Konvolúció, Möbius-féle inverziós formula

$$
\begin{aligned}
1 &= x_1 \\
2 &= x_1 + x_2 \\
3 &= x_1 + x_3 \\
4 &= x_1 + x_2 + x_4 \\
5 &= x_1 + x_5 \\
6 &= x_1 + x_2 + x_3 + x_6 \\
7 &= x_1 + x_7 \\
8 &= x_1 + x_2 + x_4 + x_8 \\
9 &= x_1 + x_3 + x_9 \\
10 &= x_1 + x_2 + x_5 + x_{10} \\
11 &= x_1 + x_{11} \\
12 &= x_1 + x_2 + x_3 + x_4 + x_6 + x_{12} \\
13 &= x_1 + x_{13} \\
14 &= x_1 + x_2 + x_7 + x_{14} \\
15 &= x_1 + x_3 + x_5 + x_{15} \\
16 &= x_1 + x_2 + x_4 + x_8 + x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1 + x_2 \\
3 &= 1 + x_3 \\
4 &= 1 + x_2 + x_4 \\
5 &= 1 + x_5 \\
6 &= 1 + x_2 + x_3 + x_6 \\
7 &= 1 + x_7 \\
8 &= 1 + x_2 + x_4 + x_8 \\
9 &= 1 + x_3 + x_9 \\
10 &= 1 + x_2 + x_5 + x_{10} \\
11 &= 1 + x_{11} \\
12 &= 1 + x_2 + x_3 + x_4 + x_6 + x_{12} \\
13 &= 1 + x_{13} \\
14 &= 1 + x_2 + x_7 + x_{14} \\
15 &= 1 + x_3 + x_5 + x_{15} \\
16 &= 1 + x_2 + x_4 + x_8 + x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+x_3 \\
4 &= 1+1+x_4 \\
5 &= 1+x_5 \\
6 &= 1+1+x_3+x_6 \\
7 &= 1+x_7 \\
8 &= 1+1+x_4+x_8 \\
9 &= 1+x_3+x_9 \\
10 &= 1+1+x_5+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+x_3+x_4+x_6+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+x_7+x_{14} \\
15 &= 1+x_3+x_5+x_{15} \\
16 &= 1+1+x_4+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+x_4 \\
5 &= 1+x_5 \\
6 &= 1+1+2+x_6 \\
7 &= 1+x_7 \\
8 &= 1+1+x_4+x_8 \\
9 &= 1+2+x_9 \\
10 &= 1+1+x_5+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+x_4+x_6+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+x_7+x_{14} \\
15 &= 1+2+x_5+x_{15} \\
16 &= 1+1+x_4+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+x_5 \\
6 &= 1+1+2+x_6 \\
7 &= 1+x_7 \\
8 &= 1+1+2+x_8 \\
9 &= 1+2+x_9 \\
10 &= 1+1+x_5+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+2+x_6+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+x_7+x_{14} \\
15 &= 1+2+x_5+x_{15} \\
16 &= 1+1+2+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+4 \\
6 &= 1+1+2+x_6 \\
7 &= 1+x_7 \\
8 &= 1+1+2+x_8 \\
9 &= 1+2+x_9 \\
10 &= 1+1+4+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+2+x_6+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+x_7+x_{14} \\
15 &= 1+2+4+x_{15} \\
16 &= 1+1+2+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+4 \\
6 &= 1+1+2+2 \\
7 &= 1+x_7 \\
8 &= 1+1+2+x_8 \\
9 &= 1+2+x_9 \\
10 &= 1+1+4+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+2+2+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+x_7+x_{14} \\
15 &= 1+2+4+x_{15} \\
16 &= 1+1+2+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+4 \\
6 &= 1+1+2+2 \\
7 &= 1+6 \\
8 &= 1+1+2+x_8 \\
9 &= 1+2+x_9 \\
10 &= 1+1+4+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+2+2+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+6+x_{14} \\
15 &= 1+2+4+x_{15} \\
16 &= 1+1+2+x_8+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+4 \\
6 &= 1+1+2+2 \\
7 &= 1+6 \\
8 &= 1+1+2+4 \\
9 &= 1+2+x_9 \\
10 &= 1+1+4+x_{10} \\
11 &= 1+x_{11} \\
12 &= 1+1+2+2+2+x_{12} \\
13 &= 1+x_{13} \\
14 &= 1+1+6+x_{14} \\
15 &= 1+2+4+x_{15} \\
16 &= 1+1+2+4+x_{16} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \\
2 &= 1+1 \\
3 &= 1+2 \\
4 &= 1+1+2 \\
5 &= 1+4 \\
6 &= 1+1+2+2 \\
7 &= 1+6 \\
8 &= 1+1+2+4 \\
9 &= 1+2+6 \\
10 &= 1+1+4+4 \\
11 &= 1+10 \\
12 &= 1+1+2+2+2+4 \\
13 &= 1+12 \\
14 &= 1+1+6+6 \\
15 &= 1+2+4+8 \\
16 &= 1+1+2+4+8 \\
&\vdots
\end{aligned}
$$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	$\cdots$
x_k	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12	10	$\cdots$

Sejtés: $x_k = \varphi(k)$, azaz $n = \sum_{k|n} \varphi(k)$.

$$
\begin{aligned}
1 &= \varphi(1) \\
2 &= \varphi(1) + \varphi(2) \\
3 &= \varphi(1) + \varphi(3) \\
4 &= \varphi(1) + \varphi(2) + \varphi(4) \\
5 &= \varphi(1) + \varphi(5) \\
6 &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) \\
7 &= \varphi(1) + \varphi(7) \\
8 &= \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) \\
9 &= \varphi(1) + \varphi(3) + \varphi(9) \\
10 &= \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) \\
11 &= \varphi(1) + \varphi(11) \\
12 &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\
13 &= \varphi(1) + \varphi(13) \\
14 &= \varphi(1) + \varphi(2) + \varphi(7) + \varphi(14) \\
15 &= \varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) \\
16 &= \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) + \varphi(16) \\
&\vdots
\end{aligned}
$$

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.

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

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.

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

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

$\Longleftarrow$: 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.

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