Konvolúció, Möbius-féle inverziós formula

Összegzési függvény

Definíció.

Az f számelméleti függvény **összegzési függvényén** az alábbi képlettel definiált F függvényt értjük:

$$F(n) = \sum_{d|n} f(d).$$

Példa.

- Az Euler-féle φ függvény összegzési függvénye az identikus függvény:

$$\sum_{d|n} \varphi(d) = n = \mathrm{id}(n).$$

- Az identikus függvény összegzési függvénye az osztók összege függvény:

$$\sum_{d|n} \mathrm{id}(d) = \sum_{d|n} d = \sigma(n).$$

- A konstans 1 függvény összegzési függvénye az osztók száma függvény:

$$\sum_{d|n} \mathbf{1}(d) = \sum_{d|n} 1 = \tau(n).$$

Összegzési függvény

Adott F függvény esetén hogyan lehet megtalálni azt a f függvényt, aminek F az összegzési függvénye? Van-e egyáltalán mindig ilyen f függvény? A kérdés megválaszolásához az alábbi egyenletrendszert kell megoldanunk az ismeretlen $f(1)$, $f(2)$, ... számokra nézve:

$$
\begin{aligned}
F(1) &= f(1) && \Longrightarrow f(1) = F(1) \\
F(2) &= f(1) + f(2) && \Longrightarrow f(2) = F(2) - F(1) \\
F(3) &= f(1) + f(3) && \Longrightarrow f(3) = F(3) - F(1) \\
F(4) &= f(1) + f(2) + f(4) && \Longrightarrow f(4) = F(4) - F(2) \\
F(5) &= f(1) + f(5) && \Longrightarrow f(5) = F(5) - F(1) \\
F(6) &= f(1) + f(2) + f(3) + f(6) && \Longrightarrow f(6) = F(6) - F(2) - F(3) + F(1) \\
&\vdots && \qquad \vdots
\end{aligned}
$$

Ez egy végtelen lineáris egyenletrendszer, de mátrixa szerencsére trianguláris, ezért a fenti módon, lépésről lépésre, egyenként megkaphatóak az $f(n)$ értékek. Tehát minden F függvényhez létezik, mégpedig egyetlen egy olyan f függvény, aminek az összegzési függvénye F. De hogyan lehetne felírni a megoldást képlettel?

A Möbius-féle μ függvény

Az általános képlet valami ilyesmi:

$$F(n) = \sum_{d|n} \pm f(d).$$

Az előjeleket az ún. Möbius-függvény adja meg:

Definíció.

Az n természetes számot **négyzetmentesnek** nevezzük, ha nem osztható egyetlen 1-nél nagyobb négyzetszámmal sem.

Megjegyzés.

Könnyű meggondolni (tegyük meg!), hogy egy szám akkor és csak akkor négyzetmentes, ha prímfelbontásában minden prím csak egyszer (azaz első hatványon) fordul elő.

Definíció.

Möbius-függvénynek nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

$$\mu(n) = \begin{cases} 0, & \text{ha } n \text{ nem négyzetmentes;} \\ (-1)^k, & \text{ha } n \text{ előáll } k \text{ különböző prím szorzataként.} \end{cases}$$

Möbius-féle inverziós formula

Tétel (Möbius-féle megfordítási képlet).

Minden F számelméleti függvényhez létezik pontosan egy f számelméleti függvény, amelynek összegzési függvénye éppen F. Ezt a f függvényt a következő képlettel számíthatjuk ki:

$$f(n) = \sum_{d|n} F(d) \cdot \mu\left(\frac{n}{d}\right).$$

A f függvényt a F függvény **megfordítási függvényének** *nevezzük.*

Példa.

$$\begin{aligned} f(6) &= \mu(1) \cdot F(6) + \mu(2) \cdot F(3) + \mu(3) \cdot F(2) + \mu(6) \cdot F(1) = \\ &= F(6) - F(3) - F(2) + F(1) \end{aligned}$$

$$\begin{aligned} f(100) &= \mu(1) \cdot F(100) + \mu(2) \cdot F(50) + \mu(4) \cdot F(25) + \mu(5) \cdot F(20) + \\ &+ \mu(10) \cdot F(10) + \mu(20) \cdot F(5) + \mu(25) \cdot F(4) + \mu(50) \cdot F(2) + \mu(100) \cdot F(1) = \\ &= F(100) - F(50) - F(20) + F(10) \end{aligned}$$

Konvolúció

Definíció.

Az f és g számelméleti függvények **konvolúcióján** az alábbi képlettel definiált $f * g$ számelméleti függvényt értjük:

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b) .$$

Tétel.

A konvolúció művelete kommutatív és asszociatív, továbbá minden f számelméleti függvényre $f * \delta = \delta * f = f$.

Bizonyítás.

A kommutativitás világos, az asszociativitáshoz pedig azt kell ellenőrizni, hogy

$$((f * g) * h)(n) = \cdots = \sum_{abc=n} f(a) g(b) h(c) = \cdots = (f * (g * h))(n) .$$

Mivel $b > 1$ esetén $\delta(b) = 0$, ezért

$$(f * \delta)(n) = \sum_{ab=n} f(a) \delta(b) = \sum_{a=n, b=1} f(a) \delta(b) = f(n) \delta(1) = f(n) . \qquad \square$$

Konvolúció

Tétel.

Gyengén multiplikatív számelméleti függvények konvolúciója is gyengén multiplikatív.

Következmény.

Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.

Bizonyítás.

$$\left.\begin{array}{l} f \text{ gyengén multiplikatív} \\ \mathbf{1} \text{ gyengén multiplikatív} \end{array}\right\} \implies F = f * \mathbf{1} \text{ is gyengén multiplikatív} \qquad \square$$

A Möbius-féle μ függvény összegzési függvénye

Tétel.

A Möbius-függvény összegzési függvénye a δ függvény, azaz $\mu * \mathbf{1} = \delta$.

Bizonyítás.

Jelölje M a μ függvény összegzési függvényét. Mivel μ gyengén multiplikatív, M is az (és persze δ is), így elegendő az $M(n) \stackrel{?}{=} \delta(n)$ egyenlőséget prímhatványokra ellenőrizni. (Az világos, hogy $M(1) = \delta(1)$.)
Tetszőleges p prím és $\alpha \in \mathbb{N}$ esetén

$$
\begin{aligned}
M(p^\alpha) &= \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu\left(p^{\alpha-1}\right) + \mu(p^\alpha) \\
&= 1 + (-1) + 0 + \cdots + 0 + 0 \\
&= 0 = \delta(p^\alpha).
\end{aligned}
$$

□

Megjegyzés.

Mivel a konvolúció műveletének δ az egységeleme ($\forall f : f * \delta = \delta * f = f$), a fenti tétel azt jelenti, hogy a μ függvény nem más, mint a konstans 1 függvény „konvolúciós inverze”.

Már megint a Möbius-féle inverziós formula

Tétel (Möbius-féle megfordítási képlet).

Tetszőleges f és F számelméleti függvények esetén

$$F = f * \mathbf{1} \iff f = F * \mu.$$

Bizonyítás.

$\implies$: Tfh. $F = f * \mathbf{1}$. „Konvolváljuk be" az egyenlőség mindkét oldalát μ-vel:

$$F = f * \mathbf{1} \implies F * \mu = (f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu) = f * \delta = f.$$

$\impliedby$: Tfh. $f = F * \mu$. „Konvolváljuk be" az egyenlőség mindkét oldalát $\mathbf{1}$-gyel:

$$f = F * \mu \implies f * \mathbf{1} = (F * \mu) * \mathbf{1} = F * (\mu * \mathbf{1}) = F * \delta = F.$$

$\square$

Möbius-féle inverziós formula

Következmény.

Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.

Bizonyítás.

$$\left.\begin{array}{l} F \text{ gyengén multiplikatív} \\ \mu \text{ gyengén multiplikatív} \end{array}\right\} \Longrightarrow f = F * \mu \text{ is gyengén multiplikatív} \qquad \square$$