

Tworzę 2 [Ogólna notacja Gauss-ów : Jacobson's sum]

χ, χ_1, χ_2 nietrywialni
multiplikacyjni
charaktery na $\mathbb{F}_2$

1) $g(\chi_0) = -1$

2) $J(\chi_0, \chi_0) = q^{-2}$, $J(\chi_0, \chi) = -1$

3) $J(\chi, \bar{\chi}) = -\chi(-1)$

4) $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$

5) $g(\chi) g(\bar{\chi}) = \chi(-1) q$, $|g(\chi)| = \sqrt{q}$

6) $J(\chi_1, \chi_2) = \frac{g(\chi_1) g(\chi_2)}{g(\chi_1 \chi_2)}$ albo je $\chi_2 \neq \bar{\chi}_1$

Do baz $\rightarrow$ domaći zadani

[4] (L.3) Za swako $a \in \mathbb{F}_2 \setminus \{0\}$: swako $m \mid (q-1) = |\mathbb{F}_2^\times|$
brój rešenja $x \in \mathbb{F}_2$ jednačine $x^m = a$ je dat sa

$$\#\{x \in \mathbb{F}_2 \mid x^m = a\} = \sum_{\chi^m = \chi_0} \chi(a)$$

- suma po svim
multiplikativnim
karakterima grupe $\mathbb{F}_2^\times$
za koje je $\chi^m = \chi_0$

- Svi multiplikativni karakteri grupe $\mathbb{F}_2^\times$ čine grupu (u odnosu na množenje karaktera) . Ovo je dualna grupa $\widehat{\mathbb{F}_2^\times}$ koja je izomorfnja sa $\mathbb{F}_2^\times$ (Teorema 1.24, str. 17, knjiga TB)
- Multiplikativna grupa $\mathbb{F}_2^\times$ konačnog stepena je ciklična, pa je onda i $\widehat{\mathbb{F}_2^\times}$ takode ciklična.

$G \leq \mathbb{F}_2^x$ podgrupa svih m -tih stepena u grupi $\mathbb{F}_2^x$

$$G = \{x^m \mid x \in \mathbb{F}_2^x\} \quad |\mathbb{F}_2^x/G| = m$$

$K \leq \widehat{\mathbb{F}_2^x}$ (jedinstvena) podgrupa reda m

$$K = \{x \in \widehat{\mathbb{F}_2^x} \mid x^m = x_0\} \quad \text{— pa je jedna strana u stvari suma po ovoj podgrupi } \sum_{x \in K}$$

Lako se proverava da je K dualna podgrupa grupe $\mathbb{F}_2^x/G$

tj. $\widehat{\mathbb{F}_2^x/G} \cong K$, pa se iz ortogonalnosti karaktera (Teorema 1.24, formula (1.11), knjige TB)

$$\sum_{x^m = x_0} \chi(a) = \sum_{x \in K} \chi(a) = \begin{cases} m = |\mathbb{F}_2^x/G| = |K|, & \text{ako } a \in G \\ 0 & \text{tj. } aG = G \text{ je neutral u } \mathbb{F}_2^x/G \\ & \text{, ako } a \notin G \end{cases}$$

$$\text{a leva strana} = \begin{cases} 0, & \text{ako } a \text{ nije } m\text{-ti stepen} \\ m, & \text{ako } a \text{ jeste } m\text{-ti stepen} \end{cases}$$

$x_0^m = a$ jedno rešenje; $\langle y_0 \rangle \leq \mathbb{F}_2^x$ ciklična podgrupa reda m

→ sva rešenja su $\{x_0, x_0 y_0, x_0 y_0^2, \dots, x_0 y_0^{m-1}\}$



• Sada se vratimo na prebrojavanje N' — broja rešenja na (1) u $\mathbb{F}_2^x \times \mathbb{F}_2$:

$$N' = \#\{u \in \mathbb{F}_2 \mid u^2 = 4n^2\} + \#\{v \in \mathbb{F}_2 \mid 0 = v^4 + 4n^2\} + \#\{u, v \in \mathbb{F}_2^x \mid u^2 = v^4 + 4n^2\} \quad (2)$$

-4-

- (L3), $p \nmid 2n$, pa $2n \neq 0 \in \mathbb{F}_2 (\supseteq \mathbb{F}_p)$

$$u^2 = (2n)^2 \leftarrow \text{ova j-na ima po (L3) tačno 2 rešenja}$$

- Kako je $g \equiv 1 \pmod{4}$ tj. $4 \mid g-1$,

u grupi $\widehat{\mathbb{F}_2^*}$ postoji bar 1 karakter tačnog reda 4.

Označimo (i fixirajmo) taj karakter sa $\chi_4 : \mathbb{F}_2^* \rightarrow \mathbb{C}^*$

(Npr. ako je $\langle g \rangle = \mathbb{F}_2^*$, onda je sa $\chi_4(g) = i (= \sqrt{-1})$ definisan takav karakter tačnog reda 4)

Onda je # 2. skupa u (2) prema (L3) za $v^4 = -4n^2$ data sa

$$\sum_{\chi^4 = \chi_0} \chi(-4n^2) = \sum_{j=0}^3 \chi_4^j(-4n^2) \stackrel{*}{=} 2 + 2\chi_4(-4n^2)$$

$$K = \langle \chi_4 \rangle = \{ \chi_0, \chi_4, \chi_4^2, \chi_4^3 \}$$

: $\left[\begin{array}{l} -1 \in \mathbb{F}_2^ \text{ je kvadrat (Ako je } b \in \mathbb{F}_2^* \text{ tačnog reda 4, mora biti } b^2 = -1) \\ \text{pa je} \end{array} \right.$

$$\chi_4^2(-4n^2) = \chi_4^2(b^2 \cdot 4n^2) = \chi_4^4(2bn) = 1$$

- Kardinalnost 3. skupa u (2):

$$= \sum_{\substack{a, b \in \mathbb{F}_2^* \\ a = b + 4n^2}} \# \{ u^2 = a \} \cdot \# \{ v^4 = b \} =$$

$$\stackrel{\textcircled{L3}}{=} \sum_{\substack{a \in \mathbb{F}_2^* \\ a-4n^2 \neq 0}} \sum_{k=0}^1 \chi_2^k(a) \sum_{j=0}^3 \chi_4^j(a-4n^2)$$

gde je $\chi_2 := \chi_4^2$ - netrivijski karakter $\mathbb{F}_2^*$ reda 2

- Zbog konvergence da je $\chi_4(0) = 0$, možemo da izbrisemo uslov $a-4n^2 \neq 0$

- Smena promenljive $\mathbb{F}_2^* \rightarrow \mathbb{F}_2^*$ - bijekcija (jer $p \neq 2n$)
 $a \mapsto x := \frac{a}{4n^2}$

$$= \sum_{x \in \mathbb{F}_2^*} \sum_{k=0,1} \chi_2^k(4n^2 x) \sum_{j=0}^3 \chi_4^j(4n^2 x - 4n^2)$$

$$= \sum_{k=0,1} \sum_{j=0}^3 \chi_4^j(-4n^2) \sum_{x \in \mathbb{F}_2^*} \chi_2^k(x) \chi_4^j(1-x)$$

$$= \sum_{k=0,1} \sum_{j=0}^3 \chi_4^j(-4n^2) \mathcal{J}(\chi_2^k, \chi_4^j)$$

$$= \mathcal{J}(\chi_0, \chi_0) + \chi_4(-4n^2) \mathcal{J}(\chi_0, \chi_4) + \chi_2(-4n^2) \mathcal{J}(\chi_0, \chi_2) + \chi_4^3(-4n^2) \mathcal{J}(\chi_0, \chi_4^3)$$

$$+ \mathcal{J}(\chi_2, \chi_0) + \chi_4(-4n^2) \mathcal{J}(\chi_2, \chi_4) + \chi_2(-4n^2) \mathcal{J}(\chi_2, \chi_2) + \chi_4^3(-4n^2) \mathcal{J}(\chi_2, \chi_4^3)$$

Twd. 2
↓

-5-

$$= (g-2) + x_4(-4n^2)(-1) + (-1) + x_4^3(-4n^2)(-1)$$

$$+ (-1) + x_4(-4n^2) J(x_2, x_4) + J(x_2, x_2) + x_4^3(-4n^2) J(x_2, x_4^3)$$

$$\begin{aligned} & \left(x_2 = \bar{x}_2 = x_2^{-1} \right) \\ & \text{2.3)} \quad = -x_2(-1) \\ & \quad \quad \quad \uparrow \\ & \quad \quad \text{kvadrat} \\ & \quad \quad = -1 \end{aligned}$$

$$\begin{aligned} & \downarrow \\ & = x_4(-4n^2) \\ & \text{(jer je } -4n^2 = \text{kvadrat)} \end{aligned}$$

$$= g-5 - 2x_4(-4n^2) + x_4(-4n^2) \left(J(x_2, x_4) + J(x_2, \bar{x}_4) \right)$$

što sve zajedno daje

$$N' = g-1 + \cancel{x_4(-4n^2)} + x_4(-4n^2) \left(J(x_2, x_4) + J(x_2, \bar{x}_4) \right)$$

(L.4) Za sve $g \equiv 1(4)$ je $x_4(-4) = 1$.

• Neka je $g \equiv 1(8)$; neka je $c \in \mathbb{F}_8^\times$ tačnog reda 8
 $c^8 = 1 \rightarrow c^4 = -1 \rightarrow x_4(-1) = x_4(c^4) = x_4(c)^4 = 1$

$$c^6 = c^4 \cdot c^2 = -c^2$$

$$(c+c^{-1})^2 = c^2 + c^{-2} + 2 = c^2 + c^6 + 2 = c^2 - c^2 + 2 = 2 \rightarrow$$

$$x_4(4) = x_4(2)^2 = x_4((c+c^{-1})^2)^2 = x_4(c+c^{-1})^4 = 1$$

• Sličaj $g \equiv 5(8)$ - dokažite da je $x_4(-1) = -1 = x_4(4)$

za domaći 

Dakle $\chi_4(-4n^2) = \chi_4(n^2) = \chi_4(n)^2 = \chi_2(n)$

Tvrđnja 5 Ako je $g \equiv 1 \pmod{4}$ i $p \nmid 2n$, onda je

$$\# E_n(\mathbb{F}_g) = g + 1 + \chi_2(n) \left(J(\chi_2, \chi_4) + J(\chi_2, \bar{\chi}_4) \right)$$

$$\# E_n(\mathbb{F}_g) = g + 1 - \alpha - \bar{\alpha}$$

gde je $\alpha = \alpha_{n,g} := -\chi_2(n) J(\chi_2, \chi_4)$

5 Hoćemo malo eksplicitnije da odredimo broj α

$$J(\chi_2, \chi_4) = \sum_{x \in \mathbb{F}_g} \underbrace{\chi_2(x)}_{\pm 1} \underbrace{\chi_4(1-x)}_{\in \{\pm 1, \pm i\}} \in \mathbb{Z}[i] \text{ - prsten celih } \mathbb{Q}(i) \text{ (kujiza TB, sekija 9.1)}$$

pa je i

$$\alpha \in \mathbb{Z}[i] \quad \alpha = a + bi, \quad a, b \in \mathbb{Z} \quad (\text{ovo } b \text{ nema veze sa prethodnim})$$

12 Tv. 2(6): $\alpha = -\chi_2(n) \frac{g(\chi_2)g(\chi_4)}{g(\bar{\chi}_4)}$

Tv. 2(5) $|\alpha| = \sqrt{g}$ tj. $|\alpha|^2 = a^2 + b^2 = g$

• Faktorizacija u $\mathbb{Z}[i]$ na prste faktore (videti: enastava.matf.bg.ac.rs/~dj.)
 $\Rightarrow$

• ako je $g = p \equiv 1 \pmod{4}$ ima 8 mogućnosti za α :

$$\pm a \pm bi, \quad \pm b \pm ai \quad (p \text{ se 'grana' u } \mathbb{Z}[i])$$

• ako je $g = p^2$, $p \equiv 3 \pmod{4}$ ima 4 mogućnosti za α :

$$\pm p, \quad \pm pi \quad (p \text{ ostaje 'inertan' u } \mathbb{Z}[i])$$

(opštije - Glava 10 u knjizi TB)

L6 Neka je $g \equiv 1 \pmod{4}$; neka su χ_2 i χ_4 karakteri $\mathbb{F}_g^\times$ tačnog reda 2 i 4, respektivno.

Onda je $1 + J(\chi_2, \chi_4)$ deljivo sa $2+2i$ u prostoru $\mathbb{Z}[i]$

Primer: $(1+i)^2 = 1+2i-1 = i \cdot 2$ (2 se 'ramifikuje' ('grane') u $\mathbb{Z}[i]$)
jedinica u $\mathbb{Z}[i]$

$1+i$ je prost u $\mathbb{Z}[i]$

(više o ramifikaciji videti u knjizi TB, 10.3)

$$2 = (-i)(1+i)^2$$

(2 je kvadrat prostog, do na jedinicu $= -i$)

i further L6 $\iff$ $(1+i)^3 \mid 1 + J(\chi_2, \chi_4)$ u $\mathbb{Z}[i]$



Tv. 2 (6): $J(\chi_4, \chi_4) = \frac{g(\chi_4)^2}{g(\chi_2)}$ $\bar{\chi}_2 = \chi_2 = \chi_2^{-1}$

$$J(\chi_2, \chi_4) = J(\chi_4, \chi_4) \frac{g(\chi_2)^2}{g(\chi_4)g(\bar{\chi}_4)} \stackrel{2.(5)}{=} J(\chi_4, \chi_4) \frac{\chi_2(-1)g}{\chi_4(-1)g}$$

$$= \chi_4(-1) J(\chi_4, \chi_4) \quad (3) \quad \left(\begin{array}{l} \text{jer je } -1 \text{ kvadrat u } \mathbb{F}_g^\times \\ \text{pa je } \chi_4(-1) = \pm 1 \end{array} \right)$$

• Dalje, po definiciji

$$J(\chi_4, \chi_4) = \sum_{x \in \mathbb{F}_g} \chi_4(x) \chi_4(1-x)$$

$$= \chi_4^2\left(\frac{p+1}{2}\right) + 2 \sum \chi_4(x) \chi_4(1-x)$$

$$\chi_4\left(1 - \frac{p+1}{2}\right) = \chi_4\left(1 - \frac{p+1}{2} + p\right)$$

suma po $\frac{p-3}{2}$ elemenata iz $\mathbb{F}_g^\times - \left\{\frac{p+1}{2}, 0, 1\right\}$

biramo po jedno x iz svakeg para $x, 1-x$

izuzev para $\frac{p+1}{2}, \frac{p+1}{2}$ (bogi je u 1. sabirku)

• Svaki $\chi_4(x) = i^k = \begin{cases} 1 \\ -1 = 1-2 \\ i = 1+i(1+i) \\ -i = 1-(1+i) \end{cases} \equiv 1 \pmod{(1+i)}$
 (kongruenija u $\mathbb{Z}[i]$)
 pa je i svaki sabirak u sumi sa desne strane

$$2 \chi_4(x) \chi_4(1-x) \equiv 2 \pmod{2+2i}$$

pa je

$$J(\chi_4, \chi_4) \equiv \chi_4^2\left(\frac{p+1}{2}\right) + 2 \frac{2^{-3}}{2} \equiv \chi_4^2\left(\frac{p+1}{2}\right) + 2 \pmod{2+2i}$$

$\underbrace{(2-5)+2}_{\substack{\text{delivo sa 4} \\ \text{pa i sa } (1+i)^3}}$

• Dodatno, $\chi_4^2\left(\frac{p+1}{2}\right)$; $\chi_4(4) = \chi_4(2^2) = \chi_4(2)$ su ± 1 , ali

$$\chi_4^2\left(\frac{p+1}{2}\right) \chi_4(4) = \chi_2\left(\frac{p+1}{2}\right) \cdot \chi_2(2) = \chi_2\left(\frac{p+1}{2} \cdot 2\right)$$

$$= \chi_2(p+1) = \chi_2(1) = 1 \quad (\text{svi karakteri su homomorfizmi})$$

$\uparrow$
 p -karakteristika
 polje $\mathbb{F}_2$

$$\text{pa } \begin{matrix} 1 \mapsto 1 \\ \uparrow \\ \mathbb{F}_2^\times \end{matrix} \quad \begin{matrix} \uparrow \\ \mathbb{C}^\times \end{matrix}$$

Što znači da je

$$\begin{aligned} \chi_4^2\left(\frac{p+1}{2}\right) &= \chi_4(4) = \chi_4((-4) \cdot (-1)) \\ &= \underbrace{\chi_4(-4)}_{\substack{=1 \\ \text{(L.4)}}} \cdot \chi_4(-1) = \chi_4(-1) \end{aligned}$$

Dakle

$$J(\chi_4, \chi_4) \equiv 2 + \chi_4(-1) \pmod{2+2i}$$

pa je iz (3):

$$1 + J(\chi_2, \chi_4) \equiv 1 + \chi_4(-1)(2 + \chi_4(-1)) = 2 + 2\chi_4(-1)$$

$$\equiv 2 \left(1 + \underbrace{\chi_4(-1)}_{\pm 1} \right) = \begin{Bmatrix} 0 \\ 4 \end{Bmatrix} \equiv 0 \pmod{(2+2i)} \quad \triangle$$

6 **Teorema 7** Neka je E_n eliptička kriva $y^2 = x^3 - n^2x$ definisana nad konačnim poljem $\mathbb{F}_p$, $p \nmid 2n$.

Onda je lokalna zeta funkcija eliptičke krive E_n jednaka

$$Z(E_n/\mathbb{F}_p; T) = \frac{1 - 2aT + pT^2}{(1-T)(1-pT)} = \frac{(1-\alpha T)(1-\bar{\alpha} T)}{(1-T)(1-pT)}$$

gde je $a = \operatorname{Re}(\alpha)$ i

$$\alpha = \begin{cases} i\sqrt{p}, & \text{ako je } p \equiv 3 \pmod{4} \\ a+bi, & a^2+b^2=p, \begin{matrix} a \text{ neparno} \\ (b \text{ parno}) \end{matrix}, \alpha \equiv a \equiv \left(\frac{n}{p}\right) \pmod{2+2i} \\ & \text{ako je } p \equiv 1 \pmod{4} \end{cases}$$

(ima 2 mogućnosti za ovako α , $a+bi$, ali jedna se ne menja!)

Treba da odredimo $N_r := \# E_n(\mathbb{F}_{p^r})$ ($q = p^r$)

• Ako je $p \equiv 3 \pmod{4}$, r -neparno: Tvrd 1: $N_r = q + 1 = p^r + 1$

• Ostaje da razmotrimo slučaj $p \equiv 1 \pmod{4}$ i slučaj $N_{2r} = \# E_n(\mathbb{F}_{p^{2r}})$ kad je $p \equiv 3 \pmod{4}$, koje pokriva Tvrd 5

Jedinstvene oznake:

$$\mathbb{Z}_1 := \begin{cases} p, & \text{ako je } p \equiv 1 \pmod{4} \\ p^2, & \text{ako je } p \equiv 3 \pmod{4} \end{cases}$$

$$\mathbb{Z}_1 \equiv 1 \pmod{4}$$

• Karakteri:

$$\chi_{2,1} = \chi_2 : \mathbb{F}_{\mathbb{Z}_1}^{\times} \rightarrow \mathbb{C}^{\times} \quad \text{jedinstven netrivijalni karakter reda 2}$$

$$\chi_{4,1} = \chi_4 : \mathbb{F}_{\mathbb{Z}_1}^{\times} \rightarrow \mathbb{C}^{\times} \quad \text{fiksirani karakter tačnog reda 4} \\ (\text{ima dva; drugi je onda } \overline{\chi}_4)$$

$$N_r : \mathbb{F}_{\mathbb{Z}_1}^{q^r} \rightarrow \mathbb{F}_{\mathbb{Z}_1} \quad \left(\text{opšta priča o Tr : N} \right. \\ \left. - \text{knjiga TB, 8.3} \right)$$

$$N_r(x) = \prod_{\sigma \in \text{Gal}(\mathbb{F}_{\mathbb{Z}_1}^{q^r}/\mathbb{F}_{\mathbb{Z}_1})} \sigma(x) = \prod_{j=0}^{r-1} \sigma_{\text{Fr}}^j(x) = \prod_{j=0}^{r-1} x^{\mathbb{Z}_1^j} = x^{\sum_{j=0}^{r-1} \mathbb{Z}_1^j} \in \mathbb{F}_{\mathbb{Z}_1} \\ \parallel \\ \langle \sigma_{\text{Fr}} \rangle \\ \sigma_{\text{Fr}} : x \mapsto x^{\mathbb{Z}_1}$$

Onda definišemo:

$$\chi_{4,r} := \chi_4 \circ N_r : \mathbb{F}_{\mathbb{Z}_1}^{q^r} \rightarrow \mathbb{C}^{\times} \quad \text{karakter tačnog reda 4}$$

$$\chi_{2,r} := \chi_2 \circ N_r : \mathbb{F}_{\mathbb{Z}_1}^{q^r} \rightarrow \mathbb{C}^{\times} \quad \text{karakter tačnog reda 2}$$

Tvrđenje 5 primenjeno na kriv E_n i polje $\mathbb{F}_{2_1^r}$
 (doble g (iz Tw. 5) $= g_1^r \equiv 1 \pmod{4}$) kaže da je

$$\# E_n(\mathbb{F}_{2_1^r}) = g_1^r + 1 - \alpha_{n, g_1^r} - \bar{\alpha}_{n, g_1^r} \quad (4)$$

gde je (prema još Tw. 2(6))

$$\alpha_{n, g_1^r} = -X_{2,r}(n) \frac{g(X_{2,r}) g(X_{4,r})}{g(\bar{X}_{4,r})}$$

Tvrđenje 8 [Hasse-Davenport-ova relacija]

Za svaki multipl. karakter $\chi: \mathbb{F}_{2_1^r}^\times \rightarrow \mathbb{C}^\times$, Gauss-ove sume $g(\chi \circ N_r)$ i $g(\chi)$ na $\mathbb{F}_{2_1^r}$ i $\mathbb{F}_{2_1}$, redom, su u sledećoj relaciji:

$$-g(\chi \circ N_r) = (-g(\chi))^r$$

▼ Dokaz: kroz zadatke na domaćem ▲

$$X_{2,r}(n) = X_2\left(N_r\left(\underset{n}{n}\right)\right) = X_2(n^r) = X_2(n)^r$$

$\mathbb{F}_{2_1}$, po ga se o fixingu

$$g(\bar{X}_{4,r}) \stackrel{(\#D)}{=} -(-g(\bar{X}_4))^r \quad \text{itd.} \rightarrow \quad (5)$$

$$\alpha_{n, g_1^r} = (-1)^r X_2(n)^r \frac{g(X_2)^r g(X_4)^r}{g(\bar{X}_4)^r} = \alpha_{n, g_1}^r, \quad \forall r$$

(L.9) Ako postoje recipročni konjugirani
 $\alpha_1, \alpha_2, \dots, \alpha_s, \beta_1, \beta_2, \dots, \beta_t \in \mathbb{C}$
 takvi da je

$$N_r = \beta_1^r + \dots + \beta_t^r - \alpha_1^r - \dots - \alpha_s^r, \quad \forall r \geq 1$$

onda je

$$\begin{aligned} Z(T) &= \frac{(1-\alpha_1 T)(1-\alpha_2 T) \dots (1-\alpha_s T)}{(1-\beta_1 T)(1-\beta_2 T) \dots (1-\beta_t T)} \\ \text{"} &= \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right) \end{aligned}$$

$\nabla \log \triangle$

Zanimljiva dokaza (T.7):

Slučaj $p \equiv 1 \pmod{4}$: $g_1 = p$:

$\chi_2(n)$ = detekcija da li je n kvadrat u $\mathbb{F}_{g_1} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$,
 a to je klasični Legendre-ov simbol (knjiga TB, glava 7)
 $= \left(\frac{n}{p}\right)$

Tvd. 5 : razmatrajući posle njega $\rightarrow \alpha := \alpha_{n, g_1} = \alpha_{n, p}$ je Gauss-ov
 ces norme $|\alpha|^2 = p$

$$\alpha = -\left(\frac{n}{p}\right) J(\chi_2, \chi_4) - \left(\frac{n}{p}\right) + \left(\frac{n}{p}\right) = -\left(\frac{n}{p}\right) \left(1 + J(\chi_2, \chi_4)\right) + \left(\frac{n}{p}\right)$$

$$\stackrel{(L.6)}{\equiv} \left(\frac{n}{p}\right) \pmod{2+2i}$$

$$\alpha = a+bi$$

$$a^2+b^2=p \text{ - neparno}$$

$\rightarrow$ b parno, a neparno

a iz formule (4) i (5) sledi:

$$\# E_n(\mathbb{F}_{p^n}) = p^n + 1^n - \alpha^n - \bar{\alpha}^n$$

pa (L.9) implicira da je $Z(E_n/\mathbb{F}_p) = \frac{(1-\alpha T)(1-\bar{\alpha} T)}{(1-T)(1-pT)}$.

Slučaj $p \equiv 3 \pmod{4}$: $g_1 = p^2$:

- Onda -1 nije kvadrat u $\mathbb{F}_p$ (inače $4 \mid p-1 = |\mathbb{F}_p^\times|$)

pa je X^2+1 nerastavljiv u $\mathbb{F}_p[X] \xrightarrow{(4/3)}$

$$\mathbb{F}_{g_1} = \mathbb{F}_{p^2} \cong \mathbb{F}_p[X]/\langle X^2+1 \rangle$$

- dakle jedan "malel" u $\mathbb{F}_{p^2}$ je $\{u+vX \mid u, v \in \mathbb{F}_p, X^2 = -1\}$

pa je u $\mathbb{F}_{p^2}$ očigledno $-1 \in (\mathbb{F}_{p^2}^\times)^2$, pa je i $\mathbb{F}_p^\times \subseteq (\mathbb{F}_{p^2}^\times)^2$

tj. svi elementi ~~polja~~ $\mathbb{F}_p^\times$ su kvadrati u $\mathbb{F}_{p^2}$

(svaki (nekvadrat u $\mathbb{F}_p^\times$) = $(-1) \cdot$ (neki kvadrat u $\mathbb{F}_p^\times$))

- Dakle, onda

$$\chi_2(n) = 1 \quad \left(\begin{array}{l} \text{jer } \chi_2 \text{ detektuje kvadrate u polju} \\ \mathbb{F}_p^\times \subseteq \mathbb{F}_{p^2}^\times \\ \mathbb{F}_{g_1} = \mathbb{F}_{p^2} \end{array} \right)$$

(p+n)

• (L.6) $\rightarrow \alpha := \alpha_{n, g_1} = \alpha_{n, p^2} \stackrel{\text{Tv.5}}{=} -J(\chi_2, \chi_4) = 1 + 1$
 $\equiv 1 \pmod{2+2i}$

$$|\alpha_{n, p^2}|^2 = p^2$$

$$\alpha \cdot \bar{\alpha} = p^2$$

jednakiost u $\mathbb{Z}[i]$ koji je UFD
 p je prost element
 $\equiv 3 \pmod{4}$

$$\Rightarrow \alpha \in \{i^j p \mid j=0,1,2,3\} = \{\pm p, \pm ip\}$$

$$-p = \underbrace{(-p-1)}_{\text{delivo sa 4 u } \mathbb{Z}} + 1 \equiv 1 \pmod{2+2i} \quad \text{zadovoljava}$$

delivo sa 4 u $\mathbb{Z}$

$\rightarrow$ delivo sa $(2+2i) \sim (1+i)^3$ u $\mathbb{Z}[i]$

Ostala 3 ne zadovoljavaju.

$$\Rightarrow \alpha_{n,p^2} = -p$$

Twist 5: za parne r

$$\begin{aligned} \# E_n(\mathbb{F}_{p^r}) &= \# E_n(\mathbb{F}_{2_1^{r/2}}) = p^r + 1^r - (-p)^{r/2} - (-p)^{r/2} \\ &= p^r + 1^r - (i\sqrt{p})^r - (-i\sqrt{p})^r \end{aligned}$$

Za neparne r važi ista formula, prema Twistu 1.

