3.1/3.2/3.3 Primtall

Def: Et tall $p \geq 2$ er et <u>primtall</u> dersom 1 og p er de eneste positive divisorene.

Merk: (1) Tallet 1 er ikke et primtall

(2) Hvis p er prim og $p \nmid a$, må $\gcd(a,p)=1$ (vis)

(3) Konsekvens av (2): hvis p er prim og $p \mid ab$, må $p \mid a$ eller $p \mid b$ (vis vha. Euklids lemma).

<u>Teorem 3.2</u> (Aritmetikkens fundamentalteorem)
Ethvert tall $n \geq 2$ er et produkt av primtall på en unik måte.

Bevis: Viser først at alle $n \geq 2$ er et prod av primtall. For $n=2$ stemmer det, siden 2 er prim. La nå $n>2$, og anta det stemmer $\forall k$ med $2 \leq k \leq n-1$. Hvis n er et primtall, så er vi i mål. Hvis ikke, finnes $1 < a,b < n$ med $n=ab$. Ved induksjon er både a og b produkter av primtall, så da må også $n=ab$ være det.

Så unikhet. Anta $n = p_1 \cdots p_t$ og $n = q_1 \cdots q_s$ hvor p_i og q_i er primtall. Siden

$$p_1 \cdots p_t = q_1 \cdots q_s \quad (*)$$

vil da $p_1 \mid q_1 \cdots q_s$, som gir (fra (3) over) at $p_1 \mid q_i$ for en i. Da må $p_1 = q_i$. Kan da fjerne p_1 og q_i fra $(*)$, og argumentere på samme måte. Konklusjon: $t=s$, og $\{p_1, \ldots, p_t\} = \{q_1, \ldots, q_t\}$. □

<u>Korollar</u> Ethvert tall $n \geq 2$ kan skrives på en unik måte som

$$n = p_1^{a_1} \cdots p_t^{a_t}$$

hvor

(1) $t \geq 1$

(2) $p_1, \ldots, p_t$ er ulike primtall

(3) $a_1, \ldots, a_t \geq 1$

Eksempler: (1) $32 = 2^5$, $17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$, $35 = 5 \cdot 7$

(2) RSA-kryptografi baserer sin sikkerhet på at faktorisering er tidkrevende.

(3) For $x \in \mathbb{R}$, la

$$\pi(x) = \text{antall primtall} \leq x$$

Så $\pi(10) = 4$, $\pi(17{,}3) = 7$. Berømt resultat innen analytisk tallteori:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1 \qquad \text{(Primtallsteoremet)}$$

Betyr at $\pi(x) \approx x/\ln x$ når x blir stor.

Teorem 3.4 (Euklid)

Det finnes uendelig mange primtall.

Bevis: Anta det bare finnes endelig mange primtall $p_1, \ldots, p_t$, og se på tallet

$$n = p_1 p_2 \cdots p_t + 1$$

Siden $n \geq 2$ er det delelig på minst ett primtall (Aritmetikkens fund. teorem), altså må $p_i \mid n$ for en $i \in \{1, \ldots, t\}$. Men ingen av primtallene $p_1, \ldots, p_t$ kan dele n, for vi får en rest på 1. □

Naturlige spørsmål:

(1) Gitt n, hvordan avgjøre på en effektiv måte om n er et primtall eller sammensatt?

(2) Gitt n, hvordan finne alle primtallene $p \leq n$?

(3) Hvordan fordeler primtallene seg blant heltallene? Er det noe mønster? Dette er beslektet med Riemannhypotesen.

Merk: På tallinjen finnes det vilkårlig lange hull hvor det ikke er primtall. La $n \geq 2$, og se på de $n-1$ etterfølgende tallene

$$n! + 2, \; n! + 3, \; \ldots, \; n! + n$$

Ingen av disse er primtall: $2 \mid (n!+2)$, $3 \mid (n!+3)$ osv.

Vi ser på to metoder for spørsmål (1).

Metode 1: (Ueffektiv)

For hver a med $1<a<n$, sjekk om $a \mid n$. Hvis ingen slik a finnes må n være prim.

Metode 2: (Mer effektiv)

For hvert primtall $p \leq \sqrt{n}$, sjekk om $p \mid n$. Hvis ingen slik p finnes må n være prim.

Hvorfor? Hvis n ikke er prim finnes $1<a,b<n$ med $n=ab$. Da må enten $a \leq \sqrt{n}$ eller $b \leq \sqrt{n}$ (hvorfor?). Både a og b har minst én primtallsfaktor, så det må $\exists$ et primtall p med $p \leq \sqrt{n}$ og $p \mid n$.

Eksempel: Se på $n=911$. Har $\sqrt{911} \approx 30{,}2$, så må sjekke om primtallene $2,3,5,7,11,13,17,19,23,29$ deler 911. Det gjør de ikke, så 911 er et primtall.

Selvstudium: Les om Eratosthenes' sil, som er en metode for spørsmål (2).