© Revista de Matemática: Teoría y Aplicaciones 2023 **30**(1) : 113–120
cimpa – ucr issn: 1409-2433 (Print), 2215-3373 (Online)
doi: https://doi.org/10.15517/rmta.v30i1.52266

SUPERFICIES ELÍPTICAS Y EL DÉCIMO PROBLEMA DE HILBERT

ELLIPTIC SURFACES AND HILBERT'S TENTH PROBLEM

Héctor Pastén*

Received: 31/08/2022; Revised: 6/12/2022;
Accepted: 23/11/2022

*Pontificia Universidad Católica de Chile, Departamento de Matemáticas, Facultad de Matemáticas, Santiago, Chile. E-Mail: hector.pasten@mat.uc.cl

Resumen

Es sabido que se obtendría una solución negativa al décimo problema de Hilbert para el anillo de enteros O_F de un campo de números F si $\mathbb{Z}$ fuera diofantino en O_F. Denef y Lipshitz conjeturaron que esto último ocurre para todo F. En esta nota se demuestra que la conjetura de Denef y Lipshitz es consecuencia de una conocida conjetura sobre superficies elípticas.

Palabras clave: Décimo problema de Hilbert; anillos de enteros; superficies elípticas; curvas elípticas.

Abstract

A negative solution to Hilbert's tenth problem for the ring of integers O_F of a number field F would follow if $\mathbb{Z}$ were Diophantine in O_F. Denef and Lipshitz conjectured that the latter occurs for every number field F. In this note we show that the conjecture of Denef and Lipshitz is a consequence of a well-known conjecture on elliptic surfaces.

Keywords: Hilbert's tenth problem; rings of integers; elliptic surfaces; elliptic curves.

Mathematics Subject Classification: Primario: 11U05; Secundario: 14J27, 11G05.

1 Introducción

En 1900 Hilbert propuso una famosa lista de 23 problemas, el décimo de los cuales pedía un algoritmo para decidir la existencia de soluciones enteras a ecuaciones diofantinas. Este problema fue resulto negativamente en 1970 [3, 10] y a partir de esa solución negativa se han investigado varias extensiones a otras estructuras. Uno de los casos abiertos más destacados es el de anillos de enteros de campos de números. En este contexto el problema se ha resuelto negativamente para el anillo de enteros O_F de varios tipos de campos de números F; ver [4, 6, 5, 16, 21, 22, 25, 12, 7, 18, 8]. Sin embargo, el caso general sigue abierto y se espera una respuesta negativa. En efecto, si $\mathbb{Z}$ es diofantino en O_F (ver la definición de "conjunto diofantino" en la sección siguiente) entonces el análogo del décimo problema de Hilbert en O_F tiene respuesta negativa, mientras que Denef y Lipshitz [6] propusieron:

Conjetura 1.1 (Denef–Lipshitz)**.** *El anillo $\mathbb{Z}$ es diofantino en O_F para todo campo de números F.*

Aunque la conjetura de Denef y Lipshitz sigue abierta en general, los trabajos de Mazur–Rubin [11] y de Murty–Pasten [14] muestran que es consecuencia de conjeturas estándar sobre curvas elípticas. En esta nota se dará evidencia adicional, demostrando que la conjetura de Denef y Lipshitz también es consecuencia de una conocida conjetura sobre superficies elípticas.

Cabe destacar que los trabajos [11] y [14], así como también el presente artículo, se basan en un criterio desarrollado por Poonen y Shlapentokh [23] que reduce la conjetura de Denef–Lipshitz a un problema de curvas elípticas; ver los detalles en la sección siguiente.

Dado un campo de números K, sea $\pi : X \to \mathbb{P}^1$ una superficie elíptica sobre K con una sección distinguida $\sigma_0 : \mathbb{P}^1 \to X$. Por [9] sabemos que el grupo de secciones $\mathrm{MW}(X, \pi, K)$ definidas sobre K con neutro σ_0 es finitamente generado. Para todos salvo finitos $t \in \mathbb{P}^1(K)$ la fibra X_t es una curva elíptica y se tiene el morfismo de especialización $\mathrm{esp}_t : \mathrm{MW}(X, \pi, K) \to X_t(K)$ dado por $\sigma \mapsto \sigma(t)$. Mejorando resultados de [15], Silverman [24] demostró lo siguiente (donde rg es el rango):

Teorema 1.2 (Silverman)**.** *El morfismo de especialización* esp_t *es inyectivo para todos salvo finitos* t *en* $\mathbb{P}^1(K)$*. Así, para todos salvo finitos* t *en* $\mathbb{P}^1(K)$ *se tiene que* $\mathrm{rg}\, X_t(K) \geq \mathrm{rg}\, \mathrm{MW}(X, \pi, K)$.

Así, es difícil no definir los conjuntos de puntos $t \in \mathbb{P}^1(K)$ donde $\mathrm{rg}\, X_t(K) = \mathrm{rg}\, \mathrm{MW}(X, \pi, K)$ y donde $\mathrm{rg}\, X_t(K) > \mathrm{rg}\, \mathrm{MW}(X, \pi, K)$, el primero de los cuales denotaremos por $\mathscr{N}(X, \pi, K)$; esto es, donde el rango no salta. Es una conjetura que forma parte del folklore del área que si $\pi : X \to \mathbb{P}^1$ no es isotrivial, entonces ambos conjuntos deberían ser infinitos. Este problema ha capturado considerable atención; ver por ejemplo el apéndice A de [1], o bien [19] y las referencias ahí citadas. Nuestra contribución es:

Teorema 1.3. *Suponga que para todo campo de números* K *y toda superficie elíptica no isotrivial* $\pi : X \to \mathbb{P}^1$ *sobre* K *con* $\mathrm{rg}\, \mathrm{MW}(X, \pi, K) = 0$ *se tiene que* $\mathscr{N}(X, \pi, K)$ *es infinito. Entonces la conjetura de Denef y Lipshitz es correcta:* $\mathbb{Z}$ *es diofantino en* O_F *para todo campo de números* F.

De la demostración será claro que la condición de infinitud de $\mathscr{N}(X, \pi, K)$ se necesita solo para superficies elípticas de un tipo bastante particular.

2 Preliminares: conjuntos diofantinos

Dado un campo de números F, un conjunto $S \subseteq O_F$ es *diofantino* si existe un polinomio $P(x, y_1, ..., y_n) \in O_F[x, y_1, ..., y_n]$ (para algún n) tal que dado

cualquier $a \in O_F$, se tiene que $a \in S$ si y solo si la ecuación $P(a, y_1, ..., y_n) = 0$ tiene solución sobre O_F. Por ejemplo, los cuadrados de O_F forman un conjunto diofantino, tomando $P(x, y_1) = x - y_1^2$.

En un trabajo pionero, Denef [5] relacionó conjuntos diofantinos en anillos de enteros con la estabilidad de rangos de curvas elípticas en extensiones. Este tema fue desarrollado por Poonen [17], Cornelissen–Pheidas–Zahidi [2], y más recientemente por Shlapentokh [23], quien obtuvo (simultáneamente con Poonen) el teorema siguiente:

Teorema 2.1 (Poonen, Shlapentokh)**.** *Sea L/K una extensión de campos de números. Si hay una curva elíptica E sobre K con $\operatorname{rg} E(L) = \operatorname{rg} E(K) > 0$, entonces O_K es diofantino en O_L.*

El resultado anterior ha jugado un papel central en todos los últimos desarrollos en la conjetura de Denef y Lipshitz.

Más aún, usando [5], Shlapentokh probó la siguiente sorprendente reducción [13]:

Lema 2.2 (Shlapentokh)**.** *Suponga que para toda extensión cuadrática de campos de números L/K se tiene que O_K es diofantino en O_L. Entonces la conjetura de Denef y Lipshitz es correcta.*

3 Preliminares: superficies elípticas

Una superficie elíptica sobre un campo de números K con base $\mathbb{P}^1$ es una superficie suave proyectiva X dotada de un morfismo $\pi : X \to \mathbb{P}^1$ y una sección $\sigma_0 : \mathbb{P}^1 \to X$ de π, todo definido sobre K, tal que la fibra genérica de π es una curva elíptica sobre $K(\mathbb{P}^1)$ cuyo elemento neutro es determinado por σ_0.

La totalidad de las secciones de $\pi : X \to \mathbb{P}^1$ forman un grupo que denotamos por $\mathrm{MW}(X, \pi, K)$. La estructura de grupo para las secciones es determinada por la estructura de grupo de la curva elíptica en la fibra genérica. En particular, $\mathrm{MW}(X, \pi, K)$ es un grupo abeliano, y el teorema de Lang-Néron [9] nos dice que es finitamente generado. En particular, $\mathrm{MW}(X, \pi, K)$ tiene un rango y una parte de torsión finita.

Concretamente, una superficie elíptica se puede pensar como una familia parametrizada de curvas elípticas en un parámetro t, y por ende, eligiendo un parámetro t afín en $\mathbb{P}^1$, se puede escribir en forma de Weierstrass

$$y^2 = x^3 + A(t)x^2 + B(t)x + C(t),$$

donde $A, B, C \in K[t]$, obteniendo así un modelo birracional de la superficie elíptica en cuestión. En este modelo, la sección σ_0 no es otra que la sección al infinito.

Además de lo anterior, necesitaremos un ejemplo conveniente de superficie elíptica.

Lema 3.1. *Existe una superficie elíptica no isotrivial $\pi : Y \to \mathbb{P}^1$ definida sobre $\mathbb{Q}$ tal que el grupo de secciones sobre $\mathbb{C}$ es exactamente $\mathrm{MW}(Y, \pi, \mathbb{Q})$, y este grupo es libre abeliano de rango positivo.*

Superficies elípticas de este tipo abundan; ver por ejemplo [20].

4 La conjetura de Denef y Lipshitz cuando el rango no salta

Sea $\pi : Y \to \mathbb{P}^1$ una superficie elíptica sobre $\mathbb{Q}$ como las dadas por el Lema 3.1. Sea $y^2 = f(T, x)$ una ecuación de Weierstrass para ella con coeficientes en $\mathbb{Q}[T]$ donde T es una coordenada afín en $\mathbb{P}^1$. Dado un campo de números K y un $\beta \in K^\times$ definimos la superficie elíptica $p : Y_K^{(\beta)} \to \mathbb{P}^1$ sobre K por medio de la ecuación $\beta y^2 = f(T, x)$, dotada de la sección σ_0 al infinito. Sobre $\mathbb{C}$ esta superficie elíptica es isomorfa a $\pi : Y \to \mathbb{P}^1$, así que no es isotrivial.

Lema 4.1. *Si K es un campo de números y $\beta \in K$ no es un cuadrado en K, entonces se tiene que $\mathrm{MW}(Y_K^{(\beta)}, p, K) = (\sigma_0)$, o sea, este grupo de secciones sobre K es trivial.*

Proof. Suponga que $\tau = (x, y) = (a, b) \neq \sigma_0$ es una sección con $a, b \in K(T)$. Tenemos $b \neq 0$ porque sobre $\mathbb{C}$ no hay secciones no triviales de 2-torsión (por el Lema 3.1). Así, si γ es una raíz cuadrada de β vemos que $\tau' = (a, \gamma b)$ es una sección de $\pi : Y \to \mathbb{P}^1$ sobre $\mathbb{C}$, y por ende sobre $\mathbb{Q}$ por el Lema 3.1. Luego, $\gamma b \in \mathbb{Q}(T)$ y como $b \in K(T)^\times$ concluimos que $\gamma \in K$; contradicción. □

Demostración del Teorema 1.3. Sea L/K cualquier extensión cuadrática de campos de números. Es generada por la raíz cuadrada de cierto $\beta \in K^\times$ que no es cuadrado. El Lema 4.1 da que $\operatorname{rg} \mathrm{MW}(Y_K^{(\beta)}, p, K) = 0$. Por hipótesis, $\mathscr{N}(Y_K^{(\beta)}, p, K)$ es infinito, así que hay infinitos $\alpha \in K$ con $\operatorname{rg} E_\alpha^{(\beta)}(K) = 0$, donde $E_\alpha^{(\beta)}$ es la curva elíptica dada por $\beta y^2 = f(\alpha, x)$. Esta última es el torcimiento cuadrático por L sobre K de la curva elíptica E_α definida por $y^2 = f(\alpha, x)$.

Como $\operatorname{rg} \mathrm{MW}(Y, \pi, K) \geq 1$ (ver el Lema 3.1), del Teorema 1.2 obtenemos que todos salvo finitos $\alpha \in K$ cumplen que $\operatorname{rg} E_\alpha(K) \geq 1$. Así, podemos elegir $\alpha \in K$ con $\operatorname{rg} E_\alpha^{(\beta)}(K) = 0$ y $\operatorname{rg} E_\alpha(K) \geq 1$. Hecho esto, se obtiene

$$\operatorname{rg} E_\alpha(L) = \operatorname{rg} E_\alpha(K) + \operatorname{rg} E_\alpha^{(\beta)}(K) = \operatorname{rg} E_\alpha(K) > 0,$$

donde la primera igualdad es un hecho estándar sobre rangos de torcimientos cuadráticos, tomando en cosideración que $L = K(\sqrt{\beta})$. Por el Teorema 2.1 deducimos que O_K es diofantino en O_L. Concluimos por el Lema 2.2. □

4.1 Agradecimientos

Agradezco a Barry Mazur por comentarios en una versión previa, y a Cecília Salgado por responder varias dudas. Además, agradezco profundamente los comentarios de los tres revisores anónimos.

4.2 Financiamiento

Investigación financiada por ANID FONDECYT Regular 1190442 de Chile.

Referencias

[1] B. Conrad, K. Conrad, H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198**(2005), no. 2, 684-731. Doi: 10.48550/arXiv.math/0408153

[2] G. Cornelissen, T. Pheidas, K. Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17**(2005), no. 3, 727-735. Doi: 10.5802/jtnb.516

[3] M. Davis, H. Putnam, J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math (2) **74**(1961), no. 3, 425-436. Doi: 10.2307/1970289

[4] J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48**(1975), no. 1, 214-220. Doi: 10.2307/2040720

[5] J. Denef, *Diophantine sets over algebraic integer rings II*, Trans. Amer. Math. Soc. **257**(1980), no. 1, 227-236. Doi: 10.2307/1998133

[6] J. Denef, L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18**(1978), no. 3, 385-391. Doi: 10.1112/jlms/s2-18.3.385

[7] N. Garcia-Fritz, H. Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*. Math. Ann. **377**(2020), no. 3-4, 989-1013. Doi: 10.1007/s00208-020-01991-w

[8] D. Kundu, A. Lei, F. Sprung, *Studying Hilbert's* 10^{th} *problem via explicit elliptic curves*, arXiv: 2207.07021(2022). Doi: 10.48550/arXiv.2207.07021

[9] S. Lang, A. Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81**(1959), no.1, 95-118. Doi: 10.2307/2372851

[10] Y. Matiyasevich, *The Diophantineness of enumerable sets*. Dokl. Akad. Nauk SSSR **191**(1970), no. 2, 279-282.

[11] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. Math. **181**(2010), no. 3, 541-575. Doi: 10.1007/s00222-010-0252-0

[12] B. Mazur, K. Rubin, *Diophantine stability*, With an appendix by Michael Larsen. Amer. J. Math. **140**(2018), no. 3, 571-616. Doi: 10.1353/ajm.2018.0014

[13] B. Mazur, K. Rubin, A. Shlapentokh, *Existential definability and Diophantine stability*, arXiv: 2208.09963 (2022), Doi: 10.48550/arXiv.2208.09963

[14] M. Murty, H. Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*. J. Number Theory **182**(2018), 1-18. Doi: 10.1016/j.jnt.2017.07.008

[15] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*. Bull. Soc. Math. France **80**(1952), 101-166. Doi: 10.24033/bsmf.1427

[16] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*. Proc. Amer. Math. Soc. **104**(1988), no. 2, 611-620. Doi: 10.2307/2047021

[17] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*. Fieker, Claus and Kohel, David R (Eds.), Algorithmic Number Theory, Sidney, 2002, 33-42. Doi: 10.1007/3-540-45455-1_4

[18] A. Ray, *Remarks on Hilbert's tenth problem and the Iwasawa theory of elliptic curves*, Bulletin of the Australian Mathematical Society Society (2022), 1-11 Doi: 10.1017/S000497272200082X

[19] C. Salgado, *On the rank of the fibers of rational elliptic surfaces*, Algebra Number Theory **6**(2012) , no. 7, 1289-1314. Doi: 10.2140/ant.2012.6.1289

[20] C. Schwartz, *An elliptic surface of Mordell-Weil rank 8 over the rational numbers*, J. Théor. Nombres Bordeaux **6**(1994) , no. 1, 1-8. Available from: `http://www.numdam.org/item/JTNB_1994__6_1_1_0.pdf`

[21] H. Shapiro, A. Shlapentokh, *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math. **42**(1989), no. 8, 1113-1122. Doi: 10.1002/cpa.3160420805

[22] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*. Comm. Pure Appl. Math. **42**(1989) , no. 7, 939-962. Doi: 10.1002/cpa.3160420703

[23] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360**(2008), no. 7, 3541-3555. Doi: 10.1090/S0002-9947-08-04302-X

[24] J. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math **342**(1983), 197-211. Doi: 10.1515/crll.1983.342.197

[25] C. Videla, (1989). *Sobre el décimo problema de Hilbert*, Atas da Xa Escola de Algebra, Vitoria, ES, Brasil, Colecao Atas 16 Sociedade Brasileira de Matematica, 95-108