Torres infinitas sorprendentes

José Ibrahim Villanueva Gutiérrez

Quinta Reunión de Matemáticos Mexicanos en el Mundo

8 de diciembre 2021

Series de Dirichlet

Una *serie de Dirichlet* es una expresión de la forma

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad a_n \in \mathbb{C}.$$

- Si existe $\sigma \in [-\infty, \infty)$ tal que la serie converge para $s \in \mathbb{C}$ con $\mathrm{Re}(s) > \sigma$, entonces la serie define una función analítica $f(s)$.
- Si $a_{mn} = a_m a_n$ entonces la serie tiene una expresión de la forma

$$\prod_{\ell \text{ primo}} (1 - a_\ell \ell^{-s})^{-1}.$$

- Cuando es posible continuar la serie analíticamente a una función meromorfa en todo $\mathbb{C}$ obtenemos una *función L*.

Ejemplo

La *función ζ de Riemann*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \prod_{\ell \text{ primo}} (1 - \ell^{-s})^{-1}$$

converge para $Re(s) > 1$.

- La función $\zeta(s)$ tiene continuación meromorfa a todo $\mathbb{C}$ con un polo simple en $s = 1$.
- $\zeta(1-n) = -\frac{B_n}{n} \in \mathbb{Q}$ para $n \geq 1$.
- *Números de Bernoulli*: $B_0 = 1,\ B_1 = \frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730},\ B_{14} = \frac{7}{6},\ B_{16} = -\frac{3617}{510},\ \ldots$.

Caracteres de Dirichlet

Sea $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times$ un carácter de Dirichlet. Podemos extenderlo a una función de $\mathbb{N}$ definiendo $\chi(n) = 0$ si $(N, n) \neq 1$. La *serie de Dirichlet asociada a χ* se define como

$$L(\chi, 1-s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{\ell \text{ primo}} (1 - \chi(\ell)\ell^{-s})^{-1}.$$

- En este caso $\sigma = 0$ a menos que $\chi = 1$.
- Para caracteres no triviales la serie asociada admite continuación holomorfa a todo $\mathbb{C}$.
- $L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \in \overline{\mathbb{Q}}$ para $n \geq 1$.

Números p-ádicos

Todo $x \in \mathbb{Q}$ no nulo lo podemos expresar como $p^k \frac{a}{b}$ donde $p \nmid a, b$. Consideremos la *valuación p-ádica*

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\} \quad x \mapsto v_p(x) := k.$$

- $v_p(x) = \infty$ si y solamente si $x = 0$,
- $v_p(xy) = v_p(x) + v_p(y)$,
- $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

La valuación p-ádica induce una métrica

$$|x|_p = \left(\frac{1}{p}\right)^{v_p(x)},$$

definimos el campo de los números p-ádicos $\mathbb{Q}_p$ como el completado de $\mathbb{Q}$ con respecto a $|\cdot|_p$.

- El anillo de enteros $\mathbb{Z}_p = \{x \text{ tal que } |x|_p \leq 1\}$,
- de ideal maximal de $p\mathbb{Z}_p = \{x \text{ tal que } |x|_p < 1\}$,
- y campo residual $k = \mathbb{Z}_p / p\mathbb{Z}_p \simeq \mathbb{F}_p$.

Congruencias de Kummer

A partir de ahora supongamos que $p \neq 2$.

Teorema

Sean $k, m, n \geq 1$ y $c \in \mathbb{Z}$ no divisible por p.
Si $m \equiv n \mod \varphi(p^{k+1})$ entonces

$$(1 - c^m)(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - c^n)(1 - p^{n-1})\frac{B_n}{n} \mod p^{k+1}.$$

Es decir, para todo $\varepsilon > 0$, existe $\delta > 0$ tal que para todo $m \equiv n \mod p - 1$,

$$|m - n|_p < \delta$$

$$\Rightarrow \left|(1 - c^m)(1 - p^{m-1})\frac{B_m}{m} - (1 - c^n)(1 - p^{n-1})\frac{B_n}{n}\right|_p < \varepsilon$$

La construcción de Leopoldt-Kubota

- La función

$$f : (p-1)\mathbb{N} \to \mathbb{Q}_p, \quad n \mapsto (1-c^n)(1-p^{n-1})\frac{B_n}{n};$$

  es *uniformemente continua* con la métrica p-ádica.
- El conjunto $(p-1)\mathbb{N}$ es denso en $\mathbb{Z}_p$, i.e. podemos extender f a una única función continua $f : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Q}_p$.
- Si definimos

$$\begin{array}{rcl} \zeta_{p,0} : \mathbb{Z}_p \setminus \{1\} & \longrightarrow & \mathbb{Q}_p \\ 1-s & \longmapsto & -\dfrac{f(s)}{1-c^s} \end{array}$$

- $\zeta_{p,0}(1-n) = (1-p^{n-1})\zeta(1-n)$ para todo $n \in (p-1)\mathbb{N}$.

De manera similar podemos construir funciones $\zeta_{p,a} : \mathbb{Z}_p \to \mathbb{Q}_p$ para $a = 1, \ldots, p-2$; tales que

$$\zeta_{p,a}(1-n) = (1-p^{n-1})\zeta(1-n),$$

para todo $n \equiv a \mod (p-1)$. En general

$$\zeta_{p,a}(1-n) = -(1-\omega^{-(n+a)}(p)p^{n-1})\frac{B_{n,\omega^{-(n+a)}}}{n},$$

para todo $n \in \mathbb{N}$. Donde el *carácter de Teichmüller* ω es una sección de la proyección

$$\pi : \mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p) \to \mathbb{F}_p^\times$$

La tesis de Tate: Cambio de dominio

- Sea $\mathbb{Q}(\mu_{p^\infty}) = \bigcup \mathbb{Q}(\mu_{p^r})$ y $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. Entonces G es isomorfo a $\mathbb{Z}_p^\times$ vía el *carácter ciclotómico*

$$\kappa : G \to \mathbb{Z}_p^\times, \quad g(\xi_{p^r}) = \xi_{p^r}^{\kappa(g)} \text{ para } g \in G.$$

- Todo $\chi : G \to \mathbb{Z}_p^\times$ es de la forma

$$\chi = \omega^a \kappa_0^s,$$

con $\kappa_0 = \omega^{-1}\kappa$, $a \in \{1, \ldots, p-1\}$ y $s \in \mathbb{Z}_p$.

Teorema

Existe una única función continua

$$\begin{aligned} \zeta_p : \mathrm{Hom}(G, \mathbb{Z}_p^\times) \setminus \{\kappa\} &\longrightarrow \mathbb{Q}_p, \\ \chi = \omega^a \kappa_0^s &\longmapsto \zeta_{p,a-1}(s); \end{aligned}$$

que satisface

$$\zeta_p(\psi^{-1}\kappa^{1-n}) = (1 - \psi(p)p^{n-1})L(\psi, 1-n)$$

para todo $n \geq 1$ y para todo carácter de Dirichlet ψ de $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

La construcción de Iwasawa

Recordemos que $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$ donde $\Delta \simeq \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ y $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))$.
Sea $\Lambda(G)$ el *álgebra de Iwasawa* de G

$$\Lambda(G) = \mathbb{Z}_p[\![G]\!] = \varprojlim_{H \trianglelefteq G} \mathbb{Z}_p[G/H].$$

- Un carácter $\psi : G \longrightarrow \overline{\mathbb{Q}}_p^\times$ induce un morfismo

$$\psi : \Lambda(G) \longrightarrow \overline{\mathbb{Q}}_p.$$

- Para $\mu \in \Lambda(G)$ definimos $\mu(\psi) = \psi(\mu)$, entonces

$$\mu : \mathrm{Hom}(G, \overline{\mathbb{Q}}_p^\times) \longrightarrow \overline{\mathbb{Q}}_p.$$

Elementos de Stickelberg

Sea $G_{p^r} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^r})/\mathbb{Q})$. Definimos los *elementos de Stickelberg de nivel p^r* como

$$\Sigma_{p^r} = -\frac{1}{p^r} \sum_{\substack{a \mod p^r \\ (a,p)=1}} a\sigma_a^{-1} \in \mathbb{Q}[G_{p^r}].$$

Definimos

$$\Sigma_{p^\infty} = (\Sigma_{p^r})_{r\geq 1} \in \mathbb{Q}[\![G_{p^\infty}]\!] := \varprojlim_k \mathbb{Q}[G_{p^k}].$$

Sea $\mu_1 = \Sigma_{p^\infty} \in \mathbb{Q}_p[\![G]\!]$. Entonces

$$\mu_1 \in \Lambda(G)[\frac{1}{h}].$$

La función L p-ádica

Teorema

Sea $\psi : G \longrightarrow \overline{\mathbb{Q}}_p^\times$ un carácter de orden finito y $n \geq 1$. Entonces

$$\mu_1(\psi^{-1}\kappa^{1-n}) = (1 - \psi(p)p^{n-1})L(\psi, 1-n).$$

- El elemento μ_1 está unicamente determinado por la fórmula de interpolación.
- μ_1 define una función en $Hom(G, \overline{\mathbb{Q}}_p^\times) \setminus \{\kappa\}$

$\mathbb{Z}_p$-extensiones

Recordemos $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ y

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p.$$

Sea $\mathbb{Q}^c$ el único subcampo de $\mathbb{Q}(\mu_{p^\infty})$ fijado por $(\mathbb{Z}/(p-1)\mathbb{Z})$ entonces $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q}) \simeq \mathbb{Z}_p$. Definimos $\mathbb{Q}_r^c$ como el único subcampo de $\mathbb{Q}^c$ que es cíclico de grado p^r sobre $\mathbb{Q}$.
Sea K un *campo de números*.

- Todo campo de números admite al menos una $\mathbb{Z}_p$-extensión: $K^c = K\mathbb{Q}^c$ la *$\mathbb{Z}_p$-extensión ciclotómica*.
- Para una $\mathbb{Z}_p$-extensión K_∞ denotamos K_r el único subcampo de K_∞ con $\mathrm{Gal}(K_r/K) \simeq \mathbb{Z}/p^r\mathbb{Z}$.

Teorema

Sea K_∞/K una $\mathbb{Z}_p$-extensión de un campo de números K. Sea p^{e_r} el orden de la p-parte del grupo de clases de K_r. Existen constantes $\mu, \lambda \geq 0$ y $\nu \in \mathbb{Z}$ tal que

$$e_r = \mu p^r + \lambda r + \nu$$

para r suficientemente grande.

- $\Gamma = \mathrm{Gal}(K_\infty/K)$
- $\Lambda = \Lambda(\Gamma) = \mathbb{Z}_p[\![\Gamma]\!] \simeq \mathbb{Z}_p[\![T]\!]$
- La demostración del teorema de Iwasawa se basa en el *teorema de estructura de Λ-módulos*.
- Todo Λ-módulo finitamente generado M es pseudo-isomorfo a un módulo
$$\Lambda^r \oplus \bigoplus \Lambda/p^{\mu_i}\Lambda \oplus \bigoplus \Lambda/P_j\Lambda.$$
- Sea $P = \prod P_j$. Entonces $\mu = \sum \mu_i$ y $\lambda = \deg P$. Definimos el *ideal característico* $\mathrm{char}_\Lambda(M) = (p^\mu P)$.
- El límite $X_\infty = \varprojlim X_r(p)$ de las p-partes del grupo de clases X_r de K_r es un Λ-módulo de torsión.

La conjetura principal de Iwasawa

Para un $\Lambda(G)$-módulo M definimos M^- el subespacio donde la conjugación compleja actúa por -1.

Theorem (Mazur & Wiles)

Tenemos la siguiente igualdad de ideales en $\Lambda(G)^-$

$$char_{\Lambda(G)^-}(X_\infty^-) = (h\mu_1).$$

El criterio de Kummer

Teorema

$$p \mid h_{\mathbb{Q}(\mu_p)} \;\Leftrightarrow\; p \text{ divide uno de } \zeta(-1), \zeta(-3), \ldots, \zeta(4-p).$$

Demostración:

$$\begin{aligned} p \mid h_{\mathbb{Q}(\mu_p)} &\Leftrightarrow X_\infty \neq 0 \\ &\Leftrightarrow X_\infty^- \neq 0 \\ &\Leftrightarrow e_i X_\infty \neq 0 \text{ para algún impar } i \end{aligned}$$

- Como X_∞^- no tiene submódulos finitos no triviales, para $\psi = \omega^i \kappa_0^s : G \to \mathbb{Z}_p^\times$ tenemos

$$h\mu_1(\psi) \in \mathbb{Z}_p^\times \;\Leftrightarrow\; e_i X_\infty^- = 0.$$

- Sabemos que $h\mu_1(\kappa) \in \mathbb{Z}_p^\times$ entonces

$$X_\infty^- = \bigoplus_{i=3 \text{ impar}}^{p-2} e_i X_\infty^- = \bigoplus_{n=2 \text{ par}}^{p-3} e_{1-n} X_\infty^-.$$

- Sea $\psi = \kappa^{1-n}$ con $n \in \{2, 4, \ldots, p-3\}$. Como $n \not\equiv 0 \mod (p-1)$ tenemos

$$h\mu_1(\kappa^{1-n}) = (1 - p^{n-1})\zeta(1-n).$$

- Por lo tanto $e_{1-n} X_\infty^- = 0$ si y sólo si $\zeta(1-n) \in \mathbb{Z}_p^\times$.

Consecuencia: El teorema de Ferrero-Washington

Iwasawa conjeturó que $\mu(K^c/K) = 0$ para todo campo de números K.

Teorema

Sea $K/\mathbb{Q}$ una extensión abeliana. Entonces

$$\mu(K^c/K) = 0.$$