Mer tallteori

Vet: Ligningen $ax+by=c$ har en løsning $x\in\mathbb{Z}, y\in\mathbb{Z}$ hvis og bare hvis $(a,b)\mid c$

Kan finne løsning via Euklids algoritme

Setning: Hvis $(a,b)=1$ og $a\mid bc$, så $a\mid c$

Teorem: Anta at x_0, y_0 er en løsning av den diofantiske ligningen $ax+by=c$. Hvis $d=(a,b)$, så er alle løsninger av ligningen gitt ved

$$x_k = x_0 + k\frac{b}{d}, \quad y_k = y_0 - k\frac{a}{d} \quad \text{der } k\in\mathbb{Z}.$$

Bevis: Viser først at x_k, y_k er en løsning:

$$ax_k + by_k = a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = \underbrace{ax_0+by_0}_{c} + \underbrace{k\frac{ab}{d} - k\frac{ab}{d}}_{0} = c$$

Så viser vi at alle løsninger er på formen x_k, y_k. Anta at x, y er en løsning og la $e = x - x_0$, $f = y - y_0$. Dermed

$$c = ax+by = a(x_0+e) + b(y_0+f) = \underbrace{ax_0+by_0}_{c} + ae+bf = c+ae+bf$$

dvs $ae+bf=0$ eller

$$ae=-bf$$

Dette gir

$$\frac{a}{d}\cdot \cancel{d}\cdot e = -\frac{b}{d}\cdot\cancel{d} f$$

så $\boxed{\frac{a}{d}\cdot e = -\frac{b}{d}\cdot f}$ dvs $\frac{b}{d} \mid \frac{a}{d}\cdot e$ der $\left(\frac{b}{d}, \frac{a}{d}\right)=1$

Ifølge setningen avenfor er dermed $\frac{b}{d}\mid e$, dvs $\boxed{e = k\frac{b}{d}}$ der $k\in\mathbb{Z}$

Dette gir

$$\frac{a}{d}\cdot k\frac{b}{\cancel{d}} = -\frac{b}{\cancel{d}}\cdot f \Rightarrow \boxed{f = -k\frac{a}{d}}$$

Altså

$$\left.\begin{aligned} x &= x_0 + e = x_0 + k\frac{b}{d} = x_k \\ y &= y_0 + f = y_0 - k\frac{a}{d} = y_k \end{aligned}\right\}$$

Konklusjon: alle løsninger er på formen $x_k = x_0 + k\frac{b}{d}, y_k = y_0 - k\frac{a}{d}$, $k\in\mathbb{Z}$.

Eksempel: Finn alle heltallige løsninger av

$$\underset{a}{74}x + \underset{b}{26}y = \underset{c}{6}$$

Plan: 1. Bruk Euklids algoritme til å finne én løsning.

2. Bruk teoremet ovenfor til å finne resten.

$$74 = 2 \cdot 26 + 22$$
$$26 = 1 \cdot 22 + 4$$
$$22 = 5 \cdot 4 + 2$$
$$4 = 2 \cdot 2$$

største felles divisor i a, b. Siden 2|6, har ligningen løsninger.

$$74 : 26 = 2$$
$$\underline{52}$$
$$22$$
$$74 = 2 \cdot 26 + 22$$

~~Skriver 2 som en~~ lin. komb. av 74 og 26:

$$2 = 22 - 5 \cdot 4 = 22 - 5 \cdot (26 - 1 \cdot 22) = 6 \cdot 22 - 5 \cdot 26 = 6(74 - 2 \cdot 26) - 5 \cdot 26$$
$$= 6 \cdot 74 - 17 \cdot 26 \quad \text{dvs} \quad 6 \cdot 74 - 17 \cdot 26 = 2$$

Ganger med 3: $18 \cdot 74 - 51 \cdot 26 = 6$ Løsning: $x_0 = 18$, $y_0 = -51$

Resten av løsningene: $x_k = x_0 + \frac{b}{d}k$, $y_k = y_0 - \frac{a}{d}k$ der $d = (a, b)$

$a = 74$, $b = 26$, $d = 2$, $\frac{a}{d} = 37$, $\frac{b}{d} = 13$

Generelle løsninger:

$$x_k = 18 + 13k, \quad y_k = -51 - 37k, \quad k \in \mathbb{Z}$$

Primtall

Definisjon: Et primtall p er et naturlig tall $p \ge 2$ som ikke er delelig på andre naturlige tall enn 1 og seg selv.

De første primtallene: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
eneste partall.

Setning: Hvis p er et primtall og $p|ab$, så vil $p|a$ eller $p|b$.

Bevis: Det er nok å vise at hvis $p \nmid a$, så $p|b$. Men hvis $p \nmid a$, så $(p,a)=1$, men dermed vil $p|ab$ medføre at $p|b$.

Eksempel (faktorisering): Faktoriser 546

$$\begin{array}{r|l} 546 & 2 \\ 273 & 3 \\ 91 & 7 \\ 13 & \end{array}$$

$91 : 7 = 13$
7
21
21
0

$546 = 2 \cdot 3 \cdot 7 \cdot 13$ (produkt av primtall)

Spørsmål 1: Alltid mulig? } JA
— " — Alltid samme produkt? } JA

Aritmetikkens fundamentalteorem: Ethvert naturlig tall $a > 1$ kan skrives som et produkt av primtall

$$a = p_1 p_2 p_3 \cdots p_n \quad \text{der } n \ge 1$$

Dette produktet er entydig i følgende forstand: Dersom

$$a = q_1 q_2 q_3 \cdots q_m$$

er en annen primtallsfaktorisering, så er $n = m$ og $p_1, \ldots, p_n$ og $q_1, q_2, \ldots q_m$ er akkurat de samme tallene, bortsett kanskje fra rekkefølgen.

Bevis: Anta for motsigelse at det finnes tall > 1 som ikke kan skrives som produkt av primtall, og la a være det minste. Da kan a ikke være et primtall q, for da ville $a = p$ være en slik faktorisering. Følgelig kan a skrives som et produkt $a = bc$ der $b, c < a$. Dermed kan b og c skrives som produkter av primtall $b = p_1 p_2 \cdots p_r$, $c = q_1 q_2 \cdots q_s$. Men dette gir

$$a = bc = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

som viser at a er et produkt av primtall.

For å vise entydigheten antar vi at den ikke holder og $a > 1$ er det minste moteksemplet, dvs

$$a = p_1 p_2 \cdots p_n \qquad a = q_1 q_2 \cdots q_m$$

Dermed er

$$p_1 (p_2 \cdots p_n) = q_1 q_2 \cdots q_m$$

som viser at $p_1 | q_1 q_2 \cdots q_m$. Siden p_1 er et primtall, betyr dette at det finnes en q_i slik at $p_1 | q_i$. Siden p_1 og q_i, betyr dette at $p_1 = q_i$. Dermed

$$\cancel{p_1} p_2 \cdots p_n = q_1 q_2 \cdots \cancel{q_i} \cdots q_m$$

$$p_2 \cdots p_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m < a$$

Som viser at et tall mindre enn a har to forskjellige primtallsfaktoriseringer, og det er umulig siden a var det minste tallet med to forskjellige faktoriseringer. QED.

Teorem: $\sqrt{2}$ er et irrasjonalt tall. ($\sqrt{2}$ kan ikke skrives på formen $\sqrt{2} = \frac{a}{b}$, $a,b \in \mathbb{Z}$)

Bevis. Anta for motsigelse at $\sqrt{2}$ er rasjonal, dvs at $\sqrt{2} = \frac{a}{b}$ der $a,b \in \mathbb{Z}$

La $a = p_1 p_2 \cdots p_n$ være primtallsfaktoriseringen til a

og $b = q_1 q_2 \cdots q_m$ — " — til b

$$\sqrt{2} = \frac{p_1 p_2 \cdots p_n}{q_1 \cdots q_m} \Rightarrow 2 = \frac{p_1^2 p_2^2 \cdots p_n^2}{q_1^2 q_2^2 \cdots q_m^2} \Rightarrow \underbrace{2 \cdot q_1^2 q_2^2 \cdots q_m^2}_{\text{odde antall faktorer som er 2}} = \underbrace{p_1^2 p_2^2 \cdots p_n^2}_{\text{like antall faktorer som er 2}}$$

Disse primtallsfaktoriseringene må være like ved entydighet, med det er umulig siden den ene har et odde antall 2'er og den andre et like antall.

Teorem (Euklid): Det finnes uendelig mange primtall.

Bevis: Anta for motsigelse at det bare finnes endelig mange

$3, 5, 7, 11, \ldots, P$

La

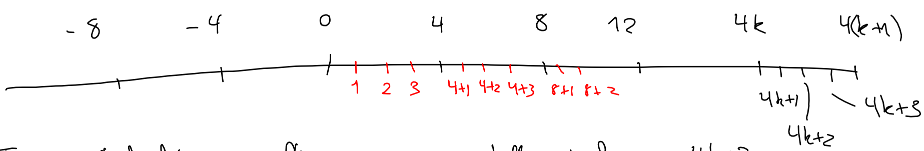
$$N = 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot P + 1$$

Siden alle tall er delelig på et primtall, må det være et primtall q som deler N. Dermed er

$$\underbrace{\frac{N}{q}}_{\substack{\text{heltall siden} \\ N \text{ er delelig på } q}} = \frac{(3 \cdot 5 \cdot 7 \cdot 11 \cdots q \cdots P) + 1}{q} = \underbrace{\underbrace{3 \cdot 5 \cdot 7 \cdots \cancel{q} \cdots P}_{\text{heltall}} + \underbrace{\frac{1}{q}}_{\text{ikke heltall}}}_{\text{ikke heltall}}$$

Dette er en selvmotsigelse, så antagelsen om at det bare finnes endelig mange primtall, må være gal.

Tre varianter av primtall:
- 2 – eneste primtall som er partall
- $4k+1$, $k \in \mathbb{Z}$, kongruente med 1 modulo 4
- $4k+3$, $k \in \mathbb{Z}$ — " — 3 — " —



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

Lemma: Hvis vi ganger sammen tall på formen $4k+1$, får vi nye tall på formen $4k+1$.

Bevis: $a = 4m+1$, $b = 4n+1$

$$ab = (4m+1)(4n+1) = \underbrace{16mn + 4m + 4n + 1} = 4\underbrace{(4mn+m+n)}_{\in \mathbb{Z}} + 1$$