Números de Bernoulli

Un estudio sobre su importancia, consecuencias y algunas aplicaciones en la Teoría de Números

David José Fernández Bretón

Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional

Defensa de Tesis
para obtener el título de
Licenciado en Física y Matemáticas

Índice

Índice

Índice

Importancia histórica de los números de Bernoulli

Tres son los principales problemas, históricamente relevantes, en los cuales los números de Bernoulli juegan un papel importante.

- Jacob Bernoulli quería determinar una fórmula general para calcular la suma $1^k + 2^k + \cdots + n^k$ con $k, n \in \mathbb{N}$ arbitrarios. Esto lo impulsó a definir y utilizar por primera vez los números que llevan su nombre.
  - Finalmente, Bernoulli encontró con éxito dicha fórmula.
- Otro problema importante era encontrar el valor de la suma infinita
$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$$
  - Después de un prolongado esfuerzo, Leonhard Euler logró demostrar que el valor de esta suma es exactamente $\frac{\pi^2}{6}$, y posteriormente desarrolló el valor, más general, de la suma $\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$, para cualquier $k \in \mathbb{N}$.

Importancia histórica de los números de Bernoulli

Tres son los principales problemas, históricamente relevantes, en los cuales los números de Bernoulli juegan un papel importante.

- Jacob Bernoulli quería determinar una fórmula general para calcular la suma $1^k + 2^k + \cdots + n^k$ con $k, n \in \mathbb{N}$ arbitrarios. Esto lo impulsó a definir y utilizar por primera vez los números que llevan su nombre.
  - Finalmente, Bernoulli encontró con éxito dicha fórmula.
- Otro problema importante era encontrar el valor de la suma infinita $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$
  - Después de un prolongado esfuerzo, Leonhard Euler logró demostrar que el valor de esta suma es exactamente $\pi^2/6$, y posteriormente determinó el valor, más general, de la suma $\sum_{n=1}^{\infty} \frac{1}{n^{2m}}$, para $m \in \mathbb{N}$ arbitrario.

Importancia histórica de los números de Bernoulli

Tres son los principales problemas, históricamente relevantes, en los cuales los números de Bernoulli juegan un papel importante.

- Jacob Bernoulli quería determinar una fórmula general para calcular la suma $1^k + 2^k + \cdots + n^k$ con $k, n \in \mathbb{N}$ arbitrarios. Esto lo impulsó a definir y utilizar por primera vez los números que llevan su nombre.
  - Finalmente, Bernoulli encontró con éxito dicha fórmula.
- Otro problema importante era encontrar el valor de la suma infinita $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$
  - Después de un prolongado esfuerzo, Leonhard Euler logró demostrar que el valor de esta suma es exactamente $\pi^2/6$, y posteriormente determinó el valor, más general, de la suma $\sum_{n=1}^{\infty} \frac{1}{n^{2m}}$, para $m \in \mathbb{N}$ arbitrario.

Importancia histórica de los números de Bernoulli

Tres son los principales problemas, históricamente relevantes, en los cuales los números de Bernoulli juegan un papel importante.

- Jacob Bernoulli quería determinar una fórmula general para calcular la suma $1^k + 2^k + \cdots + n^k$ con $k, n \in \mathbb{N}$ arbitrarios. Esto lo impulsó a definir y utilizar por primera vez los números que llevan su nombre.
  - Finalmente, Bernoulli encontró con éxito dicha fórmula.
- Otro problema importante era encontrar el valor de la suma infinita $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$
  - Después de un prolongado esfuerzo, Leonhard Euler logró demostrar que el valor de esta suma es exactamente $\pi^2/6$, y posteriormente determinó el valor, más general, de la suma $\sum_{n=1}^{\infty} \frac{1}{n^{2m}}$, para $m \in \mathbb{N}$ arbitrario.

Importancia histórica de los números de Bernoulli

Tres son los principales problemas, históricamente relevantes, en los cuales los números de Bernoulli juegan un papel importante.

- Jacob Bernoulli quería determinar una fórmula general para calcular la suma $1^k + 2^k + \cdots + n^k$ con $k, n \in \mathbb{N}$ arbitrarios. Esto lo impulsó a definir y utilizar por primera vez los números que llevan su nombre.
  - Finalmente, Bernoulli encontró con éxito dicha fórmula.
- Otro problema importante era encontrar el valor de la suma infinita $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$
  - Después de un prolongado esfuerzo, Leonhard Euler logró demostrar que el valor de esta suma es exactamente $\pi^2/6$, y posteriormente determinó el valor, más general, de la suma $\sum_{n=1}^{\infty} \frac{1}{n^{2m}}$, para $m \in \mathbb{N}$ arbitrario.

Importancia histórica de los números de Bernoulli

- Pierre de Fermat conjeturó que la ecuación $x^n + y^n = z^n$ no tiene solución con $x, y, z \in \mathbb{Z}\backslash\{0\}$ cuando $n \geq 3$.
  - Ernst Eduard Kummer demostró un caso particular de este teorema, cuando n pertenece a cierto subconjunto de los números primos.
  - Mientras desarrolló estos resultados, Kummer realizó varios avances en teoría de anillos, introduciento novedosos y fructíferos conceptos, tales como el de ideal.

Importancia histórica de los números de Bernoulli

- Pierre de Fermat conjeturó que la ecuación $x^n + y^n = z^n$ no tiene solución con $x, y, z \in \mathbb{Z}\backslash\{0\}$ cuando $n \geq 3$.
  - Ernst Eduard Kummer demostró un caso particular de este teorema, cuando n pertenece a cierto subconjunto de los números primos.
  - Mientras desarrolló estos resultados, Kummer realizó varios avances en teoría de anillos, introduciento novedosos y fructíferos conceptos, tales como el de ideal.

Importancia histórica de los números de Bernoulli

- Pierre de Fermat conjeturó que la ecuación $x^n + y^n = z^n$ no tiene solución con $x, y, z \in \mathbb{Z}\backslash\{0\}$ cuando $n \geq 3$.
  - Ernst Eduard Kummer demostró un caso particular de este teorema, cuando n pertenece a cierto subconjunto de los números primos.
  - Mientras desarrolló estos resultados, Kummer realizó varios avances en teoría de anillos, introduciento novedosos y fructíferos conceptos, tales como el de ideal.

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* $m \in \mathbb{N}$.

Lo anterior es equivalente a decir que $B_0 = 1$ y $\sum_{k=0}^{m}\binom{m+1}{k}B_k = 0$.

Haciendo los cálculos, tenemos que $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$, $B_7 = 0$, $B_8 = -\frac{1}{30}$, $B_9 = 0$, $B_{10} = \frac{5}{66}$, $B_{11} = 0$, $B_{12} = -\frac{691}{2730}, \ldots$, etc.

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* $m \in \mathbb{N}$.

Lo anterior es equivalente a decir que $B_0 = 1$ y $\sum_{k=0}^{m}\binom{m+1}{k}B_k = 0$.

Haciendo los cálculos, tenemos que $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$, $B_7 = 0$, $B_8 = -\frac{1}{30}$, $B_9 = 0$, $B_{10} = \frac{5}{66}$, $B_{11} = 0$, $B_{12} = -\frac{691}{2730}, \ldots$, etc.

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* $m \in \mathbb{N}$.

Lo anterior es equivalente a decir que $B_0 = 1$ y $\sum_{k=0}^{m}\binom{m+1}{k}B_k = 0$.

Haciendo los cálculos, tenemos que $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$, $B_7 = 0$, $B_8 = -\frac{1}{30}$, $B_9 = 0$, $B_{10} = \frac{5}{66}$, $B_{11} = 0$, $B_{12} = -\frac{691}{2730}$, $\ldots$, etc.

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* $m \in \mathbb{N}$.

Lo anterior es equivalente a decir que $B_0 = 1$ y $\sum_{k=0}^{m}\binom{m+1}{k}B_k = 0$.

Haciendo los cálculos, tenemos que $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$, $B_7 = 0$, $B_8 = -\frac{1}{30}$, $B_9 = 0$, $B_{10} = \frac{5}{66}$, $B_{11} = 0$, $B_{12} = -\frac{691}{2730}, \ldots$, etc.

Números de Bernoulli

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

- $\dfrac{t}{e^t - 1} = \displaystyle\sum_{m=0}^{\infty} \frac{B_m}{m!} t^m.$
- $S_m(n) = \dfrac{1}{m+1} \displaystyle\sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$
- 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 $k \in \mathbb{N}$,

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

Números de Bernoulli

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

- $\dfrac{t}{e^t - 1} = \displaystyle\sum_{m=0}^{\infty} \frac{B_m}{m!} t^m.$
- $S_m(n) = \dfrac{1}{m+1} \displaystyle\sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$
- 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 $k \in \mathbb{N}$,

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

Números de Bernoulli

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

- $\dfrac{t}{e^t - 1} = \displaystyle\sum_{m=0}^{\infty} \frac{B_m}{m!} t^m.$
- $S_m(n) = \dfrac{1}{m+1} \displaystyle\sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$
- 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 $k \in \mathbb{N}$,

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

Números de Bernoulli

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

- $\dfrac{t}{e^t - 1} = \displaystyle\sum_{m=0}^{\infty} \frac{B_m}{m!} t^m$.
- $S_m(n) = \dfrac{1}{m+1} \displaystyle\sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}$.
- 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 $k \in \mathbb{N}$,

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

Definición

Para cada $m \in \mathbb{N} \cup \{0\}$, se define el m-ésimo polinomio de Bernoulli de la siguiente manera:

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

De esta forma, los primeros polinomios de Bernoulli son:

$$B_0(X) = 1,\ B_1(X) = X - \frac{1}{2},\ B_2(X) = X^2 - X + \frac{1}{6}, \cdots$$

Bajo la definición anterior, se tiene que

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Definición

Para cada $m \in \mathbb{N} \cup \{0\}$, se define el m-ésimo polinomio de Bernoulli de la siguiente manera:

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

De esta forma, los primeros polinomios de Bernoulli son:

$$B_0(X) = 1,\ B_1(X) = X - \frac{1}{2},\ B_2(X) = X^2 - X + \frac{1}{6}, \cdots$$

Bajo la definición anterior, se tiene que

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Definición

Para cada $m \in \mathbb{N} \cup \{0\}$, se define el m-ésimo polinomio de Bernoulli de la siguiente manera:

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

De esta forma, los primeros polinomios de Bernoulli son:

$$B_0(X) = 1,\ B_1(X) = X - \frac{1}{2},\ B_2(X) = X^2 - X + \frac{1}{6}, \cdots$$

Bajo la definición anterior, se tiene que

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Definición

Para cada $m \in \mathbb{N} \cup \{0\}$, se define el m-ésimo polinomio de Bernoulli de la siguiente manera:

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

De esta forma, los primeros polinomios de Bernoulli son:

$$B_0(X) = 1,\ B_1(X) = X - \frac{1}{2},\ B_2(X) = X^2 - X + \frac{1}{6}, \cdots$$

Bajo la definición anterior, se tiene que

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Polinomios de Bernoulli

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

en donde

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

Polinomios de Bernoulli

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

en donde

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

Polinomios de Bernoulli

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

en donde

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

Polinomios de Bernoulli

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

en donde

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

Polinomios de Bernoulli

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

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

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

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

Se define la función zeta de Riemann como

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

- $\zeta(2m) = \dfrac{(-1)^{m+1}(2\pi)^{2m}}{2(2m)!} B_{2m}, \quad m \in \mathbb{N}.$
- $(-1)^{m+1} B_{2m} > 0, \quad m \in \mathbb{N}.$
- $\left|\dfrac{B_{2m}}{2m}\right| \longrightarrow \infty$ 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

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

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

La función orden

Dado un número primo p, todo número racional $r \in \mathbb{Q}$ se expresa de manera única en la forma $r = p^n \frac{a}{b}$, con $n, a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ y $(a, b) = 1$.

Bajo la expresión anterior de r, se define su orden p-ádico, denotado por $\mathrm{ord}_p(r)$, como $\mathrm{ord}_p(r) = 0$, y por definición $\mathrm{ord}_p(0) = \infty$.

Así, podemos decir que cada número racional se escribe de la siguiente manera:

$$r = \prod_{p \text{ es primo}} p^{\mathrm{ord}_p(r)}.$$

Dado un número primo p, y $r \in \mathbb{Q}$, decimos que r es un p-entero si $\mathrm{ord}_p(r) \geq 0$.

La función orden

Dado un número primo p, todo número racional $r \in \mathbb{Q}$ se expresa de manera única en la forma $r = p^n \frac{a}{b}$, con $n, a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ y $(a, b) = 1$.

Bajo la expresión anterior de r, se define su orden p-ádico, denotado por $\mathrm{ord}_p(r)$, como $\mathrm{ord}_p(r) = 0$, y por definición $\mathrm{ord}_p(0) = \infty$.

Así, podemos decir que cada número racional se escribe de la siguiente manera:

$$r = \prod_{p \text{ es primo}} p^{\mathrm{ord}_p(r)}.$$

Dado un número primo p, y $r \in \mathbb{Q}$, decimos que r es un p-entero si $\mathrm{ord}_p(r) \geq 0$.

La función orden

Dado un número primo p, todo número racional $r \in \mathbb{Q}$ se expresa de manera única en la forma $r = p^n \frac{a}{b}$, con $n, a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ y $(a, b) = 1$.

Bajo la expresión anterior de r, se define su orden p-ádico, denotado por $\mathrm{ord}_p(r)$, como $\mathrm{ord}_p(r) = 0$, y por definición $\mathrm{ord}_p(0) = \infty$.

Así, podemos decir que cada número racional se escribe de la siguiente manera:

$$r = \prod_{p \text{ es primo}} p^{\mathrm{ord}_p(r)}.$$

Dado un número primo p, y $r \in \mathbb{Q}$, decimos que r es un p-entero si $\mathrm{ord}_p(r) \geq 0$.

La función orden

Dado un número primo p, todo número racional $r \in \mathbb{Q}$ se expresa de manera única en la forma $r = p^n \frac{a}{b}$, con $n, a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ y $(a, b) = 1$.

Bajo la expresión anterior de r, se define su orden p-ádico, denotado por $\mathrm{ord}_p(r)$, como $\mathrm{ord}_p(r) = 0$, y por definición $\mathrm{ord}_p(0) = \infty$.

Así, podemos decir que cada número racional se escribe de la siguiente manera:

$$r = \prod_{p \text{ es primo}} p^{\mathrm{ord}_p(r)}.$$

Dado un número primo p, y $r \in \mathbb{Q}$, decimos que r es un p-entero si $\mathrm{ord}_p(r) \geq 0$.

La función orden

Dado un número primo p, todo número racional $r \in \mathbb{Q}$ se expresa de manera única en la forma $r = p^n \frac{a}{b}$, con $n, a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ y $(a, b) = 1$.

Bajo la expresión anterior de r, se define su orden p-ádico, denotado por $\mathrm{ord}_p(r)$, como $\mathrm{ord}_p(r) = 0$, y por definición $\mathrm{ord}_p(0) = \infty$.

Así, podemos decir que cada número racional se escribe de la siguiente manera:

$$r = \prod_{p \text{ es primo}} p^{\mathrm{ord}_p(r)}.$$

Dado un número primo p, y $r \in \mathbb{Q}$, decimos que r es un p-entero si $\mathrm{ord}_p(r) \geq 0$.

Los 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

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

- $pB_m \in \mathbb{Z}_{\langle p \rangle},\ \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)|2m} \frac{1}{p}$ 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}.

Los 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*

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

- $pB_m \in \mathbb{Z}_{\langle p\rangle},\ \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)\mid 2m} \frac{1}{p}$ 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}.

Los 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*

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

- $pB_m \in \mathbb{Z}_{\langle p\rangle},\ \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)\mid 2m} \frac{1}{p}$ 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}.

Los 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*

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

- $pB_m \in \mathbb{Z}_{\langle p\rangle}, \quad \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)|2m} \frac{1}{p}$ 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}.

Los 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*

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

- $pB_m \in \mathbb{Z}_{\langle p\rangle}, \quad \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)|2m} \frac{1}{p}$ 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}.

Los 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*

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

- $pB_m \in \mathbb{Z}_{\langle p\rangle}, \quad \forall\, m \in \mathbb{N}.$
- $pB_m \equiv S_m(p) \equiv \begin{cases} 0; & (p-1) \nmid m \\ -1; & (p-1) \mid m \end{cases} \mod p$, para todo m par.
- $B_{2m} = A_{2m} + \sum_{(p-1)|2m} \frac{1}{p}$ 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 $\mathbb{Z}$ y en $\mathbb{Z}_{\langle p \rangle}$

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

- $V_m S_m(n) \equiv U_m\, n \mod n^2,\ \forall\, n \in \mathbb{N}.$
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2.$
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \sum_{j=1}^{n-1} j^{m-1} \left[\dfrac{ja}{n}\right] \mod n,$

  $\forall\, a, n \in \mathbb{N}$ tales que $(a, n) = 1.$
- 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,

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

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

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

- $V_m S_m(n) \equiv U_m \; n \mod n^2, \;\; \forall \, n \in \mathbb{N}$.
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2$.
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n} \right] \mod n,$

  $\forall \, a, n \in \mathbb{N}$ tales que $(a, n) = 1$.
- 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,

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

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

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

- $V_m S_m(n) \equiv U_m \; n \mod n^2, \quad \forall \, n \in \mathbb{N}$.
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2$.
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n} \right] \mod n,$

  $\forall \, a, n \in \mathbb{N}$ tales que $(a, n) = 1$.
- 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,

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

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

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

- $V_m S_m(n) \equiv U_m\ n \mod n^2,\ \ \forall\, n \in \mathbb{N}.$
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2.$
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \mod n,$

  $\forall\, a, n \in \mathbb{N}$ tales que $(a, n) = 1.$
- 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,

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

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

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

- $V_m S_m(n) \equiv U_m\ n \mod n^2,\ \ \forall\, n \in \mathbb{N}.$
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2.$
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \mod n,$

  $\forall\, a, n \in \mathbb{N}$ tales que $(a, n) = 1.$
- 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,

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

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

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

- $V_m S_m(n) \equiv U_m\ n \mod n^2,\ \ \forall\, n \in \mathbb{N}.$
- p número primo tal que $(p-1) \nmid m \Rightarrow S_m(p) \equiv B_m p \mod p^2.$
- $(a, m) = 1 \Rightarrow (a^m - 1)U_m \equiv m a^{m-1} V_m \displaystyle\sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \mod n,$

  $\forall\, a, n \in \mathbb{N}$ tales que $(a, n) = 1.$
- 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, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0.61$.

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, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0.61$.

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, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0.61$.

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, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0.61$.

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 $\lim_{p\to\infty} \dfrac{\#\{q \mid q \leq p,\ q \text{ es irregular}\}}{\#\{q \mid q \leq p\}} = \dfrac{1}{\sqrt{e}}$. En otras palabras, $\lim_{p\to\infty} \mathcal{P}(p \text{ es irregular}) = \dfrac{1}{\sqrt{e}} \approx 0.61$.

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- *Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.*

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- *Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.*

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.

Campos y anillos ciclotómicos

Sea $n \in \mathbb{N}$, y sea ζ_n 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, denotado por $\mathcal{O}_K$, como sigue:

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

- Si p es un número primo, entonces el anillo de enteros de $\mathbb{Q}(\zeta_p)$ es exactamente $\mathbb{Z}[\zeta_p]$.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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 $\mathrm{coc}(D)$, 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:

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

- 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.

Dominios Dedekind

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.

En consecuencia, si $I \subseteq D$ es un ideal fraccional (en particular un ideal) no principal y $n \in \mathbb{N}$ es tal que I^n es principal, ello implicará que $(n, h(D)) > 1$.

Dominios Dedekind

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.

En consecuencia, si $I \subseteq D$ es un ideal fraccional (en particular un ideal) no principal y $n \in \mathbb{N}$ es tal que I^n es principal, ello implicará que $(n, h(D)) > 1$.

Dominios Dedekind

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.

En consecuencia, si $I \subseteq D$ es un ideal fraccional (en particular un ideal) no principal y $n \in \mathbb{N}$ es tal que I^n es principal, ello implicará que $(n, h(D)) > 1$.

Dominios Dedekind

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.

En consecuencia, si $I \subseteq D$ es un ideal fraccional (en particular un ideal) no principal y $n \in \mathbb{N}$ es tal que I^n es principal, ello implicará que $(n, h(D)) > 1$.

Dominios Dedekind

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.

En consecuencia, si $I \subseteq D$ es un ideal fraccional (en particular un ideal) no principal y $n \in \mathbb{N}$ es tal que I^n es principal, ello implicará que $(n, h(D)) > 1$.

Campos numéricos

Sea K un campo. Decimos que K es un campo numérico si K es de característica cero y $[K : \mathbb{Q}] < \infty$.

- Si K es un campo numérico, entonces el anillo de enteros de K es un dominio Dedekind.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Si K es un campo numérico, entonces $h(K) < \infty$.
- 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 $\mathbb{Z}[\zeta_p]$.

Campos numéricos

Sea K un campo. Decimos que K es un campo numérico si K es de característica cero y $[K : \mathbb{Q}] < \infty$.

- Si K es un campo numérico, entonces el anillo de enteros de K es un dominio Dedekind.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Si K es un campo numérico, entonces $h(K) < \infty$.
- 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 $\mathbb{Z}[\zeta_p]$.

Campos numéricos

Sea K un campo. Decimos que K es un campo numérico si K es de característica cero y $[K : \mathbb{Q}] < \infty$.

- Si K es un campo numérico, entonces el anillo de enteros de K es un dominio Dedekind.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Si K es un campo numérico, entonces $h(K) < \infty$.
- 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 $\mathbb{Z}[\zeta_p]$.

Campos numéricos

Sea K un campo. Decimos que K es un campo numérico si K es de característica cero y $[K : \mathbb{Q}] < \infty$.

- Si K es un campo numérico, entonces el anillo de enteros de K es un dominio Dedekind.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Si K es un campo numérico, entonces $h(K) < \infty$.
- 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 $\mathbb{Z}[\zeta_p]$.

Campos numéricos

Sea K un campo. Decimos que K es un campo numérico si K es de característica cero y $[K : \mathbb{Q}] < \infty$.

- Si K es un campo numérico, entonces el anillo de enteros de K es un dominio Dedekind.
- En consecuencia, el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind para p número primo.
- Si K es un campo numérico, entonces $h(K) < \infty$.
- 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 $\mathbb{Z}[\zeta_p]$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, defimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, definimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, definimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, defimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, defimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente:

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} \qquad \forall\, n \in \mathbb{Z}.$$

Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de caracteres de Dirichlet módulo m.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, defimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$.

Con este producto, el conjunto de caracteres de Dirichlet módulo m es un grupo isomorfo al grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. Así, es posible considerar al homomorfismo “inductor" χ' como un homomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$.

Caracteres de Dirichlet

Si X es un grupo finito de caracteres de Dirichlet módulo m, entonces al campo fijo de $\bigcap_{\chi\in X} \ker(\chi) = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \big| \chi(\sigma) = 1, \ \ \forall\, \chi \in X\}$ *se le conoce como el campo perteneciente a X.*

El conductor de un caracter de Dirichlet χ es el mínimo número natural f_χ tal que χ es un caracter módulo f_χ. Por otra parte, se dice que χ es par cuando $\chi(-1) = 1$, y que es impar en caso contrario.

Caracteres de Dirichlet

Si X es un grupo finito de caracteres de Dirichlet módulo m, entonces al campo fijo de $\bigcap_{\chi\in X} \ker(\chi) = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \big| \chi(\sigma) = 1, \ \ \forall\, \chi \in X\}$ *se le conoce como el campo perteneciente a X.*

El conductor de un caracter de Dirichlet χ es el mínimo número natural f_χ tal que χ es un caracter módulo f_χ. Por otra parte, se dice que χ es par cuando $\chi(-1) = 1$, y que es impar en caso contrario.

Caracteres de Dirichlet

Si X es un grupo finito de caracteres de Dirichlet módulo m, entonces al campo fijo de $\bigcap_{\chi\in X}\ker(\chi)=\{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\big|\chi(\sigma)=1,\ \ \forall\,\chi\in X\}$ se le conoce como el campo perteneciente a X.

El conductor de un caracter de Dirichlet χ es el mínimo número natural f_χ tal que χ es un caracter módulo f_χ. Por otra parte, se dice que χ es par cuando $\chi(-1)=1$, y que es impar en caso contrario.

L-series

Sea χ un caracter de Dirichlet módulo m. Definimos la L-serie de Dirichlet asociada a χ, como la siguiente función:

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

Sea χ un caracter de Dirichlet módulo su conductor m. Para cada $n \in \mathbb{N} \cup \{0\}$, se define el n-ésimo número de Bernoulli generalizado, denotado por $B_{n,\chi}$, mediante la siguiente fórmula: $\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$

El caracter identidad χ_0 se considera como módulo 1. Los números B_{n,χ_0} vendrán entonces dados por $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido que los números de Bernoulli generalizados generalizan a los números de Bernoulli.

L-series

Sea χ un caracter de Dirichlet módulo m. Definimos la L-serie de Dirichlet asociada a χ, como la siguiente función:

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

Sea χ un caracter de Dirichlet módulo su conductor m. Para cada $n \in \mathbb{N} \cup \{0\}$, se define el n-ésimo número de Bernoulli generalizado, denotado por $B_{n,\chi}$, mediante la siguiente fórmula: $\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$

El caracter identidad χ_0 se considera como módulo 1. Los números B_{n,χ_0} vendrán entonces dados por $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido que los números de Bernoulli generalizados generalizan a los números de Bernoulli.

L-series

Sea χ un caracter de Dirichlet módulo m. Definimos la L-serie de Dirichlet asociada a χ, como la siguiente función:

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

Sea χ un caracter de Dirichlet módulo su conductor m. Para cada $n \in \mathbb{N} \cup \{0\}$, se define el n-ésimo número de Bernoulli generalizado, denotado por $B_{n,\chi}$, mediante la siguiente fórmula: $\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$

El caracter identidad χ_0 se considera como módulo 1. Los números B_{n,χ_0} vendrán entonces dados por $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido que los números de Bernoulli generalizados generalizan a los números de Bernoulli.

L-series

Sea χ un caracter de Dirichlet módulo m. Definimos la L-serie de Dirichlet asociada a χ, como la siguiente función:

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

Sea χ un caracter de Dirichlet módulo su conductor m. Para cada $n \in \mathbb{N} \cup \{0\}$, se define el n-ésimo número de Bernoulli generalizado, denotado por $B_{n,\chi}$, mediante la siguiente fórmula: $\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$

El caracter identidad χ_0 se considera como módulo 1. Los números B_{n,χ_0} vendrán entonces dados por $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido que los números de Bernoulli generalizados generalizan a los números de Bernoulli.

L-series

Sea χ un caracter de Dirichlet módulo m. Definimos la L-serie de Dirichlet asociada a χ, como la siguiente función:

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

Sea χ un caracter de Dirichlet módulo su conductor m. Para cada $n \in \mathbb{N} \cup \{0\}$, se define el n-ésimo número de Bernoulli generalizado, denotado por $B_{n,\chi}$, mediante la siguiente fórmula: $\displaystyle\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$

El caracter identidad χ_0 se considera como módulo 1. Los números B_{n,χ_0} vendrán entonces dados por $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido que los números de Bernoulli generalizados generalizan a los números de Bernoulli.

Números de Bernoulli generalizados

La función que define a los números de Bernoulli generalizados, será par o impar dependiendo de si el correspondiente caracter de Dirichlet χ es par o impar. De manera que, salvo en el caso cuando $\chi = \chi_0$, en general se tiene que $B_{2k+1,\chi} = 0$ cuando χ es par, y $B_{2k,\chi} = 0$ cuando χ es impar, para cualquier $k \in \mathbb{N}$.

- Sean χ un caracter de Dirichlet módulo su conductor m, y F cualquier múltiplo de m. Entonces,

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

- Sea χ un caracter de Dirichlet primitivo y sea $k \in \mathbb{N}$. Entonces, se tiene que $L(1-k,\chi) = -\dfrac{B_{k,\chi}}{k}$.

Números de Bernoulli generalizados

La función que define a los números de Bernoulli generalizados, será par o impar dependiendo de si el correspondiente caracter de Dirichlet χ es par o impar. De manera que, salvo en el caso cuando $\chi = \chi_0$, en general se tiene que $B_{2k+1,\chi} = 0$ cuando χ es par, y $B_{2k,\chi} = 0$ cuando χ es impar, para cualquier $k \in \mathbb{N}$.

- Sean χ un caracter de Dirichlet módulo su conductor m, y F cualquier múltiplo de m. Entonces,

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

- Sea χ un caracter de Dirichlet primitivo y sea $k \in \mathbb{N}$. Entonces, se tiene que $L(1-k,\chi) = -\dfrac{B_{k,\chi}}{k}$.

Números de Bernoulli generalizados

La función que define a los números de Bernoulli generalizados, será par o impar dependiendo de si el correspondiente caracter de Dirichlet χ es par o impar. De manera que, salvo en el caso cuando $\chi = \chi_0$, en general se tiene que $B_{2k+1,\chi} = 0$ cuando χ es par, y $B_{2k,\chi} = 0$ cuando χ es impar, para cualquier $k \in \mathbb{N}$.

- Sean χ un caracter de Dirichlet módulo su conductor m, y F cualquier múltiplo de m. Entonces,

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

- Sea χ un caracter de Dirichlet primitivo y sea $k \in \mathbb{N}$. Entonces, se tiene que $L(1-k,\chi) = -\dfrac{B_{k,\chi}}{k}$.

Función zeta de Dedekind

Sean K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, se define la función zeta de Dedekind del campo K como la siguiente función de variable compleja:

$$\zeta_K(s) := \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s} = \prod_{\mathfrak{P} \text{ ideal primo de } \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}.$$

Obsérvese que $\zeta_{\mathbb{Q}}$ no es otra cosa que la función zeta de Riemann.

- Sea K un campo numérico, y considérese su función zeta ζ_K. Entonces, ésta se puede extender a una función meromorfa en todo el plano complejo salvo el punto $s = 1$, en donde se encuentra un polo simple. Más aún, se tiene que

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h(K) \operatorname{Reg}_K}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi).$$

Función zeta de Dedekind

Sean K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, se define la función zeta de Dedekind del campo K como la siguiente función de variable compleja:

$$\zeta_K(s) := \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s} = \prod_{\mathfrak{P} \text{ ideal primo de } \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}.$$

Obsérvese que $\zeta_{\mathbb{Q}}$ no es otra cosa que la función zeta de Riemann.

- Sea K un campo numérico, y considérese su función zeta ζ_K. Entonces, ésta se puede extender a una función meromorfa en todo el plano complejo salvo el punto $s = 1$, en donde se encuentra un polo simple. Más aún, se tiene que

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h(K) \operatorname{Reg}_K}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi).$$

Función zeta de Dedekind

Sean K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, se define la función zeta de Dedekind del campo K como la siguiente función de variable compleja:

$$\zeta_K(s) := \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s} = \prod_{\mathfrak{P} \text{ ideal primo de } \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}.$$

Obsérvese que $\zeta_{\mathbb{Q}}$ no es otra cosa que la función zeta de Riemann.

- Sea K un campo numérico, y considérese su función zeta ζ_K. Entonces, ésta se puede extender a una función meromorfa en todo el plano complejo salvo el punto $s = 1$, en donde se encuentra un polo simple. Más aún, se tiene que

$$\operatorname{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h(K) \operatorname{Reg}_K}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi).$$

Función zeta de Dedekind

Sean K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, se define la función zeta de Dedekind del campo K como la siguiente función de variable compleja:

$$\zeta_K(s) := \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s} = \prod_{\mathfrak{P} \text{ ideal primo de } \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}.$$

Obsérvese que $\zeta_{\mathbb{Q}}$ no es otra cosa que la función zeta de Riemann.

- Sea K un campo numérico, y considérese su función zeta ζ_K. Entonces, ésta se puede extender a una función meromorfa en todo el plano complejo salvo el punto $s = 1$, en donde se encuentra un polo simple. Más aún, se tiene que

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h(K)\mathrm{Reg}_K}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi).$$

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \neq -1 \mod (p-1)$. Si ω es un generador del grupo C_p, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo C_p, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{(p)}$: $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \mod p$.

Resultados acerca de CM-campos

Un CM-campo es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real.

- Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos.
- Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.

Es común denotar al número $h(K^+)$ como $h^+(K)$. Al cociente $h(K)/h^+(K) \in \mathbb{Z}$ se le denota como $h^-(K)$ y recibe el nombre de número de clases relativo del campo K.

- Sea p un número primo, y n un número impar, con $n \not\equiv -1 \mod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{\langle p \rangle}$: $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \mod p$.

Caracterización de los números primos regulares

- Sea p un número primo impar. Entonces, $p \mid h^-(\mathbb{Q}(\zeta_p)) \iff p|U_j$, para algún $j = 2, 4, \cdots, p-3$; en donde U_j es el numerador del j-ésimo número de Bernoulli B_j.
- Sea p un número primo impar. Si $p \mid h^+(\mathbb{Q}(\zeta_p))$, entonces $p \mid h^-(\mathbb{Q}(\zeta_p))$.
- Sea p un número primo impar. Entonces, p es regular si y sólo si $p \nmid h(\mathbb{Q}(\zeta_p))$.

Caracterización de los números primos regulares

- Sea p un número primo impar. Entonces, $p \mid h^-(\mathbb{Q}(\zeta_p)) \iff p|U_j$, para algún $j = 2, 4, \cdots, p-3$; en donde U_j es el numerador del j-ésimo número de Bernoulli B_j.
- Sea p un número primo impar. Si $p \mid h^+(\mathbb{Q}(\zeta_p))$, entonces $p \mid h^-(\mathbb{Q}(\zeta_p))$.
- Sea p un número primo impar. Entonces, p es regular si y sólo si $p \nmid h(\mathbb{Q}(\zeta_p))$.

Caracterización de los números primos regulares

- Sea p un número primo impar. Entonces, $p \mid h^-(\mathbb{Q}(\zeta_p)) \iff p|U_j$, para algún $j = 2, 4, \cdots, p-3$; en donde U_j es el numerador del j-ésimo número de Bernoulli B_j.
- Sea p un número primo impar. Si $p \mid h^+(\mathbb{Q}(\zeta_p))$, entonces $p \mid h^-(\mathbb{Q}(\zeta_p))$.
- Sea p un número primo impar. Entonces, p es regular si y sólo si $p \nmid h(\mathbb{Q}(\zeta_p))$.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

Un caso particular del último teorema de Fermat

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.
- Por lo anterior, hay un ideal I tal que $I^p = \langle x+\zeta_p^i y\rangle$. Dado que p es un número primo regular, entonces $p \nmid h(\mathbb{Q}(\zeta_p))$, de modo que I debe de ser un ideal principal.
- 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.

- Barrera Mora, Fernando, *Introducción a la teoría de grupos*, Universidad Autónoma del Estado de Hidalgo, 2004.
- Edwards, Harold M., *Fermat's Last Theorem*, Graduate Texts in Mathematics (50), Springer-Verlag, 1977.
- Edwards, Harold M., *The background of Kummer's proof of Fermat's Last Theorem for regular primes*, Arch. Hist. Exact. Sci. **14** (**3**) (1975), 219-236.
- Edwards, Harold M., *Postscript to "The background of Kummer's proof ..."*, Arch. Hist. Exact. Sci. **17** (**4**) (1977), 381-394.
- Edwards, Harold M., *Riemann's Zeta Function*, Academic Press, New York, 1974.
- Hernández Arellano, Fabián M., *Cálculo de probabilidades*, Aportaciones Matemáticas (25), Sociedad Matemática Mexicana, 2003.
- Hernández-Lerma, Onésimo y Hernández-del-Valle, Adrián, *Elementos de probabilidad y estadística*, Aportaciones Matemáticas (21), Sociedad Matemática Mexicana, 2003.

- Hungerford, T. W., *Algebra*, Springer-Verlag New York Inc., 1974.
- Ireland, Kenneth y Rosen, Michael, *A classical introduction to modern number theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1982.
- Janusz, Gerald J., *Algebraic Number Fields*, Graduate Studies in Mathematics (7), American Mathematical Society, Second Edition 1996.
- Karpilovsky, Gregory, *Field Theory*, Monographs and Textbooks in Pure an Applied Mathematics (120), Marcel Dekker, 1988.
- Lang, Serge, *Algebraic Number Theory*, Graduate Texts in Mathematics (110), Springer-Verlag, 1982.
- Rademacher, Hans, *Topics in analytic number theory*, Springer-Verlag, 1973.
- Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

- Ribenboim, Paulo, *The Book of Prime Number Records*, Springer-Verlag, 1980.
- Riemann, Bernhard, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* (en inglés: *On the Number of Prime Numbers less than a Given Quantity*, trad. David R. Wilkins) , Monatsberichte der Berliner Akademie, Noviembre de 1859.
- Rudin, Walter, *Real and Complex Analysis* Second Edition, Mc. Graw Hill, 1966.
- Silverman, Richard A., *Introductory complex analysis*, Prentice-Hall, 1967.
- Titchmarsh, E. C., *The theory of the Riemann zeta-function*, Oxford University Press, 1951.
- Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics (83), Springer-Verlag, 1982.