Primtall av typen $4k+3$

Primtallene: 2, $4k+1$, $4k+3$

Husk: Ganger vi sammen tall på formen $4k+1$, så er resultatet også på denne formen.

Teorem: Det finnes uendelig mange primtall på formen $4k+3$.

Bevis: Anta for motsigelse at det bare finnes endelig mange primtall på denne formen: $3, 7, 11, 19, 23, 31, \ldots, P$

Innfører et nytt tall

$$N = 4\cdot\cancel{3}\cdot 7\cdot 11\cdot 19 \cdot \overset{7}{\ldots} \cdot P + 3$$

: 3 går ikke opp, deler 3, men ikke produktet.

: $7 \neq 3$ deler første, men ikke 3

La oss se på primtallene til N:

(i) 2 er ikke en faktor.

(ii) Ingen av primtallene på listen $3, 7, 11, .., P$ er faktorer.

Dette betyr at alle primfaktorene til N er på formen $4k+1$. Siden produktet av tall på formen $4k+1$ selv er på formen $4k+1$, betyr dette at N er på formen $4k+1$, men det er umulig siden N åpenbart er på formen $4k+3$.

Vi ser altså at antagelsen om at det bare finnes endelig mange primtall på formen $4k+3$, leder til en selvmotsigelse. Altså finnes det uendelig mange.

$4n+3$

Bemerkning: En tallfølge på formen $\{\overset{4}{a}n+\overset{3}{b}\}_{n\in\mathbb{Z}}$ kalles aritmetisk.

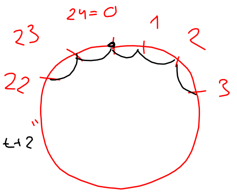
Dersom a, b har en felles faktor $d>1$, så er alle tallene i følgen delelig med d, og dermed inneholder følgen ingen primtall.

Dersom $(a,b)=1$, så kan det vises at $\{an+b\}$ alltid inneholder uendelig mange primtall (Dirichlets teorem)

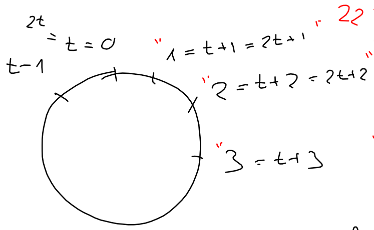
Kongruensregning

Spørsmål: Hvis klokken nå er 22, hva viser den da om 5 timer?

Løs: $22+5 = \underline{27}$ (dvs. 3)



Modulo.



Definisjon: La $t \in \mathbb{N}$. Vi innfører en relasjon $\equiv \pmod t$ ved

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

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

Bevis: Sjekker betingelsene:

(i) Refleksiv: $a \equiv a \pmod t$ fordi $t \mid a-a$ (dvs $t \mid 0$)

(ii) Symmetri: Anta $a \equiv b \pmod t$, vi må vise at $b \equiv a \pmod t$

Vet $a-b = nt$, så $b-a = (-n)t$. Dette betyr at $b \equiv a \pmod t$

(iii) Transitiv: Anta at $a \equiv b \pmod t$ og $b \equiv c \pmod t$. Vi må vise at $a \equiv c \pmod t$. Vet at $a-b = nt$, $b-c = mt$. Legger sammen

$$a-c = (a-b)+(b-c) = nt+mt = (n+m)t$$

Dermed $t \mid a-c$, dvs $\underline{a \equiv c \pmod t}$.

Uttale: $a \equiv b \pmod t$ uttales den gjerne "a er kongruent med b modulo t"

Hvilke elementer er kongruente?

$-2t, -t, 0, t, 2t, 3t, \dots$ kongruent med 0 modulo t.

$\dots, -2t+1, -t+1, 1, t+1, 2t+1, 3t+1, \dots$ — " — 1 — " — t

$\dots, -2t+2, -t+2, 2, t+2, 2t+2, 3t+2$ — 2

$\vdots$

$\dots, -2t-1, -1, t-1, 2t-1, 3t-1, \dots$ — " — t-1 — " — t

$, -t, 0, t, 2t, 3t, \dots$

Samme.

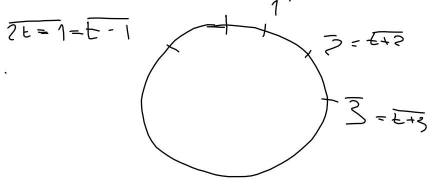
Konklusjon: $\equiv \pmod t$ har t forskjellige ekvivalensklasser, nemlig $\bar 0, \bar 1, \dots, \overline{t-1}$

$$\bar 0 = \{ \dots, -2t, -t, 0, t, 2t, \dots \}$$
$$\bar 1 = \{ \dots, -2t+1, -t+1, 1, t+1, 2t+1, \dots \}$$
$$\bar 2 = \{ -2t+2, -t+2, 2, t+2, 2t+2, \dots \}$$
$$\vdots$$
$$\overline{t-1} = \dots$$

Notasjon: Vi skriver $\mathbb{Z}/(t)$ for ekvivalensklassene til $\equiv \pmod t$. $\bar t = \bar 0$

Har

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



Regning med restklasser

Har lyst til å regne i $\mathbb{Z}/(t)$!

Idé: $[a]+[b]=[a+b]$ Potensielt problem: $a' \equiv a \pmod t$ $b' \equiv b \pmod t$

$[a][b]=[ab]$ så $[a']=[a]$ og $[b']=[b]$

er disse like

$$[a+b] = [a]+[b] = [a']+[b'] = [a'+b']$$

$$[ab] = [a][b] = [a'][b'] = [a'b']$$

er disse like

Setning: Hvis $a \equiv a' \pmod t$ og $b \equiv b' \pmod t$, så

$$a+b \equiv a'+b' \pmod t \quad \text{og} \quad ab \equiv a'b' \pmod t.$$

Bevis. Siden $a \equiv a' \pmod t$, så er $\boxed{a-a'=nt}$ (for en $n\in\mathbb{Z}$)

Siden $b \equiv b' \pmod t$, så er $\boxed{b-b'=mt}$ (— " — $m\in\mathbb{Z}$).

Vi har $(a+b)-(a'+b') = (a-a')+(b-b') = nt + mt = (n+m)t$,

så $a+b \equiv a'+b' \pmod t$

Tilsvarende: $ab - a'b' = (a'+nt)(b'+mt) - a'b' = \cancel{a'b'} + a'mt + b'nt + nmt^2 - \cancel{a'b'}$

$= (a'm + b'n + nmt)t$

så $ab \equiv a'b' \pmod t$

Definisjon: Vi kan nå definere addisjon og multiplikasjon på $\mathbb{Z}/(t)$ ved

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

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

Operasjonene er veldefinerte pga. setningen ovenfor.

Ser på disse operasjonene i $\mathbb{Z}/(6) = \{\bar 0, \bar 1, \bar 2, \bar 3, \bar 4, \bar 5\}$

$+$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$
$\bar 0$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$
$\bar 1$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$	$\bar 0$
$\bar 2$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$	$\bar 0$	$\bar 1$
$\bar 3$	$\bar 3$	$\bar 4$	$\bar 5$	$\bar 0$	$\bar 1$	$\bar 2$
$\bar 4$	$\bar 4$	$\bar 5$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$
$\bar 5$	$\bar 5$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$

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

$20 = 18+2 = 3\cdot 6+2$

$25 = 24+1 = 4\cdot 6+1$

$\underbrace{\bar 2 \cdot \bar 3}_{\text{null divisorer.}} = \bar 0$

$\cancel{\bar 4}\cdot \bar 1 = \cancel{\bar 4}\cdot \bar 4 \overset{?}{\Rightarrow} \bar 1 = \bar 4$

forkorte ?

Det snille først:

Teorem: I $\mathbb{Z}/(t)$ gjelder:

(i) $\bar a + \bar b = \bar b + \bar a$, $\bar a \cdot \bar b = \bar b\, \bar a$ (kommutative lover)

(ii) $\bar a + (\bar b + \bar c) = (\bar a + \bar b) + \bar c$, $\bar a(\bar b\, \bar c) = (\bar a\, \bar b)\bar c$ (assosiative lover)

(iii) $\bar a(\bar b + \bar c) = \bar a\bar b + \bar a\bar c$ distributive lov.

(iv) $\bar a + \bar 0 = \bar a$ og $\bar a \cdot \bar 1 = \bar a$

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

$\mathbb{Z}/(t)$ er en kommutativ ring.

Bevis for (iii): $\bar a(\bar b + \bar c) = \bar a \cdot \overline{b+c} = \overline{a(b+c)}$

$\bar a\bar b + \bar a\bar c = \overline{ab} + \overline{ac} = \overline{\underbrace{ab+ac}_{\text{tall}}} = \overline{a(b+c)}$

Setning: Dersom $\bar a + \bar b = \bar a + \bar c$, så er $\bar b = \bar c$ (forkortningsregelen for addisjon)

Bevis: Adderer $\overline{-a}$ på begge sider:

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

$\Downarrow$

Ass. lov. $\underbrace{(\overline{-a} + \bar a)}_{0} + \bar b = \underbrace{(\overline{-a} + \bar a)}_{0} + \bar c$

$\Downarrow$

$\bar 0 + \bar b = \bar 0 + \bar c$

$\Downarrow$

$\bar b = \bar c$

Definisjonen: Et element $\bar a$ i $\mathbb{Z}/(t)$ kalles en <u>nulldivisor</u> dersom $\bar a \neq \bar 0$ og det finnes en $\bar b \neq \bar 0$ slik at $\bar a\, \bar b = \bar 0$

Vi sier at forkortningsregelen gjelder for $\bar a$ i $\mathbb{Z}/(t)$ dersom

$$\bar a\, \bar b = \bar a\, \bar c \Rightarrow \bar b = \bar c \quad \text{for alle } \bar b, \bar c \in \mathbb{Z}/(t)$$

Eksempel ovenfor: I $\mathbb{Z}/(t)$ er $\bar 2$ og $\bar 3$ nulldivisorer og forkortningsregelen gjelder ikke for 4.

Resultat: $(a,t)=1 \iff \bar a$ er ikke en nulldivisor $\iff$ forkortningsregelen gjelder for $\bar a$.