9. PREDAVANJE

TEOREM (NÉRON – OGG – ŠAFAREVIČ)

Neka je K PAB, p neki prosti (konačni) ideal u K,

Tada je ekvivalentno:

(a) E ima dobru redukciju u p

(b) $\rho_{E,m}$ je nerazgranata u p $\forall m \in \mathbb{Z}$ t.d $(m,p)=1$.

$\rho_{E,m}(I_p) = \{I\}$.

Dokaz: Silverman AEC.

KOROLAR Neka su E_1/K i E_2/K eliptičke krivulje koje su izogene nad K. Tada E_1 ima dobru redukciju u $p \iff E_2$ ima dobru redukciju u p.

Dokaz: Neka je $\phi : E_1 \to E_2$ izogenija definirana nad K i neka je $m \geq 2$ t.d $(p,m)=1$ i $(\#\ker\phi, m) = 1$.

Tada $\phi' = \phi|_{E_1[m]} : E_1[m] \to E_2[m]$ je homomorfizam G_K-modula. (${}^{\sigma}\phi(P) = \phi({}^{\sigma}P)$)

($E(\bar{K})$)

$(\#\ker\phi^*, m) = 1 \Rightarrow (\#\ker\phi^*, \#E_1[m]) = 1 \Rightarrow \#\ker\phi' = 1$

($\#E_1[m] = m^2$)

$\Rightarrow \phi'$ je izomorfizam G_K-modula.

$\Rightarrow \rho_{E_1,m}$ i $\rho_{E_2,m}$ izomorfne.

$\Rightarrow$ ($\rho_{E_1,m}$ je razgranat u $p \iff \rho_{E_2,m}$ je razgranat u p)

TM NOS

$\Rightarrow$ (REZ. E_1 ima DR u $p \iff E_2$ ima DR u p).

SLIKE GALOISOVIH REPREZENTACIJA ELIPTIČKIH KRIVULJA NAD $\mathbb{Q}$

Zanima nas kako izgledi $\rho_{E,m}(G_{\mathbb{Q}})$. Promotrimo prvo kako je $m = p$ prost broj.

Ideja je ~~$\rho_{E,p}(G_{\mathbb{Q}}) =: G_E(p)$~~ $\boxed{G_E(p) := \rho_{E,p}(G_{\mathbb{Q}})}$

je ili $GL_2(\mathbb{F}_p)$ $(= GL_2(\mathbb{Z}/p\mathbb{Z}))$ ili je zatvorena u nekoj maksimalnoj podgrupi od $GL_2(\mathbb{F}_p)$ indeksa 1 ili 6

tako da $(\det G) \simeq \mathbb{F}_p^\times$.

DO NA HOMOMORFIZAM U $GL_2(\mathbb{F}_p)$:

Def. 1) $B_0(p) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbb{F}_p) \right\}$ - BORELOVA PODGRUPA

2) $\#B_0(p) = p(p-1)^2$

2) RASCJEPLJENA CARTANOVA PODGRUPA

$C_s(p) := \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \in GL_2(\mathbb{F}_p) \right\}$ - NIJE MAX.

$\#C_s(p) = (p-1)^2$

NORMALIZATOR OD $C_s(p)$ U $GL_2(\mathbb{F}_p)$ JE

$C_s^+(p) := \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\} \leq GL_2(\mathbb{F}_p)$

$\#C_s^+(p) = 2(p-1)^2$ - MAX.

3) NERASCJEPLJENA CARTANOVA PODGRUPA

~~$C_{ns}(p) \leq$~~ Fiksirajmo $\varepsilon \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$

NIJE MAX: $C_{ns}(p) := \left\{ \begin{pmatrix} a & b\varepsilon \\ b & a \end{pmatrix}, (a,b) \neq (0,0) \right\}$

$\#C_{ns}(p) = p^2 - 1$

MAX: $\nearrow C_{ns}^+(p) := C_{ns}(p) \cup \left\{ \begin{pmatrix} c & \varepsilon d \\ -d & -c \end{pmatrix}, (c,d) \neq (0,0) \right\}$.

NORMALIZATOR OD $C_{ns}(p)$ U $GL_2(\mathbb{F}_p)$ ~~$\#C_{ns}^+(p) = 2(p^2-1)$~~

$\#GL_2(\mathbb{F}_p) = (p^2-1)(p^2-p) = p(p-1)$

1. stupac: ne može biti $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ $\cdot p^2 - 1$ izbora

2. stupac $\cdot p^2 - p$

Nap $\underline{C^+_{n,2}(p)}$ je u $GL_2(\mathbb{F}_{p^2})$ je konjugirana s

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \alpha^p & 0 \end{pmatrix} \right\}$$ gdje je $\alpha \in \mathbb{F}_{p^2}^\times \setminus \mathbb{F}_p$

$C_{n,2}(p)$ je cikl. podgrupa.

4) IZNIMNE GRUPE:

$\rho : GL_2(\mathbb{F}_p) \twoheadrightarrow \boxed{PGL_2(\mathbb{F}_p)} = GL_2(\mathbb{F}_p) / Z(GL_2(\mathbb{F}_p))$ // skalarne matrice

$GL_2(\mathbb{F}_p) \supseteq E[p]$
$PGL_2(\mathbb{F}_p) \supseteq$ podgrupa od $E[p]$.

IZNIMNE GRUPE su one G za koje vrijedi $\rho(G) \cong A_4, A_5$ ili S_4.

Prop. Ako je $E/\mathbb{Q}$ koja ima potencijalno multiplikativnu redukciju u p i $G_E(p)$ iznimna, tada je $p \leq 11$.

Dokaz: Po nekoj dokaznoj $E/\mathbb{Q}_p$ je kvadratni twist od Tatove krivulje E' i

$$\rho_{E',p}|_{D_p} \sim \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix} \Rightarrow \rho_{E,p}|_{D_p} \sim \psi \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

$\exists$ element reda $\geq p-1$ u $\rho_{E',p}(G_{\mathbb{Q}}) \Rightarrow$

$\Rightarrow \exists$ element reda $\geq \frac{p-1}{2}$ u $\rho_{E,p}(G_{\mathbb{Q}})$

$\begin{pmatrix} a & * \\ & 1 \end{pmatrix}$ je reda n u $GL_2(\mathbb{F}_p)$

$\Rightarrow$ —||— je reda n u $PGL_2(\mathbb{F}_p)$

$\begin{pmatrix} a & * \\ & 1 \end{pmatrix}$ je u istoj klasi u $PGL_2(\mathbb{F}_p)$ kao $\begin{pmatrix} b & * \\ 0 & 1 \end{pmatrix}$

$\Leftrightarrow a = b$

$\Rightarrow \exists$ element reda $\geq \frac{p-1}{2}$ u slici $G_E'(p)$ od $G_E(p)$ u $PGL_2(\mathbb{F}_p)$.

Po pretpostavci $G_E'(p) \cong A_4, A_5$ ili S_4

~~Elementi~~ Elementi najvećeg reda su: $3, 5, 4$

$\Rightarrow \frac{p-1}{2} \leq$ ~~3, 4~~ 5

$\Rightarrow \boxed{p \leq 11}$. ☒

Možemo naći oko E čiji pripadajući mult. red. ... $\Rightarrow$ ... $G_E'(p)$ ima element reda $p-1$ $\Rightarrow$

$p-1 \leq 5 \Rightarrow p \leq 6$, tj. $\underline{\underline{p \leq 5}}$

0) Teorem (Serre '72) Ako je $G_E(p)$ izomno, tada je $p \leq 13$.

1) Teorem (Mazur '78) Ako je $G_E(p) \subseteq B_0(p)$ tada je $p \leq 19$ do na konj.

ili $p \in \{37, 43, 67, 163\}$. ←

2) Teorem (BILU - PARENTI - REBOLLEDO, 2011. & 2012.) Neka E nema CM. Ako $G_E(p) \subseteq C_s^+(p)$, tada je $p \in 7$ osim možda za $p = 13$.

→ Teorem (BALAKRISHNAN - DOGRA - MÜLLER - TUITMAN - VONK 2019.)

$G_E(13) \not\subseteq C_s^+(13)$.

Teorem — " — PROŠLI TJEDAN

Potpuno određeni mogući $G_E(13)$.

Nap. Ako E ima CM, tada će za sve osim konačno p-a

$G_E(p) \subseteq C_s^+(p)$ ili $C_{ns}^+(p)$

SERREOVO PITANJE / SLUTNJA O UNIFORMNOSTI

Postoji li C t.d. $\forall E/\mathbb{Q}$ bez CM, $\forall p > C$ mozi $G_E(p) = GL_2(\mathbb{F}_p)$.

Slutnja $C = 37$?

Pretpostavimo da je ostatak zamo 3) $C_{ns}^+(p)$ - ?

ŽYWINA (2015). Ako je $p \geq 17$, $E/\mathbb{Q}$ nema CM i $G_E(p) \subseteq C_{ns}^+(p)$

tada 1) Ako je $p \equiv 1 \pmod 3 \Rightarrow G_E(p) \subseteq C_{ns}^+(p)$

2) " - $p \equiv 2 \pmod 3 \Rightarrow G_E(p) \subseteq C_{ns}^+(p)$ ili $[C_{ns}^+(p) : G_E(p)] = 3$

LE FOURN - LEMOS (2021)

Za $p > 1.4 \cdot 10^{17}$ ~~zbog~~

ako je $G_E(p) \subseteq C^+_{ns}(p)$, tada je $G_E(p) = C^+_{ns}(p)$.

Jedno pitanje: $E/\mathbb{Q}$ i pitamo se za $P \in E[n]$,

$\mathbb{Q}(P) := \mathbb{Q}(x(P), y(P))$, koji su mogući za $[\mathbb{Q}(P) : \mathbb{Q}] = ?$

| ne ovisi o modelu od E

Primjetimo $P \in E(K) \iff \sigma(P) = P \quad \forall \sigma \in G_K$.

Neka je $G_1(n) := \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/n\mathbb{Z})$

$G_1'(n) = G_1(n) \cap G_E(n)$.

$G_1'(n)$ je stabilizator od P u $G_E(n) \curvearrowright E[n]$.

$\Rightarrow \underline{(\mathbb{Q}(E[n]))^{G_1'(n)} = \mathbb{Q}(P)} \Rightarrow [\mathbb{Q}(E_1[n]) : \mathbb{Q}(P)]$

$= \# G_1'(n)$.

$\Rightarrow [\mathbb{Q}(P) : \mathbb{Q}] = [G_E(n) : G_1'(n)]$

Kolika je max mogući $[\mathbb{Q}(P) : \mathbb{Q}]$ za $|P| = n$? Neka je n prost.

$G_E(p) = GL_2(\mathbb{F}_p)$

$\# G_E(p) = p(p^2-1)(p-1)$

$G_1'(p) = (p-1) \cdot p$

$\Rightarrow [\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$

TM. 05 $\Rightarrow$ $[\mathbb{Q}(P) : \mathbb{Q}]$ je stupanj dužine orbite od P

$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ nad $\mathbb{Q}$.

$[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$ = długość orbity α_1 (= działanie na $G_{\mathbb{Q}}$), tj. $\# G_{\mathbb{Q}} \cdot \alpha_1$.

$f \in \mathbb{Q}[x]$. $Gal(f)$ jest S_n gdy $n = \deg f$ dla wielu $n \geq 0$.

$\rho_{E,m}(G_{\mathbb{Q}})$.

$\rho_E(G_{\mathbb{Q}}) \subseteq Aut(E_{tors}) \leq GL_2(\hat{\mathbb{Z}}) = \varprojlim \mathbb{Z}/n\mathbb{Z}$ — ADELIŌWA REP

$G_{\mathbb{Q}} \curvearrowright E_{tors}$

$\rho_{E,p}(G_{\mathbb{Q}}) \subseteq Aut(E[p^\infty]) \leq GL_2(\mathbb{Z}_p)$ — p-adyczna REP

TEOREM (SERRE '72) TEOREM O OTWARTOŚCI OBRAZU

Niech E nie ma CM. Wtedy $\rho_E(G_{\mathbb{Q}})$ jest otwarta w $GL_2(\hat{\mathbb{Z}})$.

$([GL_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] < +\infty)$.

$\Rightarrow$ Dla ciała $E/\mathbb{Q}$. $\exists$ $\mathcal{P}_E$ t.ż. $G_E(p) = GL_2(\mathbb{F}_p)$ dla $\forall p > \mathcal{P}_E$.
