# Puntos enteros en órbitas de funciones racionales

Benjamín Macías Quezada

04 de noviembre de 2022

**Resumen**

Esa es la versión escrita de una charla que di en el Seminario de Teoría de Números de la PUC. Estudiaremos un resultado de Silverman que da condiciones para que la órbita de una función racional tenga finitos puntos enteros. Para ello, demostraremos un teorema de Siegel en aproximación diofantina, y un lema geométrico que se desprende de la fórmula de Riemann–Hurwitz. Basado en [Sil07, Chs. 3.6–7].

## 1. Preliminares aritméticos

El teorema de Siegel que nos interesa es uno de los frutos de diversos trabajos en aproximación diofantina. En particular, se desprende del siguiente resultado, publicado originalmente en [Thu09] que no probaremos. Una demostración, que ocupa el teorema de Roth, se puede encontrar en [Sil07, pp. 105–6].

**Teorema 1 (Thue, 1909).** *Sea $G \in \mathbb{Z}[x, y]$ homogéneo de grado $d \geq 3$, y $B \in \mathbb{Z}$. Si $G$ tiene al menos tres raíces distintas en $\mathbb{P}^1_{\mathbb{C}}$, entonces la ecuación $G(x, y) = B$ tiene finitas soluciones enteras.*

En [Sie09], Siegel probó que este resultado puede ser formulado en términos de valores enteros de funciones racionales.

**Teorema 2 (Siegel, 1929).** *Sea $\phi \in \mathbb{Q}(z)$. Si $\phi$ tiene al menos tres polos distintos en $\mathbb{P}^1_{\mathbb{C}}$, entonces el conjunto $\{\alpha \in \mathbb{Q} \colon \phi(\alpha) \in \mathbb{Z}\}$ es finito.*

Este teorema nos es relevante, por lo que será demostrado. Ocuparemos un poco sobre resultantes, por lo que enunciamos lo justo y necesario. La demostración del siguiente lema (y más propiedades de resultantes), se puede encontrar en [Sil07, pp. 53–6].

**Lema 3.** *Sea $k$ un cuerpo. Dados*

$$A(X, Y) := \sum_{k=0}^{n} a_k X^{n-k} Y^k \in k[X, Y],$$
$$B(X, Y) := \sum_{k=0}^{m} b_k X^{m-k} Y^k \in k[X, Y],$$

*homogéneos, existe un polinomio*

$$\mathrm{Res}(A, B) \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m],$$

*con la propiedad de que*

$$F_1(X, Y)A(X, Y) + G_1(X, Y)B(X, Y) = \mathrm{Res}(A, B)X^{m+n-1},$$
$$F_2(X, Y)A(X, Y) + G_2(X, Y)B(X, Y) = \mathrm{Res}(A, B)Y^{m+n-1},$$

*para algunos $F_1, G_1$ y $F_2, G_2 \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m][X, Y]$, de grados $m - 1$ y $n - 1$, respectivamente.*

**Definición 4.** Con la notación del lema, $\mathrm{Res}(A, B)$ se llama el *resultante de $A$ y $B$*.

Con esto, procedemos a la demostración:

*Demostración de Siegel.* Escribamos $\phi = [F(X,Y), G(X,Y)]$ para algunos polinomios $F, G \in \mathbb{Z}[X,Y]$ homogéneos de grado $d$, que podemos suponer sin factores en común. Para cada $\alpha := \frac{a}{b} \in \mathbb{Q}$, que suponemos sin términos en común, se tiene que

$$\phi(\alpha) = \frac{F(a,b)}{G(a,b)},$$

por lo que $\phi(\alpha) \in \mathbb{Z}$ si y solo si $G(a,b) \mid F(a,b)$. Sea $R := \operatorname{Res}(A,B) \in \mathbb{Z}$, por lo que podemos encontrar polinomios homogéneos $f_1, g_1, f_2, g_2 \in \mathbb{Z}[X,Y]$ de grados adecuados tales que

$$f_1(X,Y)F(X,Y) + g_1(X,Y)G(X,Y) = RX^{2d-1},$$
$$f_2(X,Y)F(X,Y) + g_2(X,Y)G(X,Y) = RY^{2d-1}.$$

Evaluando en $(a,b)$, notamos que si $G(a,b) \mid F(a,b)$, entonces

$$G(a,b) \mid Ra^{2d-1}, Rb^{2d-1}.$$

Como $(a,b) = 1$, muestra que $G(a,b) \mid R$. Esto, más la observación anterior, indica que si $\phi(\frac{a}{b}) \in \mathbb{Z}$, entonces $G(a,b)$ es un divisor de $R$. En particular,

$$\left\{\frac{a}{b} \in \mathbb{Q} \colon \phi\Big(\frac{a}{b}\Big) \in \mathbb{Z}\right\} \subseteq \bigcup_{D \mid R} \left\{\frac{a}{b} \in \mathbb{Q} \colon G(a,b) = D \in \mathbb{Z}\right\}.$$

El $\phi$ tenga al menos tres polos distintos indica que $G$ tiene al menos tres ceros distintos en $\mathbb{P}^1_{\mathbb{C}}$, por lo que el teorema de Thue nos dice que cada ecuación $G(x,y) = D$, para $D \mid R$ tiene finitas soluciones enteras, por lo que cada conjunto del lado derecho es finito, y por tanto nuestro conjunto de interés está contenido en una unión finita de conjuntos finitos, y es, por tanto, finito. □

## 2. Preliminares geométricos

Necesitamos algunos resultados geométricos. Lo relevante será demostrado, mientras que lo demás será solamente enunciado. El grueso se puede encontrar en [Sil07, Chs. 1.1–2].

**Lema 5.** *Sea $\phi \colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ una función racional.*

(1) *Si $\phi^n$ es una función polinomial para algún $n \in \mathbb{N}$, entonces $\phi^2$ lo es.*

(2) *$\phi$ fija $\infty$ si y solo si $\phi$ es un polinomio.*

El siguiente resultado es importante, en tanto nos permitirá concluir que ciertos iterados de las funciones racionales que nos interesan satisfacen las hipótesis del teorema de Siegel. Ocupa la fórmula de Riemann–Hurwitz en una versión más débil.

**Teorema 6.** *Sea $\phi \in \mathbb{C}(z)$ de grado $d \geq 2$. Si $\phi^2 \notin \mathbb{C}[z]$, entonces $\#\phi^{-4}(\{\infty\}) \geq 3$, y si además $d \geq 3$, entonces $\#\phi^{-3}(\{\infty\}) \geq 3$.*

*Demostración.* Vamos a probar las afirmaciones por separado. Primero, demostremos que $\#\phi^{-3}(\{\infty\}) \geq 3$ si $d \geq 3$. Buscando una contradicción, supongamos que, si bien $d \geq 3$, se tiene que $\#\phi^{-3}(\{\infty\}) \leq 2$, es decir, que tiene 1 o 2 elementos, lo que deja cuatro posibilidades, que representamos en al figura siguiente, y verificamos no pueden ser a mano.

- En el primer caso, $P$ no puede ser $\infty$, pues esto indicaría que $\infty$ es un punto fijo de $\phi$, lo que lo fuerza a ser un polinomio, lo que fuerza que $\phi^2$ también es uno, y estamos suponiendo que no lo es. Análogamente, $Q$ es distinto $P$ porque de lo contrario $Q$ sería punto fijo de $\phi$, y por tanto $P$ sería infinito. El argumento es análogo para $R := \bullet$. También, $Q \neq \infty$, porque de lo contrario, $\phi^2$ fija $\infty$ y por tanto es un polinomio. Por Riemann–Hurwitz, se tiene que

$$\begin{aligned} 2d - 2 &\geq (d - \#\phi^{-1}(\{\infty\}) + (d - \#\phi^{-1}(\{P\}) + (d - \#\phi^{-1}(\{Q\}) \\ &= (d-1) + (d-1) + (d-1) \\ &= 3d - 3, \end{aligned}$$

de lo que $d \leq 1$, lo que no puede ser.

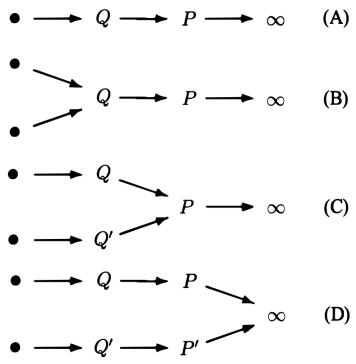


Figura 1: Algunos elementos de la órbita negativa de $\infty$ bajo $\phi$. Recuperado de [Sil93, p. 109].

- Un argumento análogo al anterior verifica que en el resto de casos los puntos son nuevamente distintos entre sí, por lo que Riemann–Hurwitz indica que $2d - 2 \geq 3d - 4$, es decir, $d \leq 2$, otra contradicción.

Por tanto, si $d \geq 3$, no puede ser que $\#\phi^{-3}(\{\infty\}) \leq 2$, es decir, debe ser que $\#\phi^{-3}(\{\infty\}) \geq 3$.

Si $d = 2$, entonces un punto tiene o 1 o 2 preimágenes, y los que tienen una son los puntos ramificados, y Riemann–Hurwitz indica que $\phi$ solo tiene dos puntos ramificados, lo que puede ocurrir solo en los últimos tres casos, en los que $\#^{-3}(\{\infty\}) = 2$. □

# 3. Resultado principal

Estamos en condiciones de enunciar y probar el teorema principal. El resultado es [Sil93, Theorem A].

**Teorema 7 (Silverman, 1993).** *Sea $\phi \in \mathbb{Q}(z)$ de grado $d \geq 2$. Si $\phi^2 \notin \mathbb{Q}[z]$, entonces la órbita de un $\alpha \in \mathbb{Q}$,*

$$\mathcal{O}_\phi(\alpha) := \{\phi^{\circ n}(\alpha) \colon n \in \mathbb{N}\},$$

*tiene finitos puntos enteros.*

*Demostración.* Si la órbita de $\alpha$ es finita, no hay nada que probar. Por tanto, podemos suponer que es infinita sin perder generalidad. En este caso, basta verificar que el conjunto de los $n \in \mathbb{Z}$ tales que $\phi^n(\alpha) \in \mathbb{Z}$,

$$N_\alpha := \{n \in \mathbb{N} \colon \phi^n(\alpha) \in \mathbb{Z}\}$$

es finito. Supongamos que es infinito.

El resultado anterior indica que $\#\phi^{-4}(\{\infty\}) \geq 3$, es decir, que $\phi^4$ tiene al menos tres polos distintos, por lo que el teorema de Siegel indica que

$$A := \left\{\beta \in \mathbb{Q} \colon \phi^4(\beta) \in \mathbb{Z}\right\}$$

es finito. Notamos que si $n \in N_\alpha$, con $n \geq 4$, entonces por definición $\phi^n(\alpha) \in \mathbb{Z}$, y por tanto

$$\phi^4(\phi^{n-4}(\alpha)) \in \mathbb{Z},$$

es decir, $\phi^{n-4}(\alpha) \in A$. Esto prueba que a cada tal $n \geq 4$ le corresponde algún elemento $\beta \in A$.

Puede ser que estos $\beta$ sean iterados distintos de $\alpha$, pero esto no pasa: para cada $\beta \in A$ hay a lo más un iterado de $\alpha$ que llega a $\beta$, pues de lo contrario $\alpha$ sería una punto pre-periódico y por tanto su órbita sería finita. □

# Referencias

[Sie09] Carl Ludwig Siegel, *Über einige anwendungen diophantischer approximationen.*

[Sil93] Joseph H. Silverman, *Integer points, diophantine approximation, and iteration of rational maps*, Duke Math **71** (1993), no. 3, 793–829.

[Sil07] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer New York, New York, NY, 2007.

[Thu09] Axel Thue, *Über annäherungswerte algebraischer zahlen.*, no. 135, 284–305.