21/10-2013

MAT1140

Kongruensregning

Fra forrige gang:

Setning: Følgende er ekvivalent for $\bar{a} \in \mathbb{Z}/(b)$:
(i) $(a, b) = 1$
(ii) $\bar{a}$ er ikke en nulldivisor
(iii) Forkortningsregelen gjelder for $\bar{a} \neq \bar{0}$.

Hvis p er et primtall, er $(a, p) = 1$ for alle ikke-null a. Følgelig:

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

Vi skal se på en liten anvendelse.
Observer at $10 \equiv 1 \pmod 3$; dvs $\bar{10} = \bar{1}$ i $\mathbb{Z}/(3)$
Følgelig er

$$\bar{10}^2 = \bar{10} \cdot \bar{10} = \bar{1} \cdot \bar{1} = \bar{1}, \quad \bar{10^3} = \bar{10^2} \cdot \bar{10} = \bar{1} \cdot \bar{1} = \bar{1}$$

osv. Det vil si at $\bar{10^n} = \bar{1}$ for alle n. For ethvert tall med sifre $a_n a_{n-1} \cdots a_1 a_0$ er dermed

$$a_n \cdot 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 = \bar{a}_n + \bar{a}_{n-1} + \cdots + \bar{a}_n \text{ i}$$

dvs tallet er delelig med 3 hvis og bare hvis tverrsummen er det.

Eksempel: Er 74321 delelig med 3? Tverrsummen er $7+4+3+2+1=17$ som ikke er delelig med 3, og følgelig er heller ikke 74321 delelig med 3.

Den samme regelen gjelder for 9 siden $10 \equiv 1 \pmod 9$. Prøver vi med 11 istedenfor, ser vi at $10 \equiv -1 \pmod{11}$, og følgelig er

$$\overline{10}^n = (\overline{-1})^n = \begin{cases} 1 & \text{hvis } n \text{ er like} \\ -1 & \text{hvis } n \text{ er odde} \end{cases}$$

Eksempel: Undersøk om 74321 er delelig med 11. I $\mathbb{Z}/(11)$ er

$$\overline{74321} = \overline{7}\cdot\overline{10}^4 + \overline{4}\cdot\overline{10}^3 + \overline{3}\cdot\overline{10}^2 + \overline{2}\cdot\overline{10} + \overline{1}$$

$$= \overline{7} + \overline{4} - \overline{3} + \overline{2} - \overline{1} = \overline{5} \neq 0$$

så 74321 er ikke delelig med 11.

Vi går tilbake til teorien

Teorem: Ligningen $\overline{a}\,\overline{x} = \overline{b}$ har en løsning i $\mathbb{Z}/(L)$ hvis og bare hvis $(a, L) \mid b$.

Bevis: Anta at $(a, L) \mid b$. Ifølge tidligere teori finnes det da tall x, y i $\mathbb{Z}$ slik at

$$b = ax + yt.$$

I $\mathbb{Z}/(t)$ er dermed

$$\overline{b} = \overline{ax+yt} = \overline{ax} + \overline{yt} = \bar{a}\cdot\bar{x} + \bar{y}\cdot\bar{t} = \bar{a}\bar{x}.$$

$\bar{t} = 0$

Altså anvendt at $\bar{b} = \bar{a}\bar{x}$. Da er $b - ax$ delelig med t, dvs

$$b = ax + yt$$

for en $y \in \mathbb{Z}$. Men dermed er b en lineærkombinasjon av a og t, og følgelig er b delelig med (a,t).

Bemerkning: Beviset ovenfor viser at å løse ligningen $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(t)$, er det samme som å løse ligningen $b = ax + by$ i heltall, og det kan vi gjøre med Euklids algoritme

Eksempel: Løs $\overline{12} = \overline{8}\bar{x}$ i $\mathbb{Z}/(28)$.
Siden $(28,8) = 4$ deler 12, er ligningen løsbar, og ekvivalent med å løse

$$12 = 8x + 28y.$$

Vi bruker Euklids algoritme på 28 og 8:

$28 = 3 \cdot 8 + \textcircled{4}$ — siste ikke-null rest.

$8 = 2 \cdot 4$

Vi får

$$4 = 1 \cdot 28 + (-3) \cdot 8$$

Ganger med 3:

$$12 = 3 \cdot 28 + (-9) \cdot 8$$

I $\mathbb{Z}/(28)$

$$\overline{12} = \overline{(-9)} \cdot \overline{8} = \overline{19} \cdot \overline{8}$$

Altså er $\bar{x} = \overline{19}$.

Anta at $(a,b) = 1$. Da har ligningen $\bar{a}\bar{x} = \bar{b}$ alltid en løsning, og denne løsningen er entydig. Siden $(a,b) = 1$, gjelder nemlig forkortningsregelen slik at hvis

$$\bar{a}\bar{x} = \bar{b} = \bar{a}\bar{y},$$

så er nødvendigvis $\bar{x} = \bar{y}$.

Ligningen $\bar{a}\bar{x} = \bar{1}$ har en løsning hvis og bare hvis $(a,b) = 1$, og denne løsningen er i så fall entydig. Vi kan dermed innføre betegnelsen $\bar{a}^{-1}$ på den entydig løsningen til $\bar{a}\bar{x} = \bar{1}$. Med andre ord er $\bar{a}^{-1}$ den entydig bestemte elementet i $\mathbb{Z}/(b)$ slik at $\bar{a} \cdot \bar{a}^{-1} = \bar{1}$

<u>Setning</u>: Anta at $(a,b) = 1$. Da har ligningen $\bar{a}\bar{x} = \bar{b}$ en entydig løsning i

$\mathbb{Z}/(t)$, nemlig $x = a^{-1}b$.

<u>Bevis</u>: Siden $(a,t) \mid b$, vet vi at ligningen har en løsning $\bar{x}$; dvs

$$\bar{a}\,\bar{x} = \bar{b}$$

Ganger vi fra venstre med $\bar{a}^{-1}$, får vi

$$\bar{a}^{-1}(\bar{a}\,\bar{x}) = \bar{a}^{-1}\bar{b}$$

$$\Downarrow$$

$$(\bar{a}^{-1}\bar{a})\,\bar{x} = \bar{a}^{-1}\bar{b}$$

$$\Downarrow$$

$$\bar{1}\cdot\bar{x} = \bar{a}^{-1}\bar{b}$$

$$\Downarrow$$

$$\bar{x} = \bar{a}^{-1}\bar{b}.$$

Dette viser at enhver løsning må være $\bar{x} = \bar{a}^{-1}\bar{b}$, og følgelig er dette en entydig løsning.

<u>Observasjon</u>: Hvis p er et primtall, er $(a,p) = 1$ for alle ikke-null $\bar{a}$. Følgelig har alle ikke-null elementer $\bar{a}$ en invers, og ligningen $\bar{a}\,\bar{x} = \bar{b}$ har alltid en entydig løsning.

Fermats lille teorem

Hittil har vi bare sett på resultater i $\mathbb{Z}/(k)$ som ligner på resultater i $\mathbb{Z}$ eller $\mathbb{R}$. Nå skal vi se på noen resultater som er helt nye. Det første gjelder bare når $k = p$ er et primtall.

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

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

Bevis: $\mathbb{Z}/(p)$ har $p-1$ ikke-null elementer: $\bar{1}, \bar{2}, \ldots, \overline{p-1}$. Siden $\bar{a} \neq 0$ og forkortningsregelen gjelder, er $\bar{a}\bar{1}, \bar{a}\cdot\bar{2}, \ldots, \bar{a}\,\overline{p-1}$ også $p-1$ forskjellige, ikke-null elementer i $\mathbb{Z}/(p)$ og følgelig er

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

Ganger vi sammen, ser vi at

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

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

Forkortningsregelen gjelder, og dermed er

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

Betingelsen om at $\bar{a} \neq \bar{0}$ kan av og til være litt ubehagelig, og da kan det være enklere å bruke:

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

Bevis: Hvis $\bar{a} = \bar{0}$, er begge sider lik $\bar{0}$. Hvis $\bar{a} \neq 0$, vet vi fra Fermats lille teorem at $\bar{a}^{p-1} = \bar{1}$, og ganger vi med $\bar{a}$ på begge sider, får vi $\bar{a}^p = \bar{a}$.

Eksempel: Vis at dersom n ikke er delelig med 17, så er $8n^{16} + 9$ delelig med 17.
I $\mathbb{Z}/(17)$ har vi

$$\bar{8}\bar{n}^{16} + \bar{9} = \bar{8}\bar{n}^{17-1} + \bar{9} = \bar{8} \cdot \bar{1} + \bar{9} = \overline{17} = \bar{0}.$$