Números de Bernoulli: Algunas aplicaciones a la Teoría de Números

David J. Fernández Bretón.
Escuela Superior de Física y Matemáticas,
Instituto Politécnico Nacional,
México.

Definición

Se define la sucesión de **números de Bernoulli** $B_0, B_1, B_2, \ldots$, como

$$B_0 = 1,$$

y

$$B_m = -\frac{1}{m+1} \sum_{k=0}^{m-1} \binom{m+1}{k} B_k$$

para cualquier $m \in \mathbb{N}$.
Asimismo se define, para cada $m \in \mathbb{N} \cup \{0\}$, el m-ésimo **polinomio de Bernoulli** de la siguiente manera

$$B_m(X) = \sum_{k=0}^{m} \binom{m}{k} B_k X^{m-k}.$$

Números de Bernoulli

Se define $S_m(n) = 1^m + 2^m + \cdots + (n-1)^m$.

- $\dfrac{t}{e^t - 1} = \displaystyle\sum_{m=0}^{\infty} \frac{B_m}{m!} t^m.$
- $S_m(n) = \dfrac{1}{m+1} \displaystyle\sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$
- De la primera ecuación, tenemos que:

$$1 + \sum_{k=2}^{\infty} \frac{B_k}{k!} t^k = \frac{t}{2} + \frac{t}{e^t - 1}.$$

Esta última es una función par, de donde se sigue que, para cualquier $k \in \mathbb{N}$,

$$B_{2k+1} = 0.$$

Polinomios de Bernoulli

- $\sum_{k=n}^{m-1} k^q = S_q(m) - S_q(n) = \frac{1}{q+1}\left(B_{q+1}(m) - B_{q+1}(n)\right).$
- $\frac{1}{m+1} B'_{m+1}(X) = B_m(X), \;\; m \in \mathbb{N} \cup \{0\}.$
- $B_m(0) = B_m(1) = B_m, \;\; m \in \mathbb{N} \cup \{0\}, \;\; m \neq 1.$
- $B_q(kX) = k^{q-1} \sum_{j=0}^{k-1} B_q\left(X + \frac{j}{k}\right), \;\; q \in \mathbb{N} \cup \{0\}.$
- $\sum_{n=a+1}^{b} f(n) = \int_a^b f(x)dx + \sum_{r=1}^{q} (-1)^r \frac{B_r}{r!}\{f^{(r-1)}(b) - f^{(r-1)}(a)\} + R_q,$
  en donde

$$R_q = \frac{(-1)^{q-1}}{q!} \int_a^b B_q(x - [x]) f^{(q)}(x)dx.$$

Los números $\zeta(2m)$ y $\zeta(1-m)$

Se define la **función zeta de Riemann** como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ es primo}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \;\; m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \;\; m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \to \infty$ cuando $m \to \infty$.
- La función zeta se extiende a una función meromorfa con un polo simple, de residuo 1, en $s = 1$. Además, se cumple la ecuación funcional

$$\zeta(s) = 2^s \pi^{s-1} \operatorname{sen}\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s).$$

- $\zeta(1-m) = -\dfrac{B_m}{m}, \;\; m \in \mathbb{N}\backslash\{1\}.$

p-enteros

$$\mathbb{Z}_{\langle p \rangle} = \left\{ r \in \mathbb{Q} \middle| \operatorname{ord}_p(r) \geq 0 \right\} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z},\ p \nmid b \right\}.$$

Si $r, s \in \mathbb{Z}_{\langle p \rangle}$, $n \in \mathbb{N} \cup \{0\}$, decimos que

$$r \equiv s \mod p^n \iff \operatorname{ord}_p(r-s) \geq n.$$

- $pB_m \in \mathbb{Z}_{\langle p \rangle}$.
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0;\ (p-1) \nmid m \\ -1;\ (p-1) \mid m \end{cases} \mod p.$
- $B_{2m} = A_{2m} + \sum_{(p-1)|2m} \frac{1}{p}$ para algunos $A_{2m} \in \mathbb{Z}$. Así, el denominador de B_{2m} es un número libre de cuadrado cuyos divisores primos son exactamente los números primos p tales que $(p-1) \mid 2m$. En particular, 6 siempre divide al denominador de B_{2m}.

Congruencias en $\mathbb{Z}_{\langle p \rangle}$

Sea $m \in \mathbb{N} \cup \{0\}$ par. Escribimos $B_m = \dfrac{U_m}{V_m},\ U_m, V_m \in \mathbb{Z}, (U_m, V_m) = 1.$

- $V_m S_m(n) \equiv U_m\, n \mod n^2.$
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2.$
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \mod n.$
- p número primo tal que $(p-1) \nmid m \Rightarrow \dfrac{B_m}{m} \in \mathbb{Z}_{\langle p \rangle}.$
- Sean $n, e \in \mathbb{N}$ con $n \equiv m \mod \phi(p^e)$. Entonces,

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

Números primos regulares e irregulares

Un número primo $p \geq 3$ se dice que es **regular** si, para $j = 2, 4, \ldots, p-3$, se tiene que $\mathrm{ord}_p(B_j) \leq 0$, o en otras palabras, $p \nmid U_j$. Cuando un número primo no es regular, se dice que es **irregular**. El 3 es regular por definición.

- Existe una infinidad de números primos irregulares.
- No se sabe nada aún acerca de la finitud o infinitud del conjunto de números primos regulares.
- Sin embargo, si se supone que los números U_j se encuentran aleatoriamente distribuidos módulo cualquier número primo (lo cual es plausible), se concluye que $\lim_{p\to\infty} \dfrac{\#\{q \,|\, q \leq p,\ q \text{ es irregular}\}}{\#\{q \,|\, q \leq p\}} = \dfrac{1}{\sqrt{e}}$. En otras palabras, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0{,}61$.

Último teorema de Fermat: Definiciones preliminares

Si $n \in \mathbb{N}$, por ζ_n entenderemos una raíz n-ésima primitiva de la unidad. Se define el n-**ésimo campo ciclotómico** como el mínimo subcampo de $\mathbb{C}$ que contiene a ζ_n, es decir, $\mathbb{Q}(\zeta_n)$. Se define el n-**ésimo anillo ciclotómico** como el mínimo subanillo de $\mathbb{C}$ que contiene a ζ_n, es decir, $\mathbb{Z}[\zeta_n]$.
Si $K/\mathbb{Q}$ es una extensión algebraica de campos, se define el **anillo de enteros** de K, denotada por $\mathcal{O}_K$, como sigue:

$$\mathcal{O}_K = \{\alpha \in K \big| \text{irr}(\alpha, \mathbb{Q}, X) \in \mathbb{Z}[X]\}.$$

Si D es un dominio entero, decimos que D es **dominio Dedekind** si D es noetheriano, enteramente cerrado, y cada ideal primo de D es un ideal maximal.
Un subconjunto $I \subseteq D$ es un **ideal fraccional** de D si I es un D-submódulo de $\text{coc}(D)$, y existe un elemento $r \in D$ tal que $rI \subseteq D$.
Dado un dominio Dedekind D, y dos ideales fraccionales I, J de D, definimos el **producto** de I y J como sigue:

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \Big| a_i \in I, b_i \in J, n \in \mathbb{N} \right\}$$

Último teorema de Fermat: Los teoremas

- Si D es un dominio Dedekind, entonces todos sus ideales fraccionales se factorizan de manera única como producto de ideales primos, y el conjunto de ideales fraccionales de D forma un grupo cuya identidad es D.
- Si $K/\mathbb{Q}$ es una extensión de Galois, entonces el anillo de enteros de K es un dominio Dedekind.
- Si p es un número primo, entonces $\mathbb{Z}[\zeta_p]$ es el anillo de enteros de $\mathbb{Q}(\zeta_p)$.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Pese a que los únicos números primos p tales que $\mathbb{Z}[\zeta_p]$ es un dominio de ideales principales (y por lo tanto un dominio de factorización única) son los $p \leq 19$, sin embargo para cualquier p se cumple la factorización única de los ideales de $\mathbb{Z}[\zeta_p]$.

Último teorema de Fermat: El número de clases

Dado un dominio Dedekind, definimos su **grupo de clases** como el grupo cociente entre el grupo de ideales fraccionales de D y su subgrupo que consta de los ideales fraccionales principales.
El **número de clases** de un dominio Dedekind D, denotado por $h(D)$, es el orden de su grupo de clases.
Si $K/\mathbb{Q}$ es una extensión de Galois, entonces el número de clases $h(K)$ del campo K es el número de clases de su anillo de enteros.

- Si $K/\mathbb{Q}$ es una extensión finita y separable, entonces $h(K) < \infty$.
- Sea p un número primo. Entonces, p es regular si y sólo si $p \nmid h(\mathbb{Q}(\zeta_p))$.

Último teorema de Fermat: Un caso particular

Supóngase que se tienen $x, y, z \in \mathbb{Z}$ tales que $x^p + y^p = z^p$, $p \nmid xyz$, en donde p es un número primo regular.

- $\langle x+y\rangle\langle x+\zeta_p y\rangle\langle x+\zeta_p^2 y\rangle \cdots \langle x+\zeta_p^{p-1} y\rangle = \langle z\rangle^p$.
- Si $i, j \in \mathbb{Z}$ con $i \not\equiv j \mod p$, entonces los ideales $\langle x+\zeta_p^i y\rangle$ y $\langle x+\zeta_p^j y\rangle$ son primos relativos.
- En consecuencia, para cada $i \in \mathbb{Z}$, el ideal $\langle x+\zeta_p^i y\rangle$ es una potencia p-ésima perfecta.
- Existe un $\beta \in \mathbb{Z}[\zeta_p]$ y un $s \in \mathbb{Z}$ tales que $\langle x+\zeta_p y\rangle = \langle \zeta_p^s \beta\rangle$, con $\beta \equiv n \mod p$ para algún $n \in \mathbb{N}$.
- $p \mid x + \zeta_p y - \zeta_p^{2s} x - \zeta_p^{2s-1} y$ en $\mathbb{Z}[\zeta_p]$.
- Esto último implica que $p \mid x$ o $p \mid y$, una contradicción.

Referencias

[1] Hungerford, T. W., *Algebra*, Springer-Verlag New York Inc., 1974.

[2] Ireland, Kenneth y Rosen, Michael, *A classical introduction to modern number theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1982.

[3] Janusz, Gerald J., *Algebraic Number Fields*, Graduate Studies in Mathematics (7), American Mathematical Society, Second Edition 1996.

[4] Karpilovsky, Gregory, *Field Theory*, Monographs and Textbooks in Pure an Applied Mathematics (120), Marcel Dekker, 1988.

[5] Lang, Serge, *Algebraic Number Theory*, Graduate Texts in Mathematics (110), Springer-Verlag, 1982.

[6] Rademacher, Hans, *Topics in analytic number theory*, Springer-Verlag, 1973.

[7] Titchmarsh, E. C., *The theory of the Riemann zeta-function*, Oxford University Press, 1951.

[8] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics (83), Springer-Verlag, 1982.