El diablo de los números

Sección a cargo de

Javier Fresán

¿Cuántas raíces de la unidad anulan un polinomio en dos variables?

por

Roberto Gualdi

En estas páginas vamos a considerar la tarea de buscar raíces de la unidad que son soluciones de un polinomio en dos variables con coeficientes algebraicos. Esta pregunta, aparentemente inocente, nos llevará por un precioso viaje a través de alturas, fenómenos de equidistribución y famosas conjeturas en el reino diofántico.

En lugar de probar nuevos resultados o dar un estudio detallado de la literatura, el enfoque de esta nota es proporcionar una presentación elemental de las herramientas y técnicas fundamentales en geometría aritmética y diofántica, y mostrar algunas de sus aplicaciones más espectaculares de manera práctica, con el objetivo secreto de motivar a estudiantes e inexpertos a sumergirse en este fascinante tema.

Al final de la nota señalamos varias direcciones que recientemente han sido (y siguen siendo) emocionantes áreas de investigación.

1. ¿Qué es la geometría aritmética?

La búsqueda de soluciones racionales de un sistema de ecuaciones polinómicas con coeficientes enteros es una de las eternas aspiraciones de las matemáticas que, bajo una formulación diferente, ya se consideraba en la India y Grecia antiguas.

Una actitud más moderna frente al problema ha sucumbido a la tentación de considerarlo desde una perspectiva más geométrica: el conjunto de soluciones de un sistema de ecuaciones polinómicas es lo que se denomina una variedad algebraica; así nuestra eterna aspiración se corresponde con describir los puntos de coordenadas racionales en dichos objetos. Este enfoque, a través del cual uno puede esperar explotar la maquinaria de la geometría para resolver problemas de teoría de números, ha tomado el nombre de *geometría aritmética*. En términos generales, uno de los desafíos que definen a esta rama es el deseo de poder encontrar todos los *puntos especiales* de una variedad algebraica.

A pesar de la formulación uniforme de este desafío, el significado preciso de «especial» varía según el problema específico considerado en el área. Podemos explicar esto mejor centrándonos en una situación particular.

Para hacer eso, consideramos un polinomio homogéneo no constante

$$F \in \overline{\mathbb{Q}}[X_0, X_1, X_2],$$

donde $\overline{\mathbb{Q}} \subset \mathbb{C}$ es el cuerpo de los números algebraicos. Esencialmente, a cualquier teórico de números le gustaría saber tanto como sea posible acerca de las soluciones de F que tienen coordenadas racionales (o más generalmente, coordenadas en un cuerpo de números dado), dando lugar a la siguiente

Pregunta 1. *¿Cómo describir las ternas de números racionales que anulan un polinomio homogéneo en tres variables?*

Para arrojar luz geométrica sobre la cuestión, se puede considerar el conjunto de puntos proyectivos $[X_0 : X_1 : X_2]$ con $X_0, X_1, X_2 \in \mathbb{C}$ cuyas coordenadas anulan el polinomio F. Este conjunto está en primer lugar bien definido, gracias a la hipótesis de homogeneidad, y se denota por

$$Z_{\text{proy}}(F) := \big\{[X_0 : X_1 : X_2] \mid F(X_0, X_1, X_2) = 0\big\} \subset \mathbb{P}^2(\mathbb{C}).$$

Esta es la *curva algebraica definida por* F en el plano proyectivo complejo.

La pregunta anterior se traduce en la búsqueda de los puntos en $Z_{\text{proy}}(F)$ que tengan coordenadas racionales. Ahora podemos precisar la Pregunta 1 con las siguientes cuestiones: ¿existen puntos en $Z_{\text{proy}}(F)$ con coordenadas racionales? ¿Es finito el conjunto de estos puntos? En caso afirmativo, ¿podemos contarlos? ¿Dónde están ubicados?

Para ello, podemos comenzar buscando dichos puntos en ciertas líneas proyectivas «distinguidas» en $\mathbb{P}^2(\mathbb{C})$, por ejemplo las que están definidas por la anulación de una de las coordenadas. Algebraicamente, esto corresponde a la búsqueda de las soluciones $[X_0 : X_1 : X_2]$ de F que tienen $X_i = 0$ para algún $i \in \{0, 1, 2\}$. Al normalizar las coordenadas proyectivas, este problema se convierte en la búsqueda de soluciones racionales de un polinomio en una variable. Cuando el polinomio F tiene, por ejemplo, coeficientes enteros, esta pregunta se puede responder fácilmente enumerando todos los números racionales que tienen numerador que divide al término independiente de F y denominador que divide su coeficiente principal, y verificando uno por uno cada uno de estos candidatos a solución.

Después de este número finito de pasos, nuestro problema original se reduce entonces a buscar puntos racionales $[X_0 : X_1 : X_2]$ que resuelvan F y para los cuales ninguna de las coordenadas sea cero. Dicho de otro modo, y después de deshomogeneizar F a f fijando (por ejemplo) $X_0 = 1$, podemos restringirnos a la búsqueda de los puntos en

$$\big\{(x_1, x_2) \in (\mathbb{C}^*)^2 \mid f(x_1, x_2) = 0\big\}$$

que tienen coordenadas racionales. Una de las ventajas de hacerlo es la introducción de una nueva estructura algebraica útil en nuestra investigación. La variedad $(\mathbb{C}^*)^2$

con estructura de grupo dada por la multiplicación coordenada a coordenada se conoce comúnmente en geometría algebraica como el *toro complejo de dimensión* 2.

En esta variedad, los monomios x_1^{-1} y x_2^{-1}, y más generalmente todos los polinomios de Laurent, inducen funciones bien definidas y por lo tanto definen subvariedades algebraicas de $(\mathbb{C}^*)^2$ tomando el conjunto de sus ceros. Más explícitamente, tomamos un polinomio de Laurent en dos variables

$$f \in \overline{\mathbb{Q}}\big[x_1^{\pm 1}, x_2^{\pm 1}\big]$$

que no sea un monomio. Análogamente al caso de los polinomios homogéneos en tres variables y del plano proyectivo, el conjunto de ceros

$$Z_{\text{tor}}(f) := \big\{(x_1, x_2) \mid f(x_1, x_2) = 0\big\} \subset (\mathbb{C}^*)^2$$

se llama la *curva algebraica definida por* f en el toro de dimensión 2.

Las consideraciones anteriores implican que buscar puntos con coordenadas racionales en $Z_{\text{tor}}(f)$ es esencialmente equivalente (salvo por un número finito de pasos) a nuestro problema original. Algebraicamente, la elección del toro algebraico en lugar del plano proyectivo como espacio ambiente da lugar al siguiente análogo de la Pregunta 1:

Pregunta 2. *¿Cómo describir los pares de números racionales distintos de cero que anulan un polinomio de Laurent en dos variables?*

Muchos de los problemas en geometría aritmética pueden expresarse como la búsqueda de puntos racionales de una curva en un toro. Por ejemplo, el famoso último teorema de Fermat puede verse como la afirmación de que la curva definida en el toro de dimensión 2 por el polinomio de Laurent $x_1^n + x_2^n - 1$ no tiene puntos racionales para $n \geq 3$. Una prueba de esta afirmación fue completada por Wiles solamente en 1994, utilizando técnicas de teoría de curvas elípticas y formas modulares, 358 años después de que Fermat la enunciara por primera vez.

El largo tiempo necesario para resolver la conjetura de Fermat deja entrever la notoria dificultad de los problemas en geometría aritmética, a pesar de sus enunciados aparentemente simples. De hecho, cada elección de un polinomio de Laurent en la Pregunta 2 presenta un rompecabezas individual, y ni siquiera hay un algoritmo general que decida la existencia de una solución racional para él, ni (en un número arbitrario de variables) lo habrá, tal como demostró Matiyasevich en su respuesta al décimo problema de Hilbert [26].

A pesar de estas dificultades, durante el siglo pasado se desarrollaron muchas técnicas generales para responder parcialmente a las Preguntas 1 y 2. Por ejemplo, Faltings [14] probó en 1983 una conjetura general de Mordell, prediciendo la finitud de los puntos racionales en una curva de género superior o igual a 2.

Si reemplazamos «soluciones racionales» por «soluciones que tienen coordenadas en un cuerpo de números fijo» en la investigación anterior, podemos adoptar una mentalidad similar; en particular, el teorema de Faltings sigue valiendo en este contexto más general, asegurando la finitud de tales soluciones para polinomios que definen curvas de gran género.

La situación cambia drásticamente cuando se permiten extensiones infinitas de $\mathbb{Q}$. Por ejemplo, cualquier polinomio de Laurent no monomial con coeficientes algebraicos resulta tener infinitas soluciones en $\left(\overline{\mathbb{Q}}^*\right)^2$. De hecho, al multiplicar adecuadamente por monomios y volver a etiquetar las variables si es necesario, se puede suponer que f es un polinomio y contiene al menos un monomio con un término en x_2 y al menos un monomio sin término en x_2. En tal caso, para todo $x_1 \in \overline{\mathbb{Q}}^*$, la ecuación $f(x_1, x_2) = 0$ tiene soluciones en $\overline{\mathbb{Q}}$ en la segunda variable, y estas soluciones son todas distintas de cero para todas salvo un número finito de opciones para x_1.

Por lo tanto, para obtener una pregunta más interesante sobre $\overline{\mathbb{Q}}$ necesitamos cambiar la noción de «puntos especiales» que queremos buscar. Recordando que la variedad ambiente $(\mathbb{C}^*)^2$ tiene una estructura de grupo, existe una elección natural para los elementos distinguidos en ella: los que tienen orden finito. Dicho de otro modo, parece razonable considerar *puntos de torsión* como puntos especiales en nuestro marco, y expresar nuestra investigación geométrica de esa manera.

Veamos cuál es el problema algebraico correspondiente. Por definición, un punto $\boldsymbol{x} = (x_1, x_2)$ en el toro de dimensión 2 es un punto de torsión si y solo si existe un entero positivo d tal que

$$\boldsymbol{x}^d = \left(x_1^d, x_2^d\right) = (1, 1),$$

es decir, si y solamente si las coordenadas de $\boldsymbol{x}$ son raíces de la unidad. Por tanto, el problema de teoría de números inspirado por nuestras consideraciones en geometría aritmética, y correspondiente a la búsqueda de puntos de torsión en curvas algebraicas en el toro de dimensión 2, es la siguiente

Pregunta 3. *¿Cómo describir los pares de raíces de la unidad que anulan un polinomio de Laurent en dos variables?*

De hecho, esta pregunta fue planteada por Lang en la década de 1960; véase, por ejemplo, [21] y [22, Capítulo 8, § 6]. Destaquemos, aunque no estudiaremos esos trabajos en estas páginas, que Mann [24] y, más tarde, Conway y Jones [9] propusieron métodos para responderla en algunas situaciones particulares.

En cambio, lo que podemos hacer para obtener una idea directa del problema es mirar un par de ejemplos simples. Como los monomios no tienen soluciones en el toro, la elección no trivial más fácil para un polinomio de Laurent es la de los binomios en los que solo aparece una variable.

Ejemplo 1. Consideramos el polinomio de Laurent $f = x_1 - \alpha$, con $\alpha \in \overline{\mathbb{Q}}^*$. Por definición, el conjunto de sus soluciones consta de todos los pares (α, x_2) con $x_2 \in \mathbb{C}^*$. En particular, dado que hay un número infinito de raíces de la unidad en $\mathbb{C}$, el polinomio de Laurent f tiene *un número infinito de pares de raíces de la unidad como soluciones* si y solo si α es una raíz de unidad, y *ninguna* de lo contrario.

Habiendo demostrado que tanto infinitos puntos de torsión como ninguno pueden estar en una curva del toro 2-dimensional, es natural preguntarse si la situación intermedia también puede ocurrir. El siguiente caso especial proporciona una respuesta afirmativa.

Ejemplo 2. Tomamos el polinomio de Laurent $f = x_1 + x_2 + 1$. En vista de

$$Z_{\mathrm{tor}}(f) = \big\{(x_1, -1 - x_1) \mid x_1 \in \mathbb{C} \setminus \{0, 1\}\big\},$$

los puntos de torsión que se encuentran en la curva definida por f en $(\mathbb{C}^*)^2$ están en correspondencia biyectiva con las raíces de la unidad ζ para las cuales $-1-\zeta$ también es una raíz de la unidad. En particular, tanto ζ como $-1-\zeta$ deben tener un valor absoluto complejo igual a 1; al dibujar una imagen en el plano complejo como en la Figura 1, podemos ver que esto solo puede ocurrir para dos elecciones de ζ, a saber, las dos raíces primitivas de la unidad de orden 3.

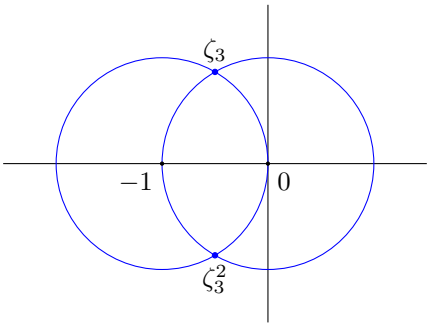


Figura 1: Investigando los puntos de torsión en la línea $x_1 + x_2 + 1 = 0$.

Dado que $-1-\zeta_3 = \zeta_3^2$ y $-1-\zeta_3^2 = \zeta_3$, obtenemos que (ζ_3, ζ_3^2) y (ζ_3^2, ζ_3) son los únicos pares de raíces de la unidad que anulan f.

La pequeña clase de ejemplos que hemos considerado muestra que cualquier respuesta posible con respecto al número de soluciones en raíces de la unidad para un polinomio de Laurent en dos variables puede ocurrir. Por lo tanto, podemos formular la Pregunta 3 de una forma geométrica cualitativa como sigue:

Pregunta 4. *¿Cómo predecir si una curva algebraica en $(\mathbb{C}^*)^2$ contiene un número finito o infinito de puntos de torsión, con solo observar la forma del polinomio de Laurent que la define?*

Esta es la pregunta que orientará nuestro camino en estas páginas. Su respuesta, que daremos en la Sección 5, fue conjeturada por el mismo Lang, y demostrada por Ihara, Serre y Tate [22, Teorema 6.1]. El argumento presentado en *loc. cit.* se basa en una aplicación del teorema de Bézout y en la consideración del polinomio de Laurent $f(x_1^d, x_2^d)$ para un d adecuado, donde f es el polinomio de Laurent que define la curva original.

En estas notas, en cambio, seguiremos una estrategia diferente. Veremos que, usando la noción de altura de puntos algebraicos (recordada en la Sección 2) y las herramientas aritméticas que ofrecen los fenómenos de equidistribución en toros (presentados en la Sección 3), seremos capaces de dar una respuesta satisfactoria a la pregunta anterior. Aún mejor, superaremos nuestras expectativas obteniendo un enunciado más fuerte (y además en una dimensión arbitraria): de hecho, probaremos

la antigua conjetura tórica de Bogomolov en la Sección 4, siguiendo la presentación de Bilu [3].

Esto será más que suficiente para probar la antigua conjetura tórica de Manin-Mumford, y deducir de ella en la Sección 5 una respuesta completa a la Pregunta 4 como corolario.

Por supuesto, hay muchas más preguntas que uno puede hacer en geometría aritmética al considerar el toro como un espacio ambiente. Por ejemplo, la noción de puntos integrales en un toro es muy diferente a la de un espacio afín o proyectivo. Esta y otras diferencias han fomentado varias vías de investigación en geometría diofántica.

Además, la pregunta de Lang ha motivado varios problemas similares en escenarios análogos; por ejemplo, al reemplazar el toro ambiente por una variedad abeliana, que también viene equipada con una estructura de grupo.

Estos temas y consideraciones han recibido mucha atención en los últimos años; mencionamos algunos de estos, con sus aplicaciones y desarrollos, en la Sección 6.

Agradecimientos. El autor está sumamente en deuda con los *referees* anónimos cuya lectura cuidadosa, informes esclarecedores y sugerencias precisas han inspirado una gran mejora de estas páginas. El autor también está agradecido a Fabien Pazuki por una discusión dinámica, a Martín Sombra por su interés y comentarios sobre una primera versión, a Eduardo Soto por su valiosa ayuda con la traducción al español, y a Javier Fresán por su propuesta de publicar el artículo en esta columna de *La Gaceta de la RSME* y por su ayuda editorial.

Durante la redacción de estas notas, el autor se ha beneficiado del apoyo financiero de la *Alexander von Humboldt Foundation* y del centro de investigación colaborativo *SFB 1085: "Higher invariants"* financiado por la Deutsche Forschungsgemeinschaft.

2. Alturas

Fijamos de ahora en adelante la elección de un entero positivo n. Introducimos en esta sección una noción que mide la «complejidad aritmética» de los puntos algebraicos en $(\mathbb{C}^*)^n$, y que se revelará fructífera para el tratamiento de los puntos de torsión. Mencionamos que en el reciente artículo [4], aparecido en esta misma columna de *La Gaceta*, se dan dos formas de capturar la cantidad de información necesaria para determinar un entero algebraico, y se presenta un resultado muy reciente para una de ellas (a saber, la prueba de la conjetura de Schinzel-Zassenhaus por Dimitrov). En el presente artículo, tomamos un punto de vista ligeramente diferente, ya que necesitamos tratar con dimensiones arbitrarias y también con puntos algebraicos que no son enteros algebraicos. Sin embargo, los temas son muy cercanos, y señalamos las conexiones entre los objetos en esta sección y los estudiados en [4] siempre que sea posible.

La intuición principal detrás de la definición que damos aquí es que un elemento de un cuerpo normado es tan complicado como grande es su valor absoluto. Aquí, por

valor absoluto sobre un cuerpo se entiende una función de valores reales no negativos sobre él, que es multiplicativa, satisface la desigualdad triangular y es igual a 0 solo en el elemento cero del cuerpo.

Los cuerpos como $\mathbb{Q}$ y sus extensiones finitas admiten varios valores absolutos. Además, los valores absolutos de cualquiera de estos cuerpos se pueden clasificar (si identificamos todos los valores absolutos que inducen la misma topología) en términos de entidades destacadas en teoría de números, como sus ideales primos. Esto da gran riqueza aritmética a los cuerpos de números. Por ejemplo, un teorema clásico de Ostrowski [28] asegura que los únicos valores absolutos no triviales sobre $\mathbb{Q}$ son, módulo la relación de equivalencia topológica:

- el *valor absoluto euclidiano* habitual $|\cdot|_\infty$;
- para cada primo p, el *valor absoluto p-ádico* $|\cdot|_p$ definido por la igualdad

$$|q|_p := \begin{cases} p^{-1} & \text{si } q = p, \\ 1 & \text{de lo contrario,} \end{cases}$$

  para todos los primos q, y extendido a $\mathbb{Q}$ multiplicativamente.

Es costumbre denotar por $\mathfrak{M}_\mathbb{Q}$ el conjunto de clases topológicas de valores absolutos no triviales sobre $\mathbb{Q}$, e identificarlo con la unión del conjunto de primos racionales y del símbolo ∞. Para todo

$$v \in \mathfrak{M}_\mathbb{Q} = \{2, 3, 5, 7, 11, \ldots\} \cup \{\infty\}$$

se puede considerar la completación $\mathbb{Q}_v$ del cuerpo $\mathbb{Q}$ con respecto a la topología definida por v. Esta construcción produce el cuerpo $\mathbb{R}$ cuando $v = \infty$, y el famoso cuerpo de números p-ádicos cuando v corresponde al número primo p. El representante de v elegido anteriormente define canónicamente un valor absoluto en $\mathbb{Q}_v$, y por [27, Teorema II.4.8] se extiende de forma única a un valor absoluto $|\cdot|_v$ sobre cualquiera clausura algebraica fijada $\overline{\mathbb{Q}_v}$ de dicho cuerpo.

Finalmente podemos combinar la información de todos los $v \in \mathfrak{M}_\mathbb{Q}$ para dar nuestra definición de complejidad aritmética de los puntos algebraicos en el toro.

Definición 1. La *altura* de un punto $\boldsymbol{x} = (x_1, \ldots, x_n) \in \left(\overline{\mathbb{Q}}^*\right)^n$ es

$$\mathrm{h}(\boldsymbol{x}) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathfrak{M}_\mathbb{Q}} \sum_{\sigma\colon K \hookrightarrow \overline{\mathbb{Q}_v}} \log \max(1, |\sigma(x_1)|_v, \ldots, |\sigma(x_n)|_v),$$

donde K es cualquier cuerpo de números que contenga todas las coordenadas de $\boldsymbol{x}$.

No es difícil demostrar que la definición no depende de la elección de K, por lo que se puede tomar como K al cuerpo de números mínimo $\mathbb{Q}(\boldsymbol{x})$ que contiene todas las coordenadas de $\boldsymbol{x}$. Los dos ejemplos siguientes justifican la interpretación de la altura como una función que mide la complejidad aritmética de un punto.

Ejemplo 3. Cuando todas las coordenadas de $\boldsymbol{x}$ son números racionales, su altura se puede calcular fácilmente. De hecho, es una igualdad obvia (aunque fundamental) conocida como *fórmula del producto* que

$$\sum_{v\in\mathfrak{M}_{\mathbb{Q}}} \log|y|_v = 0$$

para todo $y \in \mathbb{Q}^*$. Por lo tanto, al calcular la altura de $\boldsymbol{x} \in (\mathbb{Q}^*)^n$, si tomamos y como el mínimo común múltiplo de los denominadores de las coordenadas, obtenemos

$$\begin{aligned}\mathrm{h}(\boldsymbol{x}) = \sum_{v\in\mathfrak{M}_{\mathbb{Q}}} \log \max(|y|_v, |y\cdot x_1|_v, \dots, |y\cdot x_n|_v)\\ = \log \max(|y|_\infty, |y\cdot x_1|_\infty, \dots, |y\cdot x_n|_\infty).\end{aligned}$$

Por ejemplo, para $n = 1$, la altura del número racional distinto de cero a/b, siendo el numerador y el denominador coprimos, es simplemente $\mathrm{h}(a/b) = \log \max(|a|_\infty, |b|_\infty)$.

Ejemplo 4. Más cerca del espíritu de [4], cuando $n = 1$ podemos relacionar la altura de un entero algebraico distinto de cero con una medida de la complejidad de su polinomio mínimo sobre $\mathbb{Z}$. Recordemos que para cada polinomio distinto de cero f en una variable, su *medida de Mahler (logarítmica)* se define como la cantidad

$$\mathrm{m}(f) := \int_{\theta\in[0,1)} \log\left|f\left(e^{2\pi i\theta}\right)\right| d\theta.$$

Cuando f es un polinomio separable de grado d, y escribiendo $\{\alpha_1, \dots, \alpha_d\}$ para el conjunto de sus distintos ceros en el plano complejo, la fórmula de Jensen da

$$\mathrm{m}(f) = \log|f(0)| - \sum_{|\alpha_k|<1} \log|\alpha_k| = \sum_{|\alpha_k|\geq 1} \log|\alpha_k| = \sum_{k=1}^{d} \log \max(1, |\alpha_k|).$$

Sea ahora $x \in \overline{\mathbb{Z}} \setminus \{0\}$ un entero algebraico distinto de cero con polinomio mínimo f sobre $\mathbb{Z}$. Al calcular la altura de x siguiendo la Definición 1, la suma sobre $\mathfrak{M}_{\mathbb{Q}}$ se reduce al término $v = \infty$ debido a la desigualdad triangular no arquimediana, y la relación anterior permite concluir que

$$\mathrm{h}(x) = \frac{\mathrm{m}(f)}{\deg(f)}.$$

Esto demuestra que, salvo tomar logaritmos y dividir por el grado, nuestra noción de complejidad aritmética concuerda con la estudiada en [4, pág. 558] para enteros algebraicos.

La altura de los puntos algebraicos del toro de dimensión n satisface varias propiedades análogas a las presentadas en [4, § 2]. Las más elementales son las siguientes.

Lema 1. *Para todo punto* $\boldsymbol{x} = (x_1, \dots, x_n) \in \left(\overline{\mathbb{Q}}^*\right)^n$ *se tiene:*

(1) $\mathrm{h}(\boldsymbol{x}) \geq 0$*;*

(2) $\mathrm{h}(\boldsymbol{x}^r) = r \cdot \mathrm{h}(\boldsymbol{x})$ *para todo* $r \in \mathbb{Q}_{\geq 0}$*;*

(3) la altura de $\boldsymbol{x}$ *se compara con la altura* 1*-dimensional de sus coordenadas por*

$$\max\big(\mathrm{h}(x_1), \dots, \mathrm{h}(x_n)\big) \leq \mathrm{h}(\boldsymbol{x}) \leq \mathrm{h}(x_1) + \cdots + \mathrm{h}(x_n).$$

Además, si $x, y \in \overline{\mathbb{Q}}^*$ *entonces* $\mathrm{h}(x \cdot y) \leq \mathrm{h}(x) + \mathrm{h}(y)$ *y también* $\mathrm{h}(x^{-1}) = \mathrm{h}(x)$.

Demostración. El primer punto es obvio a partir de la definición. El segundo también se sigue fácilmente de la definición cuando r es un número entero; más generalmente, si $r = a/b$ es un número racional positivo, es suficiente observar que

$$b \cdot \mathrm{h}(\boldsymbol{x}^r) = \mathrm{h}\big((\boldsymbol{x}^r)^b\big) = \mathrm{h}(\boldsymbol{x}^a) = a \cdot \mathrm{h}(\boldsymbol{x}).$$

Con respecto a la tercera propiedad, la definición da $\mathrm{h}(x_i) \leq \mathrm{h}(\boldsymbol{x})$ para todo $i = 1, \dots, n$, lo que implica la primera desigualdad; la segunda se sigue de

$$\max(1, |\sigma(x_1)|_v, \dots, |\sigma(x_n)|_v) \leq \max(1, |\sigma(x_1)|_v) \cdots \max(1, |\sigma(x_n)|_v)$$

aplicada a cada término de la doble suma en la Definición 1.

Finalmente, las propiedades de la altura 1-dimensional son una consecuencia de la definición y de la fórmula del producto, ver también [5, Lema 1.5.18]. □

En secciones posteriores también necesitaremos controlar el cambio de la altura bajo la aplicación de morfismos entre toros que respetan la estructura de grupo. Para ello, recordemos que podemos asociar un morfismo $\varphi_A \colon \big(\overline{\mathbb{Q}}^*\big)^d \to \big(\overline{\mathbb{Q}}^*\big)^n$ de grupos algebraicos a cualquier matriz A de tamaño $n \times d$ con coeficientes enteros definiendo

$$\varphi_A\big((x_1, \dots, x_d)\big) = \Big(x_1^{A_{11}} \cdots x_d^{A_{1d}}, \dots, x_1^{A_{n1}} \cdots x_d^{A_{nd}}\Big). \tag{2.1}$$

El morfismo φ_A se llama la *transformación monomial* asociada a la matriz A; por [5, Proposición 3.2.17] cualquier homomorfismo entre toros es, de hecho, de esta forma.

Proposición 1. *Sea* A *una matriz de tamaño* $n \times d$ *con coeficientes enteros. En la notación* (2.1)*, tenemos*

$$\mathrm{h}(\varphi_A(\boldsymbol{x})) \leq nd\|A\| \, \mathrm{h}(\boldsymbol{x})$$

para todo $\boldsymbol{x} \in \big(\overline{\mathbb{Q}}^*\big)^d$*, donde* $\|A\|$ *indica el valor absoluto máximo de las entradas de* A*.*

Demostración. Consideremos $\boldsymbol{x} = (x_1, \dots, x_d) \in \big(\overline{\mathbb{Q}}^*\big)^d$. Aplicando la definición de φ_A y varias propiedades elementales de la altura del Lema 1 tenemos

$$\mathrm{h}(\varphi_A(\boldsymbol{x})) \leq \sum_{i=1}^{n} \mathrm{h}\left(x_1^{A_{i1}} \cdots x_d^{A_{id}}\right) \leq \sum_{i=1}^{n} \sum_{j=1}^{d} \mathrm{h}\left(x_j^{A_{ij}}\right) = \sum_{i=1}^{n} \sum_{j=1}^{d} |A_{ij}| \, \mathrm{h}(x_j).$$

Concluimos gracias a la no negatividad de la altura y la primera desigualdad del punto (3) del Lema 1. □

Investiguemos más a fondo otras propiedades de la altura. Podemos observar que, teniendo en cuenta que $\mathbb{Z}$ es discreto y el cálculo del Ejemplo 3, solo hay un número finito de puntos en $(\mathbb{Q}^*)^n$ con altura limitada por una constante fija. Una característica notable de la función altura, que es el origen de muchos resultados de finitud en geometría aritmética, es la extensión de tal observación.

Proposición 2 (propiedad de Northcott). *Existe solo un número finito de puntos de* $\left(\overline{\mathbb{Q}}^*\right)^n$ *con grado acotado y altura acotada. Dicho de otro modo, para todo* $B_1, B_2 \in \mathbb{R}_{\geq 0}$*, el conjunto*

$$\left\{\boldsymbol{x} \in \left(\overline{\mathbb{Q}}^*\right)^n \mid \ |\mathbb{Q}(\boldsymbol{x}) : \mathbb{Q}| \leq B_1 \ y \ \mathrm{h}(\boldsymbol{x}) \leq B_2\right\}$$

es finito.

Demostración. Tomemos un punto $\boldsymbol{x} = (x_1, \ldots, x_n)$ perteneciente al conjunto del enunciado. Como consecuencia del punto (3) del Lema 1, cada una de las coordenadas de $\boldsymbol{x}$ debe satisfacer las desigualdades

$$|\mathbb{Q}(x_i) : \mathbb{Q}| \leq B_1 \quad \text{y} \quad \mathrm{h}(x_i) \leq B_2.$$

Finalmente, la propiedad de Northcott en dimensión 1, para cuya demostración nos referimos a [5, Teorema 1.6.8] o (en el caso de enteros algebraicos) a [4, Teorema 2.1(2)], asegura que solo hay un número finito de opciones para x_i para todo $i = 1, \ldots, n$ y, por lo tanto, para $\boldsymbol{x}$. □

La primera consecuencia de la propiedad de Northcott es el siguiente análogo de [4, Teorema 2.3] en dimensión arbitraria.

Proposición 3 (teorema de Kronecker). *Se tiene que* $\mathrm{h}(\boldsymbol{x}) = 0$ *si y solo si* $\boldsymbol{x}$ *es un punto de torsión en* $\left(\overline{\mathbb{Q}}^*\right)^n$.

Demostración. Si $\boldsymbol{x}$ es un punto de torsión, entonces existe un entero estrictamente positivo d tal que $\boldsymbol{x}^d = \mathbf{1}$, donde $\mathbf{1} := (1, \ldots, 1)$. El punto (2) del Lema 1 implica

$$\mathrm{h}(\boldsymbol{x}) = \frac{1}{d}\,\mathrm{h}(\mathbf{1}) = 0.$$

Para la otra implicación, consideremos el conjunto $\mathcal{S} := \{\mathbf{1}, \boldsymbol{x}, \boldsymbol{x}^2, \ldots\}$. Dado que $\mathrm{h}(\boldsymbol{x}) = 0$, la misma afirmación en el lema citado asegura que todos los elementos de $\mathcal{S}$ tienen altura cero. Además, todos los puntos en $\mathcal{S}$ están claramente definidos sobre el cuerpo de definición de $\boldsymbol{x}$, por lo que la propiedad de Northcott implica que el conjunto $\mathcal{S}$ es finito. Por tanto, existen enteros positivos distintos d_1, d_2 tales que $\boldsymbol{x}^{d_1} = \boldsymbol{x}^{d_2}$, y entonces $\boldsymbol{x}$ es un punto de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$. □

Podemos expresar el contenido del teorema de Kronecker por el

Eslogan. La altura detecta torsión.

Esta es la característica clave que justifica por qué las alturas proporcionan un marco adecuado para investigar problemas sobre puntos de torsión en curvas, como el propuesto en la Pregunta 4.

3. Equidistribución

Del punto (1) del Lema 1 y del teorema de Kronecker se sigue inmediatamente que un punto algebraico del toro de dimensión n tiene altura mínima si y solo si es un punto de torsión.

El siguiente paso natural al investigar la distribución de los valores de la función altura es preguntarse si la altura de un punto $\boldsymbol{x} \in \left(\overline{\mathbb{Q}}^*\right)^n$ puede ser arbitrariamente pequeña sin anularse, y comprender cómo se pueden describir los puntos con una altura muy pequeña.

La primera observación es que, debido a la propiedad de Northcott, no podemos encontrar puntos con una altura distinta de cero arbitrariamente pequeña a menos que permitamos que el grado de los puntos sea arbitrariamente grande. Usando esta sugerencia, el siguiente ejemplo da una respuesta afirmativa simple a la existencia de una secuencia de puntos que no son de torsión con una altura que converge a 0.

Ejemplo 5. Sea $\varepsilon > 0$, y elegimos $\ell \in \mathbb{N}$ lo suficientemente grande como para que $\log(2)/\ell < \varepsilon$. Entonces, el punto (2) del Lema 1 y el Ejemplo 3 se combinan para dar

$$\mathrm{h}\left((\sqrt[\ell]{2}, 1, \ldots, 1)\right) = \frac{1}{\ell}\log(2) < \varepsilon.$$

En particular, la secuencia $\left((\sqrt[\ell]{2}, 1, \ldots, 1)\right)_\ell$ consta de puntos algebraicos de $(\overline{\mathbb{Q}}^*)^n$ que no son de torsión y cuya altura converge a cero.

Observación 1. La situación es completamente diferente para otras medidas de la complejidad aritmética de un punto algebraico, incluso para $n = 1$. Por ejemplo, tomemos el caso de la medida de Mahler del polinomio mínimo de $x \in \overline{\mathbb{Q}}$ sobre $\mathbb{Z}$. Es una pregunta abierta debida a Lehmer si tal medida, es decir, la cantidad

$$|\mathbb{Q}(x) : \mathbb{Q}| \cdot \mathrm{h}(x),$$

puede ser arbitrariamente pequeña sin anularse, y, de hecho, hoy en día se conjetura que 0 no es un punto de acumulación para los valores de dicho producto. Algunos famosos resultados parciales se deben a Dobrowolski y a Smyth, mientras que Dimitrov ha demostrado recientemente una forma débil de la conjetura, enunciada por Schinzel y Zassenhaus. Nos referimos a [4] y a las referencias allí citadas para más detalles sobre estas conjeturas y para una explicación de la prueba de Dimitrov.

Volviendo al problema de encontrar secuencias de puntos cuyas alturas converjan a 0, notemos que el soporte de la secuencia definida en el Ejemplo 5 se encuentra en el subgrupo de $\left(\overline{\mathbb{Q}}^*\right)^n$ dado por las ecuaciones $x_2 = \cdots = x_n = 1$. De manera más general, es significativo preguntar lo siguiente:

Pregunta 5. *¿En qué subvariedades de $\left(\overline{\mathbb{Q}}^*\right)^n$ se pueden encontrar puntos con altura distinta de cero arbitrariamente pequeña?*

Daremos una respuesta en el Corolario 2. Antes de eso, necesitamos entender cómo se comportan las secuencias de puntos con altura que converge a 0. El siguiente ejemplo en dimensión 1 es esclarecedor.

Ejemplo 6. Sean x un entero algebraico distinto de cero y f su polinomio mínimo sobre $\mathbb{Z}$. Recordando la relación entre la altura de x y la medida de Mahler de f explicada en el Ejemplo 4, y usando un argumento de convexidad y el teorema de Parseval (ver, por ejemplo, [5, Lema 1.6.7]), se obtiene

$$\mathrm{h}(x) \leq \frac{\log(\deg(f)+1) + 2\log|f|_\infty}{2\deg(f)}.$$

En la desigualdad anterior, $|f|_\infty$ denota el valor absoluto euclidiano máximo de los coeficientes de f.

Usando esta observación, podemos construir eficientemente secuencias de puntos en $\overline{\mathbb{Z}} \setminus \{0\}$ con una altura que converge a cero. La receta es la siguiente: fijamos un número entero positivo B, y tomamos una secuencia aleatoria de polinomios mónicos irreducibles con coeficientes enteros $(f_\ell)_{\ell\geq 2}$, con $\deg(f_\ell) = \ell$ y $|f_\ell|_\infty \leq B$ para todo ℓ. Para todo ℓ elegimos también una raíz x_ℓ de f_ℓ. De la desigualdad anterior se deduce que $(x_\ell)_{\ell\geq 2}$ es una secuencia de enteros algebraicos distintos de cero con una altura que converge a 0 a medida que ℓ crece.

Podemos usar el código `SageMath` escrito en [16] para construir tal secuencia $(x_\ell)_\ell$ y representar en el plano complejo las órbitas de Galois de estos puntos, es decir el conjunto de ceros de los polinomios f_ℓ correspondientes.

La Figura 2, que muestra el resultado del código para $B = 3$ y algún valor de ℓ, parece sugerir un patrón fuerte.

De hecho, la tendencia de secuencias de puntos con altura que converge a cero de tener órbitas de Galois que se acercan al círculo unitario es cierta incluso en dimensiones más altas. Para enunciar este comportamiento de forma precisa, recordemos que para $\boldsymbol{p} \in (\mathbb{C}^*)^n$ la notación $\delta_{\boldsymbol{p}}$ denota la medida de probabilidad de Dirac en el toro complejo de dimensión n, soportada en $\{\boldsymbol{p}\}$.

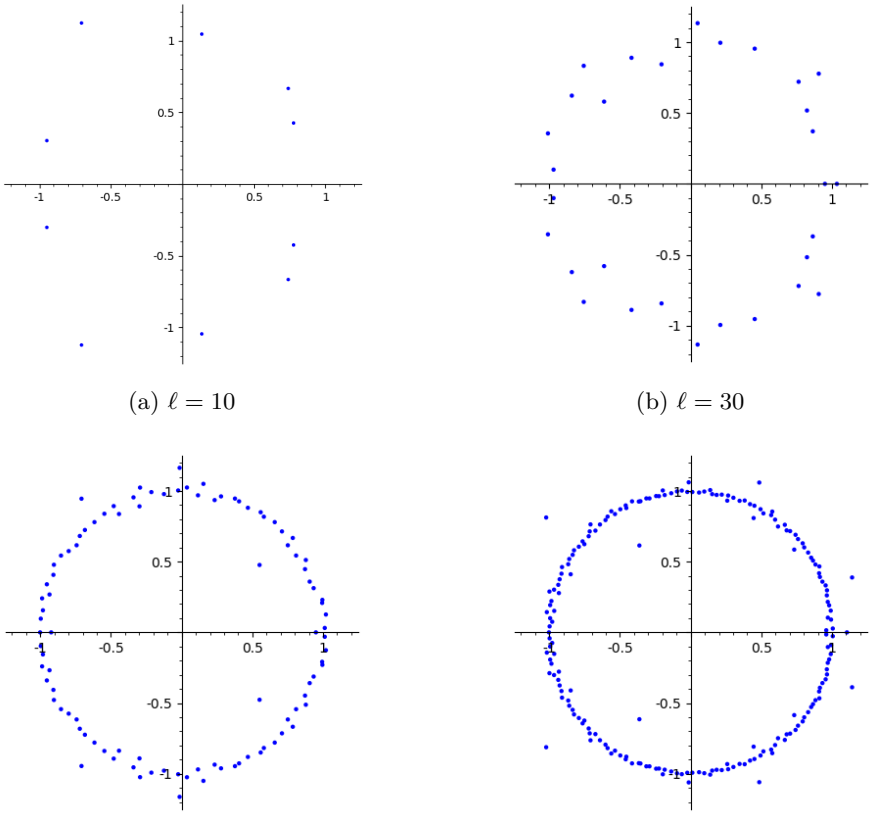
Además, un *subgrupo algebraico* del toro de dimensión n es, por definición, un subgrupo de $\left(\overline{\mathbb{Q}}^*\right)^n$ que es cerrado con respecto a la topología de Zariski.

Teorema 1 (teorema de equidistribución tórica). *Sea $(\boldsymbol{x}_\ell)_\ell$ una secuencia de puntos en $\left(\overline{\mathbb{Q}}^*\right)^n$ tal que $\mathrm{h}(\boldsymbol{x}_\ell) \to 0$ cuando $\ell \to \infty$. Supongamos también que la secuencia es estricta, lo que significa que cualquier subgrupo algebraico (irreducible) de $\left(\overline{\mathbb{Q}}^*\right)^n$ diferente del toro completo contiene $\boldsymbol{x}_\ell$ para solo un número finito de valores de ℓ. Entonces, la secuencia de medidas de probabilidad*

$$\frac{1}{[\mathbb{Q}(\boldsymbol{x}_\ell) : \mathbb{Q}]} \sum_{\sigma\colon \mathbb{Q}(\boldsymbol{x}_\ell)\hookrightarrow\mathbb{C}} \delta_{\sigma(\boldsymbol{x}_\ell)}$$

converge débilmente a la medida de probabilidad en $(\mathbb{C}^*)^n$ soportada en el policírculo unitario $|x_1| = \cdots = |x_n| = 1$, donde coincide con su medida de Haar normalizada.

En esta forma, el teorema fue probado por Bilu en [3, Teorema 1.1], reduciendo el enunciado al caso de dimensión 1. Un resultado similar en variedades abelianas fue obtenido por Szpiro, Ullmo y Zhang [33]. En los años siguientes, muchos matemáticos han colaborado en la extensión de estos teoremas de equidistribución en el marco de la geometría de Arakelov, culminando con el trabajo de Yuan [36].



(a) $\ell = 10$ (b) $\ell = 30$

(c) $\ell = 100$ (d) $\ell = 200$

Figura 2: Representando órbitas de Galois de enteros algebraicos de altura pequeña.

4. Dos teoremas tóricos

En esta sección estudiamos los dos resultados principales de estas notas. Al hacerlo, la siguiente definición es fundamental: debe interpretarse como una formulación precisa de la noción de «subvariedades especiales» de un toro algebraico, y generaliza la identificación entre «puntos especiales» de $\left(\overline{\mathbb{Q}}^*\right)^n$ y «puntos de torsión» sugerida en la Sección 1.

Definición 2. Una *subvariedad de torsión* de $\left(\overline{\mathbb{Q}}^*\right)^n$ es una subvariedad de la forma

$$T = \boldsymbol{\omega} \cdot H,$$

donde $\boldsymbol{\omega}$ es un punto de torsión y H es un subgrupo algebraico irreducible del toro ambiente.

Por ejemplo, las únicas subvariedades de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$ que tienen dimensión 0 son los puntos de torsión, mientras que la única subvariedad de torsión de dimensión n es el toro mismo.

En términos más generales, para describir todas las subvariedades de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$ es necesario comprender la forma de los subgrupos algebraicos irreducibles del toro. Existe una hermosa clasificación combinatoria de estos en términos de subgrupos primitivos de $\mathbb{Z}^n$; ver, por ejemplo, [5, § 3.2]. Usando esta descripción, se puede probar la siguiente lista de afirmaciones.

Lema 2. *Se tiene que:*

1. *Cualquier subvariedad de torsión de dimensión d de $\left(\overline{\mathbb{Q}}^*\right)^n$ es la intersección de $n-d$ subvariedades de torsión de dimensión $n-1$. En particular, cualquier subvariedad de torsión diferente del toro completo está contenida en una subvariedad de torsión de dimensión $n-1$.*
2. *Las subvariedades de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$ que tienen dimensión $n-1$ son precisamente los conjuntos de ceros de los binomios de Laurent*

$$x_1^{m_1}\cdots x_n^{m_n}-\zeta,$$

   donde $(m_1,\ldots,m_n)$ es un vector primitivo en $\mathbb{Z}^n$ y $\zeta\in\overline{\mathbb{Q}}^*$ es una raíz de la unidad.
3. *Para cualquier subvariedad de torsión T de $\left(\overline{\mathbb{Q}}^*\right)^n$ de dimensión d existe un isomorfismo $\varphi\colon\left(\overline{\mathbb{Q}}^*\right)^d\to T$, que identifica subvariedades de torsión, y dos números reales positivos B_1, B_2 tales que*

$$B_1\,\mathrm{h}(\boldsymbol{x})\le\mathrm{h}(\varphi(\boldsymbol{x}))\le B_2\,\mathrm{h}(\boldsymbol{x}) \tag{4.1}$$

   para todo $\boldsymbol{x}\in\left(\overline{\mathbb{Q}}^*\right)^d$.

Demostración. Las dos primeras propiedades derivan de las correspondientes para subgrupos algebraicos irreducibles, que se pueden demostrar mediante [5, Proposición 3.2.7 y Teorema 3.2.19].

Para probar la tercera, escribimos $T=\boldsymbol{\omega}\cdot H$ como en la Definición 2, con H un subgrupo algebraico irreducible del toro ambiente, de dimensión d. Por [5, Corolario 3.2.8 y Proposición 3.2.17] existe un isomorfismo de grupos algebraicos $\left(\overline{\mathbb{Q}}^*\right)^d\xrightarrow{\sim}H$, que, después de la inclusión, debe provenir de una transformación monomial φ_A asociada a una matriz A de tamaño $n\times d$ como en (2.1). La composición de tal isomorfismo con la traslación (multiplicativa) por $\boldsymbol{\omega}$ define un isomorfismo $\varphi\colon\left(\overline{\mathbb{Q}}^*\right)^d\to T$ que respeta las subvariedades de torsión.

En cuanto a la cadena de desigualdades (4.1), la segunda es consecuencia de la Proposición 1 y del hecho que la multiplicación por un punto de torsión preserva la altura. Para la otra, podemos aplicar el mismo argumento a la composición de la traslación por $\boldsymbol{\omega}^{-1}$ y la transformación monomial $\varphi_{A^{-1}}$ asociada a cualquier inversa por la izquierda A^{-1} de la matriz A. De hecho, esto define un morfismo $\left(\overline{\mathbb{Q}}^*\right)^n\to\left(\overline{\mathbb{Q}}^*\right)^d$ que es un inverso por la izquierda del morfismo φ. □

Observación 2. El *conjunto de puntos de torsión que se encuentran en una subvariedad de torsión T es Zariski denso en T*. Usando el isomorfismo del punto (3) del

Lema 2 podemos reducir esta afirmación a la de que los puntos de torsión son densos en $\left(\overline{\mathbb{Q}}^*\right)^d$. Este enunciado es consecuencia del hecho, que se puede demostrar por recurrencia sobre el número de variables, de que cualquier polinomio de Laurent en d variables que se anula en todos los puntos de torsión de $\left(\overline{\mathbb{Q}}^*\right)^d$ debe ser el polinomio cero, ya que las raíces de la unidad son infinitas en $\overline{\mathbb{Q}}^*$.

Volvamos ahora al objetivo principal de este artículo, y tomemos una subvariedad X del toro $\left(\overline{\mathbb{Q}}^*\right)^n$; contrariamente a la terminología estándar, no asumimos que X sea irreducible.

Definición 3. Una *subvariedad de torsión de* X es una subvariedad de torsión del toro ambiente que está contenida en X. Se llama *maximal* si no está contenida estrictamente en ninguna otra subvariedad de torsión de X.

Con estas nociones en mente, podemos enunciar el siguiente resultado diofántico, que rige la organización de los puntos de torsión en X.

Teorema 2 (Manin-Mumford tórico). *Toda subvariedad X de $\left(\overline{\mathbb{Q}}^*\right)^n$ contiene un número finito de subvariedades de torsión maximales.*

La antigua conjetura de Manin-Mumford tórica (junto con su contrapartida abeliana, que mencionamos en la Sección 6) fue formulada por Lang en [22, págs. 220–221], inspirado por los trabajos de Chabauty y por una pregunta planteada contemporáneamente por Manin y por Mumford para las variedades abelianas. Cuando $n = 2$, Ihara, Serre y Tate encontraron pruebas independientes de la conjetura, como se reconoce en [21] y en [22, Teorema VIII.6.1]. El caso general es un teorema de Laurent [23], véase también una demostración diferente posterior de Sarnak y Adams [32].

En estas notas, deduciremos el Teorema 2 de un resultado más fuerte, probado por primera vez por Zhang en [40, Teorema 6.2] y redemostrado de manera elemental en [7]. El argumento que usamos aquí sigue una prueba posterior y más simple debida a Bilu [3, Teorema 5.1] y se basa en su propio teorema de equidistribución.

Teorema 3 (Bogomolov tórico). *Sea X una subvariedad irreducible de $\left(\overline{\mathbb{Q}}^*\right)^n$. Si X no es una subvariedad de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$, entonces existe un subconjunto abierto no vacío U de X y una constante estrictamente positiva $c \in \mathbb{R}$ tal que*

$$\mathrm{h}(\boldsymbol{x}) \geq c$$

para todo $\boldsymbol{x} \in U$.

Demostración. Sea $T_1, T_2, \ldots$ la lista completa de las subvariedades de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$ de dimensión $n-1$ (el conjunto de estas es claramente numerable). Podemos suponer que X no está contenida en ninguna unión finita de estas. De lo contrario, X estaría contenida en una de ellas, por ser X irreducible, y entonces, vía un isomorfismo como el del punto (3) del Lema 2, que conserva el conjunto de subvariedades de torsión y transforma las alturas de manera controlada, podemos reducir la prueba al caso de un espacio ambiente de dimensión menor $\left(\overline{\mathbb{Q}}^*\right)^{n-1}$.

Supongamos, por reducción al absurdo, que para toda constante real $c > 0$ y para todo subconjunto abierto no vacío U de X, existe un punto $\boldsymbol{x} \in U$ tal que $\mathrm{h}(\boldsymbol{x}) < c$. Por lo tanto, para todo $\ell \in \mathbb{N}_{\geq 1}$, la consideración anterior permite elegir

$$\boldsymbol{x}_\ell \in X \setminus \bigcup_{i=1}^{\ell} T_i, \quad \text{con } \mathrm{h}(\boldsymbol{x}_\ell) < \frac{1}{\ell}.$$

Por construcción, la secuencia $(\boldsymbol{x}_\ell)_\ell$ es estricta en $\left(\overline{\mathbb{Q}}^*\right)^n$: por el punto (1) del Lema 2, cualquier subgrupo algebraico irreducible de $(\overline{\mathbb{Q}}^*)^n$ diferente del toro completo está contenido en $\bigcup_{i=1}^{\ell} T_i$ para ciertos ℓ, y la secuencia definitivamente evita estos conjuntos. Por lo tanto, el teorema de la equidistribución tórica (Teorema 1) asegura que la secuencia de medidas

$$\mu_\ell := \frac{1}{[\mathbb{Q}(\boldsymbol{x}_\ell) : \mathbb{Q}]} \sum_{\sigma\colon \mathbb{Q}(\boldsymbol{x}_\ell) \hookrightarrow \mathbb{C}} \delta_{\sigma(\boldsymbol{x}_\ell)}$$

converge débilmente a la medida de Haar normalizada en $(\mathbb{S}^1)^n$, cuando $\ell \to \infty$. Para todo $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denotamos por X_τ el correspondiente conjugado de Galois de X.

Dado que el soporte de cada una de las medidas μ_ℓ está contenido en $\bigcup_\tau X_\tau(\mathbb{C})$, así debe suceder para el soporte de su límite. Dicho de otro modo, $\bigcup_\tau X_\tau(\mathbb{C})$ debe contener $(\mathbb{S}^1)^n$, que es denso en $(\mathbb{C}^*)^n$, lo que implica que $\bigcup_\tau X_\tau = \left(\overline{\mathbb{Q}}^*\right)^n$. Dado que solo hay un número finito de conjugados de Galois de X y el toro es irreducible, debe occurrir que $X = \left(\overline{\mathbb{Q}}^*\right)^n$, lo que implica que X es una subvariedad de torsión. □

Una forma equivalente de enunciar el teorema anterior es decir que si X no es una subvariedad de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$, entonces existe un constante positiva c para la cual el conjunto $\{\boldsymbol{x} \in X \mid \mathrm{h}(\boldsymbol{x}) < c\}$ no es denso en X. Por lo tanto, el contenido de la antigua conjetura de Bogomolov tórica se expresa de manera concisa mediante el siguiente

Eslogan. Si demasiados puntos en X tienen una altura arbitrariamente pequeña, entonces X es una subvariedad de torsión.

Ahora podemos deducir fácilmente la demostración del Teorema 2 a partir del enunciado del Teorema 3, como sigue.

Prueba del teorema de Manin-Mumford tórico. Cada una de las subvariedades de torsión maximales de X debe estar contenida, por irreducibilidad, en una de las componentes irreducibles de X. Por lo tanto, después de escribir X como la unión de sus componentes irreducibles (en número finito), podemos reducirnos al caso en que la variedad X sea ella misma irreducible.

Bajo esta hipótesis, procedemos ahora por inducción sobre la dimensión. El teorema es obvio si X tiene dimensión cero, por lo que suponemos que tiene dimensión al menos 1. En tal caso, se cumple una de las siguientes alternativas: X es ella misma

una subvariedad de torsión de $\left(\overline{\mathbb{Q}}^*\right)^n$, o no lo es. En el primer caso, el teorema es de nuevo obvio, ya que X será la única subvariedad de torsión maximal de sí misma.

De lo contrario, se puede aplicar el teorema de Bogomolov tórico y el teorema de Kronecker para deducir la existencia de un subconjunto cerrado propio Z de X que contiene todos los puntos de torsión de X. Dado que los puntos de torsión en una subvariedad de torsión son densos por la Observación 2, debe suceder que cualquier subvariedad de torsión de X también esté contenida en Z. De la aplicación de la hipótesis de inducción a cada una de las componentes irreducibles de Z deducimos la finitud de las subvariedades de torsión maximales de X. □

Observación 3. En el Teorema 3 podemos tomar U como el complemento en X de la unión de sus subvariedades de torsión maximales. Dicho de otro modo, si X es una subvariedad irreducible de $\left(\overline{\mathbb{Q}}^*\right)^n$, entonces existe una constante estrictamente positiva $c \in \mathbb{R}$ tal que

$$\mathrm{h}(\boldsymbol{x}) \geq c \quad \text{para todo} \quad \boldsymbol{x} \in X \setminus \bigcup_{\substack{T \text{ subvariedad de torsión} \\ \text{maximal de } X}} T. \tag{4.2}$$

Cuando X es una subvariedad de torsión del toro, esta afirmación es vacía. De lo contrario, el enunciado se puede probar por inducción sobre la dimensión de X, siendo trivial el caso de dimensión cero. De hecho, el teorema de Bogomolov tórico da la existencia de un subconjunto abierto no vacío U y de un número real estrictamente positivo c_U con $\mathrm{h}(\boldsymbol{x}) \geq c_U$ para todo $\boldsymbol{x} \in U$. Sea $X \setminus U = Z_1 \cup \ldots \cup Z_r$, siendo cada Z_i una subvariedad cerrada irreducible de X de dimensión como máximo $\dim(X) - 1$. Aplicando la hipótesis inductiva, deducimos para todo $i = 1, \ldots, r$ la existencia de una constante estrictamente positiva c_i tal que $\mathrm{h}(\boldsymbol{x}) \geq c_i$ para todo $\boldsymbol{x} \in Z_i$ que no pertenezca a ninguna subvariedad de torsión maximal de Z_i. Entonces, (4.2) se cumple con $c = \mín(c_U, c_1, \ldots, c_r)$.

5. Respondiendo a nuestras preguntas, y un poco más

El Teorema 2 obtenido en la sección anterior es lo suficientemente fuerte como para responder a la Pregunta 4 sobre el número de puntos de torsión en una curva algebraica en $(\mathbb{C}^*)^2$.

Corolario 1. *La curva algebraica en $(\mathbb{C}^*)^2$ definida por un polinomio de Laurent irreducible $f \in \overline{\mathbb{Q}}\left[x_1^{\pm 1}, x_2^{\pm 1}\right]$ contiene infinitos puntos de torsión si y solo si, salvo multiplicación por un monomio,*

$$f = x_1^{m_1} x_2^{m_2} - \zeta$$

para un vector primitivo $(m_1, m_2) \in \mathbb{Z}^2$ y una raíz de la unidad $\zeta \in \overline{\mathbb{Q}}^*$.

Demostración. Por la antigua conjetura de Manin-Mumford tórica, la subvariedad irreducible definida por f contiene un número finito de subvariedades de torsión maximales. Por tanto, tal curva es una subvariedad de torsión ella misma, en cuyo caso

debe ser el conjunto de ceros de un binomio de Laurent como el del enunciado por el punto (2) del Lema 2 y contener infinitos puntos de torsión por la Observación 2, o solo puede contener un número finito de puntos de torsión. □

De hecho, la antigua conjetura de Bogomolov tórica afirma aún más: si f no es un binomio de Laurent de la forma que aparece en el Corolario 1, todos los puntos que no son de torsión que se encuentran en la curva definida por f deben tener altura mayor que una constante estrictamente positiva c.

Ejemplo 7. En el Ejemplo 2 hemos determinado todos los puntos de torsión de la curva definida por la ecuación $x_1 + x_2 + 1 = 0$. En [37], Zagier demostró que todos los puntos en esta curva que no son de torsión tienen altura al menos 0,1911225..., proporcionando así un valor explícito para la constante c en este caso.

Finalmente, el Teorema 3 también nos permite responder a la Pregunta 5.

Corolario 2. *Una subvariedad algebraica X de $\left(\overline{\mathbb{Q}}^*\right)^n$ contiene puntos con altura distinta de cero arbitrariamente pequeña si y solo si contiene una subvariedad de torsión de dimension* 1.

Demostración. Si X contiene una subvariedad de torsión de dimension 1 (digamos T), entonces existe un morfismo $\varphi\colon \overline{\mathbb{Q}}^* \to T \subseteq X$ como el del punto (3) del Lema 2. Como se muestra en el Ejemplo 5, el toro $\overline{\mathbb{Q}}^*$ contiene puntos de altura distinta de cero arbitrariamente pequeña, y sus imágenes por φ son puntos en X con altura distinta de cero arbitrariamente pequeña debido a (4.1).

Para la otra implicación, supongamos que X no contiene ninguna subvariedad de torsión de dimension 1. Como consecuencia, las subvariedades de torsión maximales de X son todas de dimensión 0. Esto significa, a la luz de la Observación 3 y del Teorema 2, que existe una constante estrictamente positiva $c \in \mathbb{R}$ tal que $\mathrm{h}(\boldsymbol{x}) \geq c$ para todos salvo un número finito de puntos $\boldsymbol{x}$ de X, obstruyendo así la existencia de puntos de altura distinta de cero arbitrariamente pequeña. □

6. ¿Y luego?

Las preguntas y respuestas expuestas en este artículo han motivado varias direcciones de investigación en los últimos años. Recopilamos brevemente algunas de ellas en esta sección, junto con algunas preguntas y aplicaciones tangenciales. El lector interesado puede consultar las referencias [38] y [39] para obtener muchos más detalles y un tratamiento mucho más amplio de algunos de estos temas, por lo que estas páginas pueden verse como un aperitivo.

Cotas efectivas

Es natural pedir una versión efectiva de los Teoremas 2 y 3, en dos sentidos diferentes.

Con respecto a la antigua conjetura de Manin-Mumford tórica, una de sus consecuencias es que una subvariedad X de $\left(\overline{\mathbb{Q}}^*\right)^n$ solo contiene un número finito de

puntos de torsión aislados, es decir, puntos de torsión que también son subvariedades de torsión maximales de X. El problema de encontrar cotas superiores explícitas para el número de tales puntos de torsión aislados de X fue considerado por Schmidt, Evertse, Ruppert, Beukers y Smyth, y por Amoroso y Viada, entre otros. En su tesis doctoral, Martínez [25] demostró, en particular, que si X está definida por polinomios de grado como mucho d, entonces X contiene como mucho

$$C_n \cdot d^n$$

puntos de torsión aislados para una cierta constante explícita C_n, lo que confirma conjeturas previas de Ruppert y de Aliev y Smyth.

Hacer efectiva la antigua conjetura de Bogomolov tórica consiste en dar cotas inferiores a la constante c que aparece en (4.2). Esto ya fue considerado por Bombieri y Zannier, y luego refinado por Schmidt, David y Philippon, Amoroso y David, con la idea de desarrollar la cota de Dobrowolski en dimensiones superiores. En [2], Amoroso y Viada probaron que si X está definida por polinomios de grado como mucho d, entonces la constante c de (4.2) está acotada inferiormente por

$$\frac{C_{1,n}}{d} \cdot \big(\log(n^2 d)\big)^{-C_{2,n}},$$

para constantes positivas explícitas $C_{1,n}$ y $C_{2,n}$.

Todas estas estimaciones uniformes han encontrado aplicaciones, ya que se aplican a problemas de contar ceros de recursiones lineales [13], y a ecuaciones cuantitativas S-unitarias; ver, por ejemplo, [11, Ejercicio 2.14] para la conexión entre el enunciado de Manin-Mumford tórico y un resultado de Evertse, van der Poorten y Schlickewei.

El caso abeliano

Aunque en estas notas nos hemos centrado en el caso tórico, que es más elemental, se pueden hacer preguntas similares sobre las relaciones entre las subvariedades de las *variedades abelianas* y sus puntos de torsión.

Estas variedades algebraicas también admiten una estructura de grupo y por esta razón juegan un papel destacado en la geometría aritmética. En particular, como para los toros, se pueden considerar puntos de torsión y subvariedades de torsión de variedades abelianas, e incluso existe una noción de altura, la llamada *altura de Néron-Tate*, que detecta los puntos de torsión, exactamente como en el caso tórico lo hace la altura de la Definición 1.

De ello se deduce que preguntas análogas a las conjeturas de Manin-Mumford y Bogomolov también pueden formularse en este marco, y de hecho tienen su génesis histórica en este escenario; por ejemplo, la pregunta original de Bogomolov se refiere a la cantidad de puntos en una curva de género al menos 2, inmersa en su jacobiana, que tienen altura de Néron-Tate pequeña.

La conjetura de Manin-Mumford abeliana fue probada por primera vez por Raynaud [31]; otras pruebas fueron proporcionadas por Hindry [17] y, usando argumentos

de lógica, por Hrushowski [18]. Mencionemos también las pruebas de Pink y Rössler, y de Pila y Zannier. En cambio, la conjetura de Bogomolov abeliana fue resuelta por Ullmo [34] y por Zhang [41], basándose en el teorema de equidistribución debido a Szpiro, Ullmo y Zhang [33].

Las líneas de investigación en el mundo abeliano no han dejado de latir tras la consecución de estos resultados. Por ejemplo, una versión del enunciado de Bogomolov abeliano sobre cuerpos de funciones ha sido demostrada recientemente por Yuan y Xie [35], basándose en resultados parciales previos de Yamaki, Gubler, Cinkir, Cantat, Gao, Habegger y Xie.

Por el lado efectivo, una versión uniforme del teorema de Bogomolov abeliano, probada por Dimitrov, Gao y Habegger [12] y por Kühne [20], da un control sobre el número de puntos con altura de Néron-Tate pequeña en una curva de género al menos 2, con una cota que solo depende del género de la curva. Este resultado innovador se aplica a preguntas típicas en geometría aritmética, como la Pregunta 1. Por ejemplo, combinada con resultados previos de De Diego y de Rémond, esta desigualdad uniforme de Bogomolov permite responder afirmativamente a una pregunta planteada por Mazur en 1986; más precisamente, para una curva C de género al menos 2 definida sobre un cuerpo de números K, se puede obtener la siguiente cota para el número de K-puntos racionales de C:

$$\#C(K) \leq c^{1+\mathrm{rk}\,\mathrm{Jac}(C)(K)},$$

donde c es una constante que depende únicamente del género de C, $\mathrm{Jac}(C)$ es la variedad jacobiana de la curva, y el grupo $\mathrm{Jac}(C)(K)$ tiene rango finito por el teorema de Mordell-Weil. También mencionamos que, recientemente, Yuan dio una prueba completamente diferente de este «Bogomolov uniforme» utilizando la teoría de fibrados de línea adélicos en variedades cuasi-proyectivas que desarrolló junto con Zhang.

Un análogo dinámico

Tanto la altura canónica sobre los toros como la altura de Néron-Tate sobre las variedades abelianas son casos especiales de alturas que surgen de sistemas dinámicos, tal como las definen Call y Silverman. En los dos contextos mencionados, las subvariedades de torsión son precisamente las subvariedades preperiódicas del sistema dinámico, lo que sugiere la posibilidad de generalizar las conjeturas de Manin-Mumford y Bogomolov al mundo de la dinámica aritmética, como se propone en [42].

Sin embargo, en [15] y posteriormente en [29], se construyeron contraejemplos a estas conjeturas usando productos de curvas elípticas con multiplicación compleja y productos de variedades abelianas con multiplicación compleja que son jacobianas de ciertas curvas de género 2.

Una propiedad de Bogomolov para cuerpos

Un problema de teoría de números más algebraico relacionado con el Teorema 3 es el estudio de los *cuerpos con la propiedad (B)*. Estos son subcuerpos K de $\overline{\mathbb{Q}}$ para

los cuales existe una constante $c \in \mathbb{R}$ estrictamente positiva tal que $\mathrm{h}(x) \geq c$ para todo $x \in K \setminus \{0\}$ que no es raíz de la unidad.

Algunos ejemplos no triviales de cuerpos con propiedad (B) son el cuerpo de los números algebraicos totalmente reales (por un teorema de Schinzel), la extensión abeliana máximal de $\mathbb{Q}$ (por un teorema de Amoroso y Dvornicich) y los cuerpos obtenidos al añadir a $\mathbb{Q}$ las coordenadas de todos los puntos de torsión de una curva elíptica (como lo muestra Habegger), ver [1] y sus referencias.

Trabajos recientes indican una interesante relación entre la propiedad (B) de los subcuerpos de $\overline{\mathbb{Q}}$ y ciertas características de crecimiento de sus grupos de Galois; véase por ejemplo [8] para una conexión entre la teoría geométrica de grupos y la conjetura de Lehmer.

Conclusión

Debido a limitaciones de espacio mencionamos brevemente las siguientes preguntas y temas relacionados con el contenido de este artículo:

- Como se explica en [22, Capítulo 8, § 7] se puede estudiar el conjunto de puntos en una subvariedad del toro con coordenadas que viven en el grupo de división de un subgrupo Γ finitamente generado dado (en nuestras notas, $\Gamma = \{\mathbf{1}\}$).
- En lugar de considerar el conjunto de puntos de torsión de una curva en el toro, se puede considerar su intersección con la familia de subgrupos algebraicos propios del toro, como se hace en [6]. Esto permite investigar el conjunto de puntos en la curva que tienen coordenadas multiplicativamente dependientes.
- Extender el eslogan según el cual «la clausura de un conjunto de puntos especiales es una subvariedad especial» al contexto de las variedades de Shimura fue el contenido de la célebre conjetura de André-Oort, recientemente demostrada en completa generalidad por Pila, Shankar y Tsimerman [30], después de varias contribuciones de André, Yafaev, Edixhoven, Clozel, Klingler, Ullmo y Tsimerman, solo por citar a algunos.

Además, incluso ateniéndonos al caso tórico, entre las aplicaciones más recientes del teorema de Manin-Mumford se puede citar la descripción de todos los conjuntos de vectores tridimensionales que por pares forman ángulos conmensurables con π [19], y la prueba de una condición suficiente para la resolubilidad virtual de grupos lineales sobre un cuerpo de característica cero [10].

Todo esto muestra cómo, a pesar de la pregunta muy simple con la que comenzamos, el tema en el que nos hemos sumergido no solo está conectado con conjeturas profundas y nociones poderosas en geometría aritmética, sino que también sigue inspirando a los teóricos de números que trabajan en diferentes áreas. Solo el futuro dirá si el lector de estas notas dará algún día su propia contribución a esta fantástica e inextinguible mina.

Referencias

[1] F. Amoroso, S. David y U. Zannier, On fields with Property (B), *Proc. Amer. Math. Soc.* **142** (2014), no. 6, 1893–1910.

[2] F. Amoroso y E. Viada, Small points on rational subvarieties of tori, *Comment. Math. Helv.* **87** (2012), no. 2, 355–383.

[3] Y. Bilu, Limit distribution of small points on algebraic tori, *Duke Math. J.* **89** (1997), no. 3, 465–476.

[4] Y. Bilu, J. I. Burgos Gil y M. Sombra, La casa de los números pequeños, *Gac. R. Soc. Mat. Esp.* **25** (2022), 557–575.

[5] E. Bombieri y W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.

[6] E. Bombieri, D. Masser y U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, *Internat. Math. Res. Notices* **20** (1999), 1119–1140.

[7] E. Bombieri y U. Zannier, Algebraic points on subvarieties of $\mathbf{G}_m^n$, *Internat. Math. Res. Notices* **7** (1995), 333–347.

[8] E. Breuillard, Diophantine geometry and uniform growth of finite and infinite groups, *Proceedings of the International Congress of Mathematicians—Seoul 2014*, Vol. III, 27–50, Kyung Moon Sa, Seoul, 2014.

[9] J. H. Conway y A. J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30** (1976), 229–240.

[10] P. Corvaja, A. Rapinchuk, J. Ren y U. Zannier, Non-virtually abelian anisotropic linear groups are not boundedly generated, *Invent. Math.* **227** (2022), 1–26.

[11] P. Corvaja y U. Zannier, *Applications of Diophantine approximation to integral points and transcendence*, Cambridge University Press **212**, Cambridge, 2018.

[12] V. Dimitrov, Z. Gao y P. Habegger, Uniformity in Mordell-Lang for curves, *Ann. of Math. (2)* **194** (2021), no. 1, 237–298.

[13] J.-H. Evertse, H. Schlickewei y W. Schmidt, Linear equations in variables which lie in a multiplicative group, *Ann. of Math. (2)* **155** (2002), no. 3, 807–836.

[14] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[15] D. Ghioca, T. Tucker y S. Zhang, Towards a dynamical Manin-Mumford conjecture, *Int. Math. Res. Not. IMRN* **22** (2011), 5109–5122.

[16] R. Gualdi, *Equidistribution of algebraic integers having small height*, SageMath notebook, 2022, disponible en `https://bit.ly/3jxYgR4`.

[17] M. Hindry, Autour d'une conjecture de Serge Lang, *Invent. Math.* **94** (1988), 575–603.

[18] E. Hrushowski, The Manin-Mumford conjecture and the model theory of difference field, *Ann. Pure Appl. Logic* **112** (2001), 43–115.

[19] K. Kedlaya, A. Kolpakov, B. Poonen y M. Rubinstein, Space vectors forming rational angles, 2020, https://arxiv.org/abs/2011.14232.

[20] L. Kühne, Equidistribution in families of Abelian varieties and uniformity, 2021, https://arxiv.org/abs/2101.10272.

[21] S. Lang, Division points on curves, *Ann. Mat. Pura Appl. (4)* **70** (1965), 229–234.

[22] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[23] M. Laurent, Équations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.

[24] H. B. Mann, On linear relations between roots of unity, *Mathematika* **12** (1965), 107–117.

[25] C. Martínez, The number of maximal torsion cosets in subvarieties of tori, *J. Reine Angew. Math.* **755** (2019), 103–126.

[26] Yu. V. Matiyasevich, The Diophantineness of enumerable sets, *Dokl. Akad. Nauk SSSR* **191** (1970), 279–282.

[27] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.

[28] A. Ostrowski, Über einige Lösungen der Funktionalgleichung $\psi(x) \cdot \psi(y) = \psi(xy)$, *Acta Math.* **41** (1916), no. 1, 271–284.

[29] F. Pazuki, Zhang's conjecture and squares of abelian surfaces, *C. R. Math. Acad. Sci. Paris* **348** (2010), 483–486.

[30] J. Pila, A. Shankar y J. Tsimerman, Canonical heights on Shimura varieties and the André-Oort conjecture (con un apéndice de H. Esnault y M. Groechenig), 2021, https://arxiv.org/abs/2109.08788.

[31] M. Raynaud, Sous-variétés d'une variété abélienne et points de torsion, *Arithmetic and Geometry, Vol. 1*, 327–352, *Progr. Math.* **35**, Birkhäuser Boston, Boston, MA, 1983.

[32] P. Sarnak y S. Adams, Betti numbers of congruence groups (con un apéndice de Z. Rudnick), *Israel J. Math.* **88** (1994), no. 1-3, 31–72.

[33] L. Szpiro, E. Ullmo y S. Zhang, Equirépartition des petits points, *Invent. Math.* **127** (1997), 337–347.

[34] E. Ullmo, Positivité et discrétion des points algébriques des courbes, *Ann. of Math. (2)* **147** (1998), no. 1, 167–179.

[35] J. Xie y X. Yuan, Geometric Bogomolov conjecture in arbitrary characteristics, *Invent. Math.* **229** (2022), 607–637.

[36] X. Yuan, Big line bundles over arithmetic varieties, *Invent. Math.* **173** (2008), 603–649.

[37] D. Zagier, Algebraic numbers close to both 0 and 1, *Math. Comp.* **61** (1993), no. 203, 486–491.

[38] U. Zannier, *Lecture notes on Diophantine analysis* (con un apéndice de F. Amoroso), *Appunti. Scuola Normale Superiore di Pisa (N. S.)* **8**, Edizioni della Normale, Pisa, 2009.

[39] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry* (con un apéndice de D. Masser), Annals of Mathematics Studies **181**, Princeton University Press, Princeton, NJ, 2012.

[40] S. Zhang, Positive line bundles on arithmetic varieties, *J. Amer. Math. Soc.* **8** (1995), no. 1, 187–221.

[41] S. Zhang, Equidistribution of small points on abelian varieties, *Ann. of Math. (2)* **147** (1998), no. 1, 159–165.

[42] S. Zhang, Distributions in algebraic dynamics, *Surv. Differ. Geom.* **10** (2006), 381–430.

Roberto Gualdi, Fakultät für Mathematik, Universität Regensburg, Universitätsstrasse 31, 93053 Regensburg, Alemania

Correo electrónico: roberto.gualdi@mathematik.uni-regensburg.de

Página web: https://homepages.uni-regensburg.de/~gur23971/