Teorem (Dirichlet, 1837)

Neka su $a, N \in \mathbb{N}$ t.d. $(a,N)=1$.

Tada postoji ∞ mnogo prostih brojeva

p t.d. $p \equiv a \pmod N$.

Ideja: Pokazati da je $\displaystyle\sum_{p\equiv a(N)} \frac{1}{p} = +\infty$,

odnosno preciznije, ako definiramo

$$P_a(s) = \sum_{p \equiv a(N)} p^{-s} \quad \text{za} \quad \operatorname{Re} s > 1,$$

$$\lim_{s \to 1^+} P_a(s) = +\infty.$$

Trebat će nam Dirichletovi karakteri.

Def: Dirichletov karakter mod N

je homomorfizam $\left(\mathbb{Z}/_{N\mathbb{Z}}\right)^\times \longrightarrow \mathbb{C}$

red grupe je $\varphi(m)$

$\widehat{\left(\mathbb{Z}/_{N\mathbb{Z}}\right)^\times}$ = grupa svih mod m karaktera

χ proširujemo do mult. funkcije na $\mathbb{Z}$ tako da definiramo $\chi(n) = 0$ (neutr. elem.) ako $(n, N) > 1$. χ_0 = trivijalni karakter

Neka je $1_a(n) = \begin{cases} 1 & \text{ako } n \equiv a \pmod{N} \\ 0 & \text{inače} \end{cases}$.

Lema: Za sve $n \in \mathbb{Z}$

(d.z.)

$$1_a(n) = \sum_{\chi \in \widehat{(\mathbb{Z}/_N\mathbb{Z})^\times}} \frac{\chi(a)^{-1}}{\varphi(N)} \chi(n)$$

odnosno

$$P_a(s) = \sum_{\chi \in \widehat{(\mathbb{Z}/_N\mathbb{Z})^\times}} \frac{\chi(a)^{-1}}{\varphi(N)} \sum_p \frac{\chi(p)}{p^s}$$

Dakle, dovoljno je razumijeti

$$s \longmapsto \sum_p \frac{\chi(p)}{p^s}.$$

Def: Dirichletova L-funkcija

$$L(\chi, s) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

* $L(\chi_0, s)$ je do na Eulerove faktor $p \mid N$ jednako $\zeta(s)$ $\Rightarrow$ ima analitično prošireje do $\mathbb{C}$ s jednostavnim polom u $s=1$

jedinim

* za $\chi \neq \chi_0$ $L(\chi, s)$ je holomorfna na $\mathbb{C}$

"Logaritmiranjem" produkt formule dobivamo

$$\log L(\chi, s) \text{ "}=\text{" } \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right)$$

$$\text{"}=\text{" } \sum_{p,n} \left(\frac{\chi(p)}{p^s}\right)^n \Big/ n$$

Taylorov red od $\log(1-x)$

Preciznije: definiramo funkciju

$$\ell(\chi, s) = \sum_p \sum_n \left(\frac{\chi(p)}{p^s}\right)^n \Big/ n$$

* konvergira apsolutno za $\operatorname{Re} s > 1$ a uniformno za $\operatorname{Re} s \geq 1+\delta$ $(\forall \delta > 0)$

$\Rightarrow \ell(\chi, s)$ je analitička na $\operatorname{Re} s > 1$

Lema: Za $\operatorname{Re} s > 1$ imamo

1. $$e^{\ell(\chi, s)} = L(\chi, s)$$

Uočimo

$$\ell(\chi,s) = \sum_p \frac{\chi(p)}{p^s} + \underbrace{\sum_{n\geq 2}\sum_p \frac{\chi(p)^n}{np^{ns}}}_{R(\chi,s) :=}$$

glavni član (ono što nas zanima)

greška

Važno: Greška $R(\chi,s)$ je ograničena kad $s \to 1$ jer

$$|R(\chi,1)| \leq \sum_{n\geq 2}\sum_p \frac{1}{np^n} \leq \sum_p \sum_{n\geq 2}\left(\frac{1}{p}\right)^n$$

$$\leq \sum_p \frac{1}{p^2}\frac{p}{p-1} < \infty$$

Dakle

$$P_a(s) = \sum_{\chi} \frac{\chi(a)^{-1}}{\varphi(N)} \ell(\chi, s) + O(1)$$

ostatak je ograničen kad $s \to 1$

odnosno ako razdvojimo doprinos trivijalnog karaktera χ_0 od ostalih

$$P_a(s) = \frac{1}{\varphi(N)} \sum_{p \nmid N} p^{-s} + \sum_{\chi \neq \chi_0} \frac{\chi(a)^{-1}}{\varphi(N)} \ell(\chi, s)$$

$$+ O(1)$$

neograničen kad $s \to 1$

jer $\sum_{p \nmid N} \frac{1}{p} = +\infty$ pa je dovoljno pokazati

da je za $\chi \neq \chi_0$ $\ell(\chi, s) = O(1)$ kad $s \to 1$.

Prema Lemi $L(x,s) = e^{\ell(x,s)}$ za $\operatorname{Re} s > 1$

pa imamo

za $x \neq x_0$

$$L(x,1) = \lim_{s \to 1} L(x,s)$$

$$= \lim_{s \to 1} e^{\ell(x,s)}$$

Teorem: Za $x \neq x_0$

$$L(x,1) \neq 0.$$

Lema 2: $\ell(x,s)$ je ograničen kad $s \to 1$ (uz pretp. $L(x,1) \neq 0$)

Osnovna svojstva logaritma impliciraju Lema 1 i Lema 2.

Dokaz Teorema je kompliciraniji.

Def: Dedekindova zeta funkcija

Neka je $K/\mathbb{Q}$ alg. polje brojeva, definiramo

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{(N_{K/\mathbb{Q}}(I))^s}$$

za $\operatorname{Re} s > 1$.

konvergira apsolutno.

Imamo Eulerov produkt

$$\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}} \quad \text{za } \operatorname{Re} s > 1$$

prosti ideali

prsten cijelih

norma

Napomena: analytic class number formula.

broj klasa

regulator

$$\lim_{s \to 0} s^{-r} \zeta_K(s) = -\frac{h(K)\, R(K)}{w(K)}$$

$r = r_1 + r_2 - 1$

$=$ rang grupe jedinica $\mathcal{O}_K^{\times}$

broj korijena iz 1 u K

Nas zanima slučaj kad je $K = \mathbb{Q}(\zeta_N)$

ciklotomska polja
(Webberov teorem – svako
abelovo proširenje od $\mathbb{Q}$
je sadržano u nekom ciklotom
proširenju)

Ključno:

$$\zeta_K(s) = \prod_{\substack{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} \\ \chi \neq \chi_0}} L(\chi, s) \cdot \zeta(s)$$

dovoljno je pokazati da se Eulerovi faktori nad p podudaraju:

$$\prod_{\mathfrak{P} | p} \left(1 - N_{K/\mathbb{Q}}(\mathfrak{P})^{-s}\right) \overset{(*)}{=} \prod_{\chi \neq \chi_0} \left(1 - \chi(p)\, p^{-s}\right) \cdot (1 - p^{-s})$$

$$\| $$

$$\left(1 - p^{-f(p)s}\right)^{\frac{\varphi(N)}{f(p)}}$$

opis faktorizacije od p u $\mathbb{Z}[\zeta_N]$

gdje je $f(p)$ red od p u $(\mathbb{Z}/N\mathbb{Z})^\times$

Za desnu stranu jednakosti $^{(*)}$ koristimo identitet

$$\prod_{\omega \in \mu_{f(p)}} (1-\omega T) = 1 - T^{f(p)}$$

gdje $\mu_{f(p)}$ označava grupu $f(p)$ korijena iz 1. (D.Z.)

Dokaz Teorema $L(\chi,1) \neq 0$: $\chi \neq \chi_0$

Dovoljno je dokazati da $\zeta_K(s)$ ima pol u $s=1$ jer zbog $(*)$ i činjenice da $\zeta(s)$ ima jednostavan pol u $s=1$ bi slijedilo da je $L(\chi,1) \neq 0$ $\forall\, \chi \neq \chi_0$.

Koristit ćemo Landauov teorem iz analize.
(Dedekindova zeta funkcija nam je trebala samo da pokažemo da Dirichl. red $\prod_{\chi \neq \chi_0} L(\chi,s)\,\zeta(s)$ ima ne-negativne koeficijente!)

Teorem (Landau) Neka je

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$ Dirichletov red s nenegativnim

koeficijentima $a_n \geq 0$. Pretpostavimo da

red konvergira za $\operatorname{Re} s > \sigma_0$. Pretpostavimo

da $f(s)$ ima proširenje do holomorfne

funkcije u nekoj okolini točke $s = \sigma_0$.

Tada postoji $\varepsilon > 0$ t.d. red $f(s)$

konvergira za $\operatorname{Re} s > \sigma_0 - \varepsilon$.

Kako je $\zeta_K(s) = \prod_{\chi \neq \chi_0} L(\chi, s) \cdot \zeta(s)$ red s

(koji konvergira za $\operatorname{Re} s > 1$)

ne-negativnim koeficijentima, ako pretpostavimo

da nema pol u $s = 1$ onda ima holom.

proširenje sve do $\operatorname{Re}(s) > 0$ jer sve funkcije

u produktu imaju takvo proširenje. Prema

Landauom teoremu tada i Dirichletov red

od $\zeta_K(s)$ konvergira za $Re(s) > 0$ što

ne može biti jer za $s \in \mathbb{R}^+$

$$\prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \geq \prod_{p} \frac{1}{1 - p^{-\varphi(N)s}}$$

pa ako red konvergira za $s = \frac{1}{\varphi(N)}$

onda i red od $\zeta(s)$ konvergira za $s = 1$

što je kontradikcija.

$\blacksquare$