14/10 - 2013

MAT1140

Primtall

Definisjon: Et **primtall** p er et naturlig tall større enn 1 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.

På skolen har vi lært å faktorisere tall i produkter av primtall:

204	2
102	2
51	3
17	

$\Rightarrow 204 = 2 \cdot 2 \cdot 3 \cdot 17$

Målet vårt er å bevise at ethvert naturlig tall kan faktoriseres som et produkt av primtall på en entydig måte.

Vi trenger et hjelperesultat:

Setning: Anta at et primtall p deler produktet ab av to naturlige tall a og b. Da deler p enten a eller b.

Bevis: Anta at p ikke deler a; det holder

å vise at p da deler b. Siden p er et primtall som ikke deler a, er a og p innbyrdes primiske og har største felles divisor 1. Dermed finnes det hele tall s og t slik at

$$1 = sa + tp$$

Ganger vi med b, får vi

$$b = sab + tbp$$

Siden ab er delelig med p, finnes det $m \in \mathbb{N}$ slik at $ab = mp$. Dermed a

$$b = smp + tbp = (sm + tb)p$$

som viser at b er delelig med p.

Vi er nå klar for hovedresultatet

Aritmetikkens fundamentalteorem: Ethvert helt tall $a > 1$ kan skrives som et produkt

$$a = p_1 p_2 \dots p_n .$$

Faktoriseringen er entydig i den forstand at hvis

$$a = q_1 q_2 \dots q_m$$

der $q_1, q_2, \ldots, q_m$ er primtall, så er $n = m$ og faktorene $q_1, q_2, \ldots, q_m$ er de samme som $p_1, p_2, \ldots, p_n$ bortsett fra at rekkefølgen kan være en annen.

Bemerkning: Vi godtar faktoriseringer med bare én faktor slik at faktoriseringen av et primtall p er

$$p = p_1$$

der $p_1 = p$.

Bevis: Vi viser først at det alltid finnes en faktorisering. Anta ikke, da må det finnes et minste tall c som ikke kan faktoriseres. Siden alle primtall har en triviell faktorisering, må c være sammensatt, dvs

$$c = ab.$$

Siden $a, b < c$, kan de faktoriseres

$$a = p_1 p_2 \cdots p_n$$

$$b = q_1 q_2 \cdots q_m$$

Men da har c faktoriseringen

$$c = ab = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m$$

selvmotsigelse.

Vi ser så på entydigheten. Dersom faktoriseringen ikke er entydig, må det finnes et minste tall a som kan faktoriseres på to måter

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

Siden p_1 går opp i produktet $q_1 q_2 \cdots q_m$, må det gå opp i ett av faktorene $q_1, q_2, \ldots, q_m$ ved resultatet ovenfor, la oss si q_j. Siden q_j er et primtall, må $q_j = p_1$. Dermed kan vi forkorte og få

$$p_2 \cdots p_n = q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$$

som gir to forskjellige faktoriseringer av et tall som er mindre enn a, selvmotsigelse.

La oss se på noen anvendelser

Teorem: Anta at $n \in \mathbb{N}$ ikke er et kvadrattall. Da er $\sqrt{n}$ irrasjonal.

Bevis: La

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

være primtallsfaktoriseringen der vi har samlet alle primtallsfaktorene i potenser. Siden n ikke

er et kvadrattall, er minst én k_i et oddetall, la oss si p_j.

Anta for motsigelse at $\sqrt{n}$ er rasjonal, dvs

$$\sqrt{n} = \frac{a}{b} \Rightarrow n = \frac{a^2}{b^2}$$

Dermed er

$$nb^2 = a^2$$

Primtallsfaktoriseren vi, ser vi at p_j forekommer et odde antall ganger på venstre side og et like antall på høyre side. Dette er umulig siden faktoriseringen er entydig

---

Bemerkning: Legg merke til at det er entydigheten i aritmetikkens fundamentalteorem som spiller hovedrollen i beviset ovenfor. Generelt er den minst like viktig som eksistensen.

Teorem (Euklid). Det finnes uendelig mange primtall.

Bevis: Anta for motsigelse at det bare finnes endelig mange primtall $p_1, p_2, \ldots, p_k$ og danner tallet

$$N = p_1 p_2 \cdots p_k + 1.$$

Ved aritmetikkens fundamentalteorem må N være delelig med minst ett primtall p_i. Men det er umulig siden

$$\frac{N}{p_i} = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k + \frac{1}{p_i}$$

kan ikke være et heltall.

Alle primtall bortsett fra 2 er odde, og når vi deler dem på 4, kan de dermed rest 1 eller 3, der de er enten på formen

$$4n+1$$

eller

$$4n+3.$$

Det viser seg at det er uendelig mange av begge typer, men foreløpig nøyes vi oss med å vise:

Teorem: Det finnes uendelig mange primtall på formen $4n+3$, $n \in \mathbb{N}$.

Bevis: Anta at det finnes bare et endelig antall primtall på denne formen: $3, p_2, \ldots, p_n$ og dann

$$N = 4p_2 p_3 \cdots p_n + 3$$

Minst én av primfaktorene til N må være av typen $4n+3$ (hvis alle var av typen $4n+1$, ville også N være på denne formen), la oss si det er p_i. Men deriverer vi

$$\frac{N}{p_i} = 4p_1 \cdots p_{i-1} p_{i+1} \cdots p_k + \frac{3}{p_i},$$

selvmotsigelse.

Dette er et spesialtilfelle av et berømt resultat.

Dirichlets teorem: Anta at a, b er innbyrdes primiske. Da inneholder den aritmetiske følgen $\{an+b\}_{n \in \mathbb{N}_0}$ uendelig mange primtall.

Hvor mange primtall finnes det? Anta at $\pi(x)$ er antall primtall mindre enn eller lik x. Da er

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

Andelen primtall mindre enn x er altså omtrent $\frac{1}{\log x}$ når x blir stor. Dette kalles primtallsteoremet.