

A DIRICHLET-TÉTEL

MAGA PÉTER

Dirichlet tétele azt mondja ki, hogy ha $(a, q) = 1$, akkor végtelen sok olyan p prímszám van, melyre $p \equiv a \pmod{q}$.

Ebben a jegyzetben a Dirichlet-tétel egy egyszerű bizonyítását szeretnénk bemutatni. A bizonyítás abban az értelemben lesz egyszerű, hogy néhány bevezető komplex függvénytan ismeret segítségével viszonylag fáradságmentesen fog történni.

Először ezeket tekintjük át.

1. TÉNYEK A KOMPLEX FÜGGVÉNYTANBÓL

A jegyzetnek nem célja, hogy egy komplex függvénytan kurzus teljes tananyagát az Olvasó elé tárja, ezért ebben a fejezetben a kimondott állítások csak ritkán kerülnek bizonyításra. Feltételezünk némi valós analízisbeli háttérismertetet, és csak azokat az állításokat részletezzük, amik a valós analízishez képest szokatlanok.

1.1. Komplex deriválás.

Definíció 1. Legyen $D \subseteq \mathbb{C}$ nyílt halmaz, $f : D \rightarrow \mathbb{C}$ függvény. Azt mondjuk, hogy f deriválható a $z_0 \in D$ pontban, és a deriváltja $f'(z_0)$, ha

$$f'(z_0) = \lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

A deriválásra ekkor teljesülnek a valósban megszokott egyszerű azonosságok: lineáris, szorzat deriváltjára fennáll a Leibniz-szabály, kompozíció deriváltjára a láncszabály. Polinomok deriváltja is ugyanaz, mint a valós esetben.

1.2. Hatványsorok. A $\sum_{n=0}^{\infty} a_n(z - z_0)^n$ alakú – egyelőre formális – kifejezést z_0 középpontú hatványsornak hívjuk. Tegyük fel, hogy abszolút konvergens a z_0 középpontú R sugarú nyílt körlapon (be lehet bizonyítani, hogy a konvergenciataromány lényegében mindig ilyen alakú), ekkor ott előállít egy $f(z)$ függvényt. Ekkor f deriválható, sőt, akárhányszor deriválható ezen a körlapon. Továbbá deriváltja a hatványsor formális deriváltjaként felírható, általában

$$f^{(k)}(z) = \sum_{n=k}^{\infty} n(n-1) \cdots (n-k+1) a_n (z - z_0)^{n-k}.$$

Megjegyezzük, hogy míg az $R = 0$ eset nem különösebben érdekes, az $R = \infty$ eset az egész síkon konvergens hatványsorokat jelent.

A legfontosabb példa az

$$\exp(z) = e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Könnyű látni (mivel a nevezőben levő $n!$ nagyon gyorsan tart a végtelenbe), hogy e^z az egész síkon (abszolút) konvergens, továbbá hogy $(e^z)' = e^z$. Bár nem lesz rá szükségünk, megjegyezzük, hogy $z = 1$ -et helyettesítve az e szám egyik lehetséges definícióját kapjuk vissza. Tudjuk továbbá a valós analízisből, hogy $z \in \mathbb{R}$ -re a valós e^z -t adja vissza a hatványsor.

Egy másik példa a mértani sor:

$$\sum_{n=0}^{\infty} z^n.$$

Ennek konvergenciasugara 1, vagyis minden $|z| < 1$ -re (abszolút) konvergens, és ott éppen az $1/(1-z)$ függvényt állítja elő.

Az exponenciális függvényhez hasonlóan az egész síkon konvergens a következő szögfüggvények:

$$\cos z = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!}, \quad \sin z = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!},$$

és a valós analízisből tudjuk, hogy $z \in \mathbb{R}$ -re ezek valóban a $\cos$ és $\sin$ függvényeket állítják elő.

Egyszerű számolás mutatja, hogy $z \in \mathbb{C}$ -re

$$e^{iz} = \cos z + i \sin z.$$

Ha most z befutja a $[0, 2\pi]$ intervallumot, akkor látjuk, hogy e^{iz} éppen befutja az egységgörte, erre később még szükségünk lesz. Nem lesz rá szükségünk, de kihagyhatatlan, hogy $z = \pi$ -t helyettesítve kapjuk az Euler-azonosságot:

$$e^{\pi i} + 1 = 0,$$

mely egyetlen formulában foglalja össze az egész matematika öt legfontosabb konstansát!

1.3. Komplex vonalintegrál.

Definíció 2. Legyen $\gamma: [0, 1] \rightarrow \mathbb{C}$ folytonos, rektifikálható görbe. (Az utóbbi feltétel, a rektifikálhatóság, azt jelenti, hogy van olyan M valós szám, hogy minden $0 = t_0 < t_1 < \dots < t_n = 1$ felosztásra $\sum_{j=1}^n |\gamma(t_j) - \gamma(t_{j-1})| < M$. Ez pont azt jelenti, hogy a görbe hossza véges, vagyis a hosszának minden véges közelítése egy fix véges korlát alatt marad. Ezzel nem kell sokat bajlódni, a konkrét felhasználásban a mi görbéink minden esetben triviálisan véges hosszúak lesznek.) Legyen továbbá f egy komplex értékű függvény a γ képen. Azt mondjuk, hogy $\int_{\gamma} f(z) dz = I$, ha minden $\varepsilon > 0$ -hoz létezik olyan $\delta > 0$, hogy γ minden δ -nál finomabb felosztására és hozzá tartozó belső pontokra az intergálközelítő összeg legfeljebb ε -nal tér el I -től; precízen: minden olyan $0 = t_0 < t_1 < \dots < t_n = 1$ -re, melyre igaz, hogy minden $t_{j-1} \leq \xi \leq t_j$ -re $|\gamma(\xi) - \gamma(t_j)| < \delta$ (ez jelenti azt, hogy a γ felosztása δ -nál finomabb) és minden $\xi_j \in [t_{j-1}, t_j]$ -re (ezek a hozzá tartozó belső pontok),

$$\left| I - \sum_{j=1}^n f(\gamma(\xi_j))(\gamma(t_j) - \gamma(t_{j-1})) \right| < \varepsilon.$$

A definíció talán kissé elrettentőnek tűnhet, szerencsére mi nem fogjuk használni. Következik belőle, hogy az integrál független a konkrét paraméterezéstől (tehát ha ugyanazt a görbét járjuk be, de mondjuk az elejét „gyorsabban”, a végét „lassabban”, az integrálra ugyanaz adódik). Általában fennáll a helyettesítési integrál formulája, vagyis ha γ görbe (mint fent), F a γ képen értelmezett folytonosan deriválható függvény, h pedig folytonos függvény $F(\gamma)$ -n, akkor

$$\int_{F(\gamma)} h(w) dw = \int_{\gamma} h(F(z)) F'(z) dz.$$

Ennek egy fontos alkalmazása a következő. Legyen a görbénk a $|z| = R$ körvonal, ami alatt azt a konkrét görbét értjük (egyszer s mindenkorra), ami egyszer kerüli meg a 0-t, pozitív körüljárással. Legyen a függvényünk a rajta értelmezett $1/z$. A helyettesítés legyen az $F: [0, 2\pi] \rightarrow \mathbb{C}$, $F(\theta) = Re^{i\theta}$, ekkor $F'(\theta) = iRe^{i\theta}$. Az integrál tehát

$$\int_{|z|=R} \frac{1}{z} dz = \int_{[0, 2\pi]} \frac{1}{Re^{i\theta}} iRe^{i\theta} d\theta = \int_{[0, 2\pi]} i d\theta = 2\pi i.$$

1.4. Primitív függvény. Legyen $f: D \rightarrow \mathbb{C}$ folytonos függvény a D nyílt, összefüggő tartományon. Azt mondjuk, hogy F primitív függvénye f -nek, ha $F' = f$. Mikor létezik ilyen? Be lehet bizonyítani, hogy pontosan akkor létezik az f függvénynek primitív függvénye, ha az integrál független az úttól, azaz tetszőleges $a, b \in D$ pontokra, és tetszőleges őket összekötő γ, γ' rektifikálható görbékre

$$\int_{\gamma} f(z) dz = \int_{\gamma'} f(z) dz.$$

Könnyű látni, hogy ez azzal ekvivalens, hogy minden γ zárt görbére

$$\int_{\gamma} f(z) dz = 0.$$

Ebből az is világos, hogy az $1/z$ függvénynek nincs primitív függvénye $\mathbb{C} \setminus \{0\}$ -n.

Állítás 3 (Goursat-lemma). *Ha az f függvény deriválható a konvex D tartományon, akkor $\int_{\gamma} f(z) dz = 0$ minden D -ben haladó zárt görbére (tehát konvex tartományon deriválható függvénynek van primitív függvénye).*

Bizonyítás. Elegendő belátni olyan γ -kra, amik egy háromszöget járnak körbe, mert ilyenekkel minden mást tudunk közelíteni. Legyen γ ilyen, az általa határolt H háromszög kerülete legyen K , és tegyük fel, hogy $\int_{\gamma} f(z) dz = I$. A középvonalakkal felvágva H -t, és a vele egyállású háromszögeket γ -val megegyező, a középvonalháromszöget γ -val ellentétes irányban bejárva azt kapjuk, hogy valamelyik kisebb háromszög körül az integrál legalább $|I|/4$ abszolút

értékű. Ezt nyilván tetszőlegesen sokszor megismételhetjük, így egymásba skatulyázottan minden n -re van olyan kis háromszög, ami éppen $1/2^n$ -szeres kicsinyítettje H -nak, és körülötte f integrálja legalább $|I|/4^n$ abszolút értékű. Legyen z_0 ezek közös pontja és legyen $\varepsilon > 0$ adott. Elég nagy n -et, és hozzá tartozó kicsi H' háromszöget (amit γ' határol) választva a kerületi integrál triviálisan becslülve:

$$\left| \int_{\gamma'} f(z) dz \right| < \left| \int_{\gamma'} f(z_0) dz \right| + \left| \int_{\gamma'} (z - z_0) f'(z_0) dz \right| + \varepsilon |z - z_0| \frac{K}{2^n},$$

hiszen H' kerülete $K/2^n$. Nyilván $|z - z_0| < K/2^n$. Ugyanakkor a jobb oldal első két tagja 0, hiszen a konstans és a $z - z_0$ függvénynek is van primitív függvénye. Azaz

$$\frac{|I|}{4^n} < \frac{\varepsilon K^2}{4^n}.$$

Mivel ez minden $\varepsilon > 0$ -ra igaz, $I = 0$. □

Állítás 4 (Goursat-lemma erősítése). *Tegyük fel, hogy az f függvény deriválható a konvex D tartományon, kivéve legfeljebb egy belső z_0 pontját, melyre teljesül, hogy*

$$\lim_{z \rightarrow z_0} f(z)(z - z_0) = 0.$$

Ekkor $\int_{\gamma} f(z) dz = 0$ minden D -ben haladó zárt görbére (tehát az előző tétel feltételéhez képest lehet egy kivételes pont, ahol elég azt tudnunk, hogy ott a függvény nem száll el túl gyorsan; a következmény ugyanaz).

Bizonyítás vázlata. Elegendő olyan háromszögekre, melyeknek egyik csúcsa a z_0 kivételes pont. A kivételes pont egy kicsi környezetében az integrál kicsi, a maradékra alkalmazhatjuk az előző változatot. □

1.5. Hatványsorba fejtés. Legyen most f deriválható a $|z - z_0| = R$ körlap egy környezetében. Ekkor az $(f(z) - f(z_0))/(z - z_0)$ függvényre teljesülnek a Goursat-lemma erősebb változatának feltételei, azaz

$$\int_{|z-z_0|=R} \frac{f(z) - f(z_0)}{z - z_0} dz = 0,$$

amit átrendezve, illetve a korábban kiszámolt $\int_{|z|=R} dz/z = 2\pi i$ -t alkalmazva adódik a Cauchy-integrálformula:

$$f(z_0) = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{z - z_0} dz.$$

Legyen most w tetszőleges belső pontja a $|z - z_0| < R$ körlapnak. Mivel az integrál független az úttól, és $|z - z_0| = R$ ugyanúgy egyszer kerüli meg w -t, mint $|z - w| = R - |w - z_0|$, ezért az előző minden ilyen w -re igaz:

$$f(w) = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{z - w} dz.$$

Egyszerű számolással adódik, hogy

$$\frac{1}{z - w} = \sum_{n=0}^{\infty} \frac{(w - z_0)^n}{(z - z_0)^{n+1}},$$

ezért

$$f(w) = \sum_{n=0}^{\infty} a_n (w - z_0)^n, \quad a_n = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{(z - z_0)^{n+1}} dz,$$

az integrál és a szumma (a konkrét esetben egyszerűen ellenőrizhető) felcserélésével. Tehát deriválható függvény hatványsorba fejthető. Következésképp akárhányszor deriválható, és a deriváltak a hatványsor formális deriváltjaként számolhatók. A továbbiakban ezért holomorfnak (regulárisnak, analitikusnak) nevezzük a deriválható komplex függvényeket.

Ebből egyszerűen következik, hogy ha egy konvex D tartományon értelmezett folytonos függvény integrálja minden zárt görbén eltűnik, akkor az holomorf. Valóban, legyen f ilyen, ekkor van F primitív függvénye, ami deriválható. Akkor viszont kétszer is deriválható, vagyis f is deriválható.

Ennek további következménye, hogy ha az f_n holomorf függvényekből álló függvény sorozat tart lokálisan egyenletesen f -hez (vagyis D minden K kompakt részhalmazán egyenletesen: minden $\varepsilon > 0$ -ra van olyan $n(K, \varepsilon)$ (csak

K -tól és ε -tól függő határ), hogy $|f(x) - f_n(x)| < \varepsilon$, valahányszor $n > n(K, \varepsilon)$ és $x \in K$). Valóban, lokálisan egyenletes konvergens függvénysorozat esetében a limesz integrálja megegyezik az integrálok limeszével, így

$$\int_{\gamma} f(z) dz = \int_{\gamma} \lim_{n \rightarrow \infty} f_n(z) dz = \lim_{n \rightarrow \infty} \int_{\gamma} f_n(z) dz = 0.$$

Sőt, a deriváltak sorozata is tart lokálisan egyenletesen a deriválthoz, hiszen

$$f'_n(w) = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f_n(z)}{(z-w)^2} dz \rightarrow \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{(z-w)^2} dz = f'(w).$$

Meg kell még jegyeznünk az unicitási tételt: ha egy tartományon értelmezett két holomorf függvény megegyezik egy a tartományban torlódó ponthalmazon, akkor az egész tartományon is. Ez is egyszerűen következik a hatványsorba fejtésből.

1.6. Pólusok. Még egy fogalomra van szükségünk, a pólusra. Legyen f holomorf a $0 < |z - z_0| < R$ kipontozott körlapon. Ekkor tetszőleges $0 < |w - z_0| < R$ pontjára vegyünk fel egy $r < |w - z_0|$ kört. A korábbiak szerint

$$f(w) = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{z-w} dz - \frac{1}{2\pi i} \int_{|z-z_0|=r} \frac{f(z)}{z-w} dz.$$

Az első integrál, mint fent,

$$\sum_{n=0}^{\infty} \left(\frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{(z-z_0)^{n+1}} dz \right) (w-z_0)^n.$$

A második integrálhoz

$$\frac{1}{z-w} = - \sum_{n=-\infty}^{-1} \frac{(w-z_0)^n}{(z-z_0)^{n+1}},$$

így a különbségre a hatványsorhoz hasonló módon

$$f(w) = \sum_{n=-\infty}^{\infty} a_n (w-z_0)^n, \quad a_n = \frac{1}{2\pi i} \int_{|z-z_0|=R} \frac{f(z)}{(z-z_0)^{n+1}} dz.$$

Ebben az esetben azt mondjuk, hogy f -nek izolált szingularitása van z_0 -ban. Ez a szingularitás megszüntethető, ha $a_n = 0$ minden $n < 0$ -ra; pólus, ha nem megszüntethető, de $a_n = 0$ $n < 0$ -ra véges sok kivételtől eltekintve (a pólus rendje m , ha $a_{-m} \neq 0$, de $a_n = 0$ minden $n < -m$ -re); lényeges szingularitás, ha se nem megszüntethető, se nem pólus. Ha egy függvény egy tartományon néhány pont kivételével holomorf, és a kivételes pontokban pólusa van, akkor azt mondjuk, hogy a tartományon meromorf.

Amit mi használni fogunk, az a következő: ha f, g meromorfak egy tartományon, f -nek m -edrendű pólusa, g -nek m -szeres nullhelye van z_0 -ban, akkor fg -nek megszüntethető szingularitása van z_0 -ban. Hasonlóan kivonással is lehet pólusokat eltüntetni.

2. DIRICHLET-SOROK

2.1. Pozitív számok komplex hatványai. Legyen $s \in \mathbb{C}$, és $x > 0$ valós szám. Ekkor az

$$x^s = e^{s \log x}$$

definíciót szeretnénk használni, amihez $\log x$ -et definiálnunk kell. Ha a komplex logaritmust a komplex exponenciális inverzeként akarjuk felfogni, akkor látjuk, hogy ez nem egyértelmű, hiszen $e^z = e^{z+2k\pi i}$ minden $k \in \mathbb{Z}$ -re. A komplex logaritmus általános definiálásához további fogalmakat kellene bevezetnünk. Ettől azonban a Dirichlet-tétel bizonyítása szempontjából eltekinthetünk, ha $x > 0$ valós szám esetén a $\log x$ -et a valósban megszokott logaritmusnak választjuk.

Ezzel a definícióval, ha $s = \sigma + it$ ($\sigma = \Re s, t = \Im s$ valósak),

$$x^s = e^{\sigma \log x} \cdot e^{it \log x}.$$

Itt a második tényező 1 abszolút értékű, vagyis $|x^s| = x^\sigma$, tehát amikor pozitív valós számot hatványozunk, akkor a hatvány abszolút értéke csak a kitevő valós részétől függ, a kitevő képzetes része a 0 körül forog. Általában is használjuk a mostani jelölést: az $s(s_0, s_1, \dots)$ komplex szám valós és képzetes része rendre $\sigma(s_0, \sigma_1, \dots)$ és $t(t_0, t_1, \dots)$.

2.2. Dirichlet-sorok konvergenciatartománya. Dirichlet-soron az (egyelőre formális) $\sum_{n=1}^{\infty} a_n n^{-s}$ függvényét értjük az $s \in \mathbb{C}$ számnak, ahol a_n valamilyen rögzített, komplex számokból álló együtthatósorozat.

Állítás 5. Tegyük fel, hogy $\sum_{n=1}^{\infty} a_n n^{-s_0}$ konvergens egy $s_0 \in \mathbb{C}$ pontban. Ekkor minden $H > 0$ -ra $\sum_{n=1}^{\infty} a_n n^{-s}$ egyenletesen konvergens a $\sigma > \sigma_0$, $|t - t_0|/(\sigma - \sigma_0) < H$ jobbra nyíló szögtartományon.

Bizonyítás. Legyen $R(u) = \sum_{n>u} a_n n^{-s_0}$ az összeg végszelete. Nyilván $a_n n^{-s} = (R(n-1) - R(n))n^{s_0-s}$, azaz tetszőleges $0 < M < N$ egészekre

$$\sum_{n=M+1}^N a_n n^{-s} = R(M)M^{s_0-s} - R(N)N^{s_0-s} - \sum_{n=M+1}^N R(n-1)((n-1)^{s_0-s} - n^{s_0-s}).$$

Legyen $\varepsilon > 0$ adott, és válasszuk meg M -et úgy, hogy $|R(u)| < \varepsilon$ legyen minden $u \geq M$ -re. Vegyük továbbá észre, hogy

$$n^{s_0-s} - (n-1)^{s_0-s} = (s_0 - s) \int_{n-1}^n u^{s_0-s-1} du,$$

ami abszolút értékben becslhető:

$$|n^{s_0-s} - (n-1)^{s_0-s}| \leq |s_0 - s| \int_{n-1}^n u^{\sigma_0-\sigma-1} du.$$

Ekkor összességében

$$\left| \sum_{M+1}^N a_n n^{-s} \right| \leq 2\varepsilon + \varepsilon |s_0 - s| \int_M^{\infty} u^{\sigma_0-\sigma-1} du \leq 2\varepsilon + \varepsilon \frac{|s - s_0|}{\sigma - \sigma_0} < (H+3)\varepsilon.$$

Mivel ez minden $\varepsilon > 0$ -ra igaz, készen vagyunk. □

Mivel H tetszőlegesen nagyra választható, a konvergenciatartomány egy félsík, melynek belsejében (a nyílt fél-síkon) a konvergencia lokálisan egyenletes. Mivel egyetlen tag, $a_n n^{-s}$, nyilván holomorf, a hatványsorba fejthetőségről szóló rész végén tett megjegyzésünk szerint $\sum_{n=1}^{\infty} a_n n^{-s}$ is holomorf, sőt, lehet tagonként deriválni.

Természetesen előfordulhat, hogy az előálló függvény kiterjed holomorf függvényként egy nagyobb tartományra, ahol esetleg már nem fogja a Dirichlet-sor előállítani. Gondoljunk a hatványsorokra, mint analógiára: a $\sum_{n=0}^{\infty} z^n$ hatványsor az egységkör belsejében állít elő holomorf függvényt, és máshol nem is konvergens. Azonban összege $1/(1-z)$, már a sokkal nagyobb $\mathbb{C} \setminus \{1\}$ halmazon is holomorf függvény.

A következő állítás azt fogalmazza meg, hogy egy speciális esetben ez nem fordul elő.

Állítás 6 (Landau-lemma). Tegyük fel, hogy a $\sum_{n=1}^{\infty} a_n n^{-s}$ Dirichlet-sor a_n együtthatói nemnegatív valós számok. Tegyük fel, hogy a konvergenciafélsík határának valós pontja σ_c (azaz a Dirichlet-sor konvergens minden $\Re s > \sigma_c$ -re, de nem konvergens egyetlen $\Re s < \sigma_c$ -re sem). Ekkor a Dirichlet-sor által előállított $\alpha(s)$ függvény σ_c egyetlen környezetére sem terjeszthető ki holomorfan.

Bizonyítás. Az együtthatók normalizálásával (minden a_n helyére $a_n n^{-\sigma_c}$ -t írva) feltehető, hogy $\sigma_c = 0$. Tegyük fel, hogy $\alpha(s)$ kiterjed az $|s| < \varepsilon$ körre holomorfan valamely $\varepsilon > 0$ -ra. Azt fogjuk belátni, hogy valamely kis $\delta > 0$ -ra $\sum_{n=1}^{\infty} a_n n^{\delta}$ konvergens. Az 1 körül hatványsorba fejthető α :

$$\alpha(s) = \sum_{k=0}^{\infty} c_k (s-1)^k.$$

A c_k együtthatók a hatványsor formális deriválhatósága alapján:

$$c_k = \frac{\alpha^{(k)}(1)}{k!} = \frac{1}{k!} \sum_{n=1}^{\infty} a_n (-\log n)^k n^{-1}.$$

Ekkor valamely kis $\delta > 0$ -ra $\alpha(s)$ hatványsora konvergens a $(-\delta)$ -ban, azaz

$$\alpha(-\delta) = \sum_{k=0}^{\infty} \frac{(1+\delta)^k}{k!} \sum_{n=1}^{\infty} a_n (\log n)^k n^{-1},$$

ami nemnegatív tagú sor, így átrendezhető:

$$\sum_{n=1}^{\infty} a_n n^{-1} \sum_{k=0}^{\infty} \frac{(1+\delta)^k (\log n)^k}{k!} = \sum_{n=1}^{\infty} a_n n^{-1} e^{(1+\delta) \log n} = \sum_{n=1}^{\infty} a_n n^{\delta}.$$

Ez ellentmondás. □

3. KARAKTEREK

Definíció 7. Azt mondjuk, hogy χ egy modulo q karakter, ha $\chi : \mathbb{Z} \rightarrow \mathbb{C}$, és teljesülnek rá az alábbiak:

- (i) $\chi(n) = \chi(n+q)$ minden $n \in \mathbb{Z}$ -re;
- (ii) $\chi(n) = 0$ pontosan akkor, ha $(n, q) \neq 1$;
- (iii) $\chi(mn) = \chi(m)\chi(n)$ minden $m, n \in \mathbb{Z}$ -re.

Nyilván $\chi(1) = 1$. Az is világos, hogy ha $(n, q) = 1$, akkor $|\chi(n)| = 1$. Most megadjuk az összes modulo q karaktert. Nyilván elegendő egy karaktert a multiplikatív csoporton (a redukált maradérendszer elemein) megadni. Tudjuk, hogy léteznek olyan $a_1, \dots, a_k$ redukált maradékok, és hozzá $b_1, \dots, b_k$ pozitív egészek (minden $1 \leq j \leq k$ -ra b_j a legkisebb pozitív egész, hogy $a_j^{b_j} \equiv 1 \pmod{q}$), hogy minden r redukált maradék egyértelműen írható fel $r \equiv a_1^{r_1} \dots a_k^{r_k}$ alakban, ahol minden $1 \leq j \leq k$ -ra $0 \leq r_j < b_j$ (az üres szorzatot – mint általában – 1-nek értelmezve). Ekkor a χ karaktert egyértelműen meghatározza az $a_1, \dots, a_k$ helyeken felvett értéke, amelyek pedig egymástól függetlenül tetszőlegesen megadhatók, csak a $\chi(a_j)^{b_j} = 1$ feltételnek kell fennállnia, vagyis $\chi(a_j)$ -nek b_j . egységgyöknek kell lennie minden $1 \leq j \leq k$ -ra. Tehát összesen éppen $\varphi(q)$ darab modulo q karakter van, a halmazukat jelöljük Ξ -vel.

Állítás 8. Tetszőleges $n \in \mathbb{Z}$ -re

$$\sum_{\chi \in \Xi} \chi(n) = \begin{cases} \varphi(q), & \text{ha } n \equiv 1 \pmod{q}; \\ 0, & \text{ha nem.} \end{cases}$$

Bizonyítás. Az világos, hogy minden karakter 1-et vesz fel az 1 maradékosztályon, ezek összege valóban $\varphi(q)$. Ha $(n, q) \neq 1$, akkor az állítás nyilvánvaló. Maradt tehát az az eset, amikor $(n, q) = 1$, de n nem az 1 maradékosztályában van. Állítjuk, hogy ekkor alkalmas $\chi' \in \Xi$ karakterre $\chi'(n) \neq 1$. Valóban, $n \equiv a_1^{n_1} \dots a_k^{n_k}$, ahol valamelyik $0 < n_j < b_j$. Legyen ekkor $\chi'(a_{j'}) = 1$ minden $j' \neq j$ -re, és $\chi'(a_j)$ pedig egy primitív b_j . egységgyök (ennek semelyik b_j -nél kisebb pozitív hatványa sem 1). Nyilvánvaló, hogy $\chi'(n) \neq 1$. Felhasználva, hogy amint χ befutja Ξ -t, $\chi'\chi$ is befutja Ξ -t (a karakterek csoportot alkotnak: karakterek szorzata karakter, és minden karakternek van inverze, a komplex konjugáltja),

$$\sum_{\chi \in \Xi} \chi(n) = \sum_{\chi \in \Xi} \chi'(n)\chi(n) = \chi'(n) \sum_{\chi \in \Xi} \chi(n).$$

Mivel $\chi'(n) \neq 1$, ezért $\sum_{\chi \in \Xi} \chi(n) = 0$. □

Ennek egyszerű következménye, hogy tetszőleges $(a, q) = 1$ -re

$$\sum_{\chi \in \Xi} \overline{\chi(a)} \chi(n) = \begin{cases} \varphi(q), & \text{ha } n \equiv a \pmod{q}; \\ 0, & \text{ha nem.} \end{cases}$$

Valóban, a bal oldalon álló összeg $\sum_{\chi \in \Xi} \chi(a^{-1}n)$, erre alkalmazható az előző állítás. Ennek segítségével tudjuk majd kiválogatni egy halmazból az előre adott maradékosztályba eső elemeket.

Bevezetjük a χ_0 jelölést a főkarakterre (más néven triviális karakter), ami a relatív prím maradékosztályokon konstans 1.

Állítás 9. Ha $\chi \neq \chi_0$, akkor $\sum_{n=1}^q \chi(n) = 0$.

Bizonyítás. Legyen $(a, q) = 1$, melyre $\chi(a) \neq 1$. Ekkor

$$\chi(a) \sum_{n=1}^q \chi(n) = \sum_{n=1}^q \chi(an) = \sum_{n=1}^q \chi(n).$$

Mivel $\chi(a) \neq 1$, készen vagyunk. □

4. A ζ -FÜGGVÉNY ÉS AZ L -FÜGGVÉNYEK

4.1. A Riemann- ζ .

Állítás 10. Ha $s > 1$ valós szám, akkor

$$1 < \sum_{n=1}^{\infty} \frac{1}{n^s} < \infty$$

Bizonyítás. A bal oldali egyenlőtlenség világos, elegendő tehát a konvergenciát bizonyítani. Növeljük meg az összeget úgy, hogy minden $2^k \leq n < 2^{k+1}$ helyére 2^k -t írunk. Ezzel

$$\sum_{n=1}^{\infty} \frac{1}{n^s} < \sum_{k=0}^{\infty} \frac{2^k}{2^{ks}} = \sum_{k=0}^{\infty} (2^{1-s})^k = \frac{1}{1-2^{1-s}} < \infty. \quad \square$$

Definiáljuk a

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

függvényt a $\Re s > 1$ félsíkon. A korábbiak értelmében holomorf ezen a félsíkon, és lehet tagonként deriválni.

Mivel $\sum_{n=1}^{\infty} 1/n = \infty$, ezért a ζ konvergenciafélsíkja a $\Re s > 1$. Lehet azonban folytatni a $\mathbb{C} \setminus \{1\}$ kipontozott síkra, az 1-ben elsőrendű pólussal. Nekünk ennél kevesebb is elég, ezért csak a $\Re s > 0$ félsíkra történő folytatását bizonyítjuk be.

Állítás 11. A $\zeta(s)$ függvény folytatható meromorfán a $\Re s > 0$ félsíkra, egyetlen pólusa az 1, ahol a szingularitás $1/(s-1)$, azaz $\zeta(s) - 1/(s-1)$ holomorf.

Bizonyítás. Definiáljuk az

$$\eta_2(s) = 1^{-s} - 2^{-s} + 3^{-s} - 4^{-s} \pm \dots, \quad \eta_3(s) = 1^{-s} + 2^{-s} - 2 \cdot 3^{-s} + 4^{-s} + 5^{-s} - 2 \cdot 6^{-s} \pm \dots$$

Dirichlet-sorokat. Ezek a $\Re s > 0$ félsíkon konvergensek (η_2 esetében ez Leibniz-típusú alternáló sor, η_3 egy egyszerű variáns). Továbbá $\Re s > 1$ -re és $k = 2, 3$ -ra

$$\eta_k(s) = \zeta(s) - k \cdot k^{-s} \zeta(s) = \zeta(s)(1 - k^{1-s}), \quad \zeta(s) = \frac{\eta_k(s)}{1 - k^{1-s}},$$

ahol a tört számlálója holomorf $\Re s > 0$ -n, a nevező holomorf minden olyan pontban, ahol $k^{1-s} \neq 1$ (ez a kivételes halmaz diszkrét, legyen H_k). Egyszerű számolás mutatja, hogy $H_2 \cap H_3 = \{1\}$, azaz minden pontra megfelel valamelyik kiterjesztés, és az unicitási tétel szerint azokban a pontokban, ahol mindkét kiterjesztés megfelel, ugyanazt kell adniuk.

Maradt az 1-beli szingularitás kérdése, az unicitás miatt ezt elegendő az η_2 segítségével történő folytatásra kiszámolni. Ekkor a hatványsorba fejtés szerint ($w = 1 - s$)

$$2^w = e^{w \log 2} = 1 + w \log 2 + \dots, \quad 1 - 2^{1-s} = (s-1) \log 2 + \dots,$$

ahol $\dots$ a w -ben, illetve $(s-1)$ -ben legalább másodfokú tagokat jelöli. Egy ilyen reciproka az 1 egy környezetében

$$\frac{1}{(s-1) \log 2} + \text{holomorf}.$$

Szorozva ezt $\eta_2(1) = 1 - 1/2 + 1/3 - 1/4 \pm \dots = \log 2$ -vel, készen vagyunk. $\square$

A $\Re s > 1$ félsíkon a ζ -t előállító sor abszolút konvergencia is minden pontban, amiből nem nehéz belátni, hogy

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

ahol a szorzatban p a prímeken fut végig. Ez a ζ -függvény Euler-féle szorzatalakja.

4.2. A Dirichlet-L-függvények. Legyen χ tetszőleges modulo q karakter. Ekkor definiáljuk az

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

L -függvényt a $\Re s > 1$ tartományon. Abban a speciális esetben, amikor $\chi = \chi_0$,

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} (1 - p^{-s}),$$

ami a ζ szorzatalakjából világos. Az összes többi esetben az $L(s, \chi)$ Dirichlet-sora konvergens $\Re s > 0$ -ra is.

Állítás 12. Ha $\chi \neq \chi_0$, akkor $L(s, \chi)$ Dirichlet-sora konvergens $\Re s > 0$ -ra.

Bizonyítás. Legyen $X(n) = \chi(1) + \dots + \chi(n)$. Ekkor

$$\begin{aligned} \sum_{n=M+1}^N \chi(n)n^{-s} &= \sum_{n=M+1}^N (X(n) - X(n-1))n^{-s} \\ &= \sum_{n=M+1}^N X(n)(n^{-s} - (n+1)^{-s}) - X(M)M^{-s} + X(N)(N+1)^{-s}. \end{aligned}$$

Legyen $\varepsilon > 0$ adott. Ha M elég nagy, az Abel-átrendezett összeg utolsó két tagja abszolút értékben kisebb ε -nál. Mivel $\chi \neq \chi_0$, ezért $|X(n)| \leq q$, így

$$\left| \sum_{n=M+1}^N X(n)(n^{-s} - (n+1)^{-s}) \right| \leq q \sum_{n=M+1}^N (n^{-s} - (n+1)^{-s}) < \varepsilon,$$

ha $s > 0$ valós szám, M -et esetleg még nagyobbra cserélve (pozitív valós s -ekre $\sum_{n=1}^{\infty} (n^{-s} - (n+1)^{-s})$ Leibniz-típusú sor). Azaz az $L(s, \chi)$ -t megadó Dirichlet-sor konvergencia $s > 0$ valós számokra. Mivel a konvergenciataromány félsík, készen vagyunk. $\square$

A $\Re s > 1$ félsíkban a konvergencia abszolút, ezért ekkor is van Euler-szorzat:

$$L(s, \chi) = \prod_{p \nmid q} (1 - \chi(p)p^{-s})^{-1}.$$

Vezessük be a von Mangoldt-féle Λ -függvényt: $\Lambda(n) = 0$, ha n nem prímhatalvány, és $\Lambda(n) = \log p$, ha n a p prímszám hatványa.

Állítás 13. Ha $\Re s > 1$, akkor

$$\frac{L'(s, \chi)}{L(s, \chi)} = - \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s}.$$

Bizonyítás. Felszorozva azt kell belátnunk, hogy

$$L'(s, \chi) = - \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s} \cdot L(s, \chi).$$

A bal oldal egy tipikus tagjában n^{-s} együtthatója (használva a tagonkénti deriválás lehetőségét) $-\chi(n) \log(n)$, a jobb oldalon ugyanez $\sum_{d|n} \chi(d) \Lambda(d) \chi(n/d)$. Azt kell tehát belátnunk, hogy

$$\sum_{d|n} \Lambda(d) = \log n.$$

Ha $n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ a prímtényezős felbontás, akkor világos, hogy mindkét oldal $\alpha_1 \log p_1 + \dots + \alpha_r \log p_r$. $\square$

Könnyű látni, hogy a hányadosként adódó Dirichlet-sor konvergens $\Re s > 1$ -re, így $L(s, \chi) \neq 0$, ha $\Re s > 1$.

5. $L'(s, \chi)/L(s, \chi)$ VISELKEDÉSE $s = 1$ -BEN

5.1. $\chi = \chi_0$. Ebben az esetben $L(s, \chi_0)$ -nak az 1-ben pólusa van, pontosabban

$$L(s, \chi_0) = \frac{\prod_{p|q} (1 - p^{-s})}{s-1} + \text{holomorf}.$$

Ekkor

$$L'(s, \chi_0) = - \frac{\prod_{p|q} (1 - p^{-s})}{(s-1)^2} + \text{holomorf},$$

vagyis a hányados

$$\frac{L'(s, \chi_0)}{L(s, \chi_0)} = - \frac{1}{s-1} + \text{holomorf},$$

amiről tehát látjuk, hogy elsőrendű pólus, $-1/(s-1)$ szingularitással.

5.2. $\chi \neq \chi_0$. Ebben az esetben $L(s, \chi)$ és $L'(s, \chi)$ is holomorf az 1-ben, ha tehát $L(1, \chi) \neq 0$, akkor $L'(s, \chi)/L(s, \chi)$ is holomorf az 1-ben.

Állítás 14. $L(1, \chi) \neq 0$.

Bizonyítás. Tekintsük az $F(s) = \prod_{\chi \in \Xi} L(s, \chi)$ függvényt. A $\Re s > 1$ félsíkon létező Euler-szorzatok szorzata

$$\prod_{p \nmid q} \prod_{\chi \in \Xi} (1 - \chi(p)p^{-s})^{-1}.$$

Rögzítsük $p \nmid q$ -t. A $\chi(p)$ komplex szám $\varphi(q)$. egységgyök, tehát a rendje (a legkisebb pozitív q' , melyre $\chi(p)^{q'} = 1$) osztója $\varphi(q)$ -nak. Válasszunk ki egy olyan χ' -t, amelyre q' maximális, könnyű látni, hogy ekkor minden más χ rendje osztja q' -t. Mivel $1 - x^{q'} = \prod_{j=1}^{q'} (1 - \chi'(p)^j x)$, ezért minden $\chi \in \Xi$ -re

$$\prod_{j=1}^{q'} (1 - \chi'(p)^j \chi(p)p^{-s}) = 1 - \chi(p)^{q'} p^{-q's} = 1 - p^{-q's}.$$

A teljes Ξ felírható $\varphi(q)/q'$ darab diszjunkt halmaz uniójaként, melyek mindegyike $\{\chi' \chi, \chi'^2 \chi, \dots, \chi'^{q'} \chi = \chi\}$ alakú. Összességében tehát a p prímnél az Euler-faktor

$$((1 - p^{-q's})^{-1})^{\varphi(q)/q'} = (1 + p^{-q's} + p^{-2q's} + \dots)^{\varphi(q)/q'}.$$

Ezeket tehát minden $p \nmid q$ -ra összeszorozva

$$\prod_{p \nmid q} \prod_{\chi \in \Xi} (1 - \chi(p)p^{-s})^{-1} = \prod_{p \nmid q} (1 + p^{-q's} + p^{-2q's} + \dots)^{\varphi(q)/q'}$$

nemnegatív tagú Dirichlet-sor, ráadásul $p^{-\varphi(q)s}$ együtthatója minden p -re (ami nem osztja q -t) pozitív egész. Tegyük fel indirekte, hogy valamelyik $L(1, \chi) = 0$. Mivel $L(s, \chi_0)$ pólusa elsőrendű az 1-ben, $F(s)$ holomorf az 1-ben. Ekkor $F(s)$ kiterjed a $\Re s > 0$ félsíkra holomorfan. A Landau-lemma értelmében ekkor az előállító Dirichlet-sor is konvergens a $\Re s > 0$ félsíkon. Ez azonban ellentmondás: $s = 1/\varphi(q)$ -ban a Dirichlet-sor nem lehet konvergens, hiszen a prímek reciprokösszege divergens. $\square$

6. A BIZONYÍTÁS BEFEJEZÉSE

Legyen $(a, q) = 1$, azt kell belátnunk, hogy $p \equiv a \pmod q$ végtelen sok p prímre. Az eddigiek értelmében

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s} = -\frac{L'(s, \chi)}{L(s, \chi)}$$

holomorf az 1-ben, ha $\chi \neq \chi_0$, és $1/(s-1)$ szingularitástól eltekintve holomorf az 1-ben, ha $\chi = \chi_0$.

A karakterekről szóló részben említett átlagolást és az előző rész eredményeit alkalmazva $\Re s > 1$ -re

$$\sum_{n \equiv a \pmod q} \Lambda(n) n^{-s} = \frac{1}{\varphi(q)} \sum_{n=1}^{\infty} \sum_{\chi \in \Xi} \overline{\chi(a)} \chi(n) \Lambda(n) n^{-s} = -\frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \overline{\chi(a)} \frac{L'(s, \chi)}{L(s, \chi)} = \frac{1}{\varphi(q)(s-1)} + \text{holomorf},$$

ahol a 'holomorf' az egész $\Re s > 0$ -ra holomorfan kiterjedő függvényt jelent. Ha tehát most $s \rightarrow 1$ felülről, akkor azt kapjuk, hogy a bal oldal tart a végtelenbe, azaz

$$\sum_{n \equiv a \pmod q} \frac{\Lambda(n)}{n} = \infty.$$

Ez még nem pontosan az, amit szeretnénk, hiszen $\Lambda(n)$ nemcsak a prímeken pozitív, hanem a prímszámhatványokon is. Azonban

$$\sum_{n \equiv a \pmod q} \frac{\Lambda(n)}{n} = \sum_{k=1}^{\infty} \sum_{p^k \equiv a \pmod q} \frac{\log p}{p^k} = \sum_{p \equiv a \pmod q} \frac{\log p}{p} + \sum_{k=2}^{\infty} \sum_{p^k \equiv a \pmod q} \frac{\log p}{p^k}.$$

A jobb oldal második tagjáról könnyű látni, hogy véges, tehát az első végtelen. A kitűzött célnál többet kaptunk: végtelen sok $p \equiv a \pmod q$ prím van, ha $(a, q) = 1$, ráadásként ezek $\log p/p$ összege is végtelen.