7.2 Eulers phi-funksjon

Fra sist: (1) En funksjon $f: \mathbb{N} \to \mathbb{R}$ kalles tallteoretisk

(2) To slike:

$\tau(n)$ = antall pos. div. av n (inkl 1 og n selv)

$\sigma(n)$ = summen av divisorene

(3) For $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$:

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

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

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

Def: Eulers ϕ-funksjon:

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

Eksempler: (1) For å finne $\phi(10)$, se på tallene $\{1,2,3,\ldots,10\}$. Blant disse er de fire tallene 1,3,7,9 rel. primisk med 10, mens de andre ikke er det. Så $\phi(10)=4$

(2)

$\phi(1)=1$ ⇝ 1 er rel. pr. med 1

$\phi(2)=1$ ⇝ 1 er rel. pr. med 2

$\phi(3)=2$ ⇝ 1,2 er rel. pr. med 3

$\phi(4)=2$ ⇝ 1,3 er rel. pr. med 4

$\phi(5)=4$ ⇝ 1,2,3,4 er rel. pr. med 5

$\phi(6)=2$ ⇝ 1,5 er rel. pr. med 6

(3) For p primtall er $\phi(p)=p-1$, siden tallene i mengden $\{1,2,\ldots,p\}$ rel. pr. med p er $1,2,\ldots,(p-1)$. Vis for $n \geq 2$:

$$\phi(n) = n-1 \iff n \text{ primtall}$$

Teorem 7.2 ϕ er multiplikativ: $\gcd(m,n)=1 \Rightarrow \phi(mn)=\phi(m)\phi(n)$

Bevis: Se på følgende mengder:

$$S_m = \{a \mid 1 \leq a \leq m \text{ og } \gcd(a,m)=1\}$$

$$S_n = \{b \mid 1 \leq b \leq n \text{ og } \gcd(b,n)=1\}$$

$$S_{mn} = \{c \mid 1 \leq c \leq mn \text{ og } \gcd(c,mn)=1\}.$$

Da er $\phi(m)=|S_m|$, $\phi(n)=|S_n|$ og $\phi(S_{mn})=|S_{mn}|$.

La $(a,b) \in S_m \times S_n$, og se på systemet

$$x \equiv a \pmod m$$
$$x \equiv b \pmod n.$$

Det kinesiske restteorem gir en unik c med $1 \le c \le mn$ som passer inn. Da må $\gcd(c, mn) = 1$ (sjekk dette), så $c \in S_{mn}$. Vi lager nå to avbildninger:

$$S_m \times S_n \underset{g}{\overset{f}{\rightleftarrows}} S_{mn}$$

For $(a,b) \in S_m \times S_n$ lar vi $f((a,b)) = c$ som ovv, mens for $c' \in S_{mn}$ lar vi $g(c') = (a', b')$, hvor $1 \le a' \le m$, $1 \le b' \le n$ og

$$c' \equiv a' \pmod m$$
$$c' \equiv b' \pmod n$$

Sjekk: $a' \in S_m$, $b' \in S_n$, så $(a', b') \in S_m \times S_n$. Sjekk også at $g \circ f = id$ og $f \circ g = id$, så f og g er inverse bijeksjoner. Derfor:

$$\phi(mn) = |S_{mn}| = |S_m \times S_n| = |S_m| \cdot |S_n| = \phi(m) \cdot \phi(n) \qquad \square$$

Teorem 7.1 For p primtall er $\phi(p^k) = p^k - p^{k-1}$

Bevis: Tallene $a \in \{1, 2, \dots, p^k\}$ med $\gcd(a, p^k) > 1$ er

$$p, 2p, 3p, \dots, p^{k-1} \cdot p$$

Det er p^{k-1} av disse, så $\phi(p^k) = p^k - p^{k-1}$ $\square$

Eksempel: $\phi(25) = \phi(5^2) = 5^2 - 5 = 20$. Blant tallene i mengden

$$\{1, 2, 3, \dots, 25\}$$

er disse ikke rel. pr. med 25: $5, 2 \cdot 5, 3 \cdot 5, 4 \cdot 5, 5 \cdot 5$. De resterende 20 tallene er rel. pr. med 25.

Teorem 7.3 La $n \ge 2$ med primtallstakt.

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

Da er

$$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_t^{k_t} - p_t^{k_t - 1})$$
$$= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_t)$$

Bevis: Siden ϕ er mult. fra Teorem 7.2, gir Teorem 7.1 at

$$\phi(n) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_t^{k_t})$$
$$= (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_2^{k_t} - p_2^{k_t - 1})$$
$$= p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_t) \qquad \square$$

Eksempler: (1) $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot (1-1/2)(1-1/5) = 40$

(2) Hvis $n = p_1 p_2 \cdots p_t$ hvor $p_1, \ldots, p_t$ er ulike primtall (dvs n kvadratfritt):

$$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_t - 1)$$

(3) Spesialtilfelle av (2): hvis $n = pq$ hvor $p \neq q$ er primtall, er $\phi(n) = (p-1)(q-1)$. Blir viktig når vi kommer til RSA-krypto.

Vi trenger senere i kurset følgende enkeltresultat fra Seksjon 7.4:

Teorem 7.6 (Gauss) For $n \geq 1$ er

$$\sum_{d \mid n} \phi(d) = n$$

Her betyr $\sum_{d \mid n}$ at summen går over alle de positive divisorene til n.

Eksempler: (1) For $n = 4$ har vi divisorene $1, 2, 4$. Da får vi

$$\sum_{d \mid 4} \phi(d) = \phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2 = 4$$

(2) For $n = 10$ har vi divisorene $1, 2, 5, 10$, så vi får

$$\begin{aligned} \sum_{d \mid 10} \phi(d) &= \phi(1) + \phi(2) + \phi(5) + \phi(10) \\ &= 1 + 1 + 4 + 4 \\ &= 10 \end{aligned}$$