El criteio de Néron-Ogg-Shafarevich

2021

Índice

Estas notas fueron redactadas, originalmente, con el propósito de servir de ayuda para rendir el final de Aritmética de curvas elípticas (¿2014?). La idea es enunciar y tratar de demostrar un criterio que relaciona la reducción de una curva elíptica con la ramificación de cierta representación de Galois asociada.

1 Forma de Weierstrass

Sea $\mathcal{K}$ un cuerpo completo respecto de una valuación discreta v y sean $\mathcal{R} = \{v \geq 0\}$ y $\mathcal{M} = \{v > 0\}$ su anillo de enteros y el ideal maximal del mismo, respectivamente. Sea π un generador de $\mathcal{M}$ y sea $k = \mathcal{R}/\mathcal{M}$ el cuerpo residual. Sea $E/\mathcal{K}$ una curva elíptica sobre $\mathcal{K}$ dada por ecuación de Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ . \tag{1}$$

Vía un cambio de variables ($(x, y) = (u^2x', u^3y')$, $a_i' = a_i/u^i$), (1) se puede llevar a una ecuación con coeficientes en $\mathcal{R}$. El discriminante Δ sería, entonces, un elemento de $\mathcal{R}$, de valuación no negativa. Como v es una valuación discreta, se deduce que existe una ecuación de la forma (1) con $v(\Delta)$ mínimo para la curva E.

Se puede demostrar que una ecuación con coeficientes en el anillo $\mathcal{R}$ es minimal en este sentido, si vale que $v(\Delta) < 12$, $v(c_4) < 4$ y (¿o?) $v(c_6) < 6$, donde c_4, c_6 y Δ se calculan a partir de los coeficientes a_i utilizando las expresiones:

$$\begin{aligned} b_2 &= a_1^2 + 4a_4 \ , \\ b_4 &= 2a_4 + a_1a_3 \ , \\ b_6 &= a_3^2 + 4a_6 \ , \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^3 \ , \\ c_4 &= b_2^2 + 24b_4 \ , \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \ , \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \ . \end{aligned} \tag{2}$$

Se cumple que

$$\begin{aligned} 4b_8 &= b_2b_6 - b_4^2 \quad \text{y} \\ 1728 \cdot \Delta &= c_4^3 - c_6^2 \ . \end{aligned} \tag{3}$$

Finalmente, recordamos que una ecuación de Weierstrass es minimal para la curva E es única, salvo cambio de coordenadas de la forma

$$(x, y) = (u^2x' + r, u^3y' + u^2x's + t) \ ,$$

donde $u \in \mathcal{R}^\times$ es una unidad y $r, s, t \in \mathcal{R}$ son arbitrarios.

2 Reducción

Si $E/\mathcal{K}$ viene dada por una ecuación minimal y $P \in \mathbb{P}^2(K)$, se pueden hallar coordenadas homogéneas $P = [x_0 : x_1 : x_2]$, con $x_i \in \mathcal{R}$ y, al menos, una en $\mathcal{R}^\times$. Se definen, entonces, los conjuntos

$$\begin{aligned} E_0(\mathcal{K}) &:= \left\{P \in E(\mathcal{K}) \, : \, \widetilde{P} \in \widetilde{E}_{\mathsf{ns}}(k)\right\} \quad \text{y} \\ E_1(\mathcal{K}) &:= \left\{P \in E(\mathcal{K}) \, : \, \widetilde{P} = O\right\} \ . \end{aligned}$$

Estos conjuntos son, en realidad, grupos y existe una sucesión exacta corta

$$0 \longrightarrow E_1(\mathcal{K}) \longrightarrow E_0(\mathcal{K}) \longrightarrow \widetilde{E}_{\mathsf{ns}}(k) \longrightarrow 0$$

Se había visto en clase para $\mathcal{K} = \mathbb{Q}_p$, pero los argumentos valen en general.

Otra cosa que se había visto en clase fue que, para $n \geq 1$ el conjunto

$$E_n(\mathcal{K}) := \left\{P \in E_1(\mathcal{K}) \, : \, v(x(P))/v(y(P)) \geq n\right\} \cup \{O\}$$

es un subgrupo de $E_1(\mathcal{K})$ y se cumple:

(i) $E_n(\mathcal{K})/E_{n+1}(\mathcal{K}) \simeq (k, +)$ y

(ii) $\bigcap_{n\geq 1} E_n(\mathcal{K}) = \{O\}$.

El iso viene dado por $E_u(\mathcal{K}) \xrightarrow{\phi_u} k$, donde

$$\begin{cases} \phi_u(x,y) \,=\, \pi^{-u}x/y \\ \phi_u(O) \,=\, 0 \end{cases}$$

Proposición 1. *Sea $m \in \mathbb{Z}$ coprimo con $\mathsf{car}(k)$. Entonces*

(i) $E_1(\mathcal{K})$ no tiene puntos de m-torsión y

(ii) si $\widetilde{E}$ es no singular, $E(\mathcal{K})[m] \hookrightarrow \widetilde{E}(k)$.

Demostración. Sea $P \in E(\mathcal{K})[m]$ y supongamos que $P \in E_n(\mathcal{K})$. Entonces $[m]\cdot P = O$ y, en particular,

$$m\,\phi_n(P) \,=\, \phi_n([m]\cdot P) \,=\, 0\ .$$

Como $\mathsf{car}(k) \nmid m$, $m \in k^\times$ y $\phi_n(P) = 0$. Esto quiere decir que $P \in E_{n+1}(\mathcal{K})$. En particular, por inducción, $E_1(\mathcal{K})$ no tiene puntos de m-torsión. Para la segunda parte, el núcleo de la redución es $E_1(\mathcal{K})$, pero $E(\mathcal{K})[m] \cap E_1(\mathcal{K}) = \{O\}$. □

Definición 2. Sea $E/\mathcal{K}$ una curva elíptica dada por ecuación minimal. Se dice que la curva (i) *tiene buena reducción*, si $\widetilde{E}(k)$ es no singular; (ii) *tiene reducción multiplicativa*, si la curva reducida es *nodal*; (iii) *tiene reducción aditiva*, si la curva reducida es *cuspidal*. Cuando la reducción es multiplicativa, se dice, además, que es (a) *split*, si las pendientes de las tangentes a $\widetilde{E}(k)$ en el nodo están definidas sobre k; (b) *non-split*, en caso contrario.

Observación 3. Una curva dada por ecuación de Weierstrass es no singular, si y sólo si su discriminante es no nulo. En caso contrario, tiene un nodo, si ($\Delta = 0$ y) $c_4 \neq 0$, y el punto singular es una cúspide, si ($\Delta = 0$ y) $c_4 = 0$.

La curva $E/\mathcal{K}$ tiene vuena reducción, si y sólo si $v(\Delta) > 0$ (equivalentemente, $\Delta \in \mathcal{R} \smallsetminus \mathcal{M} = \mathcal{R}^\times$). Si $\Delta \equiv 0 \,(\mathsf{mod}\,\mathcal{M})$, entonces la reducción es multiplicativa, si $v(c_4) = 0$ y es aditiva, si $v(c_4) > 0$.

Definición 4. Se dice que $E/\mathcal{K}$ tiene *mala reducción potencialmente buena*, si, vista como una curva sobre $\mathcal{K}'/\mathcal{K}$, alguna extensión finita, tiene buena reducción.

Proposición 5. *Sea $E/\mathcal{K}$ una curva elíptica y sea $\mathcal{K}'/\mathcal{K}$ una extensión de cuerpos.*

(i) Si la extensión es no ramificada, es decir, $[\mathcal{K}' : \mathcal{K}] = [k' : k]$, o, equivalentemente, $\mathcal{R}'\pi = \mathcal{M}'$, entonces el tipo de reducción de E en tanto curva sobre $\mathcal{K}'$ es el mismo que en tanto curva sobre $\mathcal{K}$;

(ii) si $\mathcal{K}'/\mathcal{K}$ es finita y la reducción de E sobre $\mathcal{K}$ es buena, o bien mala y multiplicativa, entonces la reducción sobre $\mathcal{K}'$ es buena, o, respectivamente, mala y multiplicativa;

(iii) en cualquier caso, existe $\mathcal{K}'/\mathcal{K}$ finita tal que $E/\mathcal{K}'$ tiene reducción buena o bien split multiplicativa;

(iv) la reducción es potencialmete buena, si y sólo si $j(E) \in \mathcal{R}$.

Demostración. Los items (i) y (ii) se desprenden de la minimalidad de la ecuación que define a E, de que $v'|_{\mathcal{K}} = v$, si $\mathcal{K}'/\mathcal{K}$ es no ramificada, y de que $v'|_{\mathcal{K}}$ es un múltiplo no nulo de v en el caso finito, haciendo cambios de variable que preserven la forma de Weierstrass. Para ver (iii), asumiendo característica distinta de 2, en cierta extensión finita $\mathcal{K}'/\mathcal{K}$, la curva $E/\mathcal{K}'$ se puede expresar en forma de Legendre:

$$E \,:\, y^2 \,=\, x\,(x-1)\,(x-\lambda)\ ,$$

con $\lambda \neq 0, 1$. Entonces

$$c_4 \,=\, 16\,(\lambda^2-\lambda+1) \quad \text{y} \quad \Delta \,=\, 16\,\lambda^2\,(\lambda-1)^2\ .$$

(i) Si $\lambda \in \mathcal{R}'$ y $\lambda \neq 0, 1$ en k', entonces $\Delta \not\equiv 0\,(\mathsf{mod}\,\mathcal{M}')$ y $\Delta \in {\mathcal{R}'}^{\times}$;

(ii) si $\lambda = 0$ o $\lambda = 1$ en k', $\Delta \equiv 0\,(\mathsf{mod}\,\mathcal{M})$, pero $c_4 \in {\mathcal{R}'}^{\times}$;

(iii) si $\lambda \notin {\mathcal{R}'}^{\times}$, pasa a ser una unidad en $\mathcal{R}'$, si se lo multiplica por alguna potencia positiva del uniformizadr π'.

Se hace el cambio $x = x'\pi'^{-r}$, $y = y'\pi'^{-3r/2}$, donde r es tal que $\lambda\pi'^{r} \in {\mathcal{R}'}^{\times}$. Reemplazando, posiblemente, $\mathcal{K}'$ por una extensión cuadrática,

$$\begin{aligned} y'^2\pi'^{-3r} \,&=\, x'\pi'^{-r}\,(x'\pi'^{-r}-1)\,(x'\pi'^{-r}-\lambda) \quad \text{o bien,} \\ y'^2 \,&=\, x'\,(x'-\pi'^{r})\,(x'-\lambda\pi'^{r})\ . \end{aligned}$$

Si $\Delta' = u^{-12}\Delta$ y $c_4' = u^{-4}c_4$ son los valores asociados a esta ecuación, entonces $\Delta' \in \mathcal{M}'$ y $c_4' \in {\mathcal{R}'}^{\times}$. En (i) la reducción es buena, en (ii) es multiplicativa y en (iii) es multiplicativa en una extensión, a lo sumo, cuadrática de $\mathcal{K}'$. Por otro lado, reducción non-split pasa a ser split en alguna extensión cuadrática.

Para (d), asumiendo de nuevo $\mathsf{car}(k) \neq 2$ y llevando la curva a forma de Legendre, se puede verificar que

$$256\,(1-\lambda\,(1-\lambda))^3 - j\,\lambda^2\,(1-\lambda)^2 \,=\, 0\ .$$

En particular, $v(\lambda\,(1-\lambda)) \geq 0$. Si $v(\lambda) < 0$, entonces $v(\lambda\,(1-\lambda)) = v(\lambda) + v(1-\lambda) = v(\lambda) + v(\lambda) < 0$, lo que es absurdo. Entonces

$$v(\lambda) \,\geq\, 0\ .$$

Como 256 es una unidad en $\mathcal{R}$, reduciendo, tiene que ser $\lambda \not\equiv 0, 1\,(\mathsf{mod}\,\mathcal{M})$, y la reducción es buena.

Si, recíprocamente, la reducción es potencialmente buena, y buena sobre una extensión finita $\mathcal{K}'/\mathcal{K}$, denotando con Δ' el discriminante minimal de $E/\mathcal{K}'$ y c_4' el otro valor asociado a la ecuación minimal, se deduce que

$$j(E/\mathcal{K}') \;=\; {c_4'}^3/\Delta' \;.$$

Como $c_4' \in \mathcal{R}'$ y la reducción es buena sobre $\mathcal{K}'$, el discriminante minimal es una unidad y $j(E/\mathcal{K}') \in \mathcal{R}'$. Como E está definida sobre $\mathcal{K}$, vale que $j \in \mathcal{R}' \cap \mathcal{K} = \mathcal{R}$. □

3 Inercia

Sea $\overline{\mathcal{K}}/\mathcal{K}$ una clausura algebraica de $\mathcal{K}$ y sea $\mathcal{K}^{\mathsf{nr}}/\mathcal{K}$ la máxima extensió no ramificada en $\overline{\mathcal{K}}$ ($\pi \in \mathcal{K}$ es generador de $\mathcal{M}$ y también genera el ideal maximal en el anillo de enteros de $\mathcal{K}^{\mathsf{nr}}$). Sean $G = \mathsf{Gal}\big(\overline{\mathcal{K}}/\mathcal{K}\big)$ e $I_v \equiv I := \mathsf{Gal}\big(\overline{\mathcal{K}}/\mathcal{K}^{\mathsf{nr}}\big)$ el *subgrupo de inercia* ($I \triangleleft G$). Hay una correspondencia entre extensiones no ramificadas de $\mathcal{K}$ y extensiones de su cuerpo residual k. En particular, el cuerpo residual de $\mathcal{K}^{\mathsf{nr}}$ es $\overline{k}$, una clausura de k.

El grupo de Galois G actúa sobre los puntos de m-torsión $E[m]$, para cada m y sobre los *módulos de Tate*

$$\mathsf{T}_l(E) \;:=\; \lim_{\leftarrow} E[l^r] \;, \tag{4}$$

para cada l.

Proposición 6. *Sea $E/\mathcal{K}$ una curva elíptica con buena reducción ($\widetilde{E}/k$ no singular). Sean $m, l \geq 1$ enteros coprimos con $\mathsf{car}(k)$, con l primo. Entonces*

(i) el grupo I_v actúa trivialmente sobre $E[m]$ y

(ii) la acción de I_v sobre $\mathsf{T}_l(E)$ es trivial.

Definición 7. Sea Σ un conjunto sobre el cual G actúa ($\rho : G \to \mathsf{Aut}(\Sigma)$). Si la acción del subgrupo de inercia es trivial ($I_v \subset \mathsf{ker}(\rho)$), se dice que Σ *es no ramificado (en v).*

Demostración (de 6). El ítem (ii) se deduce de (i). Para demostrar (i), supongamos que $\mathcal{K}'/\mathcal{K}$ es una extensión (finita) que contiene a toda la m-torsión/ Si la ecuación que define a E está en forma de Weierstrass (y es minimal), como la curva tiene buena reducción, tiene que ser $v_{\mathcal{K}}(\Delta) = 0$. Como el grado de $\mathcal{K}'$ sobre $\mathcal{K}$ es finito,

$$v_{\mathcal{K}'}(\Delta) \;=\; e \cdot v_{\mathcal{K}}(\Delta) \;=\; 0$$

Como los coeficientes de la ecuación para E pertenecen a $\mathcal{R}'$, la misma es una ecuación minimal sobre $\mathcal{K}'$. Además, la curva $E/\mathcal{K}'$ tiene buen a reducción, con lo que $\widetilde{E}/k'$ es no singular y

$$E[m] \;=\; E(\mathcal{K}')[m] \;\hookrightarrow\; \widetilde{E}(k') \;. \tag{5}$$

Sea $P \in E[m]$ y sea $\sigma \in I$. Se tiene que

$$[m]\,\big(P^\sigma - P\big) \;=\; ([m]\,P)^\sigma - [m]\,P \;=\; 0 \;,$$

lo que implica $P^\sigma - P \in E[m]$. Ahora,

$$\widetilde{P^\sigma - P} = \widetilde{P}^\sigma - \widetilde{P} = 0 \ ,$$

pues I actúa trivialmente en $\widetilde{E}(k')$ (por definición). La inclusión (5), implica, finalmente, que $P^\sigma = P$. □

4 El criterio

Proposición 8. *Sea $E/\mathcal{K}$ una curva elíptica tal quje los grupos de m-torsión $E[m]$ son no ramificados para una cantidad infinita de enteros $m \geq 1$ y coprimos con $\mathsf{car}(k)$. Entonces E tiene buena reducción.*

Demostración. Se tienen dos sucesiones exactas cortas de grupos

$$0 \longrightarrow E_0 \longrightarrow E \longrightarrow E/E_0 \longrightarrow 0 \quad \text{y}$$

$$0 \longrightarrow E_1 \longrightarrow E_0 \longrightarrow \widetilde{E}_{\mathsf{ns}} \longrightarrow 0$$

Si $\mathcal{K}^{\mathsf{nr}}$ es la extensión no ramificada maximal de $\mathcal{K}$ en $\overline{\mathcal{K}}$, el cuerpo residual de $\mathcal{K}^{\mathsf{nr}}$ es $\overline{k}$. Usando la de modelos de Néron para una curva elíptica, "esquemas en grupos con fibra geométrica E/k", se puede decir lo siguiente:

(i) Si $E/\mathcal{K}$ tiene reducción split multiplicativa, entonces $E(\mathcal{K})/E_0(\mathcal{K})$ es cíclico de orden $v(\Delta)$;

(ii) en cualquier otro caso, dicho cociente es un grupo finito de orden, a lo sumo, 4.

Algo de esto se había demostrado en clase, pero la demostración se basaba en la finitud del cuerpo residual, que, ciertamente, no se cumple para $\mathcal{K}^{\mathsf{nr}}$. Bajo las hipótesis de la proposición, se puede deducir que existe un (existen infinitos) enteros $m \geq 1$ que cumple(n) simultáneamente con:

(i) $(m, \mathsf{car}(k)) = 1$,

(ii) $m > \#\big(E(\mathcal{K}^{\mathsf{nr}})/E_0(\mathcal{K}^{\mathsf{nr}})\big)$ y

(iii) $E[m]$ es no ramificado.

En particular, la m-torsión está contenida en $E(\mathcal{K}^{\mathsf{nr}})$ y $E(\mathcal{K}^{\mathsf{nr}})$ contiene un subgrupo A isomorfo a $\big(\mathbb{Z}/m\mathbb{Z}\big)^2$. Ahora bien,

$$E_0(\mathcal{K}^{\mathsf{nr}}) \cap A \leq A \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \ ,$$

lo que implica que

$$E_0(\mathcal{K}^{\mathsf{nr}}) \cap A \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \ ,$$

con $a, b \mid m$. Además,

$$E(\mathcal{K}^{\mathsf{nr}})/E_0(\mathcal{K}^{\mathsf{nr}}) \supset E_0(\mathcal{K}^{\mathsf{nr}}) \cdot A/E_0(\mathcal{K}^{\mathsf{nr}}) \simeq A/E_0(\mathcal{K}^{\mathsf{nr}}) \cap A \ .$$

Así, $m > \frac{m^2}{ab}$, lo quje fuerza que exista un primo l que divida tanto a a como a b. En definitiva, existe un subgrupo B de $E_0(\mathcal{K}^{\mathsf{nr}})$ isomorfo a $\left(\mathbb{Z}/l\mathbb{Z}\right)^2$. Usando

$$0 \longrightarrow E_1(\mathcal{K}^{\mathsf{nr}}) \longrightarrow E_0(\mathcal{K}^{\mathsf{nr}}) \longrightarrow \widetilde{E}_{\mathsf{ns}}(\overline{k}) \longrightarrow 0 \ ,$$

que $l \neq \mathsf{car}(k)$ y que $E_1(\mathcal{K}^{\mathsf{nr}})$ no tiene puntos de orden l,

$$E_1(\mathcal{K}^{\mathsf{nr}}) \cap B = 1 \ ,$$

y, entonces, este grupo pasa a la curva reducida, a sus puntos no singulares. Ahora, si E tuviese mala reducción, habría dos posibilidades:

(i) $\widetilde{E}_{\mathsf{ns}}(\overline{k}) \simeq \overline{k}^{\times}$ (red. mult.), o bien

(ii) $\widetilde{E}_{\mathsf{ns}}(\overline{k}) \simeq (\overline{k}, +)$ (red. ad.).

El segundo caso no es viable, porque no hay l-torsión en $(\overline{k}, +)$. Por otra parte, en $\overline{k}^{\times}$, la l-torsión consiste en las raíces l-ésimas de la unidad en $\overline{k}$, y éstas constituyen un grupo cíclico de orden l. La primera de las opciones, tampoco es posible. En consecuencia, $E/\mathcal{K}^{\mathsf{nr}}$ tiene buena reducción. Como bajo toda extensión no ramificada, el tipo de reducción se preserva, E tampoco tiene mala reducción sobre $\mathcal{K}$. □

Teorema 9. *Las siguientes son equivalentes:*

(i) E tiene buena reducción;

(ii) $E[m]$ es no ramificado para todo $m \geq 1$ coprimo con $\mathsf{car}(k)$;

(iii) $\mathsf{T}_l(E)$ es no ramificado para (algún) primo l coprimo con $\mathsf{car}(k)$;

(iv) $E[m]$ es no ramificado para infinitos enteros $m \geq 1$ coprimos con $\mathsf{car}(k)$.

Éste es el *criterio de Néron-Ogg-Shafarevich*. Este "criterio" se puede ver desde el lado de las representaciones.

Sea $E/\mathbb{Q}$ una curva elíptica dada por ecuación de Weierstrass, (1), con $a_i \in \mathbb{Q}$. Haciendo cambios de variable de la forma

$$(x, y) = (u^2 x', u^3 y') \ ,$$

se obtiene una nueva ecuación con coeficientes

$$a_i' = a_i/u^i \ .$$

(Se puede llevar a una ecuación con coeficientes enteros). Sea $m_p(E)$ la menor potencia de p que divide al discriminante Δ de alguna de las ecuaciones con coeficientes enteros

equivalente a la ecuación que define a E –dos ecuaciones se dicen *equivalentes*, si están relacionadas por un cambio de variables "admisible". Se define el *discriminante global de* E como

$$\Delta_{\mathsf{min}}(E) := \prod_p p^{m_p(E)}$$

(si $p \nmid \Delta(E)$, entonces $m_p(E) := 0$). Es posible llevar la ecuación de E, vía cambios de variable admisibles, a una cuyo discriminante minimice todas las valuaciones, es decir, existe una ecuación equivalente E' tal que $m_p(E) = v_p(\Delta(E'))$. Así, $\Delta(E') = \Delta_{\mathsf{min}}(E)$. Una ecuación E' con estas características se denomina *ecuación de Weierstrass minimal global*.

Sea N el conductor de E, divisible exactamente por los primos de mala reducción. Dado un primo l, el módulo de Tate $\mathsf{T}_l(E)$ proporciona una representación de $G = \mathsf{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$, un morfismo continuo

$$\rho = \rho_{E,l} : G \to \mathsf{GL}_2(\mathbb{Z}_l) \subset \mathsf{GL}_2(\mathbb{Q}_l) .$$

Sea $p \in \mathbb{Z}$ un primo arbitrario y sea $\mathfrak{p} \subset \overline{\mathbb{Z}}$ primo maximal arriba de p ($\mathfrak{p} = \mathsf{ker}(\overline{\mathbb{Z}} \to \overline{\mathbb{F}_p})$). Se definen

$$\begin{aligned} D_{\mathfrak{p}} &:= \big\{\sigma \in G : \mathfrak{p}^\sigma = \mathfrak{p}\big\} \quad \text{e} \\ I_{\mathfrak{p}} &:= \big\{\sigma \in D_{\mathfrak{p}} : x^\sigma \equiv x \,(\mathsf{mod}\,\mathfrak{p})\, \forall x \in \overline{\mathbb{Z}}\big\} , \end{aligned}$$

respectivamente, el *grupo de descomposición de* $\mathfrak{p}$ y el *subgrupo de inercia*. Alternativamente, $I_{\mathfrak{p}}$ se puede describir como el núcleo de un morfismo sobreyectivo $D_{\mathfrak{p}} \to \mathsf{Gal}\big(\overline{\mathbb{F}_p}/\mathbb{F}_p\big)$. Sea $\sigma_p : x \mapsto x^p$ y se $\mathsf{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ cualquier preimagen de σ_p por este morfismo sobre.

Una representación $\rho : G \to \mathsf{GL}_d(L)$ (morfismo continuo, $d \geq 1$, $L/\mathbb{Q}_l$ extensión finita) se dice *no ramificada en* p, si $I_{\mathfrak{p}} \subset \mathsf{ker}(\rho)$, cualquiera sea $\mathfrak{p}$ arriba de p. Entonces, usando esta terminología, el criterio de Néron-Ogg-Shafarevich, Teorema 9, dice que

Teorema 10. *la rep.* $\rho_{E,l}$ *es no ramificada en todo primo* p *que no divide a* $l \cdot N$.

5 Comentarios

A modo de comentario, este criterio, junto con otros resultados no del todo triviales, permite deducir el siguiente teorema.

Teorema 11. *Sean* E, E' *curvas elípticas sobre* $\mathbb{Q}$ *(o sobre un cuerpo de números arbitrario) y sean* $V_l(E), V_l(E')$ *las representaciones asociadas vía el módulo de Tate. Si los módulos –es decir, las representaciones– son isomorfos y* $j(E)$ *no es un entero, entonces las curvas* E *y* E' *son isógenas.*

Hay, también, otros resultados simpáticos que relacionan buena reducción con isogenía:

Teorema 12 (Shafarevich)**.** *Sea $S \subset V^{\mathcal{K}}$, $\#S < \infty$, entonces el conjunto de clases de $\mathcal{K}$-isomorfismo de curvas elípticas con buena reducción fuera de S es finito.*

Teorema 13. *Dos curvas isógenas dan representaciones isomorfas.*

En particular, esto implica que, si E y E' son $\mathcal{K}$-isógenas, buena reducción de una en un lugar v es acompañada de buena reducción de la otra en el mismo lugar.

Teorema 14. *Sea $E/\mathcal{K}$ una curva elíptica. Salvo isomorfismo, hay una cantidad finita de curvas $\mathcal{K}$-isógenas a E.*

En otras palabras, cada clase de $\mathcal{K}$-isogenía está compuesta por una cantidad finita de clases de isomorfismo.

Referencias

[1] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Vol. 106. New York, NY: Springer, 2009, pp. xx + 513.