La altura de Faltings de una curva elíptica

Héctor Pastén, editado y con apuntes por José Cuevas Barrientos

Resumen. En ésta charla explicaremos qué es la altura de Faltings de una curva elíptica, y cómo se relaciona a otros invariantes tales como el discriminante minimal y el invariante j. Con esto, enunciaremos la llamada «conjetura de la altura» y veremos que ésta implica la conjetura *abc*.

1. Repaso de alturas

Esta sección resume unos resultados folclóricos incluídos, por ejemplo, en Lang **[6]**.

Sobre una extensión finita $K/\mathbb{Q}$ denotaremos por M_K al conjunto de todos los lugares de K (i.e., todos los valores absolutos no triviales, cocientados por la relación de «ser equivalentes»). Todo lugar $v \in M_K$ se restringe a un lugar $w \in M_{\mathbb{Q}}$ y estos últimos son, por un teorema de Ostrowski, o bien el valor absoluto usual $|\,|_\infty$ o bien el valor absoluto p-ádico $|\,|_p$; denotaremos por $|\,|_v$ el valor absoluto asociado a v que extiende (como función) al correspondiente valor absoluto $|\,|_w$ sobre $\mathbb{Q}$. Como consecuencia, sobre K tenemos los siguientes lugares:

1. **Lugares arquimedianos,** los cuales se restringen a $w = \infty$ el lugar usual. Estos, a su vez, se subdividen en dos clases:
   (a) **Lugares reales:** Son aquellos que están en correspondencia con los encajes $K \hookrightarrow \mathbb{R}$. Así, dado un lugar $v \in M_K$ real asociado al encaje $\sigma\colon K \to \mathbb{R}$ tenemos la fórmula $|a|_v = |\sigma a|$, donde $|\,|$ denota el valor absoluto usual en $\mathbb{R}$.
   (b) **Lugares imaginarios:** Son aquellos que están en correspondencia con los encajes $\tau\colon K \hookrightarrow \mathbb{C}$ salvo conjugación, donde $\tau[K] \nsubseteq \mathbb{R}$. Así, dado un lugar $v \in M_K$ imaginario asociado al encaje $\tau\colon K \to \mathbb{R}$ tenemos la fórmula $|a|_v = |\tau a|$, donde $|\,|$ denota el valor absoluto usual en $\mathbb{C}$.
2. **Lugares finitos:** Estos están en correspondencia con los ideales primos $\mathfrak{p}$ del anillo de enteros algebraicos $\mathcal{O}_K$.

La necesidad de las normalizaciones yace en la siguiente proposición fundamental:

Fecha: 24 de mayo de 2024.

Proposición 1.1 (fórmula del producto): Sea K un cuerpo numérico. Para todo $a \in K^\times$ se cumple que

$$\prod_{v \in M_K} |a|_v = 1.$$

DEMOSTRACIÓN: Cfr. LANG [**6,** pág. 19]. □

En general, la definición es la siguiente:

Definición 1.2: Sea K un cuerpo numérico. Definimos la ***altura multiplicativa*** sobre $\mathbb{P}^n(K)$ como

$$P := [a_0 : \cdots : a_n] \in \mathbb{P}^n(K) \qquad H_K(P) := \prod_{v \in M_K} \text{máx}\{|a_j|_v : 0 \leq j \leq n\},$$

donde M_K denota los lugares de K. Definimos la ***altura (aditiva o logarítmica)*** sobre $\mathbb{P}^n(K)$ como

$$h_K(P) := \log H_K(P) = \sum_{v \in M_K} \text{máx}\{\log |a_j|_v : 0 \leq j \leq n\}.$$

Observación 1.2.1: La fórmula del producto es precisamente el resultado necesario para probar que la definición anterior no depende de las coordenadas escogidas para un punto proyectivo. Así, el lector puede apreciar que podríamos dar la definición anterior (y muchos de los resultados de geometría diofantina) para un cuerpo con un conjunto de valores absolutos que satisfaga la fórmula del producto.

Ejemplo. Sea $x = a/b \in \mathbb{Q}$ un número racional con $a, b \in \mathbb{Z}$ enteros coprimos. Se cumple que $H_\mathbb{Q}(x) = \text{máx}\{|a|, |b|\}$, recuperando así la «definición intuitiva».

Proposición 1.3: Sea K un cuerpo numérico y L/K una extensión finita. Para todo $P \in \mathbb{P}^n(K)$ se cumple que

$$H_L(P) = H_K(P)^{[L:K]}, \qquad h_L(P) = [L : K] \cdot h_K(P).$$

Definición 1.4: Sea K un cuerpo semiglobal. Para un punto proyectivo $P \in \mathbb{P}^n(K^{\text{alg}})$ elegimos una extensión finita L/K tal que $P \in \mathbb{P}^n(L)$, y definimos sus ***alturas absolutas*** (relativas a K) por las fórmulas:

$$H_K(P) := H_L(P)^{1/[L:K]}, \qquad h_K(P) := \frac{1}{[L : K]} h_L(P).$$

Esto también induce una función de alturas sobre el espacio afín $\mathbb{A}^n_{K^{\text{alg}}}$ empleando el encaje

$$(x_1, \ldots, x_n) \longmapsto [1 : x_1 : \cdots : x_n].$$

En particular, denotando $\log^+ t := \max\{0, \log t\}$ extendida por $\log^+(0) := 0$, entonces se sigue que la altura en el espacio afín es

$$\boldsymbol{x} := (x_1, \dots, x_n) \in \mathbb{A}^n(L) \quad h(\boldsymbol{x}) = \frac{1}{[L : K]} \sum_{w \in M_L} \max_j \{\log^+ \|x_j\|_w\};$$

y, más en particular, la altura de un elemento algebraico $\alpha \in L \subseteq K^{\mathrm{alg}}$ es

$$h(\alpha) = \frac{1}{[L : K]} \sum_{w \in M_L} \log^+ \|\alpha\|_w.$$

Así, tenemos una noción de *altura* sobre puntos del espacio proyectivo. Más generalmente, dado un K-morfismo $\varphi\colon X \to \mathbb{P}^n_K$, uno puede definir la ***altura de Weil*** sobre los puntos geométricos $X(K^{\mathrm{alg}})$ como $h_\varphi(x) := h(\varphi(x))$. Es evidente que esta definición depende del K-morfismo; una situación en dónde se vuelve menos evidente es que si tomamos un haz sobre X, entonces un conjunto de secciones globales inducen una función hacia algún espacio proyectivo, lo cual induce una altura de Weil.

El siguiente resultado es también fundamental:

Teorema 1.5 (Northcott): Dado $d \in \mathbb{N}$ y $r \geq 0$, entonces existen finitos puntos proyectivos $P \in \mathbb{P}^n(\mathbb{Q}^{\mathrm{alg}})$ con $h(P) \leq r$ y $\deg P \leq d$.

DEMOSTRACIÓN: Cfr. [**6,** pág. 59], Thm. 3.2.6. Para un conteo asintótico más fino, véase un resultado de Schanuel en [**6,** pág. 71], Thm. 3.5.3. □

Aplicando este teorema a una altura de Weil asociada a un morfismo cuasifinito, obtenemos la misma conclusión. Cuando una altura satisface el teorema anterior, decimos que satisface la ***propiedad de Northcott***.

En otras palabras, *una* altura sobre una K-variedad (o sobre un esquema algebraico, en general) es una función que a puntos (o $\mathbb{Q}$-variedades de dimensión 0) les otorga números reales. La *altura de Faltings* pretende ser similarmente una función que a curvas elípticas les otorgue números reales.

Podemos dar con las siguientes definiciones:

Definición 1.6: Sea E una curva elíptica sobre un cuerpo numérico K con ecuación de Weierstrass minimal

$$E\colon \quad y^2 = x^3 - 27c_4 x - 54c_6, \qquad c_4, c_6 \in \mathcal{O}_K.$$

Definimos la ***altura intuitiva*** (eng. *naïve*) de E como $h_{\mathrm{na}}(E) := h([c_4 : c_6])$. Por otro lado, si j_E denota el invariante j de E, entonces podemos definir la ***altura de moduli*** de E como $h_{\mathrm{mod}}(E) := h(j_E)$.

Se le llama *altura de moduli* porque el invariante j determina una biyección entre puntos de $\mathbb{A}^1(K)$ y curvas elípticas (salvo isomorfismo) sobre un cuerpo algebraicamente cerrado K. Así, vemos a E como un punto de $\mathbb{A}^1_K$ y éste último posee una función de altura canónica.

Observación 1.6.1: La altura intuitiva satisface la propiedad de Northcott. En cambio, la altura de moduli no satisface la propiedad de Northcott: esto debido a que, sobre un cuerpo numérico K, hay curvas elípticas con infinitos torcimientos (eng. *twists*).

Definición 1.7 (Arakelov): Sea K un cuerpo numérico con anillo de enteros $A := \mathcal{O}_K$. Sea $\mathscr{L}$ un haz inversible sobre $\operatorname{Spec} A$ (i.e., un A-módulo proyectivo de rango 1). Un par $(\mathscr{L}, |\,|)$ se dice un ***haz metrizado*** si para cada lugar arquimediano $v \in M_K^\infty$ se cumple que $|\,|_v$ es una norma v-ádica sobre el K_v-espacio vectorial $\mathscr{L} \otimes_A K_v$.

El ***grado*** de un haz metrizado es

$$\deg(\mathscr{L}, |\,|) = \log|\mathscr{L}/At| - \sum_{v \in M_K^\infty} \log \|t\|_v,$$

donde $t \in \mathscr{L}$ es un elemento arbitrario no nulo, y donde $\|\,\|_v = |\,|_v$ cuando v es un lugar real y $\|\,\|_v = |\,|_v^2$ cuando v es imaginario.

Observación 1.7.1: Es fácil verificar que la definición del grado no depende de la elección del $t \in \mathscr{L}$.

Ejemplo 1.8: Si K es un cuerpo numérico cuyo $\mathcal{O}_K$ es un DIP (e.g., $K \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2})\}$, etc.), entonces podemos identificar a $\mathscr{L}$ con un ideal fraccionario, el cual será de la forma $\alpha\mathcal{O}_K$ con $\alpha \in K$ y así

$$\deg(\mathscr{L}, |\,|) = -\sum_{v \in M_K^\infty} \log \|\alpha\|_v. \qquad \lrcorner$$

2. La altura de Faltings

Primero describiremos la situación en general, casi siguiendo a Faltings **[4]**, y luego daremos indicaciones para el caso de curvas elípticas sobre $\mathbb{Q}$.

Sea A una variedad abeliana de dimensión g sobre un cuerpo numérico K. Denotaremos por $N(A) \to \operatorname{Spec}(\mathcal{O}_K)$ su modelo de Néron, el cual es un $\mathcal{O}_K$-esquema en grupos con sección $\varepsilon\colon \operatorname{Spec}(\mathcal{O}_K) \to N(A)$ y sea $\omega_{A/K} := \varepsilon^*\Omega^g_{N(A)/\mathcal{O}_\mathcal{K}}$, el cual es un haz inversible sobre $\operatorname{Spec}(\mathcal{O}_\mathcal{K})$. A éste podemos dotarlo de la siguiente métrica: nótese que todo lugar arquimediano $v \in M_K^\infty$ determina un encaje $K \hookrightarrow \mathbb{C}$, el cual dota a $A(K_v^{\mathrm{alg}})$ de estructura de variedad analítica compacta. Si ahora consideramos una sección meromorfa

$$\alpha \in \omega_A \otimes_A K = \Gamma(A, \Omega^g_{A/K})$$

ésta la podemos identificar con una forma diferencial analítica sobre $A(K_v^{\mathrm{alg}})$ y definimos

$$\|\alpha\|_v := \left(\frac{\mathrm{i}}{2}\right)^g \int_{A(K_v^{\mathrm{alg}})} |\alpha \wedge \overline{\alpha}|.$$

Definición 2.1: La ***altura de Faltings*** de una variedad abeliana A_K de dimensión g sobre un cuerpo numérico K es

$$h_{\mathrm{Fa}}(A_K) := \frac{1}{[K:\mathbb{Q}]} \deg(\omega_{A/K}, |\,|),$$

donde $(\omega_{A/K}, |\,|)$ es el haz metrizado construído en el párrafo anterior.

Esta definición depende del cuerpo base K para la variedad A. Para más información, véase el lema A.4 más adelante.

Desenredemos la definición en el caso de curvas elípticas. En primer lugar, tenemos la siguiente definición concreta del modelo de Néron:

Proposición 2.2: Sea E una curva elíptica sobre un cuerpo numérico K, con modelo de Néron $\mathcal{E}$ sobre el anillo de enteros $\mathcal{O}_K$. Entonces:

1. $\mathcal{E}$ es un $\mathcal{O}_K$-esquema en grupos de tipo finito. Por ende, la componente conexa del neutro $\mathcal{E}^\circ$ es un subesquema en grupos.
2. $\mathcal{E}^0$ es isomorfo (como $\mathcal{O}_K$-esquema) al *locus* suave del $\mathcal{O}_K$-esquema proyectivo dado por una ecuación de Weierstrass minimal de E.

Demostración: Cfr. Bosch *et al.* [**1,** págs. 14, 21], Prop. 1.2.6 y Prop. 1.5.1. □

Observación 2.2.1: No toda curva elíptica sobre un cuerpo numérico K admite una ecuación de Weierstrass minimal; pero este sí es el caso cuando $\mathcal{O}_K$ es un DIP (e.g., cuando $K = \mathbb{Q}$ o $\mathbb{Q}(\sqrt{-1})$).

Por la observación anterior y por el ejemplo 1.8 nos reduciremos al caso en que $\mathcal{O}_K$ sea un DIP. En este caso, llamaremos un ***diferencial de Néron*** a un generador de $\omega_{E/K}$ como $\mathcal{O}_K$-módulo libre. Gracias a la proposición anterior, no resulta sorprendente lo siguiente:

Lema 2.3: Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass minimal

$$E\colon \quad y^2 = x^3 - 27c_4 x - 54c_6, \qquad c_4, c_6 \in \mathbb{Z}, \tag{1}$$

El diferencial $\omega := \mathrm{d}x/(2y) \in \Gamma(E, \Omega^1_{E/\mathbb{Q}})$ es independiente, salvo signo, de la elección de (1).

Demostración: Cfr. Silverman [**7,** pág. 186], Prop. VII.1.3(b). □

Cuando $K=\mathbb{Q}$, hay un único lugar arquimediano correspondiente al valor absoluto usual $|\ |_\infty$, así que la definición de altura de Faltings en este contexto da

$$h_{\mathrm{Fa}}(E) = -\log\left|\frac{\mathrm{i}}{2}\int_{E(\mathbb{C})}\omega\wedge\overline{\omega}\right|.$$

Finalmente, démosle otra interpretación a la integral en la fórmula anterior: escribiendo $z=s+\mathrm{i}t$ tenemos que

$$\int_D \mathrm{d}s\wedge\mathrm{d}t = \frac{\mathrm{i}}{2}\int_D \mathrm{d}z\wedge\overline{\mathrm{d}z},$$

donde $D\subseteq\mathbb{C}$ denota un dominio.

Así, empleando que $E(\mathbb{C})$ es biholomorfo (como variedad analítica) a un cociente $\mathbb{C}/\Lambda$, donde $\Lambda\subseteq\mathbb{C}$ denota un reticulado (i.e., $\mathbb{Z}$-submódulo libre de rango 2, discreto), un cálculo demuestra que

$$\frac{\mathrm{i}}{2}\int_{E(\mathbb{C})}\omega\wedge\overline{\omega} = \text{área de un dominio fundamental de } \Lambda;$$

esto se extiende en general para variedades abelianas (cfr. [**2,** pág. 250]).

Definición 2.4: Sea E una curva elíptica sobre un cuerpo numérico K. Denotaremos por $\mathfrak{d}_{E/K}$ al (ideal) discriminante minimal de E. Sea j_E el invariante j de E, entonces existen ideales coprimos $\mathfrak{a},\mathfrak{b}$ de $\mathcal{O}_K$ tales que

$$j_E\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$$

(como $\mathcal{O}_K$-ideales fraccionarios). Es fácil probar que $\mathfrak{b}\mid\mathfrak{d}_{E/K}$, de modo que llamamos el ***discriminante minimal inestable*** de E al ideal entero

$$\Upsilon_{E/K} := \mathfrak{d}_{E/K}\mathfrak{b}^{-1}.$$

La definición viene justificada por lo siguiente:

Lema 2.5: Sea E una curva elíptica sobre un cuerpo numérico K. Si E es semiestable (i.e., no tiene primos de reducción aditiva), entonces $\Upsilon_{E/K}=(1)$.

Demostración: Sea $\mathfrak{p}\lhd\mathcal{O}_K$ un primo, entonces $\nu_\mathfrak{p}(\mathfrak{b})=n$ syss $\nu_\mathfrak{p}(j_E)=-n$; esto en el algoritmo de Tate nos da que o bien $\nu_\mathfrak{p}(\mathfrak{d}_{E/K})=n$ (en cuyo caso, $f_\mathfrak{p}(E)=1$), o bien $\nu_\mathfrak{p}(\mathfrak{d}_{E/K})=6+n$ (en cuyo caso, $f_\mathfrak{p}(E)=2$ y $\mathfrak{p}\nmid 2$). Esto nos dice, para todo $\mathfrak{p}\nmid 3$, que la reducción es aditiva. Para $\mathfrak{p}\mid 3$, tenemos que el exponente del conductor $f_\mathfrak{p}(E)$ se separa en una parte moderada $\varepsilon_\mathfrak{p}(E)$ (que es 0 cuando la reducción es buena y 1 cuando es multiplicativa), y en una parte salvaje $\delta_\mathfrak{p}(E)$. En este caso, esto nos dice que $\mathfrak{p}$ es de reducción semiestable (a decir, ¡inclusive podría haber buena reducción!). $\square$

Teorema 2.6 (Faltings-Silverman): Sea E una curva elíptica sobre un cuerpo numérico K. Existen constantes universales κ_1, κ_2 tales que

$$\begin{aligned}\kappa_1 &\leq h(j_E) + \frac{1}{[K:\mathbb{Q}]}\log \mathbf{N}\,\Upsilon_{E/K} - 12h_{\mathrm{Fa}}(E_K)\\ &\leq 6\log(1+h(j_E)) + \kappa_2.\end{aligned}$$

En particular, si E es semiestable, se cumple que

$$|h(j_E) - 12h_{\mathrm{Fa}}(E_K)| \leq 6\log(1+h(j_E)) + \kappa_2.$$

Demostración: Cfr. [**2,** pág. 258], Prop. 2.1. □

Esto permite comparar la altura de moduli con la altura de Faltings.

Definición 2.7: Sea K un cuerpo numérico, y sea D un divisor de Weil[1] de $\mathrm{Spec}(\mathcal{O}_K)$, es decir, una suma formal

$$D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \cdot [\mathfrak{p}],$$

donde $\mathfrak{p}$ recorre los primos no nulos de $\mathcal{O}_K$. Definimos su ***grado*** como

$$\deg D = \sum_{\mathfrak{p}} a_{\mathfrak{p}}\, \mathbf{N}(\mathfrak{p}) = \sum_{\mathfrak{p}} a_{\mathfrak{p}}\, p^{f(\mathfrak{p}/p)},$$

donde p denota el primo en $\mathbb{Z}$ tal que $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

Todo ideal fraccionario de $\mathcal{O}_K$ puede verse canónicamente como un divisor (de Weil) en $\mathrm{Spec}(\mathcal{O}_K)$; en particular, invariantes como el discriminante minimal y el conductor de una curva elíptica determinan divisores.

Conjetura de la altura de Frey [5] (1989) 2.8: Sea K un cuerpo numérico. Existen constantes reales $d > 0$ y $c = c(K,d)$ tales que para toda curva elíptica E_K sobre K se cumple

$$h_{\mathrm{Fa}}(E) \leq c + \frac{d}{2[K:\mathbb{Q}]}\deg(\mathfrak{N}_E) \ll \deg(\mathfrak{N}_E),$$

donde $\mathfrak{N}_E$ denota el (ideal) conductor de E.

Proposición 2.9: La conjetura de la altura de Frey implica la conjetura de Szpiro que, a su vez, implica la conjetura *abc* (débil).

[1]En realidad, como $\mathrm{Spec}(\mathcal{O}_K)$ es un esquema regular, existe una biyección entre divisores de Weil y divisores de Cartier.

Apéndice A. La propieda de Northcott para la altura de Faltings

Una pregunta relativamente inmediata es sí es que existe un análogo de la propiedad de Northcott para variedades abelianas sobre un cuerpo numérico K.

Definición A.1: Sea A una variedad abeliana sobre un cuerpo k. Una ***polarización*** es una isogenia (i.e., un homomorfismo de variedades abelianas con núcleo finito) $\lambda\colon A \to A^\vee$ sobre k tal que su cambio de base $\lambda_{k^{\mathrm{alg}}}$ es de la forma $\varphi_{\mathscr{L}}$ donde $\mathscr{L}$ es un haz inversible de $A_{k^{\mathrm{alg}}}$. El ***grado*** de λ se define como $\deg\lambda := |\ker\lambda|$. Una polarización se dice ***principal*** si tiene grado 1 (o equivalentemente, si es un isomorfismo).

Podemos considerar la categoría de pares (A, λ), donde A es una variedad abeliana y λ es una polarización sobre K. La propiedad de Northcott, cuando k es finito, es un resultado central de Tate:

Teorema A.2 (de finitud de Tate, 1966): Sea k un cuerpo finito. Tras fijar un par de enteros g, d existen finitas variedades abelianas A de dimensión g con polarización de grado d^2 (salvo k-isomorfismo).

Demostración: Cfr. Tate [**8**]. □

Una posible estrategia sería la siguiente: si existiera una variedad proyectiva cuyos puntos parametricen clases de isomorfismo de variedades abelianas con polarización de dimensión y grado fijo resp., y probaramos que la altura de Faltings coincide, entonces obtendríamos un análogo del teorema de Tate. Existe un espacio de moduli grueso[2] $\mathscr{A}_{g,d}$ cuyos puntos corresponden a los pares (A, λ) deseados; pero $\mathscr{A}_{g,d}$ no es un esquema, sino un stack algebraico, y tampoco es propio siquiera. La compactificación $\overline{\mathscr{A}}_{g,d}$ tampoco es de gran utilidad, ya que la «altura canónica» (que no hemos dicho cuál es) tiene «singularidades» en la frontera $\overline{\mathscr{A}}_{g,d} \setminus \mathscr{A}_{g,d}$.

Para ver el camino trazado por Faltings, es necesario primero introducir su altura *geométrica*.

Teorema A.3 (de reducción semiestable): Sea A una variedad abeliana sobre un cuerpo numérico K. Entonces existe una extensión finita L/K tal que la variedad abeliana $A_L = A \times_K \operatorname{Spec} L$ dada por cambio de base es semiestable sobre L.

[2]Sea よ$A\colon \mathsf{Sch} \to \mathsf{Set}$ un funtor representable por un stack A. Se dice que A es un *espacio de moduli fino* (resp. *grueso*) cuando refleja isomorfismos para una cierta clase de variedades sobre un cuerpo cualquiera (resp. sobre un cuerpo algebraicamente cerrado).

Demostración: Cfr. Bosch *et al.* [**1,** pág. 246], Thm. 9.2.7. El caso de curvas elípticas está tratado en la Prop. VIII.5.3 de Silverman [**7,** pág. 197]. □

Lema A.4: Sea A_K una variedad abeliana sobre un cuerpo numérico K. Para toda extensión finita L/K se cumple que

$$h_{\mathrm{Fa}}(A_L) \leq h_{\mathrm{Fa}}(A_K),$$

si A_K es semiestable, entonces de hecho hay igualdad.

Demostración: Cfr. [**2,** pág. 248], Rmk. 5.1.1 y 5.1.2. □

Definición A.5: La ***altura geométrica de Faltings*** de una variedad abeliana A_K sobre un cuerpo K es

$$h_{\mathrm{geom}}(A) := h_{\mathrm{Fa}}(A_L),$$

donde L/K es una extensión finita tal que el cambio de base A_L es semiestable sobre L.

Esta definición *sí* es absoluta y no depende del cuerpo base.
Finalmente un resultado de Faltings dice:

Proposición A.6: Sea $c \geq 0$ dado y g un entero fijo. Existen finitas clases de isomorfismo de variedades abelianas A sobre un cuerpo numérico K de dimensión g con $h_{\mathrm{Fa}}(A) \leq c$.

Observación A.6.1: Esto explica la discrepancia (necesaria) con la altura de moduli: considere una variedad abeliana A fija sobre un cuerpo numérico K con infinitos torcimientos. Dado otro torcimiento A' existe una extensión finita L/K tal que $A'_L \cong A_L$, por lo que $h_{\mathrm{geom}}(A') = h_{\mathrm{geom}}(A)$. Sin embargo, como solo hay finitas variedades abelianas con altura de Faltings $\leq h_{\mathrm{Fa}}(A_K)$, esto significa que eventualmente hay torcimientos con $h_{\mathrm{Fa}}(A'_K)$ arbitrariamente grande. En particular, hay infinitos torcimientos de A que no son semiestables.

La observación anterior insinua que hay «pocas» variedades abelianas con buena reducción en «muchas partes». Esta insinuación fue una conjetura de Šafarevič y su prueba sigue de los trabajos de Faltings:

Teorema A.7 (conjetura de Šafarevič): Sea K un cuerpo numérico, $S \subseteq M_K$ un conjunto finito de lugares que contiene a todos los lugares arquimedianos y sea un g entero fijo. Existen solo finitas variedades abelianas de dimensión g sobre K (salvo isomorfismo) con buena reducción fuera de S.

Esto debe hacer eco del hecho de que un cuerpo numérico solo posee finitas extensiones no ramificadas.

Para las demostraciones, se recomienda la exposición de DELIGNE **[3]**.

REFERENCIAS

1. BOSCH, S., LÜTKEBOHMERT, W. y RAYNAUD, M. *Néron models Grundlehren der mathematischen Wissenschaften* **21** (Springer-Verlag, 1990).
2. (eds. CORNELL, G. y SILVERMAN, J. H.) *Arithmetic Geometry* (Springer-Verlag, 1986).
3. DELIGNE, P. *Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings)* en *Séminaire Bourbaki : volume 1983/84, exposés 615-632* (Société mathématique de France, 1985), 25-41. http://www.numdam.org/item/SB_1983-1984__26__25_0/.
4. FALTINGS, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. math.* **73,** 349-366. doi:10.1007/BF01388432 (1983).
5. FREY, G. *Links between solutions of $A-B=C$ and elliptic curves* en *Number Theory* (eds. SCHLICKEWEI, H. P. y WIRSING, E.) (Springer Berlin Heidelberg, Berlin, Heidelberg, 1989), 31-62.
6. LANG, S. *Fundamentals of Diophantine Geometry* (Springer-Verlag, 1983).
7. SILVERMAN, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).
8. TATE, J. Endomorphisms of abelian varieties over finite fields. *Invent. math.* **2,** 134-144. doi:10.1007/BF01404549 (1966).

Correo electrónico: hector.pasten@mat.uc.cl

DEPARTAMENTO DE MATEMÁTICAS, PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE. FACULTAD DE MATEMÁTICAS, 4860 AV. VICUÑA MACKENNA, MACUL, RM, CHILE

Correo electrónico: josecuevasbtos@uc.cl