

1 Dirihleov karakter χ na $\mathbb{Z}$:

$\chi: (\mathbb{Z}/g\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ multiplikativni karakter

Proširimo ga kao funkciju na $\mathbb{Z}$: $\chi: \mathbb{Z} \rightarrow \mathbb{C}$

$$\chi(n) = \begin{cases} \chi(n \bmod g\mathbb{Z}), & \text{za } (n, g) = 1 \\ 0 & , \text{ za } (n, g) > 1 \end{cases}$$

Dirihleova teorema o prostim brojevima u AP a mod g , $(a, g) = 1$:
 $\{a, a+g, a+2g, a+3g, \dots\}$ sadrži beskonačno mnogo prostih brojeva

Dokaz: $AP \ a \pmod{g}$ detekujemo Dirihleovim karakterima mod g :

$$\frac{1}{\varphi(g)} \sum_{\chi \pmod{g}} \chi(n) \bar{\chi}(a) = \begin{cases} 1, & \text{ako } n \equiv a \pmod{g} \\ 0, & \text{inače} \end{cases}$$

$\leadsto$ prelazimo na Dirihleove L-fkce

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}, \quad \operatorname{Re}(s) > 1 \quad \left(\begin{array}{l} \text{imaju meromorfno} \\ \text{proširenje na} \\ \text{celo } \mathbb{C} \rightarrow \text{domaći} \end{array} \right)$$

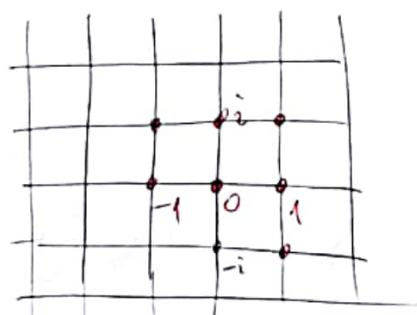
$\leadsto$ ključna komponenta dokaza:

$$L(1, \chi) \neq 0 \quad \text{za netrivijalne karaktere } \chi \neq \chi_0 \pmod{g}$$

Videti: TB, glava 4. $\triangle$

2 Dirihleov karakter χ_1' na $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] / \langle 2+2i \rangle = \{0, 1, -1, i, -i, 1+i, 1-i, -1+i\}$$



$$\begin{aligned} |\mathbb{Z}[i] / \langle 2+2i \rangle| &= N(\langle 2+2i \rangle) = N(\langle 1+i \rangle^3) \\ &= N(\langle 1+i \rangle)^3 = N(1+i)^3 = 8 \end{aligned}$$

Za svaki prost ideal $\mathfrak{p} \leq \mathbb{Z}[i]$ je

$$\psi(\mathfrak{p}^e) = |(\mathbb{Z}[i]/\mathfrak{p}^e)^\times| = N(\mathfrak{p})^e - N(\mathfrak{p})^{e-1}$$

$$|(\mathbb{Z}[i]/\langle 2+2i \rangle)^\times| = |(\mathbb{Z}[i]/\langle 1+i \rangle^3)^\times| = 4$$

$$(\mathbb{Z}[i]/\langle 2+2i \rangle)^\times = \{1, -1, i, -i\}$$

2. χ'_1 - Dirihleov karakter na $\mathbb{Z}[i]$ modulo $\langle 2+2i \rangle = \langle 1+i \rangle^3$

$$\chi'_1: \mathbb{Z}[i] \longrightarrow \mathbb{C}$$

$$\chi'_1(\gamma) = \begin{cases} i^j, & \text{ako } (1+i) \nmid \gamma : i^j \gamma \equiv 1 \pmod{2+2i} \\ 0, & \text{ako } (1+i) \mid \gamma \end{cases}$$

3. Dirihleovi karakteri χ'_n na $\mathbb{Z}[i]$ ($n \in \mathbb{Z}$)

$$\chi'_n: \mathbb{Z}[i] \longrightarrow \mathbb{C}$$

$$N \in \mathbb{D} \cup \mathbb{Z}[i]$$

$$\chi'_n(\gamma) = \begin{cases} \chi'_1(\gamma) \left(\frac{n}{N\gamma} \right), & \text{za } (\gamma, 2n) = 1 \\ 0, & \text{inače} \end{cases}$$

Orde je $N\gamma = \gamma \cdot \bar{\gamma} = |\gamma|^2 \in \mathbb{Z}_{>0}$ neparan prirodan broj
 $\left(\frac{n}{N\gamma} \right)$ je Jacobi-jev simbol koji je za neparne m
 definisan pomoću Legendre-ovih simbola (TB, sek. 7.1)

$$\left(\frac{n}{m} \right) = \left(\frac{n}{p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}} \right) := \left(\frac{n}{p_1} \right)^{e_1} \left(\frac{n}{p_2} \right)^{e_2} \dots \left(\frac{n}{p_r} \right)^{e_r}$$

Zbog multiplikativnosti nazivamo N : definicije Jacobi-jevog simbola
 za $(\gamma_1 \gamma_2, 2n) = 1$ je $\left(\frac{n}{N(\gamma_1 \gamma_2)} \right) = \left(\frac{n}{N(\gamma_1) N(\gamma_2)} \right) = \left(\frac{n}{N(\gamma_1)} \right) \cdot \left(\frac{n}{N(\gamma_2)} \right)$

$\rho = \rho$: $\chi'_n(r_1 r_2) = \chi'_n(r_1) \chi'_n(r_2)$, tj. χ'_n je dobro definisan multiplikativni karakter.

⑤ Neka je χ Dirihleov karakter na $\mathbb{Z}[i]$ modulo ideal α (nastao od nekog karaktera $\chi: (\mathbb{Z}[i]/\alpha)^{\times} \rightarrow \mathbb{C}^{\times}$). Ako je za svaki striktno veći ideal $\mathfrak{b} \supsetneq \alpha$ (tj. $\mathfrak{b} | \alpha$, $\mathfrak{b} \neq \alpha$) karakter χ netrivijalan na podgrupi $\rightarrow (n_j \equiv 1)$

$$K := \{ \gamma \in (\mathbb{Z}[i]/\alpha)^{\times} \mid \gamma \equiv 1 \pmod{\mathfrak{b}} \} \leq (\mathbb{Z}[i]/\alpha)^{\times},$$

onda bismo da je χ primitivan Dirihleov karakter mod α .

(Idealu $\mathfrak{b} \supset \alpha$ odgovara ideal $\mathfrak{b}/\alpha$ količnog prstena $\mathbb{Z}[i]/\alpha$: po teoremi o izomorfizmu za prstene veći (2. ili 3.)

$$\frac{\mathbb{Z}[i]/\alpha}{\mathfrak{b}/\alpha} \cong \mathbb{Z}[i]/\mathfrak{b}$$

odakle imamo i surjektivni homomorfizam multiplikativnih grupa :

$$(\mathbb{Z}[i]/\alpha)^{\times} \longrightarrow (\mathbb{Z}[i]/\mathfrak{b})^{\times}$$

čije jezgra je baš K , pa je $(\mathbb{Z}[i]/\alpha)^{\times}/K \cong (\mathbb{Z}[i]/\mathfrak{b})^{\times}$

Ako bi χ bio trivijalan na K , on bi se faktoriseo

$$(\mathbb{Z}[i]/\alpha)^{\times} \xrightarrow{\chi} \mathbb{C}^{\times} \quad \text{koje ovaj količnik, tj.}$$

bio bi Dirihleov karakter

za manji modul $\mathfrak{b}$ (u smislu deljivosti)

tj. veći ideal $\mathfrak{b}$ (u smislu inkluzije)

$$(\mathbb{Z}[i]/\mathfrak{b})^{\times} \cong (\mathbb{Z}[i]/\alpha)^{\times}/K$$

Primer $a = 36\mathbb{Z} \subset b = 12\mathbb{Z} \subset \mathbb{Z}$

Dirichleov karakter modulo 36 koji nastaje "podizanjem" neke
Dirichleov karaktere modulo 12 nije primitivan modulo 36.

Tvrđenje Preslikavanje $\chi_n': \mathbb{Z}[i] \rightarrow \mathbb{C}$ je primitivni

Dirichleov karakter modulo $(2+2i)n$ - za neparno n ,
 $2n$ - za parno n .

(modulo $2n$ - misli se modulo glavni ideal $\langle 2n \rangle = 2n \cdot \mathbb{Z}[i]$)

▮ n je bezvodan (dovoljno je posmatrati samo kive E_n
za tako n za problem kongruentnih brojeva)

$n = 2^E l_1 l_2 \dots l_t$, $E = 0$ ili 1 , $l_1, \dots, l_t$ - različiti
neparni prosti

• $r \in \mathbb{Z}[i]$, $(r, 2n) = 1 \rightarrow Nr =$ neparan prirodan broj

: to:

$\rightarrow$ ako $p \equiv 3 (4)$ deli Nr , $p \mid Nr = r \cdot \bar{r}$

ali p je prost u $\mathbb{Z}[i] \rightarrow p \mid r$ ili $p \mid \bar{r}$

Ako upr. $p^e \parallel r$, onda : $p^e \parallel \bar{r}$ (samo kongruje
 $r = p^e \cdot r_1$)
 $e \geq 1$

p ukupno $p^{2e} \parallel r \cdot \bar{r} = Nr$

tj. svaki p -ov ulazi u faktORIZACIJU Nr sa parnim exp.

$\rightarrow$ dakle - ako su $p_1, \dots, p_r$ svi različiti prosti koji ulaze
u faktORIZACIJU Nr sa neparnim eksponentom, svi oni
moraju biti $\equiv 1 (4)$

t_j

$$N_8 = \underbrace{p_1 p_2 \dots p_r}_{s_i \equiv 1(4)} \cdot \square \quad - \text{faktoracija u } \mathbb{Z}$$

kvadrat

ovi prosti sa parnim exp. ne utiču na definiciju Jacobijevog simbola

$$\left(\frac{2}{N_8}\right) = \left(\frac{2}{p_1}\right) \left(\frac{2}{p_2}\right) \dots \left(\frac{2}{p_r}\right) = (-1)^{\#(p_i - \text{tara} \equiv 5(8))} = \begin{cases} 1, & N_8 \equiv 1(8) \\ -1, & N_8 \equiv 5(8) \end{cases}$$

Za neparne proste p :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

- zavisi od $p \pmod{8}$

TB, Teorema 7.8

svi p_i su $\equiv 1$ ili $5 \pmod{8}$

$$\left(\frac{2}{p_i}\right) = 1$$

$$\left(\frac{2}{p_i}\right) = -1$$

• Zakon kvadratnog reciprociteta:
 p, q različiti neparni prosti

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

Kujiga, Teorema 7.7

pa je konarno

$$\left(\frac{n}{N_8}\right) = \left(\frac{2^E l_1 l_2 \dots l_t}{N_8}\right) = \left(\frac{2}{N_8}\right)^E \left(\frac{l_1 l_2 \dots l_t}{p_1 p_2 \dots p_r}\right) =$$

$$= \left(\frac{2}{N_8}\right)^E \prod_{\substack{1 \leq k \leq r \\ 1 \leq j \leq t}} \left(\frac{l_j}{p_k}\right) = \left(\frac{2}{N_8}\right)^E \prod_{k,j} \left(\frac{p_k}{l_j}\right)$$

$$= \left(\frac{2}{N_8}\right)^E \left(\frac{p_1 p_2 \dots p_r}{l_1 l_2 \dots l_t}\right) = \left(\frac{2}{N_8}\right)^E \left(\frac{p_1 p_2 \dots p_r \cdot \square}{l_1 l_2 \dots l_t}\right) = \left(\frac{2}{N_8}\right)^E \left(\frac{N_8}{n_0}\right)$$

gde je $n_0 = l_1 l_2 \dots l_t = \begin{cases} n, & \text{ako je } n \text{ neparno} \\ n/2, & \text{ako je } n \text{ parno} \end{cases}$

(1)

• Dokažemo tvrđenje za n neparno (n parno - slično)

• χ_n' je dobro definirano modulo $(2+2i)n$:

ako su $\gamma_1, \gamma_2 \in \mathbb{Z}[i]$, $\gamma_2 = \gamma_1 + (2+2i)n\beta$, $\text{za neko } \beta \in \mathbb{Z}[i]$

$$\rightarrow \gamma_1 \equiv \gamma_2 \pmod{(2+2i)n} \text{ pa je } \chi_n'(\gamma_1) = \chi_n'(\gamma_2)$$

$$\begin{aligned} \rightarrow N\gamma_2 &= (\gamma_1 + (2+2i)n\beta)(\bar{\gamma}_1 + (2-2i)n\bar{\beta}) \\ &\equiv \gamma_1\bar{\gamma}_1 = N\gamma_1 \pmod{n} \end{aligned} \quad (2)$$

a tako je iz (1)

$$\left(\frac{n}{N\gamma_1}\right) = \left(\frac{N\gamma_1}{n}\right) \quad (3)$$

sledi da su i Jacobi-ovi simboli isti:

$$\left(\frac{n}{N\gamma_1}\right) \stackrel{(1)}{=} \left(\frac{N\gamma_1}{n}\right) \stackrel{(2)}{=} \left(\frac{N\gamma_2}{n}\right) \stackrel{(1)}{=} \left(\frac{n}{N\gamma_2}\right)$$

pa sledi: $\chi_n'(\gamma_1) = \chi_n'(\gamma_2)$

• Dokažimo da je χ_n' primitivan karakter - tj. da ne postoji pravi delitelj $h \mid \langle (2+2i)n \rangle$ takav da $\chi_n'(r)$ zavisi samo od $r \pmod{h}$. Ekvivalentno, da za h karakter χ_n' nije $\equiv 1$ na $K = \{r \equiv 1 \pmod{h}\}$.

$\rightarrow$ Pretpostavimo suprotno, da χ_n' nije primitivan.

$\langle (2+2i)n \rangle = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}$ faktORIZACIJA ideala na proste ideale (jedinstvena) TB 6.45

Dakle postoji prost ideal q ($= q_j$ za neko $1 \leq j \leq r$) takav da je za $h := \frac{\langle (2+2i)n \rangle}{q}$ - pravi delitelj $\langle (2+2i)n \rangle$

— 4 —

$$\chi_n'(r) = 1 \quad \text{za sve } r \equiv 1 \pmod{h}.$$

Razmotrimo slučajeve:

$$(1) \quad \mathcal{Q} = \langle 1+i \rangle, \rightarrow h = \frac{\langle (2+2i)n \rangle}{\mathcal{Q}} = \langle 2n \rangle = 2n \cdot \mathbb{Z}[i]$$

$$r = 1 + 2n \underset{\substack{\uparrow \\ \mathbb{Z}[i]}}{\beta} \in K, \quad \text{za sve } r \in \mathbb{Z}[i]:$$

$$Nr = (1+2n\beta)(1+2n\bar{\beta}) = 1 + 4n \operatorname{Re}(\beta) + 4n^2 |\beta|^2 \equiv 1 \pmod{n} \quad \uparrow \mathbb{Z}$$

$p \neq j^2$

$$\begin{aligned} \chi_n'(r) &= \chi_1'(r) \left(\frac{n}{Nr} \right) \stackrel{(3)}{=} \chi_1'(r) \left(\frac{Nr}{n} \right) = \chi_1'(r) \left(\frac{1}{n} \right) = \chi_1'(r) \\ &= \chi_1'(1+2n\beta) = \chi_1'(1+2\beta + 4n_1\beta) = \chi_1'(1+2\beta) \end{aligned}$$

$$n = 2n_1 + 1 \quad \text{neparno}$$

$\uparrow$ delimo sa $(2+2i) = \text{gen} \chi_1'$

Ali npr. za $\beta = i$ je $1+2\beta = 1+2i = -1 + (2+2i), \quad p \neq j^2$

$$\chi_1'(1+2i) = -1 \neq 1 \quad \text{⚡}$$

$$(2) \quad \mathcal{Q} = \langle a+bi \rangle, \quad \text{gde } (a+bi)(a-bi) = l \equiv 1 \pmod{4}$$

(l je jedan od prostih delioca $l_1, l_2, \dots, l_t$ od n)

$$\rightarrow h = \frac{\langle (2+2i) l \frac{n}{l} \rangle}{\langle a+bi \rangle} = \langle (2+2i)(a-bi) \frac{n}{l} \rangle$$

$$r = 1 + (2+2i)(a-bi) \underset{\substack{\uparrow \\ \mathbb{Z}[i]}}{\frac{n}{l}} \cdot \beta \in K$$

Dodatno, potražimo kontraprimer za vrednosti $\beta = k(1-i), \quad k \in \mathbb{Z}$

tg. za r oblika

$$r = 1 + 4(a-bi) \frac{n}{l} \cdot k, \quad k \in \mathbb{Z}$$

Svakega je $r \equiv 1 \pmod{2+2i}$ pa je $\chi'_1(r) = 1$
 $\pmod{(1+i)^3}$

$$\begin{aligned}Nr &= \left(1 + 4 \frac{nk}{l} (a-bi)\right) \left(1 + 4 \frac{nk}{l} (a+bi)\right) \\&= 1 + 8ak \frac{n}{l} + 16k^2 \frac{n}{l} \cdot \frac{n}{l} \cdot \cancel{x} \\&\equiv 1 + 8ak \frac{n}{l} \pmod{n}\end{aligned}$$

i dobijamo

$$\chi'_n(r) = \left(\frac{n}{Nr}\right) = \left(\frac{Nr}{n}\right) = \left(\frac{1 + \frac{8an}{l}k}{n}\right) = \left(\frac{1 + \frac{8an}{l}k}{l_1 l_2 \dots l_t}\right)$$

(za sve $l_j \neq l$, $l_j \mid \frac{n}{l}$ i najmanje Legendre-ovog simb. je 1)

$$= \left(\frac{1 + \frac{8an}{l}k}{l}\right)$$

$\left(a^2 + b^2 = l \rightarrow (a, l) = 1, \quad l \text{ neparan, } \left(\frac{n}{l}, l\right) = 1 \right) \Rightarrow \left(\frac{8an}{l}, l\right) = 1$ ^{kvadrati}

$\rightarrow 1 + \frac{8an}{l}k$ prolazi kroz sve klase ostataka mod l , kad k šeta

Izaberimo $k \in \mathbb{Z}$ za koje je $1 + \frac{8an}{l}k$ kvadratni neostatak mod l . Za takvo k je

$$\chi'_n(r) = -1 \neq 1$$


$$(3) \quad \mathfrak{q} = \langle \ell \rangle, \quad \ell \equiv 3 \pmod{4}$$

$$\rightarrow h = \frac{\langle (2+2i)^n \rangle}{\langle \ell \rangle} = \langle (2+2i)^{\frac{n}{\ell}} \rangle$$

$$\gamma = 1 + (2+2i)^{\frac{n}{\ell}} \prod_{\substack{\mathfrak{p} \\ \mathbb{Z}[i]}} \in K$$

$$\equiv 1 \pmod{2+2i} \rightarrow \chi'_1(\gamma) = 1$$

$$\text{pa je} \quad \chi'_n(\gamma) = \left(\frac{Nr}{n} \right) = \left(\frac{Nr}{\ell} \right) \quad \text{jer je} \quad Nr \equiv 1 \pmod{\frac{n}{\ell}}$$

$$\left((2+2i)^{\frac{n}{\ell}}, \ell \right) = 1 \quad (Nr \in \mathbb{Z} \text{ u } \mathbb{Z}[i]) \text{ (opet jer je } n \text{ bez kvadrata)}$$

$\rightarrow$ slično kao u prethodnom slučaju

$$1 + (2+2i)^{\frac{n}{\ell}} \cdot \beta \quad \text{proba s} \quad \text{svim ostacima modulo } \mathfrak{q} = \langle \ell \rangle$$

(3)

U ovom slučaju je

$$\mathbb{Z}[i]/\mathfrak{q} \cong \mathbb{F}_{\ell^2}$$

Za ove $\ell \equiv 3 \pmod{4}$, -1 nije kvadrat u $\mathbb{F}_{\ell}$ tj.

t^2+1 je nerastavljiv polinom u $\mathbb{F}_{\ell}[t]$ pa je

$$\mathbb{F}_{\ell^2} \cong \mathbb{F}_{\ell}[t]/\langle t^2+1 \rangle = \{a+b\sqrt{-1} \mid a,b \in \mathbb{F}_{\ell}\}$$

gde je $\sqrt{-1} = t + \langle t^2+1 \rangle$

Isomorfizam je onda eksplisito zadan sa

$$\begin{array}{ccc}
 \mathbb{Z}[i]/\mathfrak{q} & \xrightarrow{\cong} & \mathbb{F}_{\ell^2} \\
 \uparrow & & \uparrow \\
 (a+bi)+\mathfrak{q} & \longmapsto & a+b\sqrt{-1} \\
 \downarrow & & \downarrow \\
 \mathbb{Z}/\ell\mathbb{Z} & \xrightarrow{\cong} & \mathbb{F}_{\ell}
 \end{array}$$

(gde su na desnoj strani:
 a i b u strani
 $a(\bmod \ell)$; $b(\bmod \ell) \in \mathbb{F}_{\ell}$)

Imamo 2 norme:

- normu na prstenima $\mathbb{N}: \mathbb{Z}[i] \rightarrow \mathbb{Z}$, $\mathbb{N}(a+bi) = (a+bi)(a-bi)$
 koja indukuje i preslikavanje na količnicima:
 $(a+bi)+\mathfrak{q} \mapsto \mathbb{N}(a+bi) + \ell\mathbb{Z}$ (1)

- normu na konačnim poljima (koju smo već koristili!)

$$\mathbb{N}: \mathbb{F}_{\ell^2} \rightarrow \mathbb{F}_{\ell}$$

$$\mathbb{N}(x) = \prod_{\sigma \in \text{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_{\ell})} \sigma(x) = \text{id}(x) \cdot \sigma_{\text{Fr}}(x) = x \cdot x^{\ell}$$

$$\begin{aligned}
 \mathbb{N}(a+b\sqrt{-1}) &= (a+b\sqrt{-1})(a+b\sqrt{-1})^{\ell} \stackrel{\text{char}=\ell}{=} (a+b\sqrt{-1})(a^{\ell}+b^{\ell}\sqrt{-1}^{\ell}) \\
 &= \underline{(a+b\sqrt{-1})(a-b\sqrt{-1})} \quad (2)
 \end{aligned}$$

$$\left(a^{\ell} = a, b^{\ell} = b \text{ (Mala Fermova t.)}, \sqrt{-1}^{\ell} = \sqrt{-1}^3 = -\sqrt{-1} \right)_{\ell \equiv 3(4)}$$

Jednako: (1) ; (2) nam kažu da su 2 norme
 kompatibilne, tj. da gornji dijagram komutira!

- Medutim N na konacnim poljima je surjektiva!

Npr. ako je g generator multiplikativne grupe $\mathbb{F}_l^*$
onda je

$$N(g) = g \cdot G_{Fr}(g) = g \cdot g^l = g^{l+1}$$

element multiplikativne grupe $\mathbb{F}_l^*$ reda $\frac{|\mathbb{F}_l^*|}{l+1} = \frac{l-1}{l+1} = l-1$

pa je $N(g)$ baš generator grupe $\mathbb{F}_l^*$

- Doble i norma N na levoj strani je surjektiva,

pa postoji neki ~~x~~ ostatak $y+q \in \mathbb{Z}[i]/q$

koga N slika u neostatak u $\mathbb{F}_l$ tj. $\left(\frac{N\cancel{x}}{l}\right) = -1$.

Zbog zadržke (3), $\exists x = 1 + (2+2i)\frac{n}{l}\beta \equiv y \pmod{q}$

pa je za takvo x

$$\chi'_n(x) = \left(\frac{N\cancel{x}}{l}\right) = \left(\frac{Ny}{l}\right) = -1 \quad \swarrow$$

