Capítulo 3

Aproximación diofántica

3.1. Números racionales e irracionales

Teorema de Dirichlet de aproximación diofántica. Pruebas de irracionalidad. Números trascendentes. Distribución uniforme.

El problema básico de área de la teoría de números llamada *aproximación diofántica* consiste en estudiar con qué precisión es posible aproximar un número irracional real por números racionales. En todo el capítulo representaremos estos números racionales con fracciones irreducibles para las cuales usaremos la notación a/q. Por convenio, siempre $q \in \mathbb{Z}^+$.

La descripción anterior del problema básico suena muy ingenua porque $\mathbb{Q}$ es denso en $\mathbb{R}$ y por tanto la "precisión" posible es infinita. En realidad, lo que se busca es un balance entre lo buena que es la aproximación por a/q y el tamaño de a y q que, a fin de cuentas, para cada irracional fijado viene dado por el de q. Por ejemplo, como $\sqrt{2} = 1{,}414213\dots$ tenemos buenas aproximaciones obvias como

$$\sqrt{2} \approx \frac{141421}{100000} \ \text{(error} \approx 2{,}6 \cdot 10^{-6}) \qquad \text{o} \qquad \sqrt{2} \approx \frac{1414213}{1000000} \ \text{(error} \approx 5{,}6 \cdot 10^{-7}).$$

Sin embargo, con la fracción $1393/985$, que tiene denominador mucho menor, se consigue un error más pequeño.

Un argumento elemental debido a Dirichlet, basado en su *principio del palomar*, asegura que existen infinitas fracciones irreducibles a/q para las que el número de cifras decimales correctas es aproximadamente el doble del número de cifras de q. Concretamente, el error absoluto es menor que q^{-2}.

Proposición 3.1.1. *Sea $\alpha \in \mathbb{R}$ y $N \in \mathbb{Z}^+$ entonces existe a/q con $q \le N$ tal que*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qN}.$$

▶ **Corolario 3.1.2.** *Dado $\alpha \in \mathbb{R} - \mathbb{Q}$ existen infinitas a/q tales que*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

Este resultado es consecuencia inmediata del anterior porque $qN \geq q^2$ y la infinitud se consigue tomando N en una sucesión tendiendo a infinito.

Demostración. Consideramos el conjunto $\mathcal{C} = \{\mathrm{Frac}(n\alpha) \ : \ 0 \leq n \leq N\}$ donde $\mathrm{Frac}(x) = x - \lfloor x \rfloor$ es la parte fraccionaria. Este conjunto está contenido en

$$[0, 1) = \Big[\frac{0}{N}, \frac{1}{N}\Big) \cup \Big[\frac{1}{N}, \frac{2}{N}\Big) \cup \cdots \cup \Big[\frac{N-1}{N}, \frac{N}{N}\Big).$$

Hay N subintervalos en la unión anterior y $|\mathcal{C}| = N + 1$. Por el principio del palomar algún subintervalo contiene dos elementos de $\mathcal{C}$ y existen $0 \leq n_1 < n_2 \leq N$ con $\big|\mathrm{Frac}(n_2\alpha) - \mathrm{Frac}(n_1\alpha)\big| < N^{-1}$. Como $\mathrm{Frac}(x)$ difiere de x en un entero, existe $a \in \mathbb{Z}$ tal que

$$\big|(n_2 - n_1)\alpha - a\big| < \frac{1}{N} \quad \text{o, equivalentemente,} \quad \left|\alpha - \frac{a}{n_2 - n_1}\right| < \frac{1}{(n_2 - n_1)N}.$$

Si $a/(n_2 - n_1)$ no fuera irreducible, simplificando se obtendría una desigualdad mejor. □

Hay un recíproco sencillo del Corolario 3.1.2 bajo hipótesis débiles: en cuanto el error tenga un decaimiento mayor que el de $1/q$, el número es irracional. Este es un resultado auxiliar común en muchas pruebas de irracionalidad.

Lema 3.1.3. *Sea $\{a_n/q_n\}_{n=1}^{\infty}$ una sucesión de fracciones irreducibles distintas. Si $\lim |q_n\alpha - p_n| = 0$ para cierto $\alpha \in \mathbb{R}$ entonces $\alpha \notin \mathbb{Q}$.*

Por supuesto, el valor absoluto es innecesario, solo se incluye para recordarnos a los anteriores resultados.

Demostración. Si $\alpha = a/q$ para n grande se tendrá $a_n/q_n \neq a/q$, porque los a_n/q_n son distintos, y $|q_n\alpha - p_n| = |q_n a - p_n q|/q \geq 1/q$, lo que contradice que el límite se anule. □

Con esto es fácil probar la irracionalidad de series de convergen muy rápido y gozan de algunas propiedades aritméticas. Veamos el caso de una de las constantes más famosas.

▶ **Proposición 3.1.4.** *$e \notin \mathbb{Q}$.*

Demostración. Sea $a_n/q_n = \sum_{k=0}^{n} 1/k!$. Obviamente $a_n/q_n < a_{n+1}/q_{n+1}$ por tanto son fracciones distintas. Usando el resto de Taylor para e^x, se tiene $0 < e - a_n/q_n \leq e/(n+1)!$. Por otro lado, reduciendo a común denominador, $q_n \mid n!$, por tanto $|q_n e - p_n| \leq e/(n+1)$ y el resultado es consecuencia del Lema 3.1.3. □

En lo que respecta a la constante indudablemente más famosa de las matemáticas, el número π, la situación es más complicada. No se conoce una serie para π con prueba sencilla a la que aplicar un argumento como el anterior. Por otro lado, la irracionalidad de π es conocida desde el siglo XVIII gracias al trabajo de J.H. Lambert. En el siglo XX surgieron varias pruebas basadas en integrales que eran simplificaciones de la dada por C. Hermite en 1873. Veamos aquí una de ellas. Indudablemente, a pesar de su simplicidad, es difícil atisbar su motivación.

Teorema 3.1.5. $\pi^2 \not\in \mathbb{Q}$.

Por supuesto, de aquí se deduce inmediatamente nuestro objetivo:

▶ **Corolario 3.1.6.** $\pi \not\in \mathbb{Q}$.

Demostración. Dado $n \in \mathbb{Z}^+$, para cada $k \in \mathbb{Z}_{\geq 0}$ consideramos

$$J_k = \int_0^1 f^{(k)}(x) \operatorname{sen}(\pi x)\, dx \qquad \text{con} \qquad f(x) = \frac{1}{n!} x^n (1-x)^n.$$

Es fácil ver que $f^{(k)}(0) \in \mathbb{Z}$, de hecho es cierto para cualquier polinomio de la forma $\frac{1}{n!}\big(a_n x^n + \dots a_{n+m} x^{n+m}\big)$. Por la simetría $f(x) = f(1-x)$, también se tiene $f^{(k)}(1) \in \mathbb{Z}$.

Supongamos $\pi^2 = a/q$ e integremos por partes para obtener

$$\pi a J_k = -a f^{(k)}(x) \cos(\pi x)\Big|_0^1 + a \int_0^1 f^{(k+1)} \cos(\pi x)\, dx.$$

Una segunda integración por partes muestra que la última integral es igual a $-\pi^{-1} J_{k+2} = -\pi q J_{k+1}/a$. Con ello hemos probado

$$\pi(a J_k + q J_{k+2}) \in \mathbb{Z} \qquad \text{para todo } k.$$

De hecho para $k > 2n$ esta cantidad es nula porque $f^{(k)} = f^{(k+2)} = 0$. De esta forma, $\pi a^n J_0$ es igual a la suma telescópica finita de enteros

$$\pi a^{n-1}(aJ_0 + qJ_2) - \pi a^{n-2} q (aJ_2 + qJ_4) + \pi a^{n-3} q^2 (aJ_4 + qJ_6) + \dots$$

Se cumple $\pi a^n J_0 \in \mathbb{Z}^+$ porque $f > 0$ en $(0,1)$. Por otro lado, $\lim a_n/n! = 0$ (para $n > 2a$ cada término es menos de la mitad del anterior), entonces $\lim \pi a^n J_0 = 0$, lo cual es una contradicción. □

Más allá de estas pruebas sofisticadas, hay números para los cuales la irracionalidad se deduce con argumentos muy sencillos.

El caso de $\sqrt{2}$ se suele poner como ejemplo de reducción al absurdo en los primeros cursos. Si $\sqrt{2} = a/q$ entonces $2q^2 = a^2$ y a es par. Escribiendo $a = 2A$ se tiene $q^2 = 2A^2$, luego q es también par contradiciendo la irreducibilidad de a/q. Un argumento similar funciona para obtener $\sqrt{d} \not\in \mathbb{Q}$ siempre que $d \in \mathbb{Z}^+$ no sea un cuadrado perfecto. Los antiguos griegos obtuvieron una bella prueba geométrica [45, §4] de la irracionalidad de $\sqrt{2}$ y parece que conocían la irracionalidad de otras raíces cuadradas de enteros no cuadrados perfectos, pero no de todas [21].

Otro ejemplo es $\alpha = \sum_{n=1}^{\infty} 10^{-n^2}$. Un número racional siempre tiene un desarrollo decimal finito o periódico infinito (puro o mixto). No es el caso de α porque dos unos consecutivos están separados por $(n+1)^2 - n^2 = 2n+1$ ceros y este espacio supera cualquier posible periodo para n grande. Una alternativa a este argumento elemental es usar el Lema 3.1.3.

Volviendo al Corolario 3.1.2, cabe preguntarse si es óptimo. Un conocido teorema de A. Hurwitz [6, T. 7.13] afirma que es posible cambiar $1/q^2$ por C/q^2 con $C = 1/\sqrt{5}$ y con cualquier constante menor se obtienen infinitos ejemplos de irracionales α para los que no existen aproximaciones tan buenas. Eso no significa que no haya mejoras sustanciales para ciertos α. Sin embargo, esta situación es marginal desde el punto de vista de la teoría de la medida. Un resultado [18, §10.3] de V. Jarník y A.S. Besicovitch afirma que los que admiten infinitas aproximaciones racionales con error menor que $1/q^\tau$ para un $\tau > 2$ dado son *fractales* de dimensión $2/\tau < 1$, en particular de medida cero.

Hay una clase destacada de números irracionales para los cuales se conocen limitaciones en la aproximación por racionales.

Se dice que $\alpha \in \mathbb{C}$ es *algebraico* (sobre $\mathbb{Q}$) de grado $d \geq 1$ si existe un polinomio irreducible $P \in \mathbb{Q}[x]$ de grado d tal que $P(\alpha) = 0$. Si $\alpha \in \mathbb{C}$ no es algebraico para ningún grado $d \geq 1$, se dice que es *trascendente*. Quitando denominadores siempre se puede suponer $P \in \mathbb{Z}[x]$, por tanto los números trascendentes son aquellos que no son raíces de ningún polinomio de coeficientes enteros (no idénticamente nulo). Claramente los algebraicos de grado 1 son los racionales.

Teorema 3.1.7. *Para cada $\alpha \in \mathbb{R}$ algebraico de grado $d > 1$ existe $C > 0$ tal que*

$$\left|\alpha - \frac{a}{q}\right| > \frac{C}{q^d} \qquad \textit{para todo } \frac{a}{q}.$$

Demostración. Suponemos $a/q \in I = [\alpha - 1, \alpha + 1]$ ya que fuera de I se cumple con $C = 1$. Sea $P \in \mathbb{Z}[x]$ irreducible de grado d con $P(\alpha) = 0$ y $M = \sup_{x \in I} |P'(x)|$. Por el teorema del valor medio

$$\left|\frac{P(\alpha) - P(a/q)}{\alpha - a/q}\right| \leq M \qquad \text{para} \quad \frac{a}{q} \in I.$$

Se cumple $q^d P(a/q) \in \mathbb{Z} - \{0\}$, porque los denominadores se cancelan, y se sigue el resultado para $a/q \in I$ con cualquier $C \leq M^{-1}$. □

Corolario 3.1.8. *Sea* $\{a_n/q_n\}_{n=1}^{\infty}$ *una sucesión de fracciones irreducibles distintas que converge a* $\alpha \in \mathbb{R}$. *Si* $\lim q_n^d |q_n\alpha - p_n| = 0$ *para todo* $d \in \mathbb{Z}_{\geq 2}$ *entonces* α *es trascendente.*

Los números trascendentes que verifican la hipótesis de este resultado se dice que son *números de Liouville* pues J. Liouville lo empleó para dar los primeros ejemplos de números trascendentes.

Tomando $\alpha = \sum_{k=1}^{\infty} 10^{-k!}$ y a_n/q_n su n-ésima suma parcial, se cumple

$$\alpha - \frac{a_n}{q_n} = \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \cdots < \frac{1}{10^{(n+1)!}}\Big(1 + \frac{1}{2} + \frac{1}{4} + \dots\Big) = \frac{2}{10^{(n+1)!}},$$

porque $10^{-(n+k+1)!}$ es menos de la mitad de $10^{-(n+k)!}$. Entonces

$$q_n^d\Big|\alpha - \frac{a_n}{q_n}\Big| < 2\frac{10^{dn!}}{10^{(n+1)!}} = \frac{2}{10^{(n+1-d)n!}}$$

que tiende a cero si $n \to \infty$ y el Corolario 3.1.8 asegura que α es trascendente, esto es, no satisface ninguna ecuación polinómica.

Por otro lado, en el sentido de la medida casi ningún número trascendente real es número de Liouville, por tanto el Corolario 3.1.8 es de poca utilidad para α que no esté fabricado a propósito. Dos resultados de trascendencia relacionados con la exponencial, obtenidos a finales del siglo XIX respectivamente por Hermite y C.L.F. Lindemann, son:

► **Teorema 3.1.9** (Hermite). *e es trascendente.*

Teorema 3.1.10 (Lindemann). *Si* $\alpha \in \mathbb{C} - \{0\}$ *es algebraico entonces* e^{α} *es trascendente.*

Hay pruebas fáciles de seguir, sobre todo del primer resultado, renunciando a la motivación. No las veremos aquí. Dos referencias por expertos en el área son las monografías [1] y [52]. Una consecuencia rápida y sorprendente del resultado de Lindemann es más llamativa que su formulación general:

► **Corolario 3.1.11.** π *es trascendente.*

Demostración. Si π fuera algebraico, entonces $i\pi$ también lo sería. Esto es consecuencia de que los números algebraicos forman un cuerpo [56] o, de manera más elemental, de que si $P(\pi) = 0$ con $P \in \mathbb{Z}[x]$ entonces $Q(x) = P(ix)P(-ix)$ tiene coeficientes enteros y se anula en $i\pi$. En esta situación, $e^{i\pi} = -1$ contradice el teorema de Lindemann porque -1 es algebraico. □

En el siglo XX algunos autores mejoraron el Teorema 3.1.7 culminando con un espectacular resultado de K. Roth que, esencialmente, afirma que no hay mejoras sustanciales del Corolario 3.1.2 para ningún número algebraico.

▶ **Teorema 3.1.12** (Roth). *Sea $\alpha \in \mathbb{R}$ algebraico. Para cada $\sigma > 2$ solo existe un número finito de fracciones a/q tales que*

$$\Big|\alpha - \frac{a}{q}\Big| < \frac{1}{q^\sigma}.$$

La prueba es larga y difícil y se escapa de los objetivos de este curso. Se basa en la construcción de ciertos polinomios con propiedades especiales. El lector interesado la puede encontrar por ejemplo en [55]. Sería muy deseable disponer de una demostración más trasparente. Hasta la fecha no se sabe hacer el teorema efectivo, en el sentido de que no se conoce ninguna cota para a y q en función de α y σ.

Una muestra del poder del Teorema 3.1.12 es un resultado de A. Thue, anterior a este teorema, sobre ecuaciones diofánticas. La falta de efectividad impide que sepamos acotar el número de soluciones.

▶ **Corolario 3.1.13** (Thue). *Si $P \in \mathbb{Z}[x, y]$ es un polinomio irreducilbe homogéneo de grado $d \geq 3$ y $m \in \mathbb{Z} - \{0\}$ entonces la ecuación $P(x, y) = m$ solo tiene un número finito de soluciones $(x, y) \in \mathbb{Z}^2$.*

Recordemos que un polinomio homogéneo es aquel en el que todos sus monomios tienen el mismo grado total. La condición $d \geq 3$ es necesaria, pues sabemos (Proposición 1.1.8) que $ax + by = c$ tiene infinitas soluciones enteras bajo hipótesis naturales. Por otro lado, veremos que ecuaciones como $x^2 - 2y^2 = 1$ también tienen infinitas soluciones enteras. La irreducibilidad del enunciado se puede rebajar mucho y se exige para evitar tonterías como $(x + y)^d = 1$.

Demostración. Si hubiera infinitas soluciones en $\mathbb{Z}^2$ existiría un subconjunto $\{(x_n, y_n)\}_{n=1}^\infty \subset \mathbb{Z}^2$ con $|x_n| \to \infty$ o $|y_n| \to \infty$. De hecho, con un argumento elemental deben darse ambas. De todas formas, por simetría podemos suponer lo segundo. El polinomio $P(t, 1) \in \mathbb{Z}[t]$ tendrá raíces $\alpha_1, \alpha_2, \ldots, \alpha_d$ que son números algebraicos de grado d distintos por la irreducibilidad, ya que $Q(t) \mid P(t, 1)$ implica $y^n Q(x/y) \mid P(x, y)$. Si a_0 es su coeficiente principal,

$$|a_0|\Big|\frac{x_n}{y_n} - \alpha\Big| \cdots \Big|\frac{x_n}{y_n} - \alpha_d\Big| = |y_n|^{-d}|P(x_n, y_n)| = \frac{|m|}{|y_n|^d}.$$

Como los α_j son finitos y $|y_n| \to \infty$, existe $1 \leq j_0 \leq d$ y una subsucesión x_{n_k}/y_{n_k} tal que para cada n_k el error $|x_{n_k}/y_{n_k} - \alpha_j|$ se minimiza para $j = j_0$. Si 2δ es la mínima separación entre los α_j, el error anterior es al menos δ para $j \neq j_0$ y por tanto

$$\Big|\frac{x_{n_k}}{y_{n_k}} - \alpha_{j_0}\Big| < \frac{C}{|y_{n_k}|^d} \qquad \text{para} \quad C = |a_0|^{-1}\delta^{1-d}$$

y esto es compatible con el Teorema 3.1.12 solo para $d \leq 2$ y $\alpha_{j_0} \in \mathbb{R}$, ya que $|y_{n_k}| \to \infty$. □

Por ejemplo, la ecuación $2023x^3+x^2y-2y^3=2022$ solo tiene un número finito de soluciones $(x,y)\in\mathbb{Z}^2$, entre las que se cuenta $(x,y)=(1,1)$.

Terminamos esta sección con un estudio estadístico de la parte fraccionaria de los múltiplos enteros de un número irracional. El problema ya viene motivado por la prueba de la Proposición 3.1.1.

Se dice que una sucesión $\{a_n\}_{n=1}^{\infty}$ con $a_n\in[0,1]$ está *uniformemente distribuida* en $[0,1]$ si para cualquier intervalo $I\subset[0,1]$ se cumple

$$\lim_{N\to\infty}\frac{1}{N}\big|\{n\le N\,:\,a_n\in I\}\big|=|I|.$$

Por supuesto, las primeras barras verticales indican cardinal (medida de contar) y las segundas longitud (medida usual).

Las sucesiones uniformemente distribuidas permiten aproximar integrales, este método, llamado *integración de Montecarlo*, es muy poco eficiente en comparación con los que estudia el cálculo numérico si f tiene alguna regularidad.

Proposición 3.1.14. *Una sucesión $\{a_n\}_{n=1}^{\infty}\subset[0,1]$ está uniformemente distribuida en $[0,1]$ si y solo si para toda función continua $f:[0,1]\longrightarrow\mathbb{R}$ se cumple*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}f(a_n)=\int_0^1 f.$$

Demostración. Usando la continuidad uniforme, para cada $\epsilon>0$ existe una función escalonada $S(x)=\lambda_1\chi_{I_1}+\cdots+\lambda_k\chi_{I_k}$, con χ_{I_j} la función característica del intervalo I_j, tal que $|f(x)-S(x)|<\epsilon$, lo que implica

$$\Big|\frac{1}{N}\sum_{n=1}^{N}S(a_n)-\frac{1}{N}\sum_{n=1}^{N}f(a_n)\Big|<\epsilon\qquad\text{y}\qquad\Big|\int_0^1 S-\int_0^1 f\Big|<\epsilon.$$

Si $\{a_n\}_{n=1}^{\infty}$ está uniformemente distribuida, empleando la definición,

$$\frac{1}{N}\sum_{n=1}^{N}S(a_n)=\sum_{j=1}^{k}\lambda_j|I_j|=\int_0^1 S.$$

Combinando esta igualdad con las desigualdades anteriores y tomando ϵ arbitrariamente pequeño, se deduce la implicación directa.

Para el recíproco, dado un intervalo $I\subset[0,1]$, escojamos funciones continuas $f_-\le\chi_I\le f_+$ tales que $\int_0^1(f_+-f_-)<\epsilon$. Esto se consigue, por ejemplo, con funciones lineales a trozos. Se tiene

$$\frac{1}{N}\sum_{n=1}^{N}f_-(a_n)\le\frac{1}{N}\big|\{n\le N\,:\,a_n\in I\}\big|\le\frac{1}{N}\sum_{n=1}^{N}f_+(a_n)$$

y además

$$-\epsilon + \int_0^1 f_+ < \int_0^1 \chi_I = |I| < \epsilon + \int_0^1 f_-.$$

Restando estas cadenas de desigualdades se concluye

$$\Big|\frac{1}{N}\big|\{n \le N \,:\, a_n \in I\}\big| - |I|\Big| < \epsilon + c_N \qquad \text{con} \quad c_N \to 0,$$

lo que prueba el resultado porque ϵ es arbitrariamente pequeño. $\square$

Nuestro objetivo es obtener la siguiente familia de sucesiones uniformemente distribuidas relacionada con la parte fraccionaria $\mathrm{Frac}(x) = x - \lfloor x \rfloor$.

▶ **Teorema 3.1.15.** *Si $\alpha \in \mathbb{R} - \mathbb{Q}$ la sucesión $\big\{\mathrm{Frac}(n\alpha)\big\}_{n=1}^{\infty}$ está uniformemente distribuida.*

Para ilustrar lo dicho anteriormente acerca de la poca eficiencia de la integración de Montecarlo aproximemos $\int_0^1 (1+x^2)^{-1}dx = \pi/4$ a través de la Proposición 3.1.14 usando

$$I_N = \frac{1}{N}\sum_{n=1}^{N} \frac{1}{1 + \big(\mathrm{Frac}(n\sqrt{2})\big)^2}$$

que corresponde a la sucesión $\big\{\mathrm{Frac}(n\sqrt{2})\big\}_{n=1}^{\infty}$. La siguiente tabla recoge el error absoluto e_a redondeado a tres cifras significativas para algunos valores de N

	$N = 100$	$N = 500$	$N = 1000$	$N = 2000$
e_a	$-1{,}36 \cdot 10^{-3}$	$2{,}01 \cdot 10^{-4}$	$-8{,}53 \cdot 10^{-5}$	$-1{,}79 \cdot 10^{-4}$

El comportamiento es un poco errático pues para $N = 1000$ obtenemos un error menor que para $N = 2000$. Por comparación, lo que conseguimos con 1000 evaluaciones de la función se ve superado por la regla de Simpson con solo 5 evaluaciones.

El Teorema 3.1.15 se deduce de los rudimentos de las series de Fourier por un resultado de H. Weyl, un matemático polifacético que fue pionero en el estudio de la distribución uniforme de sucesiones.

Proposición 3.1.16 (Criterio de Weyl). *Una sucesión $\{a_n\}_{n=1}^{\infty} \subset [0,1]$ está uniformemente distribuida en $[0,1]$ si y solo si*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i k a_n} = 0 \qquad \textit{para cualquier} \quad k \in \mathbb{Z} - \{0\}.$$

Demostración. La implicación directa se sigue de la Proposición 3.1.14 tomando partes reales e imaginarias puesto que las integrales $\int_0^1 \cos(2\pi kx)\,dx$ y $\int_0^1 \operatorname{sen}(2\pi kx)\,dx$ son nulas si $k \neq 0$.

Para el recíproco empleamos el teorema de Fejér [14, §1.4] que implica que cualquier función $f : [0,1] \longrightarrow \mathbb{R}$ continua se aproxima uniformemente por funciones reales que son series de Fourier finitas. Es decir, para cada $\epsilon > 0$ existe $F(x) = \sum_{k=-K}^{K} c_k e^{2\pi ikx}$ tal que $|f - F| < \epsilon$. Por la hipótesis,

$$\frac{1}{N}\sum_{n=1}^{N} F(a_n) \xrightarrow[N\to\infty]{} c_0 = \int_0^1 F.$$

De $|f - F| < \epsilon$, y por tanto $\left|\int_0^1 f - \int_0^1 F\right| < \epsilon$, se deduce que lo mismo es válido al reemplazar F por f, porque ϵ es tan pequeño como queramos. $\square$

Demostración del Teorema 3.1.15. Por la 1-periodicidad de $e^{2\pi ix}$ y la fórmula para la suma de una progresión geométrica,

$$\sum_{n=1}^{N} e^{2\pi ik\mathrm{Frac}(n\alpha)} = \sum_{n=1}^{N} e^{2\pi ikn\alpha} = \frac{e^{2\pi ik(N+1)\alpha} - e^{2\pi ik\alpha}}{e^{2\pi ik\alpha} - 1}.$$

Fijado $k \in \mathbb{Z} - \{0\}$ el denominador es constante y no nulo (porque $\alpha \notin \mathbb{Q}$) y el módulo del numerador es a lo más 2. Entonces, al dividir entre N el resultado tiene a cero y el enunciado se deduce de la Proposición 3.1.16. $\square$