1. Számelméleti függvények

Ismétlés

Definíció (FGy6.1.1–5)
Számelméleti függvény: a pozitív egészeken értelmezett,
komplex értékű f függvény.
Az f *totálisan multiplikatív*, ha minden a, b-re $f(ab) = f(a)f(b)$.
Multiplikatív, ha ezt csak $(a, b) = 1$ esetén tesszük föl.
Az f *totálisan additív*, ha minden a, b-re $f(ab) = f(a) + f(b)$.
Additív, ha ezt csak $(a, b) = 1$ esetén tesszük föl.

Ha $f(x)$ (totálisan) additív, akkor $c^{f(x)}$ (totálisan) multiplikatív.
HF (FGy6.1.6–8): Ha $f \neq 0$ multiplikatív, akkor $f(1) = 1$.
(Totálisan) multiplikatív függvény a prímhatványokon (prímeken) tetszőlegesen megadható, és ez egyértelműen meghatározza.
Ha f multiplikatív, és n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, akkor
$f(n) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})$. Példák multiplikatív függvényre:
$\varphi(n)$ (Euler-függvény), $d(n)$ (osztók száma), $\sigma(n)$ (osztók összege).

További számelméleti függvények

Definíció (FGy6.2.5, 6.2.8)
$\omega(n)$ az n különböző (pozitív) prímosztónak a száma.
$\Omega(n)$ az n összes (pozitív) prímosztónak a száma.
Azaz ha n kanonikus alakja $p_1^{\alpha_1} \dots p_k^{\alpha_k}$,
akkor $\omega(n) = k$ és $\Omega(n) = \alpha_1 + \ldots + \alpha_k$.
Nyilván ω additív és Ω totálisan additív.

Definíció (FGy6.2.3)
A $\mu(n)$ *Möbius-függvény* az a multiplikatív függvény,
ami a p^k prímhatványon 1, ha $k = 1$, és 0, ha $k > 1$.

Vagyis ha n nem négyzetmentes szám (tehát van 1-nél nagyobb négyzetszám osztója), akkor $\mu(n) = 0$, különben $\mu(n) = (-1)^{\omega(n)}$. Belátjuk majd, hogy az n-edik primitív komplex egységgyökök összege $\mu(n)$ (K3.9.18).

Összegezési függvény, konvolúció

Definíció (FGy6.5.1)
Az f függvény *összegezési függvénye* $f^+(n) = \sum_{d|n} f(d)$.

Példa: az Euler-függvény összegezési függvénye $\varphi^+(n) = n$.
Valóban: a körosztási polinomokra vonatkozó $x^n - 1 = \prod_{d|n} \Phi_d(x)$ összefüggésben vegyük mindkét oldal fokát. □
HF: Az azonosan 1 függvény összegezési függvénye $d(n)$, az $f(n) = n$ összegezési függvénye $\sigma(n)$.

Definíció (FGy6.6.1)
Az f és g számelméleti függvények *konvolúciója*
$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{cd=n} f(c)g(d)$.
„Egységelem" a konvolúcióra: $e(1) = 1$, és $e(n) = 0$, ha $n > 1$.

HF: $e * f = f$, és $1 * f = f^+$, ahol 1 az azonosan 1 függvény.

A konvolúció tulajdonságai

Tétel (FGy6.6.2, F6.6.2, F6.6.4/(a))
A konvolúció *kommutatív* és *asszociatív*, a pontonkénti összeadásra és a konvolúcióra *nullosztómentes gyűrűt* kapunk. Az e függvény *egységelem.* Az f pontosan akkor *invertálható*, ha $f(1) \neq 0$. Multiplikatív függvények konvolúciója is multiplikatív.

Asszociativitás: $(f * g) * h = f * (g * h) = \sum_{bcd=n} f(b)g(c)h(d)$.
Nullosztómentesség: Ha a, b a legkisebb, melyre $f(a) \neq 0 \neq g(b)$,
akkor $(f * g)(ab) \neq 0$.
Inverz: $f * g = e$-t akarjuk g-re megoldani. Ha $g(k)$ már megvan $k < n$-re, akkor $0 = e(n) = \sum_{d|n} f(d)g(\frac{n}{d})$-ből $g(n)$ kifejezhető, hiszen az összegben $f(1)g(n)$ szerepel, ahol $f(1) \neq 0$, a többi $f(d)g(\frac{n}{d})$ tag esetében pedig $g(\frac{n}{d})$ már ismert, mert $(n/d) < n$.
Multiplikativitás: Használjuk föl, hogy ha $(n, m) = 1$, akkor minden $d \mid mn$ egyértelműen írható $d = m'n'$ alakban, ahol $m' \mid m$ és $n' \mid n$.

Möbius-megfordítás
Adott g-re keressük azt az f függvényt, amelyre $f^+ = g$.

Lemma (FGy6.2.4)
Ha μ a Möbius-függvény, akkor $\mu^+ = e$.

Biz.: Láttuk, hogy $f^+ = f * 1$, ahol 1 az azonosan 1 függvény. Az azonosan 1 függvény nyilván totálisan multiplikatív. Ezért μ^+ multiplikatív, és persze e is, tehát a $\mu^+ = e$ összefüggést elég a $p^k > 1$ prímhatványokra igazolni. Ekkor $e(p^k) = 0$, és $\mu^+(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = 1 + (-1) = 0$. □

Möbius megfordítási formula (FGy6.5.2)
Ha $f^+ = g$, akkor $f = g * \mu$, azaz $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$.
Speciálisan f pontosan akkor multiplikatív,ha f^+ az.

Biz.: $g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * e = f$. □

A primitív komplex egységgyökök összege

Tétel (FGy6.5.9, K3.9.18): Az n-edik primitív egységgyökök összege $\mu(n)$.

Bizonyítás. Jelölje $f(n)$ az n-edik primitív egységgyökök összegét. Elég megmutatni, hogy $f^+ = e$ (mert akkor $f = e * \mu = \mu$). Ez abból következik, hogy $\sum_{d|n} f(d)$ az n-edik egységgyökök összege, amiről már láttuk, hogy $e(n)$.
Ezt bizonyíthatnánk ugyanúgy, mint a $x^n - 1 = \prod_{d|n} \Phi_d(x)$ képletet, megmutatva, hogy ha ε egy n-edik egységgyök, akkor egyetlen d-re lesz d-edik primitív egységgyök, és ez a $d \mid n$. De egyszerűbb a gyökök és együtthatók összefüggését alkalmazni.
Tekintsük az $x^n - 1 = \prod_{d|n} \Phi_d(x)$ összefüggésben x^{n-1} együtthatóját. A bal oldalon ez -1, ha $n = 1$, és 0, ha $n > 1$. Másrészt $f(d)$ a $\Phi_d(x)$ polinomban $x^{\varphi(n)-1}$ együtthatójának ellentettje. A jobb oldali szorzatban x^{n-1}-es tagot úgy kaphatunk, hogy egy kivételével mindegyik tényezőből a legmagasabb fokú tagot vesszük, a kivételesből pedig a második legmagasabb fokú tagot. □

Explicit képlet Φ_n-re

Tétel (K3.9.14)
$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$.

A képletet úgy kell érteni, hogy ha $\mu(n/d)$ negatív, akkor az $x^d - 1$ polinommal osztani kell. Például $\Phi_{12}(x)$ értéke

$$\frac{(x-1)^0(x^2-1)(x^3-1)^0(x^{12}-1)}{(x^6-1)(x^4-1)} = \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1.$$

„Bizonyítás": Az $x^n - 1 = \prod_{d|n} \Phi_d(x)$ „logaritmusa" azt fejezi ki, hogy $\log(x^n - 1)$ a $\log \Phi_n(x)$ összegezési függvénye. Ezért a tétel a Möbius-megfordítási formulából adódik.

Precízen: legyen ε egy n-edik egységgyök, $f_\varepsilon(n)$ az $(x - \varepsilon)$ kitevője $\Phi_n(x)$-ben, $g_\varepsilon(n)$ pedig $x^n - 1$-ben. Ekkor $x^n - 1 = \prod_{d|n} \Phi_d(x)$ szerint $f_\varepsilon^+ = g_\varepsilon$. A tétel pedig azt mondja, hogy $f_\varepsilon = g_\varepsilon * \mu$. □

2. Dirichlet-sorok

Relatív prím számpárok

Mi a valószínűsége annak, hogy két egész szám relatív prím?

Heurisztikus gondolatmenet: Legyen $R(n)$ azoknak az (a,b) számpároknak a száma, melyekre $1 \le a,b \le n$ és $(a,b)=1$. A keresett valószínűség $R(n)/n^2$ határértéke, ha $n \to \infty$.
A $p \le n$ prímre $\lfloor n/p \rfloor^2$ számpár tagjai oszthatók p-vel. Ezért a szita-formula miatt a relatív prím párok száma

$$n^2 - \sum_p \lfloor \tfrac{n}{p} \rfloor^2 + \sum_{p,q} \lfloor \tfrac{n}{pq} \rfloor^2 - \sum_{p,q,r} \lfloor \tfrac{n}{pqr} \rfloor^2 + - \ldots .$$

Az egészrészek elhagyása kis hibát okoz n^2-hez képest,
ezért ez körülbelül $n^2 \sum_{d=1}^{n} \frac{\mu(d)}{d^2}$. (A Möbius-függvény biztosítja az előjeleket, és hogy csak négyzetmentes számok szerepeljenek az összegben.)
Így a keresett valószínűség $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$.
Ez a végtelen sor konvergens, értéke $6/\pi^2 \approx 0.6079271$.
Ezt azzal fogjuk kapcsolatba hozni, hogy $\sum_{d=1}^{\infty} \frac{1}{d^2} = \pi^2/6$.
Tehát a számpárok több, mint fele relatív prím!

A precíz bizonyítás

Tétel (FGy6.7.5): Annak valószínűsége, hogy két egész szám relatív prím, a következő: $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = 6/\pi^2 \approx 0.6$.

Állítás. Azoknak az (a,b) pároknak a száma, melyekre $(a,b)=1$ és $1 \le a,b \le n$, éppen $R(n) = 2\big(\varphi(1) + \ldots + \varphi(n)\big) - 1$.
Indukcióval n szerint: ha a és b egyike $= n > 1$, akkor $2\varphi(n)$ ilyen pár van, hiszen $(n,n) \neq 1$. Viszont $n=1$-re $(1,1)$ megfelelő. □

Állítás (FGy6.5.8)
$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$.

Valóban, $\frac{\varphi(n)}{n}$ is, $\frac{\mu(n)}{n}$ is multiplikatív függvény, így az utóbbinak az összegezési függvénye is. Ezért az állítást elég a p^k prímhatványokra belátni. De ekkor mindkét oldal $1 - \frac{1}{p}$. □
Az állítást $\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right)$ beszorzásával is igazolhatjuk.

Átfogalmazás $\mu(n)$-re*

Az előzőekből $F = \sum_{i=1}^{n} \varphi(i) = \sum_{i=1}^{n} i \sum_{d|i} \frac{\mu(d)}{d}$. Ezt d szerint rendezve $\sum_{d=1}^{n} \mu(d) \sum_{\{i:d|i\leq n\}} \frac{i}{d}$ adódik. Nyilván $\sum_{\{i:d|i\leq n\}} \frac{i}{d} = 1+2+\ldots k = k(k+1)/2$, ahol $k = \lfloor n/d \rfloor$. Ha $k(k+1)/2$ *helyett* $(1/2)(\frac{n}{d})^2$-et írunk akkor az eredmény $M = (1/2)n^2 \sum_{d=1}^{n} \frac{\mu(d)}{d^2}$. *Becsüljük meg ennek eltérését F-től!*

Mivel $k \leq \frac{n}{d} < k+1$, ezért $|k - \frac{n}{d}| \leq 1$.
Így $|k(k+1) - (\frac{n}{d})^2| \leq k + |\big(k - \frac{n}{d}\big)\big(k + \frac{n}{d}\big)| \leq 3\big(\frac{n}{d}\big)$ a háromszög-egyenlőtlenség miatt. Ha ezeket összegezzük, akkor
$|F - M| \leq (1/2) \sum_{d=1}^{n} |\mu(d)\big(\frac{3n}{d}\big)| \leq (3n/2) \sum_{d=1}^{n} \frac{1}{d}$.
Analízis: $\sum_{d=1}^{n} \frac{1}{d} \leq \log(n) + 1$. Így $|F - M| \leq (3n/2)(\log n + 1)$.

$R(n) = 2F - 1$, így $|\frac{R(n)}{n^2} - \sum_{d=1}^{n} \frac{\mu(d)}{d^2}| \leq \big(3n(\log n + 1) + 1\big)/n^2$, ami nullához tart, hiszen $\frac{\log n}{n} \to 0$, ha $n \to \infty$. □

Dirichlet-sorok*

Definíció (FGy6.6.3)
Az f számelméleti függvényhez tartozó *Dirichlet-sor* $D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$.

Tétel (FGy6.6.4)
$D_{f*g}(s) = D_f(s) D_g(s)$, ha mindegyik sor abszolút konvergens.

Tudjuk, hogy abszolút konvergens sorok összeszorozhatók. Ezért
$D_f(s) D_g(s) = \Big(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\Big)\Big(\sum_{m=1}^{\infty} \frac{g(m)}{m^s}\Big) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)}{n^s} \frac{g(m)}{m^s}$.
Vonjuk össze azokat a tagokat, ahol $nm = k$. Ekkor $n^s m^s = k^s$,
így ez $\sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{nm=k} f(n) g(m) = \sum_{k=1}^{\infty} \frac{(f*g)(k)}{k^s} = D_{f*g}(s)$. □
Speciálisan $D_\mu(s) D_1(s) = D_{\mu*1}(s) = D_e(s) = 1$ (ahol 1 az azonosan 1 függvény). Azaz $\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{1}{n^s}\Big) = 1$.

A Riemann-függvény

Definíció (FGy, F5.6.6)
A *Riemann-féle zétafüggvény* az azonosan 1 függvényhez tartozó Dirichlet-függvény: $\zeta(s) = D_1(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Ennek igen szoros a kapcsolata a prímszámok eloszlásával. Analitikus módszerekkel kiterjeszthető $s = 1$ kivételével a teljes komplex számsíkra. A matematika egyik leghíresebb problémája az alábbi sejtés, amelynek sok mély számelméleti következménye lenne.

Riemann-sejtés (F6.6)
A Riemann-függvény minden komplex gyöke vagy negatív egész, vagy a valós része 1/2.

Analízisből látni fogjuk, hogy $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \pi^2/6$. Ezért a
$D_\mu(s) D_1(s) = 1$ összefüggés miatt $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = 6/\pi^2$.

A 29. előadás összefoglalója

Fogalmak
Additív és multiplikatív számelméleti függvény (FGy6.1.1–5).
$\omega(n)$ és $\Omega(n)$ (FGy6.2.5, 6.2.8)*. A Möbius-függvény (FGy6.2.3).
Összegezési függvény, konvolúció (FGy6.5.1, 6.6.1).
Dirichlet sor, Riemann-függvény (FGy6.6.3, F5.6.6).

Tételek
A konvolúció tulajdonságai (FGy6.6.2, F6.6.2, F6.6.4/(a)).
Möbius megfordítási formula (FGy6.5.2).
A primitív egységgyökök összege (FGy6.5.9, K3.9.18).
Explicit képlet Φ_n-re (K3.9.14).
A Dirichlet-sor és a konvolúció kapcsolata (FGy6.6.4).
Annak valószínűsége, hogy két szám relatív prím (FGy6.7.5, NB).
Riemann-sejtés (F6.6, NB).