6.1 Talltheoretiske funksjoner

Def: (1) En funksjon $f: \mathbb{N} \to \mathbb{R}$ (evt $f: \mathbb{N} \to \mathbb{C}$) kalles en talltheoretisk funksjon.

(2) To slike:

$\tau(n)$ = antall positive divisorer av n (inkl. 1 og n)

$\sigma(n)$ = summen av divisorene

Eksempler: (1) $\tau(6) = 4$ siden 6 har 4 pos. divisorer: 1, 2, 3, 6

$\sigma(6) = 1+2+3+6 = 12$

(2) $\tau(16) = 5$ siden 16 har 5 pos. divisorer: 1, 2, 4, 8, 16

$\sigma(16) = 1+2+4+8+16 = 31$

(3) La p være et primtall.

$\tau(p) = 2$ siden p har 2 pos. div: 1 og p

$\sigma(p) = 1+p$

(4) Et tall n kalles perfekt dersom n = summen av sine divisorer (unntatt n), dvs $n = \sigma(n) - n$, dvs $\sigma(n) = 2n$.

Så over at $\sigma(6) = 2 \cdot 6$, så 6 er perfekt. Neste er $n = 28$, så $n = 496$, $n = 8128$, $n = 33550336$. Det er uvisst om det finnes ∞ mange av dem.

Teorem 6.1 La $n \geq 1$ med primtallsfaktorisering $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ $(p_i \neq p_j$ for $i \neq j)$.

Da er de pos. divisorene alle tallene

$$p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

hvor $0 \leq a_i \leq k_i$.

Bevis: Aritmetikkens fundamentalteorem. □

Eksempel: Siden $200 = 2^3 \cdot 5^2$ er de pos. div gitt ved $2^a \cdot 5^b$ hvor $0 \leq a \leq 3$ og $0 \leq b \leq 2$:

$2^0 \cdot 5^0, 2^0 \cdot 5^1, 2^0 \cdot 5^2, 2^1 \cdot 5^0, 2^1 \cdot 5^1, 2^1 \cdot 5^2, 2^2 \cdot 5^0, 2^2 \cdot 5^1, 2^2 \cdot 5^2, 2^3 \cdot 5^0, 2^3 \cdot 5^1, 2^3 \cdot 5^2$

Teorem 6.2 (Formel for τ og σ)

For $n \geq 1$ m/primtallsfakt. $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ $(p_i \neq p_j$ for $i \neq j)$ er

$$\tau(n) = (k_1+1)(k_2+1)\cdots(k_t+1)$$

$$\sigma(n) = (1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})\cdots(1+p_t+p_t^2+\cdots+p_t^{k_t})$$

$$= \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_t^{k_t+1}-1}{p_t-1}$$

Bevis: Fra Teorem 6.1 er divisorene gitt ved

$$\{p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t} \mid 0\le a_1\le k_1, 0\le a_2\le k_2, \dots, 0\le a_t\le k_t\}$$

Det er k_1+1 valg for a_1, k_2+1 valg for a_2 osv, tilsammen

$$(k_1+1)(k_2+1)\cdots(k_t+1)$$

valg, så dette er $\tau(n)$. For $\sigma(n)$, merk at hver divisor opptrer nøyaktig én gang som summand når vi ekspanderer uttrykket

$$(1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})\cdots(1+p_t+p_t^2+\cdots+p_t^{k_t})$$

Så dette er $\sigma(n)$. Generelt er $1+x+x^2+\cdots+x^k = \frac{x^{k+1}-1}{x-1}$ for alle $x\in\mathbb{R}$ med $x\neq 1$. □

Eksempel: For $n=200=2^3\cdot 5^2$ får vi

$$\tau(200) = (3+1)(2+1) = 12$$

$$\sigma(200) = \frac{2^{3+1}-1}{2-1}\cdot\frac{5^{2+1}-1}{5-1} = 15\cdot 31 = 465$$

For $n=2250=2\cdot 3^2\cdot 5^3$ får vi

$$\tau(2250) = (1+1)(2+1)(3+1) = 24$$

$$\sigma(2250) = \frac{2^2-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^4-1}{5-1} = 3\cdot 13\cdot 156 = 6084$$

Def: En tallteoretisk funksjon f er <u>multiplikativ</u> dersom $f(mn)=f(m)f(n)$ når $\gcd(m,n)=1$.

<u>Teorem 6.3</u> τ og σ er multiplikative

Bevis: La $m,n>1$ med $\gcd(m,n)=1$. Hvis $m=1$ får vi

$$\tau(mn)=\tau(1\cdot n)=\tau(n)=1\cdot\tau(n)=\tau(1)\cdot\tau(n)=\tau(m)\cdot\tau(n)$$

$$\sigma(mn)=\sigma(1\cdot n)=\sigma(n)=1\cdot\sigma(n)=\sigma(1)\cdot\sigma(n)=\sigma(m)\sigma(n)$$

Så vi kan anta $m,n>2$. Primtallsfaktorisér:

$$m = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$$

$$n = q_1^{l_1}q_2^{l_2}\cdots q_s^{l_s}$$

Siden $\gcd(m,n)=1$ er $q_i\neq p_j$ $\forall\, i,j$, så mn har faktorisering

$$mn = p_1^{k_1}\cdots p_t^{k_t}q_1^{l_1}\cdots q_s^{l_s}$$

Får da

$$\tau(mn) = (k_1+1)\cdots(k_t+1)(l_1+1)\cdots(l_s+1) = \tau(m)\tau(n)$$

$$\sigma(mn) = \frac{p_1^{k_1+1}-1}{p_1-1}\cdots\frac{p_t^{k_t+1}-1}{p_t-1}\cdot\frac{q_1^{l_1+1}-1}{q_1-1}\cdots\frac{q_s^{l_s+1}-1}{q_s-1} = \sigma(m)\sigma(n)$$ □

Eksempler: (1) $\tau(2\cdot 2) = \tau(4) = 3$ mens $\tau(2)\cdot\tau(2) = 2\cdot 2 = 4$, så $\tau(2\cdot 2) \neq \tau(2)\cdot\tau(2)$

$\sigma(2\cdot 2) = \sigma(4) = 1+2+4 = 7$ mens $\sigma(2)\cdot\sigma(2) = (1+2)(1+2) = 9$ så $\sigma(2\cdot 2) \neq \sigma(2)\cdot\sigma(2)$

(2) Siden $\gcd(6,5) = 1$ er

$$\tau(30) = \tau(6\cdot 5) = \tau(6)\cdot\tau(5) = 4\cdot 2 = 8$$

$$\sigma(30) = \sigma(6\cdot 5) = \sigma(6)\,\sigma(5) = (1+2+3+6)(1+5) = 72$$

(3) Midtsem H2017, oppg 5.

La $n>1$ være odde. Vis at $\tau(n) \equiv \sigma(n) \pmod 2$.

For $n=1$ holder det siden $\tau(1) = 1 = \sigma(1)$. Anta $n>1$ og se på primtallsfaktoriseringen:

$$n = p_1^{k_1} \cdots p_t^{k_t}$$

Siden n er odde er p_i odde $\forall i$, så $p_i \equiv 1 \pmod 2$ $\forall i$. Får da

$$\begin{aligned}
\sigma(n) &\equiv (1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})\cdots(1+p_t+p_t^2+\cdots+p_t^{k_t}) \\
&\equiv (1+1+\cdots+1)(1+1+\cdots+1)\cdots(1+1+\cdots+1) \\
&\equiv (k_1+1)(k_2+1)\cdots(k_t+1) \\
&\equiv \tau(n) \pmod 2
\end{aligned}$$

Def: Eulers ϕ-funksjon:

$\phi(n)$ = antall $a \in \{1,2,\ldots,n\}$ med $\gcd(a,n) = 1$

Sentral i Kap 7 og RSA-krypto!