Tillitsstudenter:

Restklasseringene $\mathbb{Z}/(t)$

$\bar{a}$ er en nulldivisor dersom $\bar{a} \neq \bar{0}$ og det fins en $\bar{b} \neq \bar{0}$ slik at $\bar{a} \cdot \bar{b} = \bar{0}$

$\bar{a}$ tilfredsstiller forkortningsregelen dersom $\bar{a}\,\bar{b} = \bar{a}\,\bar{c} \Rightarrow \bar{b} = \bar{c}$

Teorem: (i) Hvis $(a,t) = 1$, så gjelder forkortningsregelen for $\bar{a}$ og $\bar{a}$ er ikke en nulldivisor.

(ii) Hvis $(a,t) > 1$, så gjelder ikke forkortningsregelen for $\bar{a}$ og $\bar{a}$ er en nulldivisor.

Bevis: (i) Anta at $(a,t) = 1$. Anta at $\bar{a}\,\bar{b} = \bar{a}\bar{c}$ i $\mathbb{Z}/(t)$. Det betyr $t \mid ab - ac$, altså $t \mid a(b-c)$. Siden $(a,t) = 1$, så må $t \mid b-c$, men det betyr at $\bar{b} = \bar{c}$. Forkortningsregelen gjelder.

Anta at $\bar{a} \neq \bar{0}$ og at $\bar{a} \cdot \bar{b} = \bar{0}$. Må vise at $\bar{b} = \bar{0}$.
Omformer $\bar{a}\,\bar{b} = \bar{0}$ til $\bar{a} \cdot \bar{b} = \underbrace{\bar{a}\,\bar{0}}_{\bar{0}}$. Siden forkortningsregelen gjelder, betyr dette at $\bar{b} = \bar{0}$.

(ii) Anta at $(a,t) = d > 1$. Da finnes det tall k, l slik at $a = kd$, $t = ld$. Dermed er $\bar{a} \cdot \bar{l} = \bar{k}\,\underbrace{\bar{d} \cdot \bar{l}}_{\bar{t}} = \bar{k}\,\underbrace{\bar{t}}_{\bar{0}} = \bar{0}$

Siden $\bar{l} \neq \bar{0}$, må $\bar{a}$ være en nulldivisor.
Forkortningsregelen gjelder heller ikke siden $\quad 0 \cdot 7 = 0 \cdot 231$

$\bar{a} \cdot \bar{l} = \underbrace{\bar{a} \cdot \bar{0}}_{\bar{0}}$ men $\bar{l} \neq \bar{0}$.

Korollar: Hvis t er et primtall, så finnes det ikke nulldivisorer i $\mathbb{Z}/(t)$ og forkortningsregelen gjelder for alle $\bar{a} \neq \bar{0}$.

Bevis: Siden t er et primtall, så er t innbyrdes primisk med $1, 2, 3, \ldots, t-1$.

Ligningsløsning i $\mathbb{Z}/(t)$

Ser på ligninger av typen $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(t)$

Setning: Ligningen $\bar{a}\bar{x} = \bar{b}$ har en løsning i $\mathbb{Z}/(t)$ hvis og bare hvis $(a,t) \mid b$

Bevis: Anta først at $(a,t) \mid b$. Da vet vi at det finnes x og y slik at $ax + ty = b$. Tar vi restklassen på begge sider, får vi

$$\bar{a}\bar{x} = \underbrace{\bar{a}\bar{x} + \bar{t}\cdot\bar{y}}_{\bar{t} = \bar{0}} = \overline{ax+ty} = \bar{b} \Rightarrow \bar{a}\bar{x} = \bar{b}.$$

Anta så at ligningen $\bar{a}\bar{x} = \bar{b}$ har en løsning. Det betyr at $t \mid b - ax$, dvs at det finnes et tall $y \in \mathbb{Z}$ slik at $b - ax = t\cdot y$. Dermed $b = ax + ty$, dvs b er en lin. komb. av a og t. Dette er bare mulig når $(a,t) \mid b$.

Korollar: Anta at ligningen $\bar{a}\bar{x} = \bar{b}$ har en løsning $\bar{x}_0$ i $\mathbb{Z}/(t)$. Dersom $d = (a,t)$, så ligningen nøyaktig d løsninger i $\mathbb{Z}/(t)$ og de er

$$\bar{x}_k = \bar{x}_0 + k\,\overline{\tfrac{t}{d}} \quad \text{der } k = 0, 1, \ldots, d-1$$

Bevis: Følger fra det vi vet om løsninger av $ax + ty = b$.

Eksempel: Finn alle løsningene til $\overline{48}\,\bar{x} = \bar{2}$ i $\mathbb{Z}/(110)$

Bruker Euklids algoritme på $\underset{t}{110}$ og $\underset{a}{48}$

$$110 = 2\cdot 48 + 14$$
$$48 = 3\cdot 14 + 6$$
$$14 = 2\cdot 6 + 2 \quad \text{— største felles faktor.}$$
$$6 = 3\cdot 2$$

Nøster opp over: $2 = 14 - 2\cdot 6$
$$= 14 - 2\cdot(48 - 3\cdot 14)$$
$$= 7\cdot 14 - 2\cdot 48$$
$$= 7\cdot(110 - 2\cdot 48) - 2\cdot 48$$
$$= 7\cdot 110 - 16\cdot 48 \Rightarrow 2 = 7\cdot 110 - 16\cdot 48$$

Altså er $(-16)\cdot 48 = 2 - 7\cdot 110$

Tar kongruensklassen: $\overline{(-16)}\cdot\overline{48} = \bar{2} - \bar{7}\cdot\underbrace{\overline{110}}_{\bar{0}}$

dvs $\overline{(-16)}\cdot\overline{48} = \bar{2}$.

Har en løsning: $\bar{x}_0 = \overline{-16} = \overline{-16+110} = \overline{94}$.

Hva med resten? Det er $d = 2$ løsninger i alt.

$$\bar{x}_1 = \bar{x}_0 + 1\cdot\overline{\tfrac{t}{d}} = \overline{94} + \overline{\tfrac{110}{2}} = \overline{94} + \overline{55} = \overline{149} = \overline{149 - 110} = \overline{39}$$

Løsningene er $\bar{x}_0 = \overline{94}$ og $\bar{x} = \overline{39}$.

Setning: Hvis p er et primtall, så har ligningen $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(p)$ en løsning for $\bar{a} \neq \bar{0}$. Denne løsningen er entydig.

Bevis: Siden $(a,p) = 1$, så er $(a,p) \mid b$. Antall løsninger er $d = (a,p) = 1$.

Setning: Anta at p er primtall. Da har ethvert element $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$ en entydig invers, dvs et element $\bar{a}^{-1}$ slik $\bar{a} \cdot \bar{a}^{-1} = \bar{1}$.

Bevis: En invers er det samme som en løsning av ligningen $\bar{a} \cdot \bar{x} = \bar{1}$, og det vi det finnes nøyaktig én av.

Setning: Hvis $\bar{a} \neq \bar{0}$, så er løsningen til ligning $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(p)$ gitt ved $\bar{x} = \bar{a}^{-1}\bar{b}$.

Bevis: Hvis x er løsningen på er $\bar{a}\bar{x} = \bar{b}$. Ganger på begge sider med $\bar{a}^{-1}$: $\bar{a}^{-1}(\bar{a}\bar{x}) = \bar{a}^{-1}\bar{b}$. Ved ass. lov er dette lik $\underbrace{(\bar{a}^{-1}\bar{a})}_{1}\bar{x} = \bar{a}^{-1}\bar{b}$, dvs $\bar{1} \cdot \bar{x} = \bar{a}^{-1}\bar{b}$, dvs $\bar{x} = \bar{a}^{-1}\bar{b}$.

Fermats lille teorem

Fermats lille teorem: Anta at p er et primtall. For alle $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$ er

da $\bar{a}^{p-1} = 1$

Bevis: De ikke-null elementene i $\mathbb{Z}/(p)$ er

$\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}$ (p−1) stykker

Ganger hver av dem med $\bar{a}$

$\bar{a}\bar{1}, \bar{a}\bar{2}, \bar{a}\bar{3}, \ldots, \bar{a}(\overline{p-1})$ ikke-null (siden $\bar{a}$ ikke er en nulldivisor) forskjellige (siden forkortningsregelen gjelder) (p−1) stykker.

Siden det bare finnes p−1 forskjellige, ikke-null elementer i $\mathbb{Z}/(p)$, må de to listene inneholde de samme elementene.

$$\cancel{\bar{1}} \cdot \cancel{\bar{2}} \cdot \cancel{\bar{3}} \cdot \ldots \cdot \cancel{(\overline{p-1})} = \bar{a}\cancel{\bar{1}} \cdot \bar{a}\cancel{\bar{2}} \cdot \ldots \cdot \bar{a}\cancel{(\overline{p-1})}$$

$$1 = \bar{a}^{p-1}$$

Hurra!

Korollar: Hvis p er et primtall og $\bar{a} \in \mathbb{Z}/(p)$, så er $\bar{a}^p = \bar{a}$.

Bevis: Hvis $\bar{a} \neq 0$, sier Fermat at $\bar{a}^{p-1} = \bar{1}$, så hvis vi ganger med $\bar{a}$, får vi $\bar{a}^p = \bar{a}$

Hvis $\bar{a} = 0$, sier ligningen $\bar{0}^p = \bar{0}$, som er sann.

Eksempel: Vis at for alle $n \in \mathbb{Z}$ er $n^7 + 14n^2 - n$ delelig med 7.

Observasjon: a er delelig med 7 $\Leftrightarrow$ $\bar{a} = \bar{0}$ i $\mathbb{Z}/(7)$

Undersøker restklassen til $n^7 + 14n^2 - n$ i $\mathbb{Z}/(7)$

$$\overline{n^7 + 14n^2 - n} = \overline{n^7} + \overline{14n^2} - \bar{n} = \underset{\substack{\parallel \\ \bar{n}}}{\bar{n}^7} + \underset{\substack{\parallel \\ \bar{0}}}{\overline{14}}\,\bar{n}^2 - \bar{n} = \bar{n} + \bar{0} - \bar{n} = \bar{0}.$$

Eulers teorem

Hva skjer med lille Fermat når t ikke er et primtall?

Virker ikke

Kan vi modifisere argumentet slik at det virker?

La $\bar{a}_1, \bar{a}_2, \bar{a}_3, \ldots, \bar{a}_k$ være de elementene i $\mathbb{Z}/(t)$ som er innbyrdes primisk med t.

$k = \varphi(t)$

Definisjon: Hvis t er et naturlig tall, lar vi $\varphi(t)$ være antall elementer i $\{1,2,3,\ldots,t-1\}$ som er innbyrdes primiske med t. Vi kaller φ Eulers φ-funksjon.

Eksempel: $t=6$: $\{1,\cancel{2},\cancel{3},\cancel{4},5\}$ $\quad \varphi(6)=2$.

Observasjon: Hvis p er et primtall, så er $\varphi(p)=p-1$ $\quad \{1,2,3,\ldots,p-1\}$

Eulers teorem: Anta at $(a,t)=1$. Da er

$$\bar{a}^{\varphi(t)} = \bar{1} \quad \text{i } \mathbb{Z}/(t).$$

Bevis: La $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{\varphi(t)}$ være de restklassene som er innbyrdes primiske med t. Gang alle elementene med $\bar{a}$

$$\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \ldots, \bar{a}\bar{a}_{\varphi(t)}$$

disse er forskjellige (faktoriseringsregelen gjelder siden $(a,t)=1$)

de er innbyrdes primiske med t.

De to listene må derfor inneholde nøyaktig de samme elementene: Ganger dem sammen.

$$\cancel{\bar{a}_1}\cdot\cancel{\bar{a}_2}\cdots\cancel{\bar{a}_{\varphi(t)}} = \bar{a}\cdot\cancel{\bar{a}_1}\cdot\bar{a}\cdot\cancel{\bar{a}_2}\cdots\bar{a}\,\cancel{\bar{a}_{\varphi(t)}}$$

(faktoriseringsregelen gjelder siden $a_1, a_2, \ldots$ er innbyrdes primiske med t)

$$\bar{1} = \bar{a}^{\varphi(t)}$$

Wilsons teorem: Hvis p er et primtall, så er $\overline{\underbrace{(p-1)!}} = -\bar{1}$

produktet av alle elementene i $\mathbb{Z}/(p)$