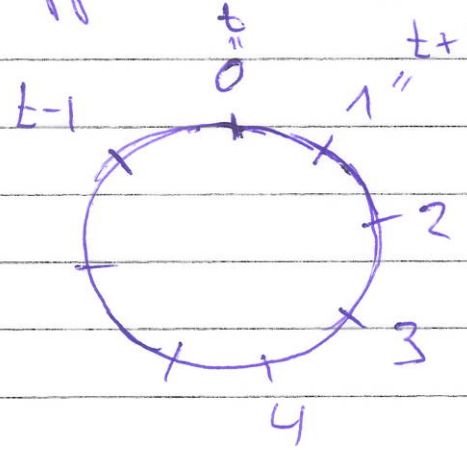


Oppsummering: La $\bar{a}$ betegne ekvivalensklassen til a. Det finnes t forskjellige ekvivalensklasser: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{t-1}$.

Hvis $0 \leq r < t$, består ekvivalensklassen $\bar{r}$ av de tallene som gir r til rest når de deles med r.

Oppkvikingsbildet: Tenk på tallinjen

som en vendelig hageslange og kveil den opp i sirkler med omkrets t



Da er to tall ekvivalente modulo t dersom de havner på samme sted etter oppkvikingen.

Setning: Anta at $a_1 \equiv a_2 \pmod{t}$ og $b_1 \equiv b_2 \pmod{t}$. Da er

(i) $a_1 + b_1 \equiv a_2 + b_2 \pmod{t}$

(ii) $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{t}$

Bevis: Siden $a_1 \equiv a_2 \pmod{t}$ og $b_1 \equiv b_2 \pmod{t}$, finnes det hele tall n og m slik at $a_2 - a_1 = nt$, $b_2 - b_1 = mt$, dvs.

$$a_2 = a_1 + nt \quad , \quad b_2 = b_1 + mt.$$

Dermed er:

(i) $a_2 + b_2 = a_1 + nt + b_1 + mt = (a_1 + b_1) + (n+m)t$, så $a_1 + b_1 \equiv a_2 + b_2 \pmod{t}$

(ii) $a_2 \cdot b_2 = (a_1 + nt)(b_1 + mt) = a_1 b_1 + a_1 mt + b_1 nt + nmt^2 = a_1 b_1 + (a_1 m + b_1 n + nmt)t$, som viser at $a_1 b_1 \equiv a_2 b_2 \pmod{t}$

La $\mathbb{Z}/(t) = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{t-1}\}$

være ekvivalensklassene $\bar{k} \equiv \pmod{t}$.
Vi innfører binære operasjoner på $\mathbb{Z}/(t)$ ved

(i) $\bar{a} + \bar{b} = \overline{a+b}$

(ii) $\bar{a} \cdot \bar{b} = \overline{ab}$

Legg merke til at disse operasjonene er veldefinerte p.g.a. setningen ovenfor – det spiller ingen rolle hvilke representanter vi velger for ekvivalensklassene.

Eksempel: Multiplikasjonstabell for $\mathbb{Z}/(6)$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

OBS: Vi kan ha $\bar{a}\cdot\bar{b}=\bar{0}$ selv om hverken $\bar{a}=\bar{0}$ eller $\bar{b}=\bar{0}$

Setning: For alle $\bar{a},\bar{b},\bar{c}\in\mathbb{Z}/(L)$ gjelder

(i) $\bar{a}+\bar{b}=\bar{b}+\bar{a}$ og $\bar{a}\bar{b}=\bar{b}\cdot\bar{a}$ (kommutative lover)

(ii) $(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$ og $(\bar{a}\bar{b})\bar{c}=\bar{a}(\bar{b}\bar{c})$ (assosiative lover)

(iii) $\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$ distributiv lov

(iv) $\bar{a}+\bar{0}=\bar{a}$ (nullelement)

(v) $\bar{a}\cdot\bar{1}=\bar{a}$ (nøytralt element)

(vi) $\bar{a}+(-\bar{a})=0$ (motsatt element)

Bevis: Alle bevises på samme måte. Vi tar (ii) som eksempel:

$$\left.\begin{aligned}(\bar{a}+\bar{b})+\bar{c}&=\overline{a+b}+\bar{c}=\overline{a+b+c}\\ \bar{a}+(\bar{b}+\bar{c})&=\bar{a}+\overline{b+c}=\overline{a+b+c}\end{aligned}\right\}\text{ like}$$

$$\left.\begin{aligned}(\bar{a}\cdot\bar{b})\bar{c}&=\overline{ab}\cdot\bar{c}=\overline{abc}\\ \bar{a}(\bar{b}\cdot\bar{c})&=\bar{a}\cdot\overline{bc}=\overline{abc}\end{aligned}\right\}\text{ like}$$

Setning (Forkortningsregel for addisjon). Hvis $\bar{x}+\bar{a}=\bar{y}+\bar{a}$, så er $\bar{x}=\bar{y}$.

Bevis: Siden $\bar{x}+\bar{a}=\bar{y}+\bar{a}$, er $(\bar{x}+\bar{a})+(\overline{-a})=\bar{y}+\bar{a}+(\overline{-a})$
Videre er

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

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

Følgelig er $\bar{x}=\bar{y}$.

Spørsmål: Finnes det en tilsvarende forkortingsregel for multiplikasjon:

$$\bar{x}\,\bar{a}=\bar{y}\cdot\bar{a} \Longrightarrow \bar{x}\cdot\bar{y} \;?$$

Dette er et mye mer komplisert spørsmål

Definisjon: Et element $\bar{a}\in\mathbb{Z}/(L)$ heter en nulldivisor dersom $\bar{a}\neq\bar{0}$ og $\bar{a}\cdot\bar{b}=\bar{0}$ for en $\bar{b}\neq\bar{0}$.

Observasjon: Fra tabellen ovenfor ser vi at $\bar{2}$, $\bar{3}$ og $\bar{4}$ er nulldivisorer i $\mathbb{Z}/(6)$.

Definisjon: Vi sier at forkortningsregelen gjelder for $\bar{a}$ dersom $\bar{a}\,\bar{x}=\bar{a}\,\bar{y} \Rightarrow \bar{x}=\bar{y}$ for $\bar{x},\bar{y}\in\mathbb{Z}/(L)$

Setning: Anta $\bar{a} \neq \bar{0}$. Da er

$\bar{a}$ er en nulldivisor $\Leftrightarrow (a,t) \neq 1$

og

forkortningsregelen holder for $a \Leftrightarrow (a,t) = 1$

Bevis: Anta først at $(a,t) = 1$. Vi skal vise at forkortningsregelen holder og $\bar{a}$ ikke er en nulldivisor.

Anta $\bar{a}\bar{x} = \bar{a}\bar{y}$, da $t \mid a(x-y)$. Siden $(a,t) = 1$, må $t \mid (x-y)$ og følgelig er $\bar{x} = \bar{y}$. Følgelig gjelder forkortningsregelen.

Anta så er $\bar{a}\,\bar{x} = \bar{0}$. Da er $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{0}$, og ifølge forkortningsregelen er $\bar{x} = 0$. Følgelig er $\bar{a}$ ikke en nulldivisor.

Anta så at $(a,t) \neq 1$. Vi skal vise at forkortningsregelen ikke gjelder og at $\bar{a}$ er en nulldivisor. La $d = (a,t)$ og la $k, l \in \mathbb{Z}$ være slik at $a = kd$, $t = ld$. Da er $\bar{a} \cdot \bar{l} = \bar{k}\bar{d}\bar{l} = \bar{k} \cdot \bar{t} = \bar{0}$

Siden $l < t$, er $\bar{l} \neq \bar{0}$, og følgelig er $\bar{a}$ en nulldivisor. I tillegg er

$$\bar{a} \cdot \bar{l} = \bar{0} = \bar{a} \cdot \bar{0}$$

ulen at $\bar{d} = \bar{0}$, og det viser at forkortningsregelen ikke gjelder for $\bar{a}$

Korollar: Anta at t er et primtall. Da har $\mathbb{Z}/(t)$ ingen nulldivisorer og forkortningsregelen gjelder for alle $\bar{a} \in \mathbb{Z}/(t)$, $\bar{a} \neq \bar{0}$.

Bevis: $(a, t) = 1$ for alle $a \in \{1, 2, \ldots, t-1\}$