

Zeta funkcije varijeteta

[1] p -prost broj
 $\mathbb{F}_p$ - konačno polje sa p elemenata ($\cong \mathbb{Z}/p\mathbb{Z}$)
 $q = p^r$, $r \geq 1$
 $\mathbb{F}_q$ - konačno polje sa q elemenata
 $\cong \mathbb{F}_p[t] / \langle f(t) \rangle$, $f(t) \in \mathbb{F}_p[t]$ ireducibilan polinom stepena r
 $f(t) \mid t^{p^r} - t$
za sve $d \geq 1$ je $\mathbb{F}_{q^d} / \mathbb{F}_q$ Galuovo proširenje:

$$\text{Gal}(\mathbb{F}_{q^d} / \mathbb{F}_q) = \left\{ \phi: \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_{q^d} \right\} = \text{ciklična reda } d$$
$$\left| \begin{array}{ccc} \mathbb{F}_{q^d} & \xrightarrow{\phi} & \mathbb{F}_{q^d} \\ \downarrow & & \downarrow \\ \mathbb{F}_q & \xrightarrow{\phi_{Fr}} & \mathbb{F}_q \end{array} \right. = \langle \phi_{Fr}: x \mapsto x^q \rangle$$

[2] K polje
 K'/K proširenje polja
 $A_{K'}^m = \{ (x_1, \dots, x_m) : x_i \in K' \}$ afini prostor
• $f_j \in K[X_1, \dots, X_m]$, $j=1, 2, \dots, J$ polinomi
 $V = \{ (x_1, \dots, x_m) \in A_{K'}^m \mid f_j(x_1, \dots, x_m) = 0, j=1, 2, \dots, J \} \subseteq A_{K'}^m$
- afini algebarski varijetet u m -dim. afnom prostoru
f. $V = V(K')$ njegov skup K' tačaka

- Ako su $f_j(x_0, x_1, \dots, x_m)$ homogeni polinomi u $K[x_0, \dots, x_m]$ za sve $1 \leq j \leq J$ onda je

$$V := \{(x_0, x_1, \dots, x_m) \in \mathbb{P}_{K'}^m \mid f_j(x_0, x_1, \dots, x_m) = 0, j=1, 2, \dots, J\} \subseteq \mathbb{P}_{K'}^m$$

- projektni varijetet u m -dim. projektnom prostoru
(tj. npr. skup $V = V(K')$ K' -tačka)

3) ② V - afini ili projektni varijetet definisan nad $\mathbb{F}_2$

$$N_r := \# V(\mathbb{F}_{2^r}), \quad r=1, 2, 3, \dots$$

Zeta funkcija varijeteta V je formalni stepeni red

$$Z(V/\mathbb{F}_2, T) := \exp\left(\sum_{r=1}^{\infty} \frac{\# V(\mathbb{F}_{2^r})}{r} T^r\right)$$

$$\exp(u) = \sum_{k=0}^{\infty} \frac{u^k}{k!}$$

Weil-ove hipoteze (1949.)

① $Z(V/\mathbb{F}_2, T)$ je racionalna fka po T

(Npr. za glatke krive je oblika

$$\frac{P(T)}{(1-T)(1-2T)}, \quad \text{gde je } P(T) \in \mathbb{Z}[T] : P(0)=1)$$

② Ali je $V/\mathbb{F}_p$ dobrišen "redukirani mod p "
varieteta $\tilde{V}/\mathbb{Q}$ (koeficiente polinoma f redukujemo
mod p) onda je

$$\deg P = 2g, \quad \text{gde je } g = \text{rod kompleksne analitične mnogostvornosti } \tilde{V}(\mathbb{C})$$

③ Ali je α recipročni koren broja $P(T)$, $(= \prod_{\alpha} (1 - \alpha T))$
onda je to: $\frac{g}{\alpha}$

④ Svi recipročni koreni broja $P(T)$ imajo
kompleksnu absolutnu vrednost $\sqrt{g}$.

• Najteži del je ④ - dokaz ga je Deligne, 1973.
(④ je "Rimanova hipoteza" za ove zeta funkcije
nad končnim poljima! Videvemo kasneje zašto...)

1

$$|E_n(\mathbb{F}_2)|$$

- 1 -

Tvrđenje 1

n beskonačan prirodan broj
 $p \nmid 2n$

$q = p^r$, $\mathbb{F}_2$ - binarno polje

$$E_n: y^2 = x^3 - n^2 x$$

- eliptička kriva nad $\mathbb{F}_p$
(glatka, jer $p \nmid 2n$)

Ako je $q \equiv 3 \pmod{4}$, onda je $|E_n(\mathbb{F}_2)| = q + 1$

Imamo tačku u beskonačnosti: $O = (0, 1, 0) \in \mathbb{P}_{\mathbb{F}_2}^2$

3 tačke reda 2: u grupi $E(\mathbb{F}_2)$:

$$(0, 0), (n, 0), (-n, 0).$$

• Neka je sada $x \neq 0, n, -n$ (tj. $y \neq 0$ i (x, y) u afinoj ravni)
 $q-3$ takvih x -ova - podelimo ih u parove $\{x, -x\}$

$$|\mathbb{F}_2^x| / (\mathbb{F}_2^x)^2 = 2$$

↑
podgrupa kvadrata

-1 nije kvadrat u $\mathbb{F}_2$

(ako bi bio, $\exists a \in \mathbb{F}_2^x$:
 $a^2 = -1 \rightarrow a^4 = 1 \rightarrow$
 $4 \mid |\mathbb{F}_2^x| = q-1 \nmid$)

$$f(x) = x^3 - n^2 x$$

$$f(-x) = (-x)^3 - n^2(-x) = (-1)f(x)$$

Dakle, od dve vrednosti $f(x)$, $f(-x)$, tačno jedna je kvadrat u polju $\mathbb{F}_2$, a druga nije (pa ne može rešavati $y^2 = f(x)$)

Ona koja jeste, upr. se, daje tačno 2 rešenja:

$$(x, \sqrt{f(x)}), (x, -\sqrt{f(x)}).$$

Dakle, $\frac{g-3}{2}$ parova daje ukupno $g-3$ tačaka.

Još one 4... 

[2] [?] Ako je $g \equiv 1 (4)$ ono 'ne radi'... Nadajte: $g \equiv 1 (4)$

• Posmatrajmo pomoćnu krivu (i dajte $p \nmid 2n$)

$$\boxed{E_n' : u^2 = v^4 + 4n^2} \quad (1)$$

- Ako je $(u, v) \in E_n'(\mathbb{F}_2)$, onda je

$$(x, y) = \left(\frac{1}{2}(u+v^2), \frac{1}{2}v(u+v^2) \right) \stackrel{=:\phi(u,v)}{\in} E_n(\mathbb{F}_2)$$

$$\left(\frac{1}{2} = 2^{-1} \text{ u polju } \mathbb{F}_2 \right)$$

- Ako je $(x, y) \in E_n$, $x \neq 0$ (tj. $(x, y) \neq (0, 0)$)
onda je

$$(u, v) = \psi(x, y) := \left(2x - \frac{y^2}{x^2}, \frac{y}{x} \right) \in E_n'(\mathbb{F}_2)$$

Dakle, proverite da su $\phi; \psi$ međusobno inverzna preslikavanja

$$E_n'(\mathbb{F}_2) \xrightleftharpoons[\psi]{\phi} E_n(\mathbb{F}_2) \setminus \{(0, 0)\} \quad \text{bijekcija}$$

$$N' := \# \left\{ (u, v) \in \mathbb{F}_2^2 \mid u^2 = v^4 + 4n^2 \right\} = \# \text{ afin. tačaka na } E_n'(\mathbb{F}_2)$$

Onda je

$$\# E_n(\mathbb{F}_2) = N' + 1 + 1 = N' + 2$$

↓
baza (1,0) 0

Ideja za ovaj trik: jednačina krive E_n je u dijagonalnom obliku - svaki monom sadrži tačno 1 promenljivu, i svaka promenljiva se pojavljuje u najviše 1 monomu.

- "razdvojene promenljive"

- olakšava ono što sledi (a što je 'harmonijska analiza' na konačnom polju $\mathbb{F}_2$)

3 Karakteri

$$\psi: \mathbb{F}_2 \longrightarrow \mathbb{C}^\times$$

trivijalan: ako sve ide u 1

netrivijalni: aditivni karakter
↓
 $\mathbb{Z}(\mathbb{F}_2, +)$ homomorfizam
u $(\mathbb{C}^\times, \cdot)$

$$(U stvari, \text{im}(\psi) \subseteq \mu_2 \subseteq \mathbb{C}^\times)$$

↳ grupa 2-tih korena iz 1

Dovoljno je da fixiramo jedan takav karakter; npr.

$$\text{Tr}: \mathbb{F}_2 \longrightarrow \mathbb{F}_p$$

$$\text{Tr}(x) = \sum_{\sigma \in \text{Gal}(\mathbb{F}_2/\mathbb{F}_p)} \sigma(x) = \sum_{m=0}^{r-1} \sigma_{\text{Frob}}^m(x) = \sum_{m=0}^{r-1} x^{p^m}$$

ova vrednost je očigledno $\text{Gal}(\mathbb{F}_2/\mathbb{F}_p)$ -invariantna, pa mora

prigledati: $\mathbb{F}_2^{\text{Gal}(\mathbb{F}_2/\mathbb{F}_p)} = \mathbb{F}_p$

Tr je netrivialno aditivno preslikovanje: $\text{im}(Tr) = \mathbb{F}_p$ p -se

$$\psi(x) := e^{\frac{2\pi i \text{Tr}(x)}{p}}$$

primer netrivialnog aditivnog
karaktera $\mathbb{F}_2 \rightarrow \mathbb{C}^\times$

• $\chi: \mathbb{F}_2^\times \rightarrow \mathbb{C}^\times$

multiplikativni karakter
↓
iz grupe $(\mathbb{F}_2^\times, \cdot)$
↓
homomorfizam $\mathbb{C}^\times$

(aditivni smo fibrali, a multiplikativni χ ce da se menjaju)

Dodefnisacemo: $\chi(0) := 0$ za sve multiplikativne karaktere
↓
nije u $\mathbb{C}^\times$!

Oznaka: χ_0 - trivialni karakter

$$\chi_0(x) = \begin{cases} 1, & x \in \mathbb{F}_2^\times \\ 0, & x=0 \end{cases}$$

Oznaka: $\bar{\chi}: \bar{\chi}(x) = \overline{\chi(x)}, \forall x$

② Gauss-ova suma: za multiplikativni karakter χ na $\mathbb{F}_2^\times$

$$g(\chi) := \sum_{x \in \mathbb{F}_2} \chi(x) \psi(x)$$

"Feynman-ova
transformacija
karaktera χ "

Jacobi-jeva suma za 2 multiplikativna karaktera χ_1, χ_2

$$J(\chi_1, \chi_2) := \sum_{x \in \mathbb{F}_2} \chi_1(x) \chi_2(1-x)$$

"aditivna
konvolucija
 χ_1, χ_2 "