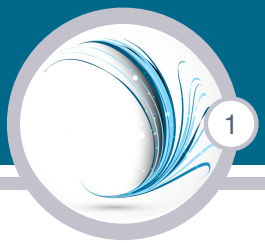
UdelaR

Conjetura de Serre y aplicaciones

Santiago Radi

June 11, 2020

Representaciones de Galois



Fijemos inmersiones $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p} \hookrightarrow \mathbb{C}$ para cada primo p. Sea $\overline{\mathbb{F}_p} = \mathcal{O}_{\overline{\mathbb{Q}_p}}/\mathfrak{M}_{\overline{\mathbb{Q}_p}}$ la clausura algebraica de $\mathbb{F}_p$ obtenida como el cuerpo residual. Llamaremos $\widetilde{\cdot} : \mathcal{O}_{\overline{\mathbb{Q}_p}} \to \overline{\mathbb{F}_p}$ al mapa reducción.

Representación de Galois

Una **representación de Galois** es un morfismo continuo

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

con V un $\overline{\mathbb{F}_p}$-espacio vectorial de dimensión 2.

Propiedad: ρ factoriza por un grupo finito G que es isomorfo a un subgrupo de $\mathrm{GL}_2(\mathbb{F}_q)$ con q una potencia de p.

Representaciones de Galois

Representaciones conjugadas

Dos representaciones ρ_1 , ρ_2 son **equivalentes** si existe $\tau \in \mathrm{GL}(V)$ tal que

$$\rho_1(g) = \tau\rho_2(g)\tau^{-1}, \forall g \in G_{\mathbb{Q}}$$

Subrepresentaciones

Sea $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ una representación. Sea W un subespacio vectorial de V estable bajo la acción de $G_{\mathbb{Q}}$ por ρ. Podemos entonces considerar la representación $\rho^W : G_{\mathbb{Q}} \to \mathrm{GL}(W)$. Diremos que ρ^W es una **subrepresentación** de ρ.

Una representación $\rho : G \to \mathrm{GL}(V)$ se dice **irreducible** si no tiene subrepresentaciones propias.

Representaciones de Galois

Las representaciones de Galois pueden construirse a partir de otros objetos como:

- Curvas elípticas
- Formas modulares

Representación modular

que una representación es **modular** si es equivalente a una representación que proviene de una forma modular.

Representación de curvas elípticas

Sea $E/\mathbb{Q}$ una curva elíptica.

Sea p primo y sea $E[p] = \left\{P \in E(\overline{\mathbb{Q}}) : [p]P = 0\right\}$. Se sabe que $E[p] \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. Así que $\mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$

Sea $\sigma \in G_{\mathbb{Q}}$. Como $E/\mathbb{Q}$, $\sigma[p] = [p]\sigma$, así que si $P \in E[p]$ entonces $P^\sigma \in E[p]$.

La representación de una curva elíptica es $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ dada por

$$\rho_{E,p}(\sigma)(P) = P^\sigma$$

Propiedad: $\det \rho_{E,p} = \chi_p$

Ejemplo: $\rho_{E,2}$

Sea $E : y^2 = f(x)$ con $f \in \mathbb{Q}[x]$, f mónico, $\deg(f) = 3$ y $p = 2$. Los puntos de orden 2 son de la forma $(r_i, 0)$ con r_i las tres raíces de f. $G_{\mathbb{Q}}$ actúa permutando los puntos, por lo que la representación factoriza por $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$. Por otro lado $E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Llamemos P_1, P_2, P_3 a los puntos de orden 2 y tomemos $\{P_1, P_2\}$ como generador del módulo.

Tres casos:

1. Dos puntos racionales: entonces los tres son racionales y $\rho_E(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

2. Solo un punto racional: pongamos $P_1 = (x_0, 0)$ racional, entonces $f(x) = (x - x_0)g(x)$ con g irreducible. Entonces $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ y $\sigma(P_2) = P_3 = P_1 + P_2$, entonces $\rho_E(\sigma) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Ejemplo: $\rho_{E,2}$

Tres casos:

1. Dos puntos racionales: entonces los tres son racionales y $\rho_E(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

2. Solo un punto racional: pongamos $P_1 = (x_0, 0)$ racional, entonces $f(x) = (x - x_0)g(x)$ con g irreducible. Entonces $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ y $\sigma(P_2) = P_3 = P_1 + P_2$, entonces $\rho_E(\sigma) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

3. Ningún punto racional: f irreducible y $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) = S_3$ ó A_3. Si es S_3 hay dos generadores $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ de orden 2 y $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ de orden 3, $\rho_E(\sigma) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ y $\rho_E(\tau) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Si es A_3, τ genera y $\rho_E(\tau) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

Ramificación y conductor de representaciones

Ramificación en representaciones

Una representación ρ se dice que **ramifica en** ℓ con ℓ primo si $\rho(I_\ell) \neq \{1\}$.

Conductor de una representación

El **conductor** de una representación ρ se define como el entero positivo

$$N_\rho = \prod_{\ell \neq p} \ell^{n(\ell,\rho)}$$

.

- El número N_ρ es el producto de los primos ℓ para los cuales ρ ramifica en ℓ ($n(\ell, \rho) = 0$ sí y solo sí ρ es no ramificada en ℓ).
- $n(\ell, \rho)$ es más grande cuanto más "compleja" es la acción de los grupos de ramificación en ℓ a través de ρ.

Ramificación en representaciones de curvas elípticas

Teorema

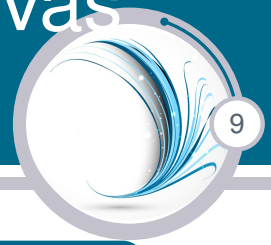
Sea $E/\mathbb{Q}$ una curva elíptica, ℓ, p primos con $\ell \neq p$.

1. Si E tiene buena reducción en ℓ, entonces $\rho_{E,p}$ es no ramificada en ℓ.
2. Si E tiene reducción multiplicativa en ℓ, entonces $n(\ell, \rho_{E,p}) = 0$ si y solo si $p \mid \nu_\ell(\Delta^{min}(E))$

Sea $K = \mathbb{Q}_\ell(E[p])$. Entonces $\ker \rho_E = G_K$.

1. Si E tiene buena reducción, $\nu_\ell(\Delta) = 0$, entonces $\nu_K(\Delta) = 0$ y E/K tiene buena reducción. Entonces $E(K)[p] \hookrightarrow \widetilde{E}(k)$ es inyectivo, (k es el cuerpo residual de K).

Sea $\sigma \in I_\ell$ y $P \in E[p]$, entonces $\widetilde{P^\sigma - P} = \widetilde{P^\sigma} - P = \widetilde{O}$. Luego $P^\sigma = P$.



Teorema

Sea $E/\mathbb{Q}$ una curva elíptica, ℓ, p primos con $\ell \neq p$.

1. Si E tiene buena reducción en ℓ, entonces $\rho_{E,p}$ es no ramificada en ℓ.
2. Si E tiene reducción multiplicativa en ℓ, entonces $n(\ell, \rho_{E,p}) = 0$ si y solo si $p \mid \nu_\ell(\Delta^{min}(E))$

Sea $K = \mathbb{Q}_\ell(E[p])$. Entonces $\ker \rho_E = G_K$.

2. Sea $q_E \in \mathbb{Q}_\ell$ el período de Tate. $E(\overline{\mathbb{Q}_\ell}) \simeq \overline{\mathbb{Q}_\ell}^\times / q_E^{\mathbb{Z}}$.
Entonces $E[p] \simeq \left\langle \mu_p, q_E^{1/p} \right\rangle / q_E^{\mathbb{Z}}$ y $K = \mathbb{Q}_\ell(\mu_p, q_E^{1/p})$.

I_ℓ actúa trivial $\iff$ $K/\mathbb{Q}_\ell$ no ramificada $\iff$ $\mathrm{Im}(\nu_K) = \mathrm{Im}(\nu_\ell) \iff$ $\nu_K(q_E^{1/p}) \in \mathbb{Z} \iff p \mid \nu_\ell(q_E) = \nu_\ell(\Delta^{min}(E))$.

Formas modulares en $\mathbb{C}$

Subgrupo de congruencia

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Formas modulares

Sea $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un caracter de Dirichlet, $k \geq 2$, $N \geq 1$ enteros. Una **forma modular de peso k y nivel N asociada a ϵ_0** es una función $F : \mathcal{H} \to \mathbb{C}$ tal que

1. F es holomorfa en $\mathcal{H}$
2. $F(z) = \epsilon_0(d)(cz+d)^{-k} F(\frac{az+b}{cz+d})$ para toda $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$
3. F es holomorfa en las cúspides $\mathbb{Q} \cup \{\infty\}$.

El conjunto $\mathcal{M}_k(N, \epsilon_0)$ de estas formas modulares, es un $\mathbb{C}$-espacio vectorial de dimensión finita.

Formas modulares en $\mathbb{C}$

Estas formas modulares admiten una expansión de Fourier

$$F(z) = \sum_{n=0}^{\infty} A_n q^n$$

con $q = e^{2\pi i z}$ en cada cúspide.

Formas cuspidales

Una forma modular es **cuspidal** si $A_0 = 0$ en todas las cúspides.

Llamamos $\mathcal{S}_k(N, \epsilon_0)$ a este subespacio vectorial de $\mathcal{M}_k(N, \epsilon_0)$.

Formas cuspidales normalizadas

Una forma cuspidal es **normalizada** si $A_1 = 1$ para la cúspide ∞.

Formas modulares en $\overline{\mathbb{F}_p}$

Sea p primo y sean $N \geq 1$ entero coprimo a p, $k \geq 2$ entero (par si $p = 2$) y $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}_p}^\times$ tal que $\epsilon(-1) = (-1)^k$.

Existe un único $\epsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Z}} \subseteq \mathbb{C}^\times$ tal que $\widetilde{\epsilon_0(x)} = \epsilon(x)$ para todo $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Una **forma cuspidal** de tipo (N, k, ϵ) con coeficientes en $\overline{\mathbb{F}_p}$ es una serie formal

$$f(z) = \sum_{n \geq 1} a_n q^n$$

tal que existe una forma cuspidal F de $\mathcal{S}_k(N, \epsilon_0)$

$$F(z) = \sum_{n \geq 1} A_n q^n$$

con $A_n \in \overline{\mathbb{Z}}$ que cumple que $\widetilde{A_n} = a_n$ para todo $n \geq 1$.

Formas modulares en $\overline{\mathbb{F}_p}$

Operadores de Hecke

Dado $\mathcal{S}_k(N, \epsilon)$ en $\overline{\mathbb{F}_p}$, existen operadores lineales T_ℓ con $\ell \nmid pN$ y U_ℓ con $\ell \mid pN$ que actúan en $\mathcal{S}_k(N, \epsilon)$. Trabajaremos con vectores propios normalizados de estos operadores.

Si $f(z) = \sum_{n \geq 1} a_n q^n$ es un vector propio normalizado de los operadores de Hecke, cumple que $T_\ell(f) = a_\ell f$ para $\ell \nmid pN$ y $U_\ell(f) = a_\ell f$ para $\ell \mid pN$.

Representaciones asociadas a formas modulares

(Deligne, Serre, 1974). Dada $f(z) = \sum_{n \geq 1} a_n q^n$ forma cuspidal en $\overline{\mathbb{F}_p}$ de tipo (N, k, ϵ), existe una representación

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

continua tal que en los primos ℓ que no dividen a pN, ρ_f no ramifica, $\operatorname{tr} \rho_f(\mathrm{Frob}_\ell) = a_\ell$ y $\det \rho_f = \epsilon \chi_p^{k-1}$.

Representación impar

Representación impar

Una representación ρ es **impar** si $\det \rho(c) = -1$, con c la conjugación compleja.

Sobre $\det \rho$

Por ser una representación sobre $\overline{\mathbb{F}_p}$ factoriza y como $\overline{\mathbb{F}_p}^\times$ es abeliano, factoriza por una extensión abeliana.

Por el teorema de Kronecker-Weber se puede tomar $\det \rho : \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \to \overline{\mathbb{F}_p}^\times$ con $n = pN_\rho$. Por TCR,

$$\det \rho = \epsilon \chi_p^h$$

con $\epsilon : (\mathbb{Z}/N_\rho\mathbb{Z})^\times \to \overline{\mathbb{F}_p}^\times$, $h \in \mathbb{Z}$ y χ_p el carácter ciclotómico.

Si ρ es impar, $\epsilon(c) = \epsilon(-1) = (-1)^{h+1}$.

Conjetura de Serre (primer versión)

Conjetura de Serre (primer versión)

Si $\rho : G_{\mathbb{Q}} \to \overline{\mathbb{F}_p}$ es una representación impar e irreducible, entonces es modular, es decir, $\rho \sim \rho_f$ para una forma modular f con coeficientes en $\overline{\mathbb{F}_p}$.

Más detalles...

Serre precisó algunas cuestiones más en su conjetura:

1. La forma modular puede tomarse cuspidal, normalizada y forma propia de todos los operadores de Hecke
2. El tipo (N, k, ϵ) de la forma cuspidal. El nivel $N = N_\rho$. El carácter ϵ cumple que $\det \rho = \epsilon \chi_p^h$. El peso k depende de $\rho\,|_{I_p}$.
   Se cumple que $\det \rho\,|_{I_p} = \chi_p^{k-1}$. Observar que $k - 1 \equiv h \pmod{p-1}$
3. El tipo (N, k, ϵ) es minimal en el sentido de que si ρ es modular de tipo (N', k', ϵ'), entonces $N \mid N'$ y $k' \geq k$.

Peso para representaciones de curvas elípticas

Teorema

Sea $E/\mathbb{Q}$ una curva elíptica y p primo.

1. Si E tiene buena reducción en p entonces $k = 2$
2. Si E tiene reducción multiplicativa, entonces

$$k = \begin{cases} 2 & \text{si } p \mid \nu_p(\Delta^{min}(E)) \\ \text{p+1} & \text{si no} \end{cases}$$

1. (Serre, 1973) $k = 2$ sí y solo sí $\det \rho_p \mid_{I_p} = \chi_p$ y ρ_p es finita en p.

Si E tiene buena reducción en p, ρ_p es finita.

Peso para representaciones de curvas elípticas

2. En reducción multiplicativa, considero $L/\mathbb{Q}_p$ extensión cuadratica no ramificada para que sea split. Usando el período de Tate,

$$E[p] \simeq \left\langle \mu_p, q_E^{1/p} \right\rangle / q_E^{\mathbb{Z}}$$

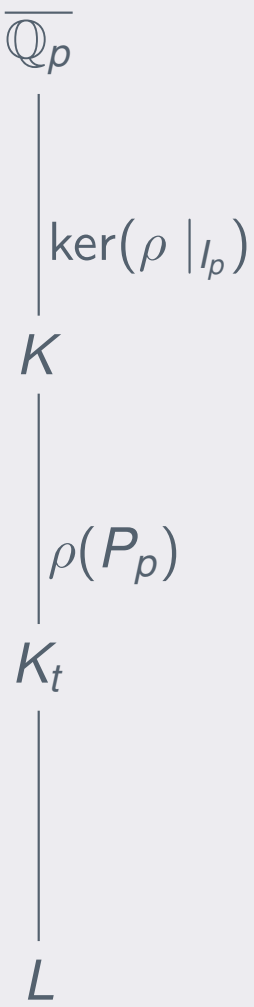
con acción de Galois compatible. Por lo tanto

$$\rho\,|_{I_p} \simeq \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

Sea $K = \mathrm{Fix}(\ker(\rho\,|_{I_p})) = L(E[p]) = L(\mu_p, q_E^{1/p})$ y $K_t = \mathrm{Fix}(\rho(P_p)) \subseteq K$. Como $\rho(P_p)$ es un p-Sylow en $\rho(I_p)$,

$$\mathrm{Gal}(K_t/L) \simeq (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

Por lo tanto $K_t = L(\mu_p)$ y $K = K_t(q_E^{1/p})$.



Peso para representaciones de curvas elípticas

$\rho\,|_{I_p} \simeq \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$.
$K_t = \mathrm{Fix}(\rho(P_p)) = L(\mu_p)$.
$K = \mathrm{Fix}(\ker(\rho\,|_{I_p})) = L(E[p]) = L(\mu_p, q_E^{1/p}) = K_t(q_E^{1/p})$.

Extensión poco ramificada

K/K_t es **poco ramificada** si es generada por $(1/p)$-potencias de unidades de $\mathcal{O}_L$. En caso contrario es **muy ramificada**.

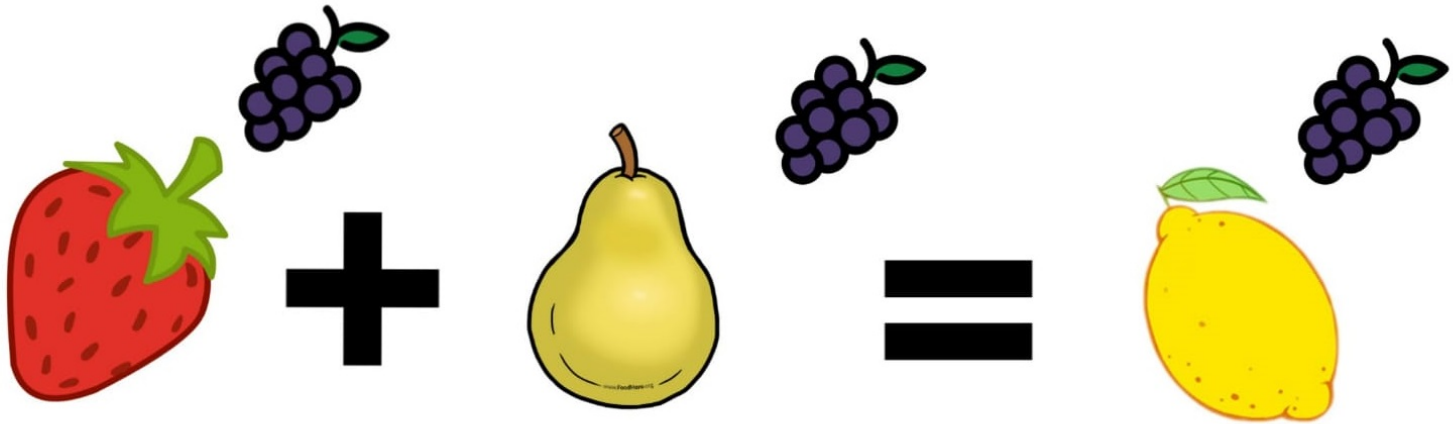
Serre define

$$k = \begin{cases} 2 & \text{si } K/K_t \text{ es poco ramificada} \\ \text{p+1} & \text{si es muy ramificada y } p \neq 2 \end{cases}$$

En nuestro caso, K/K_t es poco ramificada $\iff K = K_t(u^{1/p})$ con $\nu_p(u) = 0 \iff q_E = u\pi^{kp} \iff p \mid \nu_p(q_E) = \nu_p(\Delta^{min}(E))$

Aplicaciones: Último Teorema de Fermat

95% of people can't solve this! 😂😂



Find any integer solution!

Aplicaciones: Último Teorema de Fermat

Último Teorema de Fermat

(Wiles, 1995) Si $n > 2$ entero, y existen enteros a, b, c tales que $a^n + b^n = c^n$, entonces $abc = 0$.

Caso $n = 3$ (Euler, 1753) y caso $n = 4$ (Fermat, ≈ 1670). Con esto, el problema es equivalente a $a^q + b^q = c^q$ con $q \geq 5$ primo.

Por ser una ecuación homogénea, se pueden tomar coprimos. Uno de ellos debe ser par (pongamos b) y los otros dos impares. Reduciendo módulo 4 uno de ellos debe ser $3 \pmod 4$ (pongamos a). Denotemos $(A, B, C) = (a^q, b^q, c^q)$. Entonces $A \equiv -1 \pmod 4$, $B \equiv 0 \pmod{32}$.

Aplicaciones: Último Teorema de Fermat

Considero la curva elíptica

$$E = E_{A,B} : y^2 = x(x + A)(x - B)$$

Entonces,

1. $\Delta^{min}(E) = 2^{-8} A^2 B^2 C^2$
2. $N(E) = \text{rad}(ABC)$, es decir,
3. E tiene reducción multiplicativa en todos los primos que dividen al discriminante.

Aplicaciones: Último Teorema de Fermat

Teorema

Si $p \geq 5$ primo, entonces $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$, la representación de los puntos de p-torsión de E es irreducible.

Si es reducible, $\rho_{E,p} = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ con H (la primer columna) un subgrupo de orden p $G_{\mathbb{Q}}$-invariante. E semiestable , así que $(\varphi_1, \varphi_2) \in \{(1, \chi_p), (\chi_p, 1)\}$.

En el primer caso E tiene un punto de orden p y como los puntos de orden 2 son racionales, $|E_{tor}(\mathbb{Q})| \geq 4p \geq 20$ (absurdo por la clasificación de Mazur).

En el segundo caso $E' = E/H$ tiene un punto de orden p y aplica el mismo argumento.

Aplicaciones: Último Teorema de Fermat

Vimos que $\rho_{E,p}$ es irreducible con $p \geq 5$ y que $\Delta^{min}(E) = 2^{-8}A^2B^2C^2$

En curvas elípticas, $\det \rho_{E,p} = \chi_p$. En particular, $\epsilon = 1$, ρ es impar y $k \equiv 2 \pmod{p-1}$.

El conductor $N_{\rho_{E,p}}$ es el producto de los primos $\ell \neq p$ de mala reducción tal que $p \nmid \nu_\ell(\Delta^{min}(E))$. Si $\ell \neq 2$ y $\ell \mid abc$ (pongamos $r = \nu_\ell(abc)$), entonces $\nu_\ell(\Delta^{min}(E)) = 2qr$. Si $\ell = 2$, $\nu_2(\Delta(E)) = 2qr - 8$. Eligiendo $p = q$, entonces $N_{\rho_{E,p}} = 2$.

Con respecto al peso, como $p \mid \nu_p(\Delta^{min}(E)) = 2pr$, entonces $k = 2$.

La conjetura de Serre establece que $\rho_{E,p}$ debe ser isomorfa a una representación ρ_f con f una forma cuspidal de tipo $(2, 2, 1)$. Tal forma cuspidal no existe.

Aplicaciones: Conjetura de Szpiro con N_E prim

Conjetura de Szpiro (1981)

Para cada $\epsilon > 0$ existe un K_ϵ tal que para toda curva elíptica $E/\mathbb{Q}$

$$|\Delta(E)| \leq K_\epsilon (N(E))^{6+\epsilon}$$

Conjetura ABC (1985)

Para cada $\epsilon > 0$, existe una constante K_ϵ tal que para todo $A, B, C \in \mathbb{Z}$, que satisface $A + B = C$ y $\text{mcd}(A, B, C) = 1$ se cumple que

$$\max\{|A|, |B|, |C|\} \leq K_\epsilon \left(\prod_{p|ABC} p \right)^{1+\epsilon}$$

Teorema

1. ABC $\Rightarrow$ Szpiro
2. Szpiro $\Rightarrow$ ABC con exponente $3/2$

Aplicaciones: Conjetura de Szpiro con N_E prim

Teorema

2. Szpiro $\Rightarrow$ ABC con exponente $3/2$

2. $A + B = C$. Renombrando se puede tomar $C > B > A > 0$.
Considero $E_{A,B} = E : y^2 = x(x + A)(x - B)$. Entonces
$|\Delta| \geq \left|\Delta^{min}\right| = 2^{-8}(ABC)^2$ y $N = 2^e \prod p$ con $p \geq 3$ y $p \mid ABC$ y $e \leq 2$.
Aplicando Szpiro,

$$2^{-8}(ABC)^2 \leq |\Delta| \leq K_\epsilon N^{6+\epsilon} \leq K_\epsilon 2^{12+2\epsilon} \prod_{p|ABC} p^{6+\epsilon}$$

Como $A \geq 1$ y $B > \frac{C}{2}$, entonces

$$2^{-10} C^4 \leq K_\epsilon 2^{12+2\epsilon} \left(\prod_{p|ABC} p \right)^{6+\epsilon}$$

Aplicaciones: Conjetura de Szpiro con N_E prim

Teorema

2. Szpiro $\Rightarrow$ ABC con exponente $3/2$

2. $A+B=C$. Renombrando se puede tomar $C>B>A>0$.
Considero $E_{A,B}=E: y^2=x(x+A)(x-B)$. Entonces
$|\Delta| \geq \left|\Delta^{min}\right| = 2^{-8}(ABC)^2$ y $N=2^e\prod p$ con $p\geq 3$ y $p \mid ABC$ y $e\leq 2$.
Aplicando Szpiro,

$$2^{-8}(ABC)^2 \leq |\Delta| \leq K_\epsilon N^{6+\epsilon} \leq K_\epsilon 2^{12+2\epsilon} \prod_{p|ABC} p^{6+\epsilon}$$

Como $A\geq 1$ y $B>\frac{C}{2}$, entonces

$$2^{-5/2}C \leq (K_\epsilon)^{1/4} 2^{3+\epsilon/2} \left(\prod_{p|ABC} p\right)^{3/2+\epsilon/4}$$

Aplicaciones: Conjetura de Szpiro con N_E prim

Teorema

Sea $E/\mathbb{Q}$ una curva elíptica semiestable con $\left|\Delta^{min}(E)\right|$ una potencia de p. Entonces E tiene un subgrupo $\mathbb{Q}$-racional de orden p y $p \leq 7$.

Δ^{min} es una potencia de p así que $p \mid \nu_\ell(\Delta^{min})$ para todo primo ℓ, así que $\mathbb{Q}(E[p])/\mathbb{Q}$ es no ramificada fuera de p.

Si no tiene un subgrupo $\mathbb{Q}$-racional de orden p, entonces no tiene isogenias racionales de orden p. Por [Properties galoisiennes des points dordre fini des courbes elliptiques, Serre, 1972], $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_p)$.

Sea $d = \Delta_{\mathbb{Q}(E[p])/\mathbb{Q}}$ y $n = [\mathbb{Q}(E[p]) : \mathbb{Q}]$. Entonces $|d|^{1/n} = p^\alpha$ con α conocido (ver [The rank of elliptic curves, Brumer Kramer, 1977, proposición 9.2]). En todos los casos de α para $p \leq 7$, $|d|^{1/n}$ viola cotas inferiores de Odlyzko que mejoran cotas de Minkowski.

Aplicaciones: Conjetura de Szpiro con N_E prim

Teorema

Sea $E/\mathbb{Q}$ una curva elíptica semiestable con $\left|\Delta^{min}(E)\right|$ una potencia de p. Entonces E tiene un subgrupo $\mathbb{Q}$-racional de orden p y $p \leq 7$.

Si $p > 7$, por el teorema de Mazur, $\rho_{E,p}$ es irreducible. Del hecho de que $p \mid \nu_\ell(\Delta^{min})$ para todo ℓ primo, $(N, k, \epsilon) = (1, 2, 1)$. Llegamos a una contradicción porque no existen formas cuspidales de peso 2 y nivel 1.

Aplicaciones: Conjetura de Szpiro con N_E prim

Teorema

Sea $E/\mathbb{Q}$ una curva elíptica con $N(E) = P$ primo. Sea $\Delta^{min}(E) = \pm P^m$. Entonces $m = 1$ salvo finitos casos.

E es semiestable por ser $N(E)$ primo. Si $m > 1$ hay un primo $p \mid m$ y por el lema anterior $p \leq 7$.

Si $p = 2$, hay un subgrupo $\mathbb{Q}$-racional de orden 2. [Elliptic curves of primer conductor, Setzer, 1975, teorema 2] prueba que es una curva de Setzer-Neumann si $P \neq 17$ y hay dos opciones si $P = 17$.

Para $p = 3, 5, 7$, [Elliptic curves of prime power conductor with $\mathbb{Q}$-rational points of finite order, Miyawaki, 1973] demuestra que las únicas opciones son $(P, p) \in \{(11, 5), (19, 3), (37, 3)\}$.

Aplicaciones: Conjetura de Szpiro con N_E prim

Ec. de la curva / LMFDB label	**Conductor**	**Discriminante minimal**
$y^2 + xy = x^3 + \frac{u-1}{4}x^2 + 4x + u$ $(p = u^2 + 64)$	p	$-p^2$
11.a2	11	-11^5
17.a2	17	17^2
17.a3	17	-17^4
19.a2	19	-19^3
37.b2	37	37^3

GRACIAS!!!