Números de Bernoulli

Alexey Beshenov (cadadr@gmail.com)

Febrero de 2017

Los números de Bernoulli son ciertos números racionales

$$B_0 = 1,\ B_1 = \frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30},\ B_5 = 0,\ B_6 = \frac{1}{42},\ B_7 = 0,\ B_8 = -\frac{1}{30},\ \dots$$

que aparecen en varios contextos de la teoría de números, combinatoria y análisis. En estos apuntes vamos a revisar sus diferentes definiciones: una que surge del estudio de sumas de potencias $1^k + 2^k + \cdots + n^k$, y otra definición por una función generatriz:

$$\frac{t\,e^t}{e^t - 1} = \sum_{k \geq 0} \frac{B_k}{k!}\, t^k.$$

Luego vamos a ver la demostración de la famosa fórmula de Euler para los valores especiales de la función zeta:

$$\zeta(2k) := 1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \cdots = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k}.$$

Finalmente, vamos a demostrar el **teorema de Clausen–von Staudt** sobre los denominadores de B_k y las **congruencias de Kummer**.

Un aspecto atractivo de este tema es que todos los resultados se tratan de números concretos y el lector puede experimentar y hacer cálculos por sí mismo. Afortunadamente, ya no estamos en los tiempos de Euler y Bernoulli y podemos usar la computadora. Mi programa preferido para la teoría de números es PARI/GP, y voy a ilustrar todo con su código. El lector puede descargar PARI/GP de la página

`http://pari.math.u-bordeaux.fr/`

Para preparar estos apuntes, he usado principalmente los primeros capítulos del libro [AIK2014], y el lector interesado puede consultarlo para más información sobre los números de Bernoulli y las funciones zeta.

Le doy gracias a Gabriel Chicas Reyes de la Universidad de El Salvador por su ayuda con la redacción de estos apuntes.

Índice

1 Sumas de potencias de números naturales

La suma de n números naturales consecutivos puede ser calculada mediante la fórmula

$$1 + 2 + \cdots + n = \frac{(n+1)\,n}{2} = \frac{1}{2}\,n^2 + \frac{1}{2}\,n.$$

Probablemente el lector también conoce la fórmula para las sumas de cuadrados:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6} = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$

—es fácil demostrarla por inducción. Muchos matemáticos trataron de encontrar la fórmula similar para las sumas de cubos y otras potencias superiores. Es un problema muy natural, y la solución fue descubierta al principio del siglo XVIII por el matemático suizo Jacob Bernoulli (1654–1705) y independientemente por el matemático japonés Seki Takakazu (1642–1708). Denotemos por $S_k(n)$ la suma de las k-ésimas potencias de los números naturales hasta n:

$$S_k(n) := \sum_{1 \le i \le n} i^k = 1^k + 2^k + \cdots + n^k.$$

En particular,

$$S_0(n) = n, \quad S_1(n) = \frac{1}{2}\,n^2 + \frac{1}{2}\,n, \quad S_2(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$

Para obtener las fórmulas para $S_3(n), S_4(n), S_5(n)$, etcétera, recordemos primero el **teorema del binomio**:

$$(x+y)^k = \sum_{0 \le i \le k} \binom{k}{i} x^{k-i}\, y^i,$$

donde

$$\binom{k}{i} = \frac{k!}{(k-i)!\,i!}$$

denota un **coeficiente binomial**, definido como el número de posibilidades de escoger i objetos entre un total de k objetos.

En PARI/GP, `binomial(k,i)` $= \binom{k}{i}$.

```
/* vector (n,i,expr) devuelve un vector con la expresión
   expr evaluada con i=1, i=2, ..., i=n: */
? vector (7,i,binomial (6,i-1))
% = [1, 6, 15, 20, 15, 6, 1]
```

En particular, tenemos

$$(m+1)^{k+1} - m^{k+1} = \sum_{0 \le i \le k} \binom{k+1}{i}\, m^i.$$

La suma de estas identidades para $m = 1, 2, \ldots, n$ nos da

$$(n+1)^{k+1} - 1 = \sum_{0 \le i \le k} \binom{k+1}{i}\, S_i(n),$$

de donde tenemos una expresión de $S_k(n)$ en términos de $S_0(n), S_1(n), \ldots, S_{k-1}(n)$:

$$S_k(n) = \frac{1}{k+1}\left((n+1)^{k+1} - 1 - \sum_{0\le i\le k-1} \binom{k+1}{i} S_i(n)\right). \tag{1.1}$$

Por inducción se ve que $S_k(n)$ es un polinomio en n de grado $k+1$, con coeficiente principal $\frac{1}{k+1}$. Para evitar una posible confusión, denotemos la variable por x. El polinomio $S_k(x) \in \mathbb{Q}[x]$ está determinado por sus valores en $x = n \in \mathbb{N}$ (¿por qué?). Por la definición de $S_k(n)$, tenemos $S_k(n+1) - S_k(n) = (n+1)^k$ para $n = 1, 2, 3, \ldots$ Para los polinomios, esto nos da la relación

$$S_k(x+1) - S_k(x) = (x+1)^k. \tag{1.2}$$

En particular, $S_k(1) - S_k(0) = 1$, y ya que $S_k(1) = 1$, esto significa que $S_k(0) = 0$; es decir, el término constante del polinomio $S_k(x)$ es nulo (también podemos verlo por inducción de la fórmula (1.1)). Usando (1.1), podemos calcular algunos $S_k(x)$.

Implementemos nuestra fórmula para S_k en PARI/GP:

```
S(k) = if (k == 0, x, 1/(k+1)*((x+1)^(k+1) - 1 - sum (i=0, k-1, binomial(k+1,i) * S(i))));

? S(3)
% = 1/4*x^4 + 1/2*x^3 + 1/4*x^2
```

El lector que conoce un poco de programación puede notar que el código de arriba es muy ineficaz; por ejemplo, para calcular `S(20)` ya se necesita mucho tiempo. He aquí otra versión mucho más rápida:

```
/* La tabla de S (k): */
s_table = [];

S (k) = {
  if (k == 0, return (x));

  /* Extender la tabla de valores, de ser necesario: */
  if (length(s_table) < k, s_table = concat(s_table, vector(k-length(s_table))));

  /* Devolver el valor, si está en la tabla;
     sino, calcularlo y poner en la tabla: */
  if (s_table[k], s_table[k],
      s_table[k] = 1/(k+1)*((x+1)^(k+1) - 1 - sum (i=0, k-1, binomial(k+1,i) * S(i))))
}
```

(Trate de calcular, por ejemplo, `S(20)` usando ambas versiones.)

$$
\begin{aligned}
S_0(x) &= x,\\
S_1(x) &= \frac{1}{2}\,x^2 + \frac{1}{2}\,x,\\
S_2(x) &= \frac{1}{3}\,x^3 + \frac{1}{2}\,x^2 + \frac{1}{6}\,x,\\
S_3(x) &= \frac{1}{4}\,x^4 + \frac{1}{2}\,x^3 + \frac{1}{4}\,x^2,\\
S_4(x) &= \frac{1}{5}\,x^5 + \frac{1}{2}\,x^4 + \frac{1}{3}\,x^3 - \frac{1}{30}\,x,\\
S_5(x) &= \frac{1}{6}\,x^6 + \frac{1}{2}\,x^5 + \frac{5}{12}\,x^4 - \frac{1}{12}\,x^2,\\
S_6(x) &= \frac{1}{7}\,x^7 + \frac{1}{2}\,x^6 + \frac{1}{2}\,x^5 - \frac{1}{6}\,x^3 + \frac{1}{42}\,x,\\
S_7(x) &= \frac{1}{8}\,x^8 + \frac{1}{2}\,x^7 + \frac{7}{12}\,x^6 - \frac{7}{24}\,x^4 + \frac{1}{12}\,x^2,\\
S_8(x) &= \frac{1}{9}\,x^9 + \frac{1}{2}\,x^8 + \frac{2}{3}\,x^7 - \frac{7}{15}\,x^5 + \frac{2}{9}\,x^3 - \frac{1}{30}\,x,\\
S_9(x) &= \frac{1}{10}\,x^{10} + \frac{1}{2}\,x^9 + \frac{3}{4}\,x^8 - \frac{7}{10}\,x^6 + \frac{1}{2}\,x^4 - \frac{3}{20}\,x^2,\\
S_{10}(x) &= \frac{1}{11}\,x^{11} + \frac{1}{2}\,x^{10} + \frac{5}{6}\,x^9 - x^7 + x^5 - \frac{1}{2}\,x^3 + \frac{5}{66}\,x.
\end{aligned}
$$

Las expresiones de arriba, también hasta $S_{10}(n)$, aparecen en la página 97 del libro de Bernoulli [Ber1713], publicado póstumamente en 1713. Luego Bernoulli escribe que, usando sus fórmulas, calculó en un "semi-cuarto de hora" la suma

$$1^{10} + 2^{10} + \cdots + 1000^{10} = S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500.$$

Con ayuda de una computadora, se puede verificar que ¡el resultado es correcto!

```
? { local(x); x = 1000; eval (S(10)) }
% = 91409924241424243424241924242500

? sum (i=1,1000,i^10)
% = 91409924241424243424241924242500
```

1.1. Definición. El ***k*-ésimo número de Bernoulli** B_k es el coeficiente de x en el polinomio $S_k(x)$. En otras palabras,

$$B_k := S_k'(0).$$

Euler leyó "Ars Conjectandi" y estudió los números B_k, llamándolos los "números de Bernoulli", en el capítulo II.5 de su libro [Eul1755]. Varias identidades para B_k que aparecen en nuestro curso fueron descubiertas por Euler. Por ejemplo, la derivada de (1.1) nos da

$$S_k'(x) = \frac{1}{k+1}\left((k+1)\,(x+1)^k - \sum_{0\le i\le k-1}\binom{k+1}{i}\,S_i'(x)\right),$$

y para $x = 0$ tenemos

$$B_k = S'_k(0) = 1 - \frac{1}{k+1} \sum_{0 \le i \le k-1} \binom{k+1}{i} B_i.$$

1.2. Proposición. *Para todo $k \ge 0$ se tiene*

$$\sum_{0 \le i \le k} \binom{k+1}{i} B_i = k + 1.$$

Esto nos da una definición recursiva de los B_k:

$$\begin{aligned} B_0 &= 1, \\ B_0 + 2\,B_1 &= 2, \\ B_0 + 3\,B_1 + 3\,B_2 &= 3, \\ B_0 + 4\,B_1 + 6\,B_2 + 4\,B_3 &= 4, \\ &\vdots \end{aligned}$$

A partir de estas identidades se pueden calcular sucesivamente $B_1, B_2, B_3, B_4, \ldots$

```
/* La tabla de B (k): */
b_table = [];

B (k) = {
  if (k == 0, return (1));

  if (length(b_table) < k, b_table = concat(b_table, vector(k-length(b_table))));
  if (b_table[k], b_table[k],
      b_table[k] = 1 - 1/(k+1)*sum (i=0, k-1, binomial(k+1,i)*B (i)))
}

? polcoeff (S(10),1,n)
% = 5/66
? B(10)
% = 5/66
```

Luego los primeros números de Bernoulli son

k:	0	1	2	3	4	5	6	7	8	9	10	$\cdots$
B_k:	1	$\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	$\cdots$

(Bernoulli y Euler no usaban la notación B_k, sino que escribían $A = \frac{1}{6}$, $B = -\frac{1}{30}$, $C = \frac{1}{42}$, $D = -\frac{1}{30}$, etcétera.)

La derivada de (1.2) es

$$S'_k(x+1) - S'_k(x) = k\,(x+1)^{k-1},$$

y la suma de estas identidades para $x = 0, 1, 2, \ldots, n-1$ nos da

$$S'_k(n) - S'_k(0) = k\,S_{k-1}(n).$$

Entonces, los polinomios $S_k(x)$ satisfacen la identidad

$$S_k'(x) = k\, S_{k-1}(x) + B_k.$$

Esto, junto con $S_1(x) = x$, define completamente a todos los $S_k(x)$ (el término constante es nulo).

1.3. Ejercicio (La fórmula de Faulhaber). *Demuestre la identidad*

$$S_k(n) = \frac{1}{k+1} \sum_{0\le i\le k} \binom{k+1}{i} B_i\, n^{k+1-i}.$$

Indicación: si $p(x) \in \mathbb{Q}[x]$ es un polinomio de grado d, entonces

$$p(x) = \sum_{0\le i\le d} \frac{p^{(i)}(0)}{i!}\, x^i,$$

donde $p^{(i)}(x)$ es la i-ésima derivada iterada de $p(x)$:

$$p^{(0)}(x) := p(x),\ p^{(1)}(x) := p'(x),\ p^{(2)}(x) := p''(x),\ p^{(3)}(x) := p'''(x),\ \ldots$$

Revisemos nuestra tabla de los primeros números de Bernoulli. Se observan dos patrones:

- $B_k = 0$ para $k \ge 3$ impar. Esto va a ser evidente en §5 a partir de otra representación de B_k mediante una función generatriz par.
- $B_k \ne 0$ para k par, y los signos se alternan. Es posible demostrar esto directamente de modo combinatorio (véase ejercicios 5.5 y 5.6) o a partir de la fórmula

$$(-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k} = \zeta(2k) := \sum_{n\ge 1} \frac{1}{n^{2k}} > 0$$

—véase §8.

En cuanto a los valores de B_k, no se nota ningún patrón evidente. Por ejemplo, en $B_{12} = -\frac{691}{2730}$ el numerador 691 es un número primo que aparentemente no tiene nada que ver con 12. Sin embargo, si factorizamos los *denominadores* de B_k, se revelan números primos relacionados con k de alguna manera:

k:	0	1	2	4	6	8	10	12	14	16	18	20	$\cdots$
B_k:	1	$\frac{1}{2}$	$\frac{1}{2\cdot 3}$	$-\frac{1}{2\cdot 3\cdot 5}$	$\frac{1}{2\cdot 3\cdot 7}$	$-\frac{1}{2\cdot 3\cdot 5}$	$\frac{5}{2\cdot 3\cdot 11}$	$-\frac{691}{2\cdot 3\cdot 5\cdot 7\cdot 13}$	$\frac{7}{2\cdot 3}$	$-\frac{3617}{2\cdot 3\cdot 5\cdot 17}$	$\frac{43867}{2\cdot 3\cdot 7\cdot 19}$	$-\frac{174611}{2\cdot 3\cdot 5\cdot 11}$	$\cdots$

El lector puede formular su propia conjetura sobre los denominadores; más adelante vamos a ver la respuesta en el **teorema de Clausen–von Staudt** (§15).

Por supuesto, PARI/GP ya sabe calcular los números de Bernoulli. La función `bernfrac(k)` devuelve B_k:

```
? bernfrac(1)
% = -1/2
? bernfrac(10)
% = 5/66
```

Atención: PARI/GP (y también muchos libros de texto) usa otra definición de B_k según la cual $B_1 = -\frac{1}{2}$ (note el signo "$-$"). Para $k > 1$, los B_k de PARI/GP son los mismos que los nuestros. La función `bernreal(k)` calcula el valor aproximado de B_k:

```
? bernreal(4)
% = -0.033333333333333333333333333333333333333
```

2 Series formales de potencias

Toda sucesión de números a_k puede ser vista como los coeficientes de una serie de potencias $\sum_k a_k\, t^k$. A veces esta serie surge como la **serie de Taylor** de una función real o compleja f:

$$\sum_{k\geq 0} \frac{f^{(k)}(t_0)}{k!}\,(t-t_0)^k$$

(cuando las derivadas de f en t_0 existen). Las funciones que pueden ser representadas de tal manera se llaman **analíticas**. He aquí algunos ejemplos de series de Taylor:

$$\textbf{la serie geométrica } \frac{1}{1-t} = \sum_{k\geq 0} t^k \quad \text{para } |t|<1,$$

$$e^t = \sum_{k\geq 0} \frac{t^k}{k!}, \qquad \ln(1+t) = \sum_{k\geq 1} (-1)^{k+1}\,\frac{t^k}{k} \quad \text{para } |t|<1,$$

$$\operatorname{sen} t = \sum_{k\geq 0} \frac{(-1)^k}{(2k+1)!}\,t^{2k+1}, \qquad \cos t = \sum_{k\geq 0} \frac{(-1)^k}{(2k)!}\,t^{2k}.$$

En general, la serie $\sum_k a_k\, t^k$ que corresponde a una sucesión arbitraria (a_k) no tiene por qué ser convergente, aunque sería útil manipular con expresiones como "$\sum_k a_k\, t^k$" de manera puramente formal, como en efecto hacían los matemáticos de la época de Euler, cuando todavía no había una base rigurosa de análisis.

2.1. Definición. Sea R un anillo conmutativo. Una **serie formal de potencias** en variable t con coeficientes en R es una expresión

$$f(t) = \sum_{k\geq 0} a_k\, t^k = a_0 + a_1\, t + a_2\, t^2 + a_3\, t^3 + \cdots$$

donde $a_k \in R$.

Las series formales se pueden manipular de la misma manera que los polinomios. A saber, la suma de dos series se calcula término por término:

$$\left(\sum_k a_k\, t^k\right) + \left(\sum_k b_k\, t^k\right) := \sum_k (a_k + b_k)\, t^k. \tag{2.1}$$

El producto de dos series se calcula mediante la distributividad formal:

$$\begin{aligned}(a_0 + a_1\, t + a_2\, t^2 + a_3\, t^3 + \cdots)\cdot(b_0 + b_1\, t + b_2\, t^2 + b_3\, t^3 + \cdots) = {}& a_0\, b_0 + \\ & (a_0\, b_1 + a_1\, b_0)\, t + \\ & (a_0\, b_2 + a_1\, b_1 + a_2\, b_0)\, t^2 + \\ & (a_0\, b_3 + a_1\, b_2 + a_2\, b_1 + a_3\, b_0)\, t^3 + \cdots\end{aligned}$$

Es decir,

$$\left(\sum_k a_k\, t^k\right)\cdot\left(\sum_k b_k\, t^k\right) := \sum_k \left(\sum_{i+j=k} a_i\, b_j\right)\, t^k. \tag{2.2}$$

Se ve que las series formales respecto las operaciones de arriba forman un anillo conmutativo, que vamos a denotar por $R[\![t]\!]$. Los polinomios $R[t]$ forman un subanillo de $R[\![t]\!]$. En efecto, la adición y multiplicación de polinomios están definidos mediante las mismas fórmulas (2.1) y (2.2), y todo polinomio $a_n\,t^n + a_{n-1}\,t^{n-1} + \cdots a_1\,t + a_0$ puede ser visto como una serie formal de potencias

$$a_0 + a_1\,t + \cdots + a_{n-1}\,t^{n-1} + a_n\,t^n + 0\,t^{n+1} + 0\,t^{n+2} + \cdots$$

En otras palabras, un polinomio es una serie formal donde casi todos los coeficientes son nulos.

Un ejemplo muy importante de las series formales de potencias que nos va a servir mucho es el siguiente.

2.2. Definición. Si $\mathbb{Q} \subset R$, entonces la **función exponencial formal** es la serie en $R[\![t]\!]$ definida como

$$e^t := \sum_{k\geq 0} \frac{t^k}{k!}.$$

2.3. Observación. *Si R es un dominio de integridad ($a \cdot b \neq 0$ para $a, b \neq 0$), entonces $R[\![t]\!]$ es también un dominio de integridad ($f(t) \cdot g(t) \neq 0$ para $f(t), g(t) \neq 0$).*

Demostración. Sean $f(t) = \sum_{k\geq 0} a_k\,t^k$ y $g(t) = \sum_{k\geq 0} b_k\,t^k$ dos series de potencias no nulas. Sea a_i el primer coeficiente no nulo de $f(t)$ y sea b_j el primer coeficiente no nulo en $g(t)$. El coeficiente de t^{i+j} en $f(t)\cdot g(t)$ es

$$a_0\,b_{i+j} + a_1\,b_{i+j-1} + \cdots + a_i\,b_j + a_{i+1}\,b_{j-1} + \cdots + a_{i+j}\,b_0,$$

donde por nuestra elección de a_i y b_j todos los términos son nulos excepto $a_i\,b_j$, que no es nulo porque $a_i \neq 0$, $b_j \neq 0$. ∎

A partir de ahora vamos a suponer que R es un dominio de integridad.

2.4. Observación. *Una serie $f(t) = \sum_{k\geq 0} a_k\,t^k \in \mathbb{Q}[\![t]\!]$ es invertible si y solamente si $a_0 =$ "$f(0)$" es invertible.*

Note que, en general, sumas infinitas en R no están definidas, así que no se puede evaluar $f(t)$ en un elemento de R; es posible solo en análisis, donde hay nociones de convergencia. Sin embargo, $f(0)$ sí tiene sentido, y es el término constante de $f(t)$.

Demostración. Estamos buscando otra serie $g(t) = \sum_{k\geq 0} b_k\,t^k \in R[\![t]\!]$ tal que $f(t)\cdot g(t) = 1$, es decir,

$$\begin{aligned}
a_0\,b_0 &= 1,\\
a_0\,b_1 + a_1\,b_0 &= 0,\\
a_0\,b_2 + a_1\,b_1 + a_2\,b_0 &= 0,\\
&\vdots\\
\sum_{0\leq i\leq k} a_i\,b_{k-i} &= 0 \quad (k \geq 1)
\end{aligned}$$

De la primera ecuación se ve que a_0 tiene que ser invertible. En este caso, podemos calcular b_k sucesivamente:

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_1 &= -a_0^{-1}\,(a_1\,b_0), \\ b_2 &= -a_0^{-1}\,(a_1\,b_1 + a_2\,b_0), \\ &\vdots \\ b_k &= -a_0^{-1} \sum_{1\le i\le k} a_i\,b_{k-i}. \end{aligned}$$

■

2.5. Ejemplo. Tenemos

$$\begin{aligned} (1-t)\cdot(1+t+t^2+t^3+t^4+\cdots) &= (1+t+t^2+t^3+t^4+\cdots) - (t+t^2+t^3+t^4+t^5+\cdots) = 1, \\ (1+t)\cdot(1-t+t^2-t^3+t^4-\cdots) &= (1-t+t^2-t^3+t^4-\cdots) + (t-t^2+t^3-t^4+t^5-\cdots) = 1. \end{aligned}$$

Es un análogo de la serie geométrica $\frac{1}{1-t} = \sum_{k\ge 0} t^k$, que en análisis tiene sentido para $|t| < 1$. En nuestro caso, t es una variable formal. ▲

Si $R = k$ es un cuerpo, una serie

$$f(t) = a_0 + a_1\,t + a_2\,t^2 + a_3\,t^3 + \cdots$$

tal que $a_0 = 0$ no es invertible en $k[\![t]\!]$. Para resolver este problema, podemos introducir potencias negativas de t y escribir

$$f(t) = t^{-n}\,(a_n + a_{n+1}\,t + a_{n+2}\,t^2 + a_{n+3}\,t^3 + \cdots),$$

donde a_n es el primer coeficiente no nulo en $f(t)$. Aquí la serie entre paréntesis es invertible en $k[\![t]\!]$. Para que tenga sentido el término "t^{-n}", podemos introducir la siguiente generalización.

2.6. Definición. Una **serie formal de Laurent**[*] es una serie formal con un número finito de potencias negativas:

$$f(t) = \sum_{k\ge -N} a_k\,t^k \quad \text{para algún } N \in \mathbb{N}.$$

Para las series de Laurent también tienen sentido adición y multiplicación, definidas mediante las mismas fórmulas (2.1) y (2.2), y toda serie puede ser vista como una serie de Laurent con coeficientes negativos nulos. El anillo de las series de Laurent se denota por $R((t))$.

Tenemos las siguientes generalizaciones de los resultados de arriba:

1) Si R es un dominio de integridad, entonces $R((t))$ es también un dominio de integridad (la demostración es la misma).

2) Una serie de Laurent $f(t) \in R((t))$ es invertible si y solamente si su primer coeficiente no nulo es invertible en R. En particular, si $R = k$ es un cuerpo, todas las series de Laurent no nulas son invertibles, y se ve que $k((t))$ es el cuerpo de fracciones de $k[\![t]\!]$.

[*] Pierre Alphonse Laurent (1813–1854), un matemático y oficial militar francés.

2.7. Ejemplo. La serie $t + t^2 + t^3 + \cdots$ es invertible como serie de Laurent:

$$(t^{-1} - 1)\,(t + t^2 + t^3 + \cdots) = (1 + t + t^2 + \cdots) - (t + t^2 + t^3 + \cdots) = 1.$$

▲

PARI/GP puede trabajar con series de potencias. Para indicar que los términos de grado $\geq n$ están omitidos, se escribe "`+ O(t^n)`":

```
? 1/(1-t + O(t^10))
% = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + O(t^10)

? (t + 2*t^2 + 3*t^3 + 4*t^4 + 5*t^5 + O (t^6))^2
% = t^2 + 4*t^3 + 10*t^4 + 20*t^5 + 35*t^6 + O(t^7)
```

Series de Laurent:

```
? 1/(t + t^2 + t^3 + t^4 + t^5 + t^6 + O (t^7))
% = t^-1 - 1 + O(t^5)
```

PARI/GP conoce la exponencial formal:

```
? exp (t)
% = 1 + t + 1/2*t^2 + 1/6*t^3 + 1/24*t^4 + 1/120*t^5 + 1/720*t^6 +
     1/5040*t^7 + 1/40320*t^8 + 1/362880*t^9 + 1/3628800*t^10 +
     1/39916800*t^11 + 1/479001600*t^12 + 1/6227020800*t^13 +
     1/87178291200*t^14 + 1/1307674368000*t^15 + 1/20922789888000*t^16 +
     O(t^17)
```

El número de términos se puede cambiar con el parámetro `seriesprecision`:

```
? default (seriesprecision, 6)
? exp (t)
% = 1 + t + 1/2*t^2 + 1/6*t^3 + 1/24*t^4 + 1/120*t^5 + 1/720*t^6 + O(t^7)
```

2.8. Definición. Dadas dos series de potencias $f(t) = \sum_{k\geq 0} a_k\, t^k$ y $g(t) = \sum_{k\geq 0} b_k\, t^k$, si $g(0) = b_0 = 0$, entonces la **composición** $(f \circ g)(t)$ (**sustitución de** g **en** f) es la serie

$$(f \circ g)(t) := f(g(t)) := \sum_{k\geq 0} a_k\, g(t)^k.$$

Ya que $b_0 = 0$, toda potencia $g(t)^k$ no tiene términos de grado $< k$, así que la suma infinita tiene sentido.

2.9. Ejemplo. Si $f(t)$ es una serie formal tal que $f(0) = 0$, entonces

$$\frac{1}{1 - f(t)} = 1 + f(t) + f(t)^2 + f(t)^3 + f(t)^4 + \cdots,$$
$$\frac{1}{1 + f(t)} = 1 - f(t) + f(t)^2 - f(t)^3 + f(t)^4 - \cdots$$

—es una generalización de la serie geométrica. ▲

2.10. Ejemplo. Podemos "evaluar" e^t en $-t$. El resultado de la sustitución es la serie formal

$$e^{-t} = \sum_{k\geq 0} (-1)^k \frac{t^k}{k!}.$$

En general, podemos componer e^t con toda $f(t)$ tal que $f(0) = 0$. Tenemos la identidad habitual

$$e^{f(t)+g(t)} = e^{f(t)} \cdot e^{g(t)}.$$

En efecto,

$$\begin{aligned} e^{f(t)} \cdot e^{g(t)} &= \left(\sum_{i\geq 0} \frac{f(t)^i}{i!}\right) \cdot \left(\sum_{j\geq 0} \frac{g(t)^j}{j!}\right) \\ &= \sum_{k\geq 0} \sum_{i+j=k} \frac{k!}{k!} \frac{f(t)^i}{i!} \frac{g(t)^j}{j!} \\ &= \sum_{k\geq 0} \frac{1}{k!} \sum_{i\geq 0} \binom{k}{i} f(t)^i \, g(t)^{k-i} \\ &= \sum_{k\geq 0} \frac{(f(t)+g(t))^k}{k!} = e^{f(t)+g(t)}. \end{aligned}$$

▲

3 Derivadas formales

3.1. Definición. La **derivada formal** de una serie formal de potencias $f(t) = \sum_{k\geq 0} a_k \, t^k \in R[\![t]\!]$ está definida por

$$f'(t) := \sum_{k\geq 1} k \, a_k \, t^{k-1}.$$

3.2. Ejemplo.

$$(e^t)' = \left(\sum_{k\geq 0} \frac{t^k}{k!}\right)' = \sum_{k\geq 1} k \, \frac{t^{k-1}}{k!} = \sum_{k\geq 1} \frac{t^{k-1}}{(k-1)!} = e^t.$$

▲

3.3. Observación (Serie de Taylor formal). *Para las derivadas iteradas de $f(t) = \sum_{k\geq 0} a_k \, t^k \in R[\![t]\!]$ se tiene $f^{(k)}(0) = k! \, a_k$, lo que nos da*

$$f(t) = \sum_{k\geq 0} \frac{f^{(k)}(0)}{k!} \, t^k,$$

cuando $\mathbb{Q} \subset R$.

Demostración. Se ve inmediatamente de las definiciones. ■

3.4. Observación. *Para $f(t), g(t) \in R[\![t]\!]$ se tiene*

$$(f(t)+g(t))' = f'(t) + g'(t).$$

Demostración. Evidente de la definición. ■

3.5. Observación (Regla de Leibniz). *Para $f(t), g(t) \in R[\![t]\!]$ se tiene*

$$(f(t)\cdot g(t))' = f'(t)\cdot g(t) + f(t)\cdot g'(t).$$

Demostración. Para $f(t) = \sum_{k\geq 0} a_k\, t^k$ y $g(t) = \sum_{k\geq 0} b_k\, t^k$

$$\begin{aligned}
\left(\left(\sum_{k\geq 0} a_k\, t^k\right)\cdot\left(\sum_{k\geq 0} b_k\, t^k\right)\right)' &= \left(\sum_{k\geq 0}\left(\sum_{0\leq i\leq k} a_i\, b_{k-i}\right) t^k\right)' \\
&= \sum_{k\geq 1} k\left(\sum_{0\leq i\leq k} a_i\, b_{k-i}\right) t^{k-1} \\
&= \sum_{k\geq 1}\left(\sum_{0\leq i\leq k} i\, a_i\, b_{k-i} + \sum_{0\leq i\leq k}(k-i)\, a_i\, b_{k-i}\right) t^{k-1} \\
&= \sum_{k\geq 1}\left(\sum_{0\leq i\leq k} i\, a_i\, b_{k-i}\right) t^{k-1} + \sum_{k\geq 1}\left(\sum_{0\leq i\leq k-1} a_i\,(k-i)\, b_{k-i}\right) t^{k-1} \\
&= f'(t)\cdot g(t) + f(t)\cdot g'(t).
\end{aligned}$$

■

3.6. Ejercicio. *Demuestre que para $f(t), g(t) \in R((t))$ se tiene*

$$\left(\frac{f(t)}{g(t)}\right)' = \frac{f'(t)\cdot g(t) - f(t)\cdot g'(t)}{g(t)^2}.$$

3.7. Corolario. *Para $f(t) \in R[\![t]\!]$ se tiene*

$$(f(t)^k)' = k\, f(t)'\, f(t)^{k-1}.$$

Demostración. Por inducción, usando la regla de Leibniz. ■

3.8. Observación (Regla de la cadena). *Sean $f(t), g(t) \in R[\![t]\!]$ dos series de potencias formales tales que $g(0) = 0$. Entonces para la composición se tiene*

$$(f(g(t)))' = f'(g(t))\cdot g'(t).$$

Demostración. Si $f(t) = \sum_{k\geq 0} a_k\, t^k$, entonces

$$(f(g(t)))' = \sum_{k\geq 1} k\, a_k\, g'(t)\,(g(t))^{k-1} = \left(\sum_{k\geq 1} k\, a_k\,(g(t))^{k-1}\right) g'(t) = f'(g(t))\cdot g'(t).$$

■

En PARI/GP:

```
? default (seriesprecision, 6)

? deriv (t*exp(t), t)
% = 1 + 2*t + 3/2*t^2 + 2/3*t^3 + 5/24*t^4 + 1/20*t^5 + 7/720*t^6 + O(t^7)
```

Para resumir, las derivadas formales se comportan como las derivadas habituales: son lineales, cumplen la regla de Leibniz y la regla de la cadena.

4 Logaritmo formal

4.1. Definición. Si $\mathbb{Q} \subset R$, el **logaritmo formal** es la serie en $R[\![t]\!]$ definida por

$$\ln(1+t) := \sum_{k\geq 1} (-1)^{k+1} \frac{t^k}{k}.$$

Observamos que la derivada formal de $\ln(1+t)$ es precisamente lo que se espera del logaritmo:

$$(\ln(1+t))' = \frac{1}{1+t} = 1 - t + t^2 - t^3 + t^4 - t^5 + \cdots.$$

En PARI/GP:

```
? log (1+t)
% = t - 1/2*t^2 + 1/3*t^3 - 1/4*t^4 + 1/5*t^5 + O(t^6)
```

4.2. Teorema. *Tenemos*

$$\ln(1+(e^t-1)) = t, \quad e^{\ln(1+t)} = 1+t,$$

en el sentido de sustitución de una serie formal en otra.

Las identidades de 4.2 nos dan un ejemplo de series inversas respecto a la composición:

4.3. Proposición. *Para una serie de potencias formal $f(t) = \sum_{k\geq 0} a_k\, t^k$ existe otra serie $g(t)$ tal que $g(0) = 0$ y $f(g(t)) = t$ si y solamente si $a_0 = 0$ y a_1 es invertible. En este caso la serie $g(t)$ es única, y además se tiene $g(f(t)) = t$. Es decir, f y g son mutuamente inversas respecto a la composición.*

Demostración. La condición sobre a_0 y a_1 es necesaria: si existe $g(t) = \sum_{k\geq 0} b_k\, t^k$ con $b_0 = 0$ tal que $f(g(t)) = \sum_{k\geq 0} a_k\, g(t)^k = t$, entonces $a_0 = 0$ y $a_1\, b_1 = 1$.

Ahora sea $f(t)$ una serie con $a_0 = 0$ y a_1 invertible. Tenemos que encontrar una serie $g(t) = \sum_{k\geq 0} b_k\, t^k$ con $b_0 = 0$ tal que $f(g(t)) = t$. La última identidad implica que necesitamos poner $b_1 := a_1^{-1}$. Luego, para $k \geq 2$, el coeficiente de t^k en $f(g(t))$ es igual al coeficiente de t^k en la suma

$$a_1\, g(t) + a_2\, g(t)^2 + \cdots + a_k\, g(t)^k$$

(ya que $g(0) = 0$, en las potencias $g(t)^{k+1}, g(t)^{k+2}, \ldots$ ya no hay términos de grado k). Pero este coeficiente tiene que ser nulo, lo que nos da las ecuaciones

$$a_1\, b_k + (\text{algún polinomio en } a_2, a_3, \ldots, a_k, b_1, b_2, \ldots, b_{k-1}) = 0.$$

Puesto que $a_1 \neq 0$, estas ecuaciones por inducción definen *de modo único* todos los coeficientes $b_2, b_3, b_4, \ldots$ Esto demuestra que $g(t)$ existe y es único.

Para ver que también se tiene $g(f(t)) = t$, notamos que en $g(t)$ también $b_0 = 0$ y b_1 es invertible, entonces existe $h(t)$ tal que $g(h(t)) = t$. Luego,

$$\begin{aligned} t &= f(g(t)), \\ h(t) &= f(g(h(t))) = f(t), \\ g(h(t)) &= g(f(t)) = t. \end{aligned}$$

■

En PARI/GP, la serie inversa respecto a la composición puede ser calculada por la función `serreverse`:

```
? serreverse (exp (t) - 1)
% = t - 1/2*t^2 + 1/3*t^3 - 1/4*t^4 + 1/5*t^5 - 1/6*t^6 + O(t^7)
```

Demostración de 4.2. La primera tentación es calcular directamente los coeficientes de las series

$$\ln(1+(e^t-1)) \quad \text{y} \quad e^{\ln(1+t)},$$

pero esto no es tan fácil. Por ejemplo, las potencias de la serie e^t-1 tienen como coeficientes los números de Stirling:

$$\frac{(e^t-1)^\ell}{\ell!} = \sum_{k\geq\ell} \left\{ {k \atop \ell} \right\} \frac{t^k}{k!};$$

los vamos a necesitar de todas maneras más adelante y §13 está dedicado a las definiciones y las propiedades básicas de $\left\{ {k \atop \ell} \right\}$. Para el logaritmo también hay una fórmula parecida con otros números de Stirling:

$$\frac{\ln(1+t)^\ell}{\ell!} = (-1)^\ell \sum_{k\geq\ell} (-1)^k \left[{k \atop \ell} \right] \frac{t^k}{k!}.$$

Vamos a establecer estas identidades en 14.1 y 14.2. Afortunadamente, por el momento se puede evitar esta pesadilla combinatoria. Primero notemos que gracias a 4.3, será suficiente demostrar que por ejemplo,

$$e^{\ln(1+t)} = 1+t,$$

y $\ln(1+(e^t-1)) = t$ se sigue automáticamente. Gracias a la serie de Taylor 3.3, podemos simplemente verificar que

$$\begin{aligned} e^{\ln(1+0)} &= 1, \\ (e^{\ln(1+t)})'(0) &= 1, \\ (e^{\ln(1+t)})''(0) &= 0, \\ (e^{\ln(1+t)})'''(0) &= 0, \\ &\dots \end{aligned}$$

En efecto, $\ln(1+0) = 0$ y $e^0 = 1$. Luego, por la regla de la cadena 3.8,

$$(e^{\ln(1+t)})' = e^{\ln(1+t)} \frac{1}{1+t},$$

y así $(e^{\ln(1+t)})'(0) = 1$. La segunda derivada nos da

$$\begin{aligned} (e^{\ln(1+t)})'' &= \left(e^{\ln(1+t)} \frac{1}{1+t} \right)' \\ &= (e^{\ln(1+t)})' \frac{1}{1+t} - e^{\ln(1+t)} \frac{1}{(1+t)^2} \\ &= e^{\ln(1+t)} \frac{1}{1+t} \frac{1}{1+t} - e^{\ln(1+t)} \frac{1}{(1+t)^2} = 0. \end{aligned}$$

■

5 La función generatriz para B_k

5.1. Teorema. *Los números de Bernoulli pueden ser definidos por*

$$\frac{t\,e^t}{e^t-1} = \sum_{k\geq 0} B_k \frac{t^k}{k!}.$$

Aunque se puede pensar en esta identidad como en la serie de Taylor para $\frac{t\,e^t}{e^t-1}$ en un entorno de 0, para nosotros esto significa nada más que el cociente de series formales $\frac{t\,e^t}{e^t-1}$ en $\mathbb{Q}((t))$ es igual a la serie formal $\sum_{k\geq 0} B_k \frac{t^k}{k!}$.

Demostración. Tenemos que ver que la identidad

$$\left(\sum_{k\geq 0} B_k \frac{t^k}{k!}\right)(e^t-1) = t\,e^t.$$

define los números de Bernoulli. Calculemos el producto al lado izquierdo:

$$\begin{aligned}
\left(\sum_{k\geq 0} B_k \frac{t^k}{k!}\right)(e^t-1) &= \left(\sum_{k\geq 0} B_k \frac{t^k}{k!}\right)\left(\sum_{k\geq 1} \frac{t^k}{k!}\right) \\
&= \sum_{k\geq 1}\left(\sum_{0\leq i\leq k-1} \frac{B_i}{i!}\frac{1}{(k-i)!}\right) t^k \\
&= \sum_{k\geq 1}\left(\sum_{0\leq i\leq k-1} \frac{B_i}{i!}\frac{k!}{(k-i)!}\right) \frac{t^k}{k!} \\
&= \sum_{k\geq 1}\left(\sum_{0\leq i\leq k-1} \binom{k}{i} B_i\right) \frac{t^k}{k!} \\
&\overset{???}{=} \sum_{k\geq 1} \frac{t^k}{(k-1)!} = t\,e^t.
\end{aligned}$$

La última igualdad se cumple si y solamente si

$$\sum_{0\leq i\leq k-1} \binom{k}{i} B_i = k.$$

Como hemos visto en 1.2, esta identidad define los números de Bernoulli. ■

5.2. Ejemplo. Calculemos algunos términos de la serie formal $\frac{t\,e^t}{e^t-1}$. Tenemos

$$e^t - 1 = t + \frac{t^2}{2} + \frac{t^3}{6} + \frac{t^4}{24} + \frac{t^5}{120} + \cdots = t\left(1 + \frac{t}{2!} + \frac{t^2}{3!} + \frac{t^3}{4!} + \frac{t^4}{5!} + \cdots\right).$$

Luego,

$$\frac{t}{e^t-1} = \frac{1}{1 + \frac{t}{2!} + \frac{t^2}{3!} + \frac{t^3}{4!} + \frac{t^4}{5!} + \cdots}$$

Podemos calcular la última serie usando nuestra observación en 2.9. Tenemos

$$1-\left(\frac{t}{2!}+\frac{t^2}{3!}+\frac{t^3}{4!}+\frac{t^4}{5!}+\cdots\right)+\left(\frac{t}{2!}+\frac{t^2}{3!}+\frac{t^3}{4!}+\frac{t^4}{5!}+\cdots\right)^2$$
$$-\left(\frac{t}{2!}+\frac{t^2}{3!}+\frac{t^3}{4!}+\frac{t^4}{5!}+\cdots\right)^3+\left(\frac{t}{2!}+\frac{t^2}{3!}+\frac{t^3}{4!}+\frac{t^4}{5!}+\cdots\right)^4-\cdots$$
$$=1-\left(\frac{t}{2}+\frac{t^2}{6}+\frac{t^3}{24}+\frac{t^4}{120}+\cdots\right)+\left(\frac{t^2}{4}+\frac{t^3}{6}+\frac{5\,t^4}{72}+\cdots\right)-\left(\frac{t^3}{8}+\frac{t^4}{8}+\cdots\right)+\left(\frac{t^4}{16}+\cdots\right)-\cdots$$
$$=1-\frac{t}{2}+\frac{t^2}{12}+0\cdot t^3-\frac{t^4}{720}+\cdots$$

Multiplicando las seres, se obtiene

$$\frac{t\,e^t}{e^t-1}=\left(1+t+\frac{t^2}{2!}+\frac{t^3}{3!}+\frac{t^4}{4!}+\cdots\right)\cdot\left(1-\frac{t}{2}+\frac{t^2}{12}+0\cdot t^3-\frac{t^4}{720}+\cdots\right)=1+\frac{t}{2}+\frac{t^2}{12}-\frac{t^4}{720}+\cdots$$

y entonces

$$B_0=1,\quad B_1=\frac{1}{2},\quad B_2=2!\cdot\frac{1}{12}=\frac{1}{6},\quad B_3=0,\quad B_4=-4!\cdot\frac{1}{720}=-\frac{1}{30}.$$

▲

Por supuesto, el último ejemplo es un poco masoquista: todo esto se puede hacer en PARI/GP.

```
? ser = (t*exp(t))/(exp(t)-1)
% = 1 + 1/2*t + 1/12*t^2 - 1/720*t^4 + 1/30240*t^6 - 1/1209600*t^8 + 1/47900160*t^10
- 691/1307674368000*t^12 + 1/74724249600*t^14 + O(t^16)

? vector (11,k, polcoeff(ser,(k-1),t)*(k-1)!)
% = [1, 1/2, 1/6, 0, -1/30, 0, 1/42, 0, -1/30, 0, 5/66]
```

En muchos libros (y también en PARI/GP) se usa otra convención para los números de Bernoulli según la cual $B_1=-\frac{1}{2}$. En este caso la función generatriz es $\frac{t\,e^t}{e^t-1}-t=\frac{t}{e^t-1}$.

5.3. Ejemplo. La fórmula $\frac{t\,e^t}{e^t-1}=\sum_{k\geq 0}\frac{B_k}{k!}\,t^k$ nos permite demostrar que $B_k=0$ para $k\geq 3$ impar. En efecto, para ignorar el caso excepcional $B_1=\frac{1}{2}$, examinemos la función

$$f(t):=\frac{t\,e^t}{e^t-1}-\frac{t}{2}=B_0+\frac{B_2}{2!}\,t^2+\frac{B_3}{3!}\,t^3+\frac{B_4}{4!}\,t^4+\frac{B_5}{5!}\,t^5+\cdots$$

Tenemos

$$f(t)=\frac{t\,e^t}{e^t-1}-\frac{t}{2}=\frac{t\,(e^t-1+1)}{e^t-1}-\frac{t}{2}=\frac{t}{e^t-1}+\frac{t}{2}.$$

Luego,

$$f(-t)=\frac{(-t)\,e^{-t}}{e^{-t}-1}-\frac{(-t)}{2}=\frac{t}{e^t-1}+\frac{t}{2}.$$

Entonces, $f(t)=f(-t)$, lo que implica que los coeficientes impares de $f(t)$ son nulos. ▲

Los números de Bernoulli también surgen en otras series. Por ejemplo, tenemos la siguiente

5.4. Proposición.

$$t\,\cot(t) = 1 + \sum_{k\geq 1} (-1)^k\, 2^{2k}\, \frac{B_{2k}}{(2k)!}\, t^{2k}.$$

Esto ya tiene que ser interpretado analíticamente. Las series con números de Bernoulli para varias funciones como $\tan(t)$, $\cot(t)$, $\tanh(t)$, $\coth(t)$ fueron descubiertas por Euler.

Demostración. Se tiene

$$\cos(t) = \frac{e^{it} + e^{-it}}{2}, \quad \operatorname{sen}(t) = \frac{e^{it} - e^{-it}}{2i}.$$

Luego,

$$\begin{aligned} t\,\cot(t) = t\,\frac{\cos(t)}{\operatorname{sen}(t)} &= it\,\frac{e^{it} + e^{-it}}{e^{it} - e^{-it}} = it\,\frac{e^{2it} + 1}{e^{2it} - 1} = -it + \frac{2it\, e^{2it}}{e^{2it} - 1} \\ &= -it + \sum_{k\geq 0} \frac{B_k \cdot (2it)^k}{k!} = 1 + \sum_{k\geq 1} (-1)^k\, 2^{2k}\, \frac{B_{2k}}{(2k)!}\, t^{2k}. \end{aligned}$$

■

5.5. Ejercicio (Euler). *Demuestre la identidad*

$$(2k+1)\, B_{2k} = -\sum_{1\leq \ell \leq k-1} \binom{2k}{2\ell} B_{2\ell}\, B_{2\,(k-\ell)} \quad \text{para } k \geq 2.$$

Por ejemplo, para $k = 3$ tenemos

$$-7\, \underbrace{B_6}_{=\frac{1}{42}} = \underbrace{\binom{6}{2} B_2\, B_4}_{=15\cdot\frac{1}{6}\cdot\left(-\frac{1}{30}\right)} + \underbrace{\binom{6}{4} B_4\, B_2}_{=15\cdot\left(-\frac{1}{30}\right)\cdot\frac{1}{6}}.$$

Indicación: considere la función generatriz para los números pares $f(t) := \frac{t\,e^t}{e^t-1} - \frac{t}{2} = \sum_{k\geq 0} \frac{B_{2k}}{(2k)!}\, t^{2k}$. Demuestre la identidad con la derivada formal $f(t) - t\,f(t)' = f(t)^2 - \frac{t^2}{4}$; sustituya $f(t)$ por $\sum_{k\geq 0} \frac{B_{2k}}{(2k)!}\, t^{2k}$ y compare los coeficientes de t^{2k}.

5.6. Ejercicio. *Demuestre por inducción que $(-1)^{k+1}\, B_{2k} > 0$ para todo $k \geq 1$. Véase §8 para la explicación. Indicación: use el ejercicio anterior.*

6 Polinomios de Bernoulli

Hay varios modos de definir los polinomios de Bernoulli; el más común es por una función generatriz. Vamos a necesitar las series de potencias formales en dos variables:

$$\sum_{k,\ell\geq 0} a_{k,\ell}\, t^k\, x^\ell,$$

respecto a la suma término por término y multiplicación que extiende la multiplicación de polinomios en dos variables. Tenemos la serie formal $\frac{t}{e^t-1} \in \mathbb{Q}[\![t]\!] \subset \mathbb{Q}[\![t,x]\!]$ y podemos multiplicarla por la serie

$$e^{tx} := \sum_{k\geq 0} \frac{t^k\, x^k}{k!} \in \mathbb{Q}[\![t,x]\!].$$

Un momento de reflexión demuestra que el resultado es de la forma

$$\frac{t\,e^{tx}}{e^t-1} := \sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!}, \tag{6.1}$$

donde $B_k(x)$ son algunos *polinomios* en x.

6.1. Definición. El **polinomio de Bernoulli** $B_k(x)$ es el polinomio definido por (6.1).

6.2. Ejemplo. Vamos a ver un poco más adelante cómo calcular los polinomios $B_k(x)$; por el momento podemos obtener algunos de los primeros. Como hemos calculado en 5.2,

$$\frac{t}{e^t-1} = 1 - \frac{t}{2} + \frac{t^2}{12} - \frac{t^4}{720} + \cdots$$

Luego,

$$\frac{t}{e^t-1}\,e^{tx} = \left(1-\frac{t}{2}+\frac{t^2}{12}-\cdots\right)\left(1+t\,x+\frac{t^2\,x^2}{2}+\cdots\right) = 1+\left(x-\frac{1}{2}\right)\,t+\left(\frac{x^2}{2}-\frac{x}{2}+\frac{1}{12}\right)\,t^2+\cdots$$

de donde

$$B_0(x)=1,\quad B_1(x)=x-\frac{1}{2},\quad B_2(x)=x^2-x+\frac{1}{6}.$$

▲

6.3. Observación. *Para todo $k \geq 0$,*

$$B_k(1) = B_k$$

es el k-ésimo número de Bernoulli.

Demostración. Comparando (6.1) con la función generatriz $\frac{t\,e^t}{e^t-1} = \sum_{k\geq 0} B_k\,\frac{t^k}{k!}$. ■

Resulta que el término constante de $B_k(x)$ es también igual a B_k:

6.4. Observación. *Para todo $k \geq 0$*

$$B_k(x+1) - B_k(x) = k\,x^{k-1}. \tag{6.2}$$

En particular, para $x = 0$ y $k \neq 1$ tenemos

$$B_k(1) = B_k(0) = B_k.$$

Demostración. Tenemos la identidad

$$\frac{t\,e^{(x+1)\,t}}{e^t-1} - \frac{t\,e^{t\,x}}{e^t-1} = t\,e^{t\,x},$$

de donde

$$\sum_{k\geq 0}\left(B_k(x+1)-B_k(x)\right)\frac{t^k}{k!} = \sum_{k\geq 0}\frac{x^k}{k!}\,t^{k+1}.$$

Comparando los coeficientes de t^k, se obtiene (6.2). ■

Note que para $k = 1$ tenemos $B_1(0) = -\frac{1}{2}$ y $B_1(1) = +\frac{1}{2}$.

6.5. Observación. *Para todo $k \geq 0$*

$$B_k(1-x) = (-1)^k B_k(x).$$

(En particular, para $x = 0$ tenemos $B_k = (-1)^k B_k$ para $k \geq 3$, lo que implica que $B_k = 0$ para $k \geq 3$ impar, como ya hemos visto.)

Demostración. Usando funciones generatrices,

$$\sum_{k\geq 0} B_k(1-x)\,\frac{t^k}{k!} = \frac{t\,e^{(1-x)\,t}}{e^t-1} = \frac{(-t)\,e^{x\,(-t)}}{e^{-t}-1} = \sum_{k\geq 0}(-1)^k\,B_k(x)\,\frac{t^k}{k!}.$$

■

Los polinomios de Bernoulli pueden ser expresados en términos de los números de Bernoulli:

6.6. Proposición.

$$B_k(x) = \sum_{0\leq i\leq k}(-1)^i \binom{k}{i} B_i\,x^{k-i}.$$

Demostración. Calculemos el producto de series de potencias

$$\frac{t}{e^t-1}\cdot e^{tx}.$$

Tenemos

$$\frac{t}{e^t-1} = \frac{(-t)\,e^{-t}}{e^{-t}-1} = \sum_{k\geq 0}(-1)^k\,B_k\,\frac{t^k}{k!}, \quad e^{tx} = \sum_{k\geq 0}\frac{(tx)^k}{k!}.$$

Luego,

$$\begin{aligned}\left(\sum_{k\geq 0}(-1)^k\,B_k\,\frac{t^k}{k!}\right)\cdot\left(\sum_{k\geq 0}\frac{(tx)^k}{k!}\right) &= \sum_{k\geq 0}\left(\sum_{0\leq i\leq k}(-1)^i\,\frac{1}{i!\,(k-i)!}\,B_i\,x^{k-i}\right)t^k\\ &= \sum_{k\geq 0}\left(\sum_{0\leq i\leq k}(-1)^i\binom{k}{i}B_i\,x^{k-i}\right)\frac{t^k}{k!}.\end{aligned}$$

■

6.7. Proposición. *Para todo $k \geq 1$ se tiene*

$$B_k'(x) = k\,B_{k-1}(x), \quad \int_0^1 B_k(x)\,dx = 0.$$

Demostración. Hay varios modos de verificar esto. Se puede usar la expresión de 6.6. También podemos tomar las derivadas formales de la identidad

$$\frac{t\,e^{tx}}{e^t-1} = \sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!}.$$

Se obtiene

$$\frac{\partial}{\partial x}\left(\frac{t\,e^{tx}}{e^t-1}\right) = \frac{t\cdot t\,e^{tx}}{e^t-1} = t\sum_{k\geq 0}B_k(x)\,\frac{t^k}{k!} = \sum_{k\geq 1}B_{k-1}(x)\,\frac{t^k}{(k-1)!} = \sum_{k\geq 0}B_k'(x)\,\frac{t^k}{k!}.$$

Luego, para ver que $\int_0^1 B_k(x)\,dx = 0$, es suficiente observar que $\int B_k(x)\,dx = \frac{1}{k+1}\,B_{k+1}(x) + C$, donde $B_{k+1}(0) = B_{k+1}(1)$. ■

Esto nos da otra definición de los polinomios de Bernoulli:

6.8. Definición alternativa. Los polinomios $B_k(x)$ están definidos por

$$B_0(x) := 1$$

y

$$B_k'(x) = k\,B_{k-1}(x), \quad \int_0^1 B_k(x)\,dx = 0 \quad \text{para } k \geq 1.$$

(En efecto, la identidad $B_k'(x) = k\,B_{k-1}(x)$ define $B_k(x)$ salvo el término constante, pero el último se recupera de la condición $\int_0^1 B_k(x)\,dx = 0$.) Recordemos que los polinomios $S_k(x)$ que hemos estudiado en §1 satisfacen la identidad

$$S_k'(x) = k\,S_{k-1}(x) + B_k.$$

Esto significa que las derivadas $S_k'(x)$ satisfacen la misma identidad que $B_k(x)$:

$$S_k''(x) = k\,S_{k-1}'(x).$$

Además, para $k \neq 1$ tenemos $B_k(0) = S_k'(0) =: B_k$, y se ve que los polinomios de Bernoulli son simplemente las derivadas de los polinomios $S_k(x)$:

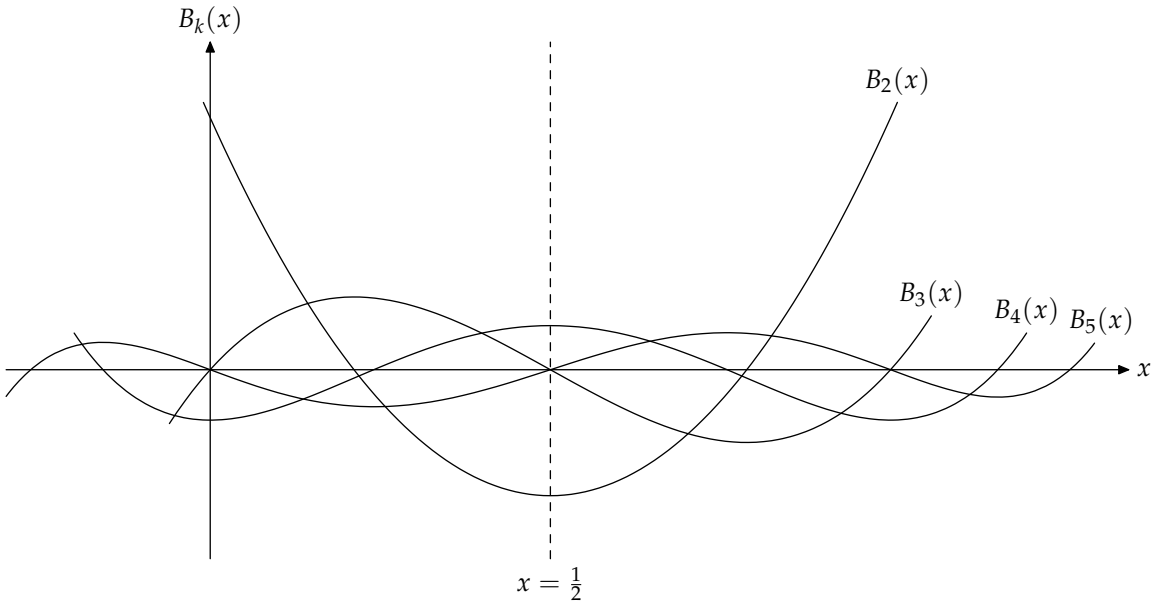
$$B_k(x) = S_k'(x), \quad \text{para } k \neq 1.$$

(El caso $k = 1$ es excepcional: $S_1(x) = \frac{1}{2}\,x^2 + \frac{1}{2}\,x$, $B_1(x) = x - \frac{1}{2}$.)

Ahora podemos compilar fácilmente una lista de los primeros polinomios de Bernoulli:

$$
\begin{aligned}
B_0(x) &= 1, \\
B_1(x) &= x - \frac{1}{2}, \\
B_2(x) &= x^2 - x + \frac{1}{6}, \\
B_3(x) &= x^3 - \frac{3}{2}\,x^2 + \frac{1}{2}\,x, \\
B_4(x) &= x^4 - 2\,x^3 + x^2 - \frac{1}{30}, \\
B_5(x) &= x^5 - \frac{5}{2}\,x^4 + \frac{5}{3}\,x^3 - \frac{1}{6}\,x, \\
B_6(x) &= x^6 - 3\,x^5 + \frac{5}{2}\,x^4 - \frac{1}{2}\,x^2 + \frac{1}{42}, \\
B_7(x) &= x^7 - \frac{7}{2}\,x^6 + \frac{7}{2}\,x^5 - \frac{7}{6}\,x^3 + \frac{1}{6}\,x, \\
B_8(x) &= x^8 - 4\,x^7 + \frac{14}{3}\,x^6 - \frac{7}{3}\,x^4 + \frac{2}{3}\,x^2 - \frac{1}{30}, \\
B_9(x) &= x^9 - \frac{9}{2}\,x^8 + 6\,x^7 - \frac{21}{5}\,x^5 + 2\,x^3 - \frac{3}{10}\,x, \\
B_{10}(x) &= x^{10} - 5\,x^9 + \frac{15}{2}\,x^8 - 7\,x^6 + 5\,x^4 - \frac{3}{2}\,x^2 + \frac{5}{66}.
\end{aligned}
$$

Podemos dibujar algunas gráficas para visualizar la relación $B_k(1-x) = (-1)^k\,B_k(x)$:



```
? Bpoly (k) = sum (i=0,k, (-1)^i * binomial(k,i) * B(i) * x^(k-i));

? vector (10,k,Bpoly(k))
% = [x - 1/2,
     x^2 - x + 1/6,
     x^3 - 3/2*x^2 + 1/2*x,
     x^4 - 2*x^3 + x^2 - 1/30,
     x^5 - 5/2*x^4 + 5/3*x^3 - 1/6*x,
     x^6 - 3*x^5 + 5/2*x^4 - 1/2*x^2 + 1/42,
     x^7 - 7/2*x^6 + 7/2*x^5 - 7/6*x^3 + 1/6*x,
     x^8 - 4*x^7 + 14/3*x^6 - 7/3*x^4 + 2/3*x^2 - 1/30,
     x^9 - 9/2*x^8 + 6*x^7 - 21/5*x^5 + 2*x^3 - 3/10*x,
     x^10 - 5*x^9 + 15/2*x^8 - 7*x^6 + 5*x^4 - 3/2*x^2 + 5/66]

? deriv (Bpoly(10),x)
% = 10*x^9 - 45*x^8 + 60*x^7 - 42*x^5 + 20*x^3 - 3*x
? 10 * Bpoly(9)
% = 10*x^9 - 45*x^8 + 60*x^7 - 42*x^5 + 20*x^3 - 3*x
```

Para comprobar los resultados, podemos directamente calcular la serie $\frac{t\,e^{tx}}{e^t-1}$:

```
? ser = t*exp (t*x) / (exp (t) - 1);
? polcoeff(ser,10,t)*10!
% = x^10 - 5*x^9 + 15/2*x^8 - 7*x^6 + 5*x^4 - 3/2*x^2 + 5/66
```

También podemos calcular las derivadas de $S_k(x)$:

```
? deriv (S(10),x)
% = x^10 + 5*x^9 + 15/2*x^8 - 7*x^6 + 5*x^4 - 3/2*x^2 + 5/66
```

En PARI/GP, la función predefinida `bernpol(k)` devuelve el polinomio de Bernoulli $B_k(x)$:

```
? bernpol(1)
% = x - 1/2
? bernpol(2)
% = x^2 - x + 1/6
? bernpol(3)
% = x^3 - 3/2*x^2 + 1/2*x
```

7 La función zeta de Riemann

7.1. Definición. La **función zeta de Riemann** está definida por la serie infinita

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots$$

7.2. Observación. *La serie de arriba es absolutamente convergente para todo* $s \in \mathbb{C}$ *tal que* $\operatorname{Re} s > 1$.

Demostración. Si $s = a + i\,b$, tenemos

$$\left|\frac{1}{n^s}\right| = \frac{1}{n^a}.$$

Podemos usar el **criterio integral de convergencia**: $\sum_{n\geq 1} \frac{1}{n^a}$ es convergente si y solamente si

$$\int_1^\infty \frac{1}{x^a}\,dx < \infty.$$

En efecto, tenemos

$$\int_1^\infty \frac{1}{x^a}\,dx = \lim_{n\to\infty} \left[\frac{x^{1-a}}{1-a}\right]_1^n = \lim_{n\to\infty} \left(\frac{n^{1-a}}{1-a} - \frac{1}{1-a}\right).$$

Este límite existe precisamente cuando $a > 1$. ■

Note que para $s = 1$ se obtiene la **serie armónica**

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

que es divergente.

Demostración (Nicolás Oresme, siglo XIV). En la serie

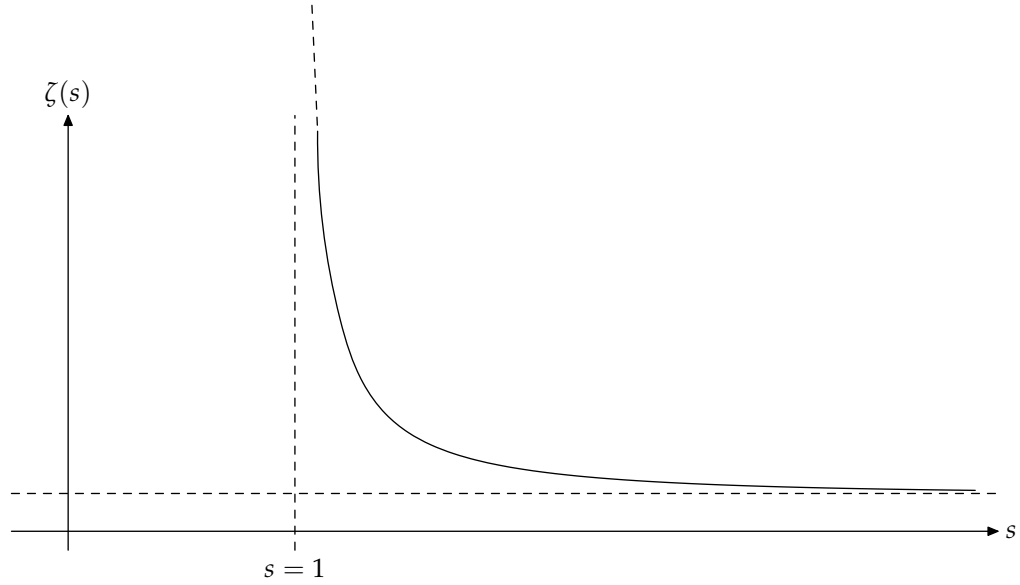
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16} + \cdots$$

reemplacemos cada término $\frac{1}{n}$ por el número máximo $\frac{1}{2^k} \leq \frac{1}{n}$. Se obtiene una serie

$$1 + \frac{1}{2} + \underbrace{\left(\frac{1}{4} + \frac{1}{4}\right)}_{=\frac{1}{2}} + \underbrace{\left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right)}_{=\frac{1}{2}} + \underbrace{\left(\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16}\right)}_{=\frac{1}{2}} + \cdots$$

que es obviamente divergente. Por tanto la serie armónica es también divergente. ■

Para $s > 1$ la función $\zeta(s)$ es monótonamente decreciente, y se tiene $\lim_{s\to\infty} \zeta(s) = 1$:



7.3. Teorema (Fórmula del producto de Euler).

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}.$$

La fórmula de arriba tiene una gran importancia en la teoría de números y fue descubierta por Euler. He aquí la demostración original, reproducida de su artículo [Eul1744]:

Si

$$x = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots, \tag{7.1}$$

entonces

$$\frac{1}{2^s}\, x = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \frac{1}{12^s} + \cdots, \tag{7.2}$$

y subtraendo (7.1) − (7.2) se obtiene

$$\frac{2^s - 1}{2^s}\, x = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots \tag{7.3}$$

Luego,

$$\left(\frac{2^s - 1}{2^s}\right) \frac{1}{3^s}\, x = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \cdots \tag{7.4}$$

y (7.3) − (7.4) nos da

$$\left(\frac{2^s-1}{2^s}\right)\left(\frac{3^s-1}{3^s}\right)x = 1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\cdots$$

Después de aplicar operaciones similares para todos los números primos, todos los términos excepto el primero se eliminan:

$$1 = \left(\frac{2^s-1}{2^s}\right)\left(\frac{3^s-1}{3^s}\right)\left(\frac{5^s-1}{5^s}\right)\left(\frac{7^s-1}{7^s}\right)\left(\frac{11^s-1}{11^s}\right)\cdots x,$$

de donde se encuentra la serie x:

$$\left(\frac{2^s}{2^s-1}\right)\left(\frac{3^s}{3^s-1}\right)\left(\frac{5^s}{5^s-1}\right)\left(\frac{7^s}{7^s-1}\right)\left(\frac{11^s}{11^s-1}\right)\cdots = x = 1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\cdots$$

Q.E.D.

Dejo al lector pensar por qué esta demostración es esencialmente correcta.

El siguiente resultado necesita más análisis de lo que conocía Euler y no lo vamos a demostrar (véase [Ahl1978, Chapter 5, §4] o cualquier libro de la teoría de números).

7.4. Hecho. *La función $\zeta(s)$ tiene prolongación analítica al plano complejo como una función meromorfa que tiene un polo simple en $s = 1$ de residuo 1. Esta prolongación analítica, que también se denota por $\zeta(s)$, satisface la* ***ecuación funcional***

$$\zeta(s) = 2^s\,\pi^{s-1}\,\operatorname{sen}\left(\frac{\pi s}{2}\right)\,\Gamma(1-s)\,\zeta(1-s). \tag{7.5}$$

Aquí $\Gamma(z) := \int_0^\infty x^{z-1}\,e^{-x}\,dx$ denota la **función gamma**. En particular, $\Gamma(n) = (n-1)!$ para $n = 1, 2, 3, 4, \ldots$

8 Los valores $\zeta(2k)$

El siguiente resultado fue descubierto por Euler y aparece en sus artículos [Eul1740], [Eul1768], etc.:

8.1. Teorema. *Para todo $k \geq 1$*

$$\zeta(2k) := 1+\frac{1}{2^{2k}}+\frac{1}{3^{2k}}+\frac{1}{4^{2k}}+\cdots = (-1)^{k+1}\,B_{2k}\,\frac{2^{2k-1}}{(2k)!}\,\pi^{2k}.$$

Es algo sorprendente: ¡los números de Bernoulli surgen del estudio de las sumas de potencias $\sum_{1\leq i\leq n} i^k$, y ahora los mismos números aparecen en sumas de potencias infinitas! Los primeros valores de $\zeta(2k)$ son entonces

$$\begin{aligned}
\zeta(2) &= \frac{\pi^2}{6} \approx 1{,}644934\ldots,\\
\zeta(4) &= \frac{\pi^4}{90} \approx 1{,}082323\ldots,\\
\zeta(6) &= \frac{\pi^6}{945} \approx 1{,}017343\ldots,\\
\zeta(8) &= \frac{\pi^8}{9450} \approx 1{,}004077\ldots,\\
\zeta(10) &= \frac{\pi^{10}}{93\,555} \approx 1{,}000994\ldots,\\
\zeta(12) &= \frac{691\,\pi^{12}}{638\,512\,875} \approx 1{,}000246\ldots
\end{aligned}$$

En particular, el cálculo de $\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots$ se conoce como el **problema de Basilea** que fue formulado por el matemático italiano Pietro Mengoli (1626–1686) en 1644. La primera solución fue encontrada por Euler en 1735.

8.2. Ejercicio. *Calcule las sumas parciales* $\sum_{1\le n\le N} \frac{1}{n^2}$ *en PARI/GP. Note que su convergencia a* $\zeta(2)$ *es bastante lenta. Esto explica un siglo de sufrimiento de los matemáticos que trataban de obtener un valor aproximado de* $\zeta(2)$*... hasta la llegada de Euler.*

8.3. Corolario. $(-1)^{k+1}\, B_{2k} > 0$ *para todo* $k \ge 1$*. Es decir,* $B_{2k} \neq 0$ *y los signos de los números de Bernoulli pares se alternan.*

Demostración.

$$(-1)^{k+1}\, B_{2k} = \frac{(2k)!\,\zeta(2k)}{2^{2k-1}\,\pi^{2k}}.$$

■

También se ve que $|B_{2k}| \xrightarrow{k\to\infty} \infty$, y que $|B_{2k}|$ crece muy rápido con k:

$$\begin{aligned}
B_2 &\approx +0{,}166667,\\
B_4 &\approx -0{,}033333,\\
B_6 &\approx +0{,}023810,\\
B_8 &\approx -0{,}033333,\\
B_{10} &\approx +0{,}075758,\\
B_{12} &\approx -0{,}253114,\\
B_{14} &\approx +1{,}166667,\\
B_{16} &\approx -7{,}092157,\\
B_{18} &\approx +54{,}971178,\\
B_{20} &\approx -529{,}124242.
\end{aligned}$$

Hay muchas demostraciones del teorema 8.1; se puede encontrar una colección en la página

http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf

Primera demostración de 8.1. Hemos visto en 5.4 la serie

$$t\,\cot(t) = 1 + \sum_{k\geq 1} (-1)^k\, 2^{2k}\, \frac{B_{2k}}{(2k)!}\, t^{2k}. \tag{8.1}$$

En el análisis complejo se deduce otra serie [Ahl1978, Chapter 5, §2]

$$\cot(t) = \sum_{n\in\mathbb{Z}} \frac{1}{t-\pi n},$$

que corresponde a la "descomposición en fracciones simples" de una función meromorfa: $\cot(t)$ tiene polos simples en $t = \pi n$ para todo $n \in \mathbb{Z}$ con residuo

$$\lim_{t\to \pi n} (t-\pi n)\,\cot(t) = \lim_{t\to 0} \cos(t+\pi n)\,\frac{t}{\operatorname{sen}(t+\pi n)} = \lim_{t\to 0} (-1)^n\,\cos(t)\,\frac{t}{(-1)^n\,\operatorname{sen}(t)} = 1.$$

Por "$\sum_{n\in\mathbb{Z}} \frac{1}{t-\pi n}$" se entiende $\lim_{N\to\infty} \sum_{-N\leq n\leq N} \frac{1}{t-\pi n}$. Luego,

$$\begin{aligned}
t\,\cot(t) &= t\left(\frac{1}{t} + \sum_{n\geq 1}\left(\frac{1}{t-\pi n} + \frac{1}{t+\pi n}\right)\right) = 1 - 2\sum_{n\geq 1}\left(\frac{t^2}{(\pi n)^2 - t^2}\right) = 1 - 2\sum_{n\geq 1} \frac{t^2}{(\pi n)^2}\,\frac{1}{1-\left(\frac{t}{\pi n}\right)^2} \\
&= 1 - 2\sum_{n\geq 1}\frac{t^2}{(\pi n)^2}\sum_{k\geq 0}\left(\frac{t}{\pi n}\right)^{2k} = 1 - 2\sum_{n\geq 1}\sum_{k\geq 1}\left(\frac{t}{\pi n}\right)^{2k} \quad \text{(la serie geométrica)} \\
&= 1 - 2\sum_{k\geq 1}\left(\sum_{n\geq 1}\frac{1}{n^{2k}}\right)\frac{t^{2k}}{\pi^{2k}} = 1 - 2\sum_{k\geq 1}\frac{\zeta(2k)\,t^{2k}}{\pi^{2k}}. \quad \text{(cambiando el orden de sumación)}
\end{aligned}$$

Comparando coeficientes con (8.1), tenemos

$$(-1)^k\, 2^{2k}\,\frac{B_{2k}}{(2k)!} = -2\,\frac{\zeta(2k)}{\pi^{2k}}.$$

■

9 Series de Fourier para $B_k(x)$

Vamos a necesitar el siguiente resultado del análisis armónico:

9.1. Hecho. *Sea $f\colon \mathbb{R}\to\mathbb{R}$ una función continua por trozos y periódica:*

$$f(x+1) = f(x).$$

Entonces para todo $x_0 \in \mathbb{R}$ donde f es continua y la derivada izquierda y derecha de f existen (pero no necesariamente coinciden) se tiene

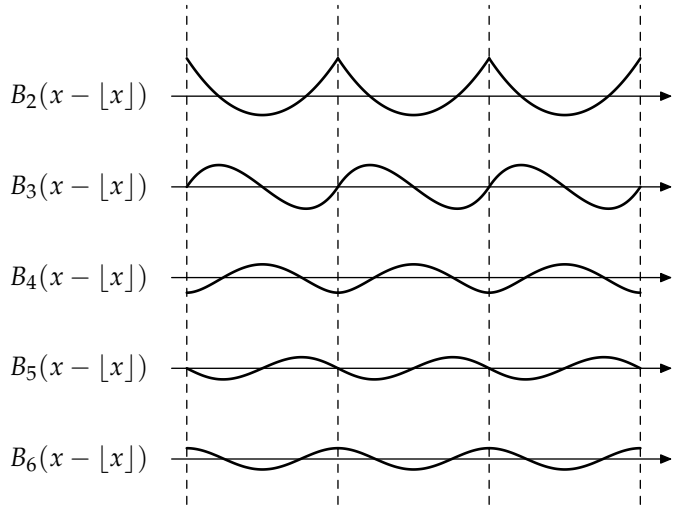
$$f(x_0) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)\, e^{2\pi i n x_0}, \quad \text{donde } \widehat{f}(n) := \int_0^1 e^{-2\pi i n x}\, f(x)\, dx.$$

Es un caso especial de las **series de Fourier** que va a ser suficiente para nosotros; para la teoría general véase por ejemplo [Kat2004].

En nuestro caso, nos interesan las funciones

$$f(x) := B_k(x - \lfloor x \rfloor),$$

donde $B_k(x)$ es el k-ésimo polinomio de Bernoulli. Para $k > 1$ la función $B_k(x - \lfloor x \rfloor)$ es continua y para $k = 1$ es discontinua en los puntos $x = n \in \mathbb{Z}$. También $B_k(x - \lfloor x \rfloor)$ es lisa para $k > 2$, pero $B_2(x)$ no es lisa en los puntos $x = n \in \mathbb{Z}$, donde existen la derivada izquierda y derecha, pero son diferentes.



Los coeficientes de la serie de Fourier para $f(x)$ se calculan fácilmente. Para $n = 0$ tenemos

$$\widehat{f}(0) = \int_0^1 B_k(x)\,dx = 0.$$

Luego, para $n \neq 0$ y $k = 1$ podemos usar integración por partes ($\int_a^b f'(x)\,g(x)\,dx = [f(x)\,g(x)]_a^b - \int_a^b f(x)\,g'(x)\,dx$):

$$\begin{aligned}\int_0^1 e^{-2\pi i n x}\left(x - \frac{1}{2}\right)dx &= -\frac{1}{2\pi i n}\int_0^1 \left(e^{-2\pi i n x}\right)'\left(x - \frac{1}{2}\right)dx \\ &= -\frac{1}{2\pi i n}\left(\left[e^{-2\pi i n x}\left(x - \frac{1}{2}\right)\right]_0^1 - \underbrace{\int_0^1 e^{-2\pi i n x}\,dx}_{=0}\right) = -\frac{1}{2\pi i n}.\end{aligned}$$

Para $k > 1$ integración por partes y la relación $B_k'(x) = k\, B_{k-1}(x)$ nos dan

$$\begin{aligned}
\widehat{f}(n) = \int_0^1 e^{-2\pi i n x}\, B_k(x)\, dx &= -\frac{1}{2\pi i n} \int_0^1 (e^{-2\pi i n x})'\, B_k(x)\, dx \\
&= -\frac{1}{2\pi i n} \left(\left[e^{-2\pi i n x}\, B_k(x) \right]_0^1 - k \int_0^1 e^{-2\pi i n x}\, B_{k-1}(x)\, dx \right) \\
&= \frac{k}{2\pi i n} \int_0^1 e^{-2\pi i n x}\, B_{k-1}(x)\, dx \\
&= \frac{k\,(k-1)}{(2\pi i n)^2} \int_0^1 e^{-2\pi i n x}\, B_{k-2}(x)\, dx \\
&= \cdots \\
&= \frac{k!}{(2\pi i n)^{k-1}} \int_0^1 e^{-2\pi i n x} \left(x - \frac{1}{2} \right) dx \\
&= \frac{k!}{(2\pi i n)^{k-1}} \cdot \left(-\frac{1}{2\pi i n} \right) = -\frac{k!}{(2\pi i n)^k}.
\end{aligned}$$

Entonces, la serie de Fourier es

$$B_k(x - \lfloor x \rfloor) = -\frac{k!}{(2\pi i)^k} \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}} \frac{e^{2\pi i n x}}{n^k}. \tag{9.1}$$

Como un caso especial, se obtiene la fórmula para $\zeta(2k)$:

Segunda demostración de 8.1. Para $x = 0$ la identidad (9.1) nos da

$$B_{2k} = B_{2k}(0) = -\frac{(2k)!}{(-1)^k\,(2\pi)^{2k}}\, 2 \sum_{n \geq 1} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2k)!}{2^{2k-1}\,\pi^{2k}}\, \zeta(2k).$$

■

Note que los valores en los enteros impares $\zeta(2k+1)$ no se obtienen con este método.

10 Los valores de $\zeta(-1), \zeta(-2), \zeta(-3), \ldots$

Gracias a la ecuación funcional

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

y la fórmula de Euler

$$\zeta(2k) = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k},$$

podemos obtener los valores en los enteros negativos. En efecto, para los enteros negativos pares $s = -2k$ tenemos

$$\zeta(-2k) = 2^{-2k}\, \pi^{-2k-1}\, \underbrace{\operatorname{sen}\left(-\frac{\pi k}{2} \right)}_{=0}\, \Gamma(2k+1)\, \zeta(2k+1) = 0.$$

Y para $s = -(2k+1)$ impares,

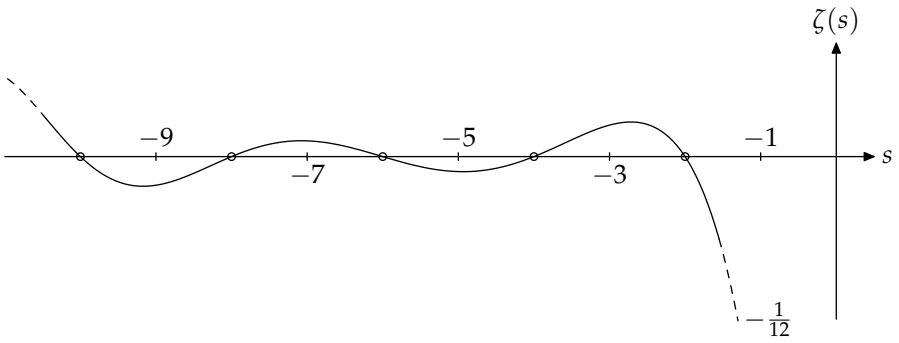
$$\begin{aligned}\zeta(-(2k+1)) &= 2^{-(2k+1)}\,\pi^{-(2k+2)}\,\operatorname{sen}\left(-\frac{\pi\,(2k+1)}{2}\right)\,(2k+1)!\,\zeta(2k+2)\\ &= 2^{-(2k+1)}\,\pi^{-(2k+2)}\,(-1)^{k+1}\,(2k+1)!\,(-1)^k\,B_{2k+2}\,\frac{2^{2k+1}}{(2k+2)!}\,\pi^{2k+2}\\ &= -\frac{B_{2k+2}}{2k+2}.\end{aligned}$$

Ya que $B_n = 0$ para n impar, en ambos casos se tiene

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

Además, para $n = 0$ la prolongación analítica nos da $\zeta(0) = -\frac{1}{2} = -B_1$, así que esta fórmula es valida también para $n = 0$.

n:	0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	$\cdots$
$\zeta(n)$:	$-\frac{1}{2}$	$-\frac{1}{12}$	0	$\frac{1}{120}$	0	$-\frac{1}{252}$	0	$\frac{1}{240}$	0	$-\frac{1}{132}$	0	$\cdots$



(Después $\zeta(s)$ es decreciente hasta su polo en $s = 1$.)

Terminamos por el cálculo de $\zeta(-1) = -\frac{1}{12}$ encontrado por Euler en su artículo [Eul1760]:

Para la serie geométrica

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + \cdots = \frac{1}{1-x}$$

la derivada formal nos da

$$1 + 2\,x + 3\,x^2 + 4\,x^3 + 5\,x^4 + 6\,x^5 + 7\,x^6 + 8\,x^7 + \cdots = \frac{1}{(1-x)^2},$$

de donde para $x = -1$ (¡sic!)

$$1 - 2 + 3 - 4 + 5 - 6 + 7 - 8 + \cdots = \frac{1}{4}.$$

Luego,

$$\begin{aligned}-3\,\zeta(-1) &= \zeta(-1) - 4\,\zeta(-1)\\ &= (1+2+3+4+\cdots) - (4+8+12+16+\cdots)\\ &= 1-2+3-4+5-6+7-8+\cdots = \frac{1}{4},\end{aligned}$$

lo que implica $\zeta(-1) = -\frac{1}{12}$, Q.E.D.

El lector no debería tomar en serio el argumento de arriba y usar métodos similares en sus demostraciones.

En PARI/GP, la función `zeta(s)` calcula $\zeta(s)$:

```
? zeta (0.0)
% = -0.50000000000000000000000000000000000000

? zeta (-1)
% = -0.083333333333333333333333333333333333333
? -bernreal(2)/2
% = -0.083333333333333333333333333333333333333

? zeta (-2)
% = 0

? zeta (-3)
% = 0.0083333333333333333333333333333333333334
? -bernreal(4)/4
% = 0.0083333333333333333333333333333333333334
```

11 * Conjetura de Lichtenbaum

El matemático estadounidense Stephen Lichtenbaum formuló en 1973 la hipótesis que los valores $\zeta(-n)$ están relacionados con ciertos grupos abelianos $K_i(\mathbb{Z})$ asociados al anillo $\mathbb{Z}$ (los **grupos K**, definidos por el matemático estadounidense Daniel Quillen (1940–2011)):

$$\zeta(-n) = \pm 2^{?}\,\frac{\#K_{2n}(\mathbb{Z})}{\#K_{2n+1}(\mathbb{Z})_{tors}},$$

donde $K_{2n}(\mathbb{Z})$ son grupos abelianos finitos, y $\#K_{2n+1}(\mathbb{Z})_{tors}$ denota la parte de torsión de grupos $K_{2n+1}(\mathbb{Z})$ que tienen rango 1. El factor $2^{?}$ denota alguna potencia de 2.

La definición de los $K_i(\mathbb{Z})$ requiere otro curso de nivel de posgrado, así que no voy a entrar en detalles... Estos grupos son muy difíciles de calcular, y solo hasta en los años 2000 fueron determinados en gran parte. Como sugiere la conjetura de Lichtenbaum, estos en efecto están relacionados con los números de Bernoulli. Por ejemplo, $K_{22}(\mathbb{Z}) \cong \mathbb{Z}/691\mathbb{Z}$ y $K_{23}(\mathbb{Z}) \cong \mathbb{Z}/65\,520\mathbb{Z}$,

$$\zeta(-11) = -\frac{B_{12}}{12} = \frac{691}{12\cdot 2730}, \quad \frac{\#K_{22}(\mathbb{Z})}{\#K_{23}(\mathbb{Z})} = \frac{691}{2\cdot 12\cdot 2730}$$

—los valores coinciden salvo una potencia de 2.

He aquí la tabla de algunos de los grupos $K_i(\mathbb{Z})$:

i:	2	3	4	5
$K_i(\mathbb{Z})$:	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/48\mathbb{Z}$	0	$\mathbb{Z}$
i:	6	7	8	9
$K_i(\mathbb{Z})$:	0	$\mathbb{Z}/240\mathbb{Z}$	(0?)	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
i:	10	11	12	13
$K_i(\mathbb{Z})$:	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/1008\mathbb{Z}$	(0?)	$\mathbb{Z}$
i:	14	15	16	17
$K_i(\mathbb{Z})$:	0	$\mathbb{Z}/480\mathbb{Z}$	(0?)	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
i:	18	19	20	21
$K_i(\mathbb{Z})$:	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/528\mathbb{Z}$	(0?)	$\mathbb{Z}$
i:	22	23	24	25
$K_i(\mathbb{Z})$:	$\mathbb{Z}/691\mathbb{Z}$	$\mathbb{Z}/65\,520\mathbb{Z}$	(0?)	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$

Los grupos $K_{4i}(\mathbb{Z})$ son *conjeturalmente* nulos, pero este hecho es equivalente a la **conjetura de Vandiver** de la teoría de números, que tampoco ha sido resuelta. La rama de matemáticas que estudia los grupos $K_i(\mathbb{Z})$ se llama la **teoría K algebraica**. Estos grupos están relacionados con otros objetos, más adecuados para el estudio de los valores de las funciones zeta: los grupos de **cohomología motívica**. Para más información, véase [Kah2005] y [Wei2005].

12 * Los valores $\zeta(2k+1)$

Hemos visto que los valores de la función zeta en los enteros positivos pares $\zeta(2k)$ y los enteros negativos $\zeta(-n)$ se expresan por los números de Bernoulli. Los valores en los enteros positivos impares

$$\zeta(3),\ \zeta(5),\ \zeta(7),\ \zeta(9),\ \zeta(11),\ \ldots$$

son más misteriosos. Note que la ecuación funcional (7.5) no dice nada sobre ellos. *Al parecer*, son números trascendentes. Por supuesto, los números

$$\zeta(2k) = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k}$$

son también transcendentes, ya que π es trascendente (¡de hecho, uno de los pocos números específicos cuya trascendencia se puede demostrar!). Los valores $\zeta(2k+1)$ deberían de ser trascendentes por alguna razón más sofisticada, y se supone que entre $\zeta(2k+1)$ distintos no hay ninguna relación algebraica.

Sin embargo, todavía no hay demostraciones ni siquiera de que los $\zeta(2k+1)$ sean irracionales. En 1977 el matemático francés Roger Apéry demostró que el número

$$\zeta(3) \approx 1{,}202056903159594285399738 16\ldots$$

es irracional. La tumba de Apéry en París lleva la inscripción

Roger APÉRY
1916–1994

$$1+\tfrac{1}{8}+\tfrac{1}{27}+\tfrac{1}{64}+\cdots \neq \tfrac{p}{q}$$

Para más información sobre el teorema de Apéry, véase el artículo [vdP1979].

Los métodos de Apéry no se generalizan para demostrar que $\zeta(5)$ es irracional. Hay pocos resultados en esta dirección. El matemático francés Tanguy Rivoal demostró en 2000 que entre los números $\zeta(3), \zeta(7), \zeta(9), \ldots$ hay una infinidad de irracionales, mientras que el matemático ruso Wadim Zudilin demostró en 2001 que por lo menos un número entre $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ y $\zeta(11)$ es irracional [Zud2004].

13 Digresión combinatoria: los números de Stirling

Nuestro próximo objetivo es obtener algunas expresiones para los números de Bernoulli que permitan estudiar sus propiedades aritméticas, específicamente sus numeradores y denominadores. En el camino surgen ciertos números combinatorios, conocidos como los **números de Stirling**.

13.1. Definición. Sean k y ℓ dos números naturales positivos.

El **número de Stirling de primera clase** $\left[\begin{smallmatrix} k \\ \ell \end{smallmatrix}\right]$ es el número de permutaciones en el grupo simétrico S_k que consisten en ℓ ciclos disjuntos.

El **número de Stirling de segunda clase** $\left\{\begin{smallmatrix} k \\ \ell \end{smallmatrix}\right\}$ es el número de posibilidades de escribir un conjunto de k elementos como una unión disjunta de ℓ conjuntos no vacíos.

13.2. Ejemplo. $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right] = 11$. Las permutaciones correspondientes en S_4 son

$$(1)\,(2\ 3\ 4),\ (1)\,(2\ 4\ 3),\ (2)\,(1\ 3\ 4),\ (2)\,(1\ 4\ 3),$$
$$(3)\,(1\ 2\ 4),\ (3)\,(1\ 4\ 2),\ (4)\,(1\ 2\ 3),\ (4)\,(1\ 3\ 2),$$
$$(1\ 2)\,(3\ 4),\ (1\ 3)\,(2\ 4),\ (1\ 4)\,(2\ 3).$$

▲

13.3. Ejemplo. $\left\{\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right\} = 7$. Las descomposiciones de conjuntos correspondientes son

$$\{1,2,3,4\} = \{1\} \cup \{2,3,4\} = \{2\} \cup \{1,3,4\} = \{3\} \cup \{1,2,4\} = \{4\} \cup \{1,2,3\}$$
$$= \{1,2\} \cup \{3,4\} = \{1,3\} \cup \{2,4\} = \{1,4\} \cup \{2,3\}.$$

▲

De la definición se siguen las identidades

$$\begin{bmatrix} k \\ \ell \end{bmatrix} = 0 \quad \text{para } \ell > k, \tag{13.1}$$

$$\begin{bmatrix} k \\ k \end{bmatrix} = 1, \tag{13.2}$$

$$\begin{bmatrix} k \\ 1 \end{bmatrix} = (k-1)!, \tag{13.3}$$

$$\sum_{1 \le \ell \le k} \begin{bmatrix} k \\ \ell \end{bmatrix} = k!, \tag{13.4}$$

$$\begin{bmatrix} k+1 \\ \ell \end{bmatrix} = \begin{bmatrix} k \\ \ell - 1 \end{bmatrix} + k \begin{bmatrix} k \\ \ell \end{bmatrix}, \tag{13.5}$$

(13.6)

$$\left\{ {k \atop \ell} \right\} = 0 \quad \text{para } \ell > k, \tag{13.7}$$

$$\left\{ {k \atop k} \right\} = 1, \tag{13.8}$$

$$\left\{ {k \atop 1} \right\} = 1, \tag{13.9}$$

$$\sum_{1 \le \ell \le k} \left\{ {k \atop \ell} \right\} = b(k), \tag{13.10}$$

$$\left\{ {k+1 \atop \ell} \right\} = \left\{ {k \atop \ell-1} \right\} + \ell \left\{ {k \atop \ell} \right\}. \tag{13.11}$$

(13.2) significa que la única permutación en S_k que se descompone en el producto de k ciclos disjuntos es la permutación identidad. (13.3) significa que en S_k hay $(k-1)!$ diferentes k-ciclos (¿por qué?).

(13.4) es el hecho de que el tipo cíclico es una relación de equivalencia sobre los elementos de S_k (en efecto, los tipos cíclicos corresponden a las clases de conjugación). (13.10) es el análogo de esta identidad: el número total de particiones se conoce como el **número de Bell** $b(k)$. Los primeros números de Bell son $b(1) = 1$, $b(2) = 2$, $b(3) = 5$, $b(4) = 15$, $b(5) = 52$, $b(6) = 203$, ...; véase http://oeis.org/A000110 En este curso, no vamos estudiar estos números (también porque la notación parece mucho a los números de Bernoulli :-)

Las recurrencias (13.5) y (13.11) se siguen de la definición combinatoria. Por ejemplo, en (13.5), consideremos las permutaciones de elementos $\{1, \dots, k, k+1\}$. Sea $\sigma \in S_{k+1}$ una permutación que se descompone en el producto de ℓ ciclos disjuntos. Si $\sigma(k+1) = k+1$, entonces $(k+1)$ forma un ciclo sí mismo, y para el resto de los elementos hay $\left[{k \atop \ell-1} \right]$ posibles descomposiciones. Si $\sigma(k+1) \neq k+1$, entonces $k+1$ pertenece a algún ciclo. Para enumerar todas las posibilidades, podemos primero considerar $\left[{k \atop \ell} \right]$ descomposiciones de las permutaciones de $\{1, \dots, k\}$ en ℓ ciclos disjuntos, y luego para cada descomposición hay k posibilidades de poner $k+1$ en uno de los ciclos. La fórmula (13.11) se explica de la misma manera: si tenemos un conjunto X de $k+1$ elemento, podemos considerar un elemento $x \in X$. Para las descomposiciones de X en la unión de ℓ subconjuntos hay dos casos: o bien $\{x\}$ forma un conjunto en la descomposición, y quedan $\left\{ {k \atop \ell-1} \right\}$ posibilidades para descomponer $X \setminus \{x\}$; o bien x pertenece a algún conjunto. En el segundo caso, hay $\left\{ {k \atop \ell} \right\}$ posibilidades de descomponer $X \setminus \{x\}$ en ℓ subconjuntos, y luego en cada caso hay ℓ posibilidades de poner x en uno de los conjuntos.

También será útil definir $\left[{k \atop \ell} \right]$ y $\left\{ {k \atop \ell} \right\}$ para $k, \ell = 0$:

13.4. Definición.

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} k \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \ell \end{bmatrix} = 0 \text{ para } k, \ell \neq 0,$$
$$\begin{Bmatrix} 0 \\ 0 \end{Bmatrix} = 1, \quad \begin{Bmatrix} k \\ 0 \end{Bmatrix} = \begin{Bmatrix} 0 \\ \ell \end{Bmatrix} = 0 \text{ para } k, \ell \neq 0.$$

Podemos definir $\left[{k \atop \ell} \right]$ y $\left\{ {k \atop \ell} \right\}$ por los valores iniciales 13.4 y las relaciones de recurrencia (13.5) y (13.11). Esta definición está compatible con 13.1. Por ejemplo, en el caso de $\left[{k \atop \ell} \right]$, podemos ver que las identidades

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} k \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \ell \end{bmatrix} = 0 \text{ para } k, \ell \neq 0$$

implican

$$\begin{bmatrix} k \\ 1 \end{bmatrix} = (k-1)! \text{ para } k \geq 1, \quad \begin{bmatrix} 1 \\ \ell \end{bmatrix} = 0 \text{ para } \ell \geq 1.$$

En efecto,

$$\begin{bmatrix} k \\ 1 \end{bmatrix} = \underbrace{\begin{bmatrix} k \\ 0 \end{bmatrix}}_{0} + (k-1)\begin{bmatrix} k-1 \\ 1 \end{bmatrix} = (k-1)(k-2)\begin{bmatrix} k-2 \\ 1 \end{bmatrix} = \cdots$$

$$= (k-1)(k-2)\cdots 2\cdot 1\left(\underbrace{\begin{bmatrix} 0 \\ 0 \end{bmatrix}}_{1} + \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{0}\right) = (k-1)!$$

y para $\ell > 1$

$$\begin{bmatrix} 1 \\ \ell \end{bmatrix} = \begin{bmatrix} 0 \\ \ell - 1 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 \\ \ell \end{bmatrix} = 0.$$

En PARI/GP, `stirling(k,l,2)` $= \{{k \atop \ell}\}$ (el parametro "2" significa "de segunda clase"):

```
? stirling (4,2,2)
% = 7
```

PARI/GP usa otra definición de los números de Stirling de primera clase. La única diferencia es el signo: `stirling(k,l)` $= (-1)^{k-\ell}\left[{k \atop \ell}\right]$:

```
? stirling (4,2)
% = 11
? stirling(4,3)
% = -6
```

13.5. Ejercicio. *Demuestre que* $\left[{k \atop k-1}\right] = \binom{k}{2}$.

13.6. Ejercicio. *Note que las recurrencias de arriba con los valores iniciales para* $k, \ell = 0$ *nos permiten definir* $\left[{k \atop \ell}\right]$ *y* $\{{k \atop \ell}\}$ *para todo* $k, \ell \in \mathbb{Z}$. *Demuestre que*

$$\begin{bmatrix} k \\ \ell \end{bmatrix} = \begin{Bmatrix} -\ell \\ -k \end{Bmatrix}.$$

Esto significa que los números de Stirling de primera y de segunda clase son esencialmente el mismo objeto.

13.7. Ejercicio. *Demuestre que* $\{{k \atop \ell}\} = 0$ *para* $k\ell < 0$.

(Los últimos dos ejercicios sirven solo para acostumbrarse a las recurrencias con $\left[{k \atop \ell}\right]$ y $\{{k \atop \ell}\}$; no vamos a usar los números de Stirling para k y ℓ negativos.)

k \ ℓ	0	1	2	3	4	5	6	7	8	9
0	1									
1	0	1								
2	0	1	1							
3	0	2	3	1						
4	0	6	11	6	1					
5	0	24	50	35	10	1				
6	0	120	274	225	85	15	1			
7	0	720	1764	1624	735	175	21	1		
8	0	5040	13068	13132	6769	1960	322	28	1	
9	0	40320	109584	118124	67284	22449	4536	546	36	1

Valores de $\begin{bmatrix} k \\ \ell \end{bmatrix}$

k \ ℓ	0	1	2	3	4	5	6	7	8	9
0	1									
1	0	1								
2	0	1	1							
3	0	1	3	1						
4	0	1	7	6	1					
5	0	1	15	25	10	1				
6	0	1	31	90	65	15	1			
7	0	1	63	301	350	140	21	1		
8	0	1	127	966	1701	1050	266	28	1	
9	0	1	255	3025	7770	6951	2646	462	36	1

Valores de $\left\{ \begin{matrix} k \\ \ell \end{matrix} \right\}$

14 Relación entre B_k y los números de Stirling

14.1. Lema. *Para todo $\ell \geq 0$*

$$\frac{(e^t-1)^\ell}{\ell!} = \sum_{k\geq \ell} \left\{ {k \atop \ell} \right\} \frac{t^k}{k!}.$$

Demostración. Tenemos que ver que

$$\frac{d^k}{dt^k}\left(\frac{(e^t-1)^\ell}{\ell!}\right)(0) = \left\{ {k \atop \ell} \right\}.$$

Los valores iniciales coinciden, y va a ser suficiente demostrar que la recurrencia

$$\left\{ {k+1 \atop \ell} \right\} = \left\{ {k \atop \ell-1} \right\} + \ell \left\{ {k \atop \ell} \right\}$$

se cumple en nuestro caso:

$$\frac{d^{k+1}}{dt^{k+1}}\left(\frac{(e^t-1)^\ell}{\ell!}\right)(0) = \frac{d^k}{dt^k}\left(\frac{(e^t-1)^{\ell-1}}{(\ell-1)!}\right)(0) + \ell\,\frac{d^k}{dt^k}\left(\frac{(e^t-1)^\ell}{\ell!}\right)(0).$$

En efecto,

$$\begin{aligned}\frac{d^{k+1}}{dt^{k+1}}\left(\frac{(e^t-1)^\ell}{\ell!}\right) &= \frac{d^k}{dt^k}\left(\frac{(e^t-1)^{\ell-1}}{(\ell-1)!}\,e^t\right) = \frac{d^k}{dt^k}\left(\frac{(e^t-1)^{\ell-1}\,(1+e^t-1)}{(\ell-1)!}\right)\\ &= \frac{d^k}{dt^k}\left(\frac{(e^t-1)^{\ell-1}}{(\ell-1)!} + \frac{(e^t-1)^\ell}{(\ell-1)!}\right)\\ &= \frac{d^k}{dt^k}\left(\frac{(e^t-1)^{\ell-1}}{(\ell-1)!}\right) + \ell\,\frac{d^k}{dt^k}\left(\frac{(e^t-1)^\ell}{\ell!}\right).\end{aligned}$$

■

14.2. Ejercicio. *Demuestre la identidad*

$$\frac{(-\ln(1-t))^\ell}{\ell!} = \sum_{k\geq \ell} \left[{k \atop \ell} \right] \frac{t^k}{k!}.$$

(De nuevo, es suficiente considerar las derivadas formales y verificar que se cumple la misma recurrencia que define los números de Stirling correspondientes: $\left[{k+1 \atop \ell} \right] = \left[{k \atop \ell-1} \right] + k \left[{k \atop \ell} \right]$.)

Lo que acabamos de ver en 14.1 y 14.2 son las funciones generatrices para los números de Stirling, pero no soy tan sádico para dar esto como la definición de $\left\{ {k \atop \ell} \right\}$ y $\left[{k \atop \ell} \right]$.

14.3. Lema. *Para $k, \ell \geq 0$*

$$\left\{ {k \atop \ell} \right\} = \frac{(-1)^\ell}{\ell!} \sum_{0\leq i\leq \ell} (-1)^i \binom{\ell}{i} i^k.$$

Demostración. De nuevo, podemos verificar que los valores iniciales coinciden y la suma satisface la misma recurrencia que $\left\{{k \atop \ell}\right\}$:

$$\left\{{k+1 \atop \ell}\right\} = \left\{{k \atop \ell-1}\right\} + \ell \left\{{k \atop \ell}\right\}.$$

Para los valores iniciales, si $k = \ell = 0$, la suma nos da $\left\{{0 \atop 0}\right\} = 1$ (como siempre en el contexto algebraico/combinatorio, $0^0 = 1$); si $k > 0$, $\ell = 0$, la suma nos da 0; si $k = 0$, $\ell > 0$, la suma también nos da $\sum_{0\le i\le \ell}(-1)^i \binom{\ell}{i} = 0$. Para la recurrencia,

$$\begin{aligned}
\frac{(-1)^\ell}{\ell!} \sum_{0\le i\le \ell} (-1)^i \binom{\ell}{i} i^{k+1} &= \frac{(-1)^\ell}{(\ell-1)!} \sum_{0\le i\le \ell} (-1)^i \frac{i}{\ell} \binom{\ell}{i} i^k \\
&= \frac{(-1)^\ell}{(\ell-1)!} \sum_{0\le i\le \ell} (-1)^i \left(\binom{\ell}{i} - \binom{\ell-1}{i} \right) i^k \\
&= \frac{(-1)^{\ell-1}}{(\ell-1)!} \sum_{0\le i\le \ell-1} (-1)^i \binom{\ell-1}{i} i^k + \ell \frac{(-1)^\ell}{\ell!} \sum_{0\le i\le \ell} (-1)^i \binom{\ell}{i} i^k.
\end{aligned}$$

Aquí hemos usado la identidad

$$\binom{\ell}{i} - \binom{\ell-1}{i} = \frac{i}{\ell}\binom{\ell}{i}.$$

■

14.4. Teorema.

$$B_k = (-1)^k \sum_{0\le \ell\le k} \frac{(-1)^\ell\, \ell!\, \left\{{k \atop \ell}\right\}}{\ell+1} = (-1)^k \sum_{0\le \ell\le k} \frac{1}{\ell+1} \sum_{0\le i\le \ell} (-1)^i \binom{\ell}{i} i^k.$$

La segunda igualdad viene de la expresión 14.3 y (¡por fin!) nos da una expresión para B_k sin recurrencias.

Demostración. La función generatriz para B_k es $\frac{t\,e^t}{e^t-1}$. Gracias a 4.2, podemos escribir

$$\frac{t\,e^t}{e^t-1} = \frac{t}{1-e^{-t}} = \frac{-\ln(1-(1-e^{-t}))}{1-e^{-t}}.$$

Luego,

$$\begin{aligned}
\frac{-\ln(1-(1-e^{-t}))}{1-e^{-t}} &= \frac{1}{1-e^{-t}} \sum_{\ell\ge 1} \frac{(1-e^{-t})^\ell}{\ell} \\
&= \sum_{\ell\ge 1} \frac{(1-e^{-t})^{\ell-1}}{\ell} \\
&= \sum_{\ell\ge 0} \frac{(-1)^\ell\, \ell!}{\ell+1} \sum_{k\ge \ell} \left\{{k \atop \ell}\right\} \frac{(-t)^k}{k!} \quad \text{por 14.1} \\
&= \sum_{k\ge 0} (-1)^k \left(\sum_{0\le \ell\le k} \frac{(-1)^\ell\, \ell!\, \left\{{k \atop \ell}\right\}}{\ell+1} \right) \frac{t^k}{k!}.
\end{aligned}$$

■

```
? bernbin (k) = (-1)^k * sum (l=0,k, 1/(l+1)*sum(i=0,l, (-1)^i*binomial(l,i)*i^k));
? vector (10,k,bernbin(k))
% = [1/2, 1/6, 0, -1/30, 0, 1/42, 0, -1/30, 0, 5/66]
```

15 Denominadores de B_k (el teorema de Clausen–von Staudt)

15.1. Teorema. *Para todo $k \geq 2$ par se tiene*

$$B_k = -\sum_{\substack{p \text{ primo} \\ p-1 \mid k}} \frac{1}{p} + C_k,$$

donde $C_k \in \mathbb{Z}$ y la suma es sobre todos los p tales que $p-1$ divide a k.

Este resultado fue descubierto de manera independiente por el astrónomo y matemático danés Thomas Clausen (1801–1885) y el matemático alemán Karl Georg Christian von Staudt (1798–1867).

15.2. Ejemplo.

$$\begin{aligned}
B_2 &= \frac{1}{6} = -\left(\frac{1}{2}+\frac{1}{3}\right)+1,\\
B_4 &= -\frac{1}{30} = -\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{5}\right)+1,\\
B_6 &= \frac{1}{42} = -\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{7}\right)+1,\\
&\cdots\\
B_{14} &= \frac{7}{6} = -\left(\frac{1}{2}+\frac{1}{3}\right)+2,\\
&\cdots
\end{aligned}$$

▲

En particular, el denominador de B_k es precisamente el producto de todos los primos p tales que $p-1 \mid k$. Esto explica por qué los denominadores de B_k son libres de cuadrados y divisibles por 6. No tenemos mucho control sobre el número C_k (véase §17); solo podemos notar que el valor de C_k va a estar cerca de B_k, así que $|C_{2k}| \xrightarrow{k\to\infty} \infty$.

Demostración. Gracias a la fórmula

$$B_k = (-1)^k \sum_{0\leq \ell \leq k} \frac{(-1)^\ell\, \ell!\, \left\{ {k \atop \ell} \right\}}{\ell+1},$$

sabemos que en el denominador aparecen solamente los primos que dividen a $\ell+1$; los primos $p > k+1$ no aparecen en el denominador. Vamos a analizar las contribuciones del término $\frac{(-1)^\ell\, \ell!\, \left\{ {k \atop \ell} \right\}}{\ell+1}$ para diferentes ℓ.

(1) Supongamos que $\ell+1$ es compuesto, es decir $\ell+1 = ab$ para algunos $1 < a, b < \ell$.

(1.1) Si $a \neq b$, entonces $ab \mid \ell!$, y el término $\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell+1}$ es entero.

(1.2.1) Si $a = b$ y $2a \leq \ell$, entonces $a \mid \ell!$ y $2a \mid \ell!$, entonces $a^2 = \ell + 1$ divide a $\ell!$ y el término $\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell+1}$ es entero.

(1.2.2) Si $a = b$ y $2a > \ell$, entonces $\ell + 1 = a^2 \geq 2a \geq \ell + 1$, y por lo tanto $a^2 = 2a$ y $a = 2$, $\ell = 3$. Usando 14.3, podemos escribir

$$\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell + 1} = \frac{1}{4} \sum_{0 \leq i \leq 3} (-1)^i \binom{3}{i} i^k = \frac{1}{4} \left(0 - 3 + 3 \cdot 2^k - 3^k \right).$$

Este término es nulo para $\ell > k$, así que $k > 3$, y es un número par según la hipótesis del teorema. Tenemos

$$-3 + \cancel{3 \cdot 2^k} - 3^k \equiv 1 - (-3)^k \equiv 1 - 1^k \equiv 0 \pmod 4.$$

Esto demuestra que el término $\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell+1}$ es entero.

Hemos demostrado que si $\ell + 1$ es compuesto, el término $\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell+1}$ es entero.

(2) Supongamos que $\ell + 1 = p$ es primo. Tenemos por 14.3

$$\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell + 1} = \frac{(-1)^{p-1} (p-1)! \left\{ {k \atop p-1} \right\}}{p} = \frac{1}{p} \sum_{0 \leq i \leq p-1} (-1)^i \left({p-1 \atop i} \right) i^k.$$

Tenemos $\binom{p-1}{i} \equiv (-1)^i \pmod p$, entonces

$$\sum_{0 \leq i \leq p-1} (-1)^i \left({p-1 \atop i} \right) i^k \equiv \sum_{0 \leq i \leq p-1} i^k \equiv \begin{cases} p - 1 \equiv -1, & p - 1 \mid k, \\ 0, & p - 1 \nmid k. \end{cases} \pmod p$$

Para ver la última congruencia, notamos que si $p - 1 \mid k$, entonces $i^{p-1} \equiv 1 \pmod p$ por el **pequeño teorema de Fermat** ($p \nmid i$). Si $p - 1 \nmid k$, podemos escribir la suma $\sum_{0 \leq i \leq p-1} i^k$ como

$$\sum_{1 \leq i \leq p-1} x^{ik} = \frac{1 - x^{pk}}{1 - x^k} - 1 \equiv 0 \pmod p,$$

donde x es una raíz primitiva de la unidad módulo p. Aquí $x^{pk} \equiv x^k \not\equiv 1 \pmod p$ por el pequeño teorema de Fermat.

Entonces, ci $\ell + 1 = p$ es primo, el término $\frac{(-1)^\ell \ell! \left\{ {k \atop \ell} \right\}}{\ell+1}$ va a contribuir $-\frac{1}{p}$ en el denominador si $p - 1 \mid k$, y va a ser entero si $p - 1 \nmid k$.

■

16 Congruencias de Kummer

Para un primo p denotemos por $\mathbb{Z}_{(p)}$ el anillo de los números racionales donde p no aparece en el denominador:

$$\mathbb{Z}_{(p)} := \{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \}.$$

(Es un caso particular de **localización** de un anillo afuera de un ideal primo.) Los elementos invertibles en $\mathbb{Z}_{(p)}$ son las fracciones no nulas donde p no aparece ni en el numerador ni en el denominador:

$$\mathbb{Z}_{(p)}^{\times} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid a,\ p \nmid b\}.$$

El siguiente resultado es un caso particular de las **congruencias de Kummer** (véase [AIK2014, §11.3]):

16.1. Teorema (Kummer, 1851). *Sea p un número primo y k un entero positivo tal que $p-1 \nmid k$.*

1) p no aparece en el denominador del número B_k/k:

$$\frac{B_k}{k} \in \mathbb{Z}_{(p)}.$$

2) Para todo k' tal que $k' \equiv k \pmod{p-1}$ se cumple

$$\frac{B_{k'}}{k'} \equiv \frac{B_k}{k} \pmod{p}.$$

Aquí la última relación puede ser interpretada como $B_{k'} \cdot k \equiv B_k \cdot k' \pmod{p}$. También podemos interpretar una fracción $\frac{B_k}{k}$ como un residuo módulo p dado por $B_k \cdot k^{-1}$, donde k^{-1} es el residuo inverso a k módulo p, que existe porque en este caso $p \nmid k$.

16.2. Ejemplo. Sea $p = 7$, $k = 10$, $k' = 4$. En este caso $(p-1) \nmid k, k'$ y $k \equiv k' \pmod{p-1}$. Luego,

$$\frac{B_4}{4} = -\frac{1}{30}\frac{1}{4} = -\frac{1}{120} \equiv -1 \equiv 6 \pmod 7 \quad \text{y} \quad \frac{B_{10}}{10} = \frac{5}{66}\frac{1}{10} = \frac{1}{132} \equiv \frac{1}{6} \equiv 6 \pmod 7.$$

▲

Para demostrar el teorema, nos va a servir el siguiente

16.3. Lema. *Sea p un primo impar y sea $f(t) \in \mathbb{Z}_{(p)}[\![t]\!]$ una serie formal de potencias con coeficientes en $\mathbb{Z}_{(p)}$. Entonces para los coeficientes de Taylor de la serie*

$$f(e^t - 1) = \sum_{k \geq 0} a_k \frac{t^k}{k!}$$

se cumple

$$a_k \in \mathbb{Z}_{(p)} \quad y \quad a_{k+(p-1)} \equiv a_k \pmod{p}.$$

Demostración. Si $f(t) = \sum_{\ell \geq 0} b_\ell\, t^\ell$, tenemos

$$\begin{aligned} f(e^t - 1) &= \sum_{\ell \geq 0} b_\ell\, (e^t - 1)^\ell \\ &= \sum_{\ell \geq 0} b_\ell \sum_{0 \leq i \leq \ell} (-1)^i \binom{\ell}{i} e^{t\,(\ell - i)}. \end{aligned}$$

Los coeficientes de la serie de Taylor son

$$a_k = \frac{d^k}{dt^k}\left(f(e^t - 1)\right)_{t=0} = \sum_{\ell \geq 0} b_\ell \sum_{0 \leq i \leq \ell} (-1)^i \binom{\ell}{i} (\ell - i)^k.$$

Notemos que en $(e^t-1)^\ell$ no hay términos de grado $k<\ell$, así que la suma de arriba es finita: en efecto es sobre $0\le \ell \le k$. Ya que $b_\ell \in \mathbb{Z}_{(p)}$, de esta fórmula se deduce que $a_k \in \mathbb{Z}_{(p)}$. Luego,

$$a_{k+(p-1)} - a_k = \sum_{\ell\ge 0} b_\ell \sum_{0\le i\le \ell} (-1)^i \binom{\ell}{i} (\ell-i)^k \left((\ell-i)^{p-1}-1\right).$$

Ahora si $\ell - i$ es divisible por p, la fórmula demuestra que $a_{k+(p-1)} - a_k$ es también divisible por p. Si $\ell - i$ no es divisible por p, entonces por el pequeño teorema de Fermat $(\ell-i)^{p-1}-1 \equiv 0 \pmod p$, y $a_{k+(p-1)} - a_k$ es también divisible por p. ■

Demostración del teorema 16.1. Sea $c \neq 1$ algún número natural tal que $p \nmid c$. Consideramos la serie de potencias

$$f(t) := \frac{1}{t} - \frac{c}{(1+t)^c - 1}.$$

Ya que $p \nmid c$, el polinomio $\frac{(1+t)^c-1}{c}$ tiene coeficientes en $\mathbb{Z}_{(p)}$ y es invertible en $\mathbb{Z}_{(p)}((t))$:

$$\frac{c}{(1+t)^c-1} = \frac{1}{t} - \frac{c-1}{2} + \frac{c^2-1}{12}\,t + \cdots$$

Se sigue que

$$f(t) = \frac{1}{t} - \frac{c}{(1+t)^c-1} = \frac{c-1}{2} - \frac{c^2-1}{12}\,t + \cdots$$

tiene coeficientes en $\mathbb{Z}_{(p)}$. Podemos aplicar el lema de arriba a la serie

$$\begin{aligned} f(e^t-1) &= \frac{1}{e^t-1} - \frac{c}{e^{ct}-1} = \frac{1}{t}\left(\frac{t}{e^t-1} - \frac{ct}{e^{ct}-1}\right) \\ &= -\frac{1-c}{2} + \sum_{k\ge 2}\left((1-c^k)\,\frac{B_k}{k}\,\frac{t^{k-1}}{(k-1)!}\right). \end{aligned}$$

Aquí hemos usado la función generatriz $\frac{t}{e^t-1} = \frac{t\,e^t}{e^t-1} - t = 1 - \frac{t}{2}\sum_{k\ge 0} B_k\,\frac{t^k}{k!}$. El lema precedente implica que $(1-c^k)\,\frac{B_k}{k} \in \mathbb{Z}_{(p)}$ y que para todo $k' \equiv k \pmod{p-1}$ se tiene

$$(1-c^k)\,\frac{B_k}{k} \equiv (1-c^{k'})\,\frac{B_{k'}}{k'} \pmod p.$$

Sea c una raíz primitiva módulo p (un generador del grupo $(\mathbb{Z}/p\mathbb{Z})^\times$). Si $p-1 \nmid k$, como en la hipótesis del teorema, entonces $p-1 \nmid k'$, y se tiene $(1-c^k), (1-c^{k'}) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Esto implica que $\frac{B_k}{k} \in \mathbb{Z}_{(p)}$ y $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod p$. ■

17 * Numeradores de B_k (primos irregulares)

Sea p un número primo. Una **raíz p-ésima de la unidad** es un número complejo ζ tal que $\zeta^p = 1$. Las raíces p-ésimas de la unidad son precisamente

$$1,\ \zeta_p := e^{2\pi i/p},\ \zeta_p^2 = e^{2\pi i\,2/p},\ \ldots,\ \zeta_p^{p-1} = e^{2\pi i\,(p-1)/p}.$$

Estas son las raíces del **polinomio ciclotómico**

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

(en efecto, $\sum_{0\le k\le p} e^{2\pi ik/p} = 1$). Si añadimos al cuerpo $\mathbb{Q}$ las raíces p-ésimas de la unidad, se obtiene el cuerpo $\mathbb{Q}(\zeta_p)$ que recibe el nombre de **cuerpo ciclotómico**. Este cuerpo contiene el anillo

$$O_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p] := \{a_0 + a_1\,\zeta_p + a_2\,\zeta_p^2 + \cdots + a_{p-2}\,\zeta_p^{p-2}\},$$

llamado el **anillo de enteros** de $\mathbb{Q}(\zeta_p)$; es precisamente el anillo formado por todos los elementos $\alpha \in \mathbb{Q}(\zeta_p)$ tales que $f(\alpha) = 0$ para algún polinomio **mónico** $f(x) \in \mathbb{Z}[x]$ (es decir, el coeficiente mayor de $f(x)$ es 1).

A semejanza de $\mathbb{Z}$, muchos anillos son **dominios de factorización única**: todo elemento $x \neq 0$ puede ser escrito como un producto de primos

$$x = p_1 \cdot p_2 \cdots p_n,$$

y esta expresión es única, en el sentido de que si existe otra factorización $x = q_1 \cdot q_2 \cdots q_m$, entonces $n = m$ y, salvo alguna permutación de los factores, $q_i = u_i\,p_i$, donde u_i es invertible ($u_i = \pm 1$ en el caso de $\mathbb{Z}$).

No voy a entrar en detalles, pero resulta que el anillo $\mathbb{Z}[\zeta_p]$ es un dominio de factorización única para $p < 23$ y a partir de $p = 23$ la factorización única no se cumple. Este fenómeno se estudia en la **teoría de números algebraica**. A saber, a $\mathbb{Q}(\zeta_p)$ se asocia un grupo abeliano $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$, llamado el **grupo de clases** de $\mathbb{Q}(\zeta_p)$. Es un grupo finito, y su orden se llama el **número de clase**:

$$h_{\mathbb{Q}(\zeta_p)} := \#\mathrm{Cl}(\mathbb{Q}(\zeta_p)).$$

Resulta que $\mathbb{Z}[\zeta_p]$ es un dominio de factorización única si y solamente si $h_{\mathbb{Q}(\zeta_p)} = 1$ (es decir, si el grupo de clases $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ es trivial). La definición de $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ y la demostración de su finitud formaría parte de un curso de la teoría de números algebraica (véase por ejemplo [Neu1999] y [Mar1977]), pero intuitivamente, $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ mide qué tan lejos $\mathbb{Z}[\zeta_p]$ está de ser un dominio de factorización única.

He aquí una tabla de los grupos de clases de algunos cuerpos ciclotómicos $\mathbb{Q}(\zeta_p)$, calculados con ayuda de PARI/GP:

$$\begin{aligned}
\mathrm{Cl}(\mathbb{Q}(\zeta_2)) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{23})) &\cong \mathbb{Z}/3\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_3)) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{29})) &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_5)) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{31})) &\cong \mathbb{Z}/9\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_7)) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{37})) &\cong \mathbb{Z}/37\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_{11})) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{41})) &\cong \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_{13})) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{43})) &\cong \mathbb{Z}/211\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_{17})) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{47})) &\cong \mathbb{Z}/695\mathbb{Z},\\
\mathrm{Cl}(\mathbb{Q}(\zeta_{19})) &= 0, & \mathrm{Cl}(\mathbb{Q}(\zeta_{53})) &\cong \mathbb{Z}/4889\mathbb{Z}.
\end{aligned}$$

Todo esto está relacionado con una historia embarazosa que pasó al famoso matemático francés Gabriel Lamé (1795–1870). En 1847 Lamé presentó a la Academia de Ciencias de Francia una supuesta demostración del **último teorema de Fermat** [Lam1847]:

> Para $n > 2$ la ecuación $x^n + y^n = z^n$ no tiene soluciones para x, y, z enteros positivos.

Joseph Liouville (1809–1882) observó que su demostración usaba la hipótesis sospechosa de que $\mathbb{Z}[\zeta_p]$ era un dominio de factorización única. En efecto, el matemático alemán Ernst Kummer (1810–1893) había demostrado tres años antes en 1844 que para $\mathbb{Z}[\zeta_{23}]$ esto era falso, pero su resultado fue publicado en una revista poco conocida. Kummer comunicó su ejemplo a Liouville, y este en fin fue publicado en la revista de la Academia de Ciencias. Kummer logró demostrar el último teorema de Fermat para ciertos números primos $n = p$ que él llamó regulares:

17.1. Definición. Un primo p es **irregular** si p divide al número de clase $h_{\mathbb{Q}(\zeta_p)}$ del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$.

Por ejemplo, los primeros primos irregulares son $p = 37, 59, 67$, porque los números de clases correspondientes son

$$h_{\mathbb{Q}(\zeta_{37})} = 37, \quad h_{\mathbb{Q}(\zeta_{59})} = 3 \cdot 59 \cdot 233, \quad h_{\mathbb{Q}(\zeta_{67})} = 67 \cdot 12739.$$

Otro criterio, más fácil para nosotros, es el siguiente

17.2. Hecho (Kummer, 1850). *p es irregular si y solamente si p divide al numerador de algún número de Bernoulli B_{2k} para $2k \leq p - 3$.*

Para la demostración, véase por ejemplo [Was1997, Chapter 5].

No es tan fácil calcular $h_{\mathbb{Q}(\zeta_p)}$. Por ejemplo, en PARI/GP tenemos

```
? bnfinit(polcyclo(37)).clgp.no
% = 37
```

Para compilar una lista de los primos irregulares, tenemos que usar el criterio con los números de Bernoulli:

```
irregular_primes (n) = {
  local (p);
  for(i=1,n,
      p = prime (i);
      for (k=1, (p-3)/2,
          if (numerator(bernfrac(2*k))%p == 0, printf ("p = %d, B_%d\n", p,2*k))))
}
```

He aquí los primeros primos irregulares con los números de Bernoulli correspondientes. Note que 157 aparece en el numerador de B_{62} y B_{110}:

$$p = 37: \quad B_{32} = -\frac{37 \cdot 683 \cdot 305065927}{2 \cdot 3 \cdot 5 \cdot 17};$$

$$p = 59: \quad B_{44} = -\frac{11 \cdot 59 \cdot 8089 \cdot 2947939 \cdot 1798482437}{2 \cdot 3 \cdot 5 \cdot 23};$$

$$p = 67: \quad B_{58} = \frac{29 \cdot 67 \cdot 186707 \cdot 6235242049 \cdot 37349583369104129}{2 \cdot 3 \cdot 59};$$

$$p = 101: \quad B_{68} = -\frac{17 \cdot 37 \cdot 101 \cdot 123143 \cdot 1822329343 \cdot 55254733665109300282227481}{2 \cdot 3 \cdot 5};$$

$$p = 103: \quad B_{24} = -\frac{103 \cdot 2294797}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13};$$

$$p = 131: \quad B_{22} = \frac{11 \cdot 131 \cdot 593}{2 \cdot 3 \cdot 23};$$

$$p = 149: \quad B_{130} = \frac{5 \cdot 13 \cdot 149 \cdot 463 \cdot 2264267 \cdot 3581984682522167 \cdots}{2 \cdot 3 \cdot 11 \cdot 131};$$

$$p = 157: \quad B_{62} = \frac{31 \cdot 157 \cdot 266689 \cdot 329447317 \cdot 28765594733083851481}{6},$$

$$B_{110} = \frac{5 \cdot 157 \cdot 76493 \cdot 150235116317549231 \cdot 36944818874116823428357691 \cdots}{2 \cdot 3 \cdot 11 \cdot 23}.$$

Otro ejemplo curioso: 2017 divide el numerador de B_{1204} y es un primo irregular.

2	233	547	877	1229	1597	1993	2371	2749	3187
3	239	557	881	1231	1601	1997	2377	2753	3191
5	241	563	883	1237	1607	1999	2381	2767	3203
7	251	569	887	1249	1609	2003	2383	2777	3209
11	257	571	907	1259	1613	2011	2389	2789	3217
13	263	577	911	1277	1619	2017	2393	2791	3221
17	269	587	919	1279	1621	2027	2399	2797	3229
19	271	593	929	1283	1627	2029	2411	2801	3251
23	277	599	937	1289	1637	2039	2417	2803	3253
29	281	601	941	1291	1657	2053	2423	2819	3257
31	283	607	947	1297	1663	2063	2437	2833	3259
37	293	613	953	1301	1667	2069	2441	2837	3271
41	307	617	967	1303	1669	2081	2447	2843	3299
43	311	619	971	1307	1693	2083	2459	2851	3301
47	313	631	977	1319	1697	2087	2467	2857	3307
53	317	641	983	1321	1699	2089	2473	2861	3313
59	331	643	991	1327	1709	2099	2477	2879	3319
61	337	647	997	1361	1721	2111	2503	2887	3323
67	347	653	1009	1367	1723	2113	2521	2897	3329
71	349	659	1013	1373	1733	2129	2531	2903	3331
73	353	661	1019	1381	1741	2131	2539	2909	3343
79	359	673	1021	1399	1747	2137	2543	2917	3347
83	367	677	1031	1409	1753	2141	2549	2927	3359
89	373	683	1033	1423	1759	2143	2551	2939	3361
97	379	691	1039	1427	1777	2153	2557	2953	3371
101	383	701	1049	1429	1783	2161	2579	2957	3373
103	389	709	1051	1433	1787	2179	2591	2963	3389
107	397	719	1061	1439	1789	2203	2593	2969	3391
109	401	727	1063	1447	1801	2207	2609	2971	3407
113	409	733	1069	1451	1811	2213	2617	2999	3413
127	419	739	1087	1453	1823	2221	2621	3001	3433
131	421	743	1091	1459	1831	2237	2633	3011	3449
137	431	751	1093	1471	1847	2239	2647	3019	3457
139	433	757	1097	1481	1861	2243	2657	3023	3461
149	439	761	1103	1483	1867	2251	2659	3037	3463
151	443	769	1109	1487	1871	2267	2663	3041	3467
157	449	773	1117	1489	1873	2269	2671	3049	3469
163	457	787	1123	1493	1877	2273	2677	3061	3491
167	461	797	1129	1499	1879	2281	2683	3067	3499
173	463	809	1151	1511	1889	2287	2687	3079	3511
179	467	811	1153	1523	1901	2293	2689	3083	3517
181	479	821	1163	1531	1907	2297	2693	3089	3527
191	487	823	1171	1543	1913	2309	2699	3109	3529
193	491	827	1181	1549	1931	2311	2707	3119	3533
197	499	829	1187	1553	1933	2333	2711	3121	3539
199	503	839	1193	1559	1949	2339	2713	3137	3541
211	509	853	1201	1567	1951	2341	2719	3163	3547
223	521	857	1213	1571	1973	2347	2729	3167	3557
227	523	859	1217	1579	1979	2351	2731	3169	3559
229	541	863	1223	1583	1987	2357	2741	3181	3571

Los primeros primos irregulares

Desafortunadamente, hay un número infinito de primos irregulares. Esto fue demostrado por el matemático danés K. L. Jensen en 1915. En efecto, su resultado era más fuerte: hay un número infinito de primos irregulares de la forma $4k+3$. Nosotros no contentaremos con el siguiente

17.3. Teorema. *Hay un número infinito de primos irregulares; es decir, p que dividen el numerador de algún número de Bernoulli entre $B_2, B_4, \dots, B_{p-3}$.*

Demostración. El argumento es un poco similar a la demostración clásica del teorema de Euclides sobre la infinitud de los números primos: podemos suponer que $p_1, \dots, p_r$ son todos los primos irregulares. Nuestro objetivo es encontrar otro primo irregular.

Sea

$$k := N \cdot (p_1 - 1) \cdots (p_r - 1),$$

donde N es algún número tal que $|B_k/k| > 1$. Tal N existe porque para $k = 2n$ par,

$$|B_{2n}/2n| = \frac{(2n-1)!}{2^{2n-1}\,\pi^{2n}}\,\zeta(2n) \xrightarrow{n\to\infty} \infty.$$

Entonces existe algún primo p tal que p divide el numerador de B_k/k. Por el teorema de Clausen–von Staudt, los $p_1, \dots, p_r$ están en el denominador de B_k, de donde $p \notin \{p_1, \dots, p_r\}$. También tenemos $p - 1 \nmid k$, porque en el caso $p - 1 \mid k$ el primo p estaría en el denominador.

Sea $0 < k' < p - 1$ el número tal que $k' \equiv k \pmod{p-1}$. Por las congruencias de Kummer

$$\frac{B_{k'}}{k'} \equiv \frac{B_k}{k} \pmod{p},$$

y entonces $p \mid B_{k'}$ y p es irregular. ■

Todavía no se sabe si el número de primos regulares es también infinito, pero conjeturalmente, solo $1 - e^{-1/2} \approx 39\,\%$ de los primos son irregulares.

17.4. Ejercicio. *Calcule en PARI/GP el porcentaje de los primos irregulares entre los primeros N primos para algún N razonable (por ejemplo, $N = 300$).*

Para más información sobre el último teorema de Fermat para los primos regulares, véase el libro [Rib1979] (escrito mucho antes de la demostración definitiva del teorema por Andrew Wiles en 1995, pero con buenas explicaciones de los resultados de Kummer).

Referencias

[Ahl1978] Lars V. Ahlfors, *Complex analysis*, third ed., McGraw-Hill Book Co., New York, 1978, An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics. MR510197

[AIK2014] Tsuneo Arakawa, Tomoyoshi Ibukiyama, and Masanobu Kaneko, *Bernoulli numbers and zeta functions*, Springer Monographs in Mathematics, Springer, Tokyo, 2014, With an appendix by Don Zagier. MR3307736
http://dx.doi.org/10.1007/978-4-431-54919-2

[Ber1713] Jacob Bernoulli, *Ars conjectandi*, Impensis Thurnisiorum, fratrum, 1713.
http://books.google.com/books?id=kD4PAAAAQAAJ

[Eul1740] Leonhard Euler, *De summis serierum reciprocarum*, Commentarii academiae scientiarum Petropolitanae **7** (1740), 123–134.
http://eulerarchive.maa.org/pages/E041.html

[Eul1744] ———, *Variae observationes circa series infinitas*, Commentarii academiae scientiarum Petropolitanae **9** (1744), 160–188.
http://eulerarchive.maa.org/pages/E072.html

[Eul1755] Leonhardo Eulero, *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum*, Impensis Academiae imperialis scientiarum Petropolitanae, 1755.
http://eulerarchive.maa.org/pages/E212.html

[Eul1760] Leonhard Euler, *De seriebus divergentibus*, Commentarii academiae scientiarum Petropolitanae **5** (1760), 205–237.
http://eulerarchive.maa.org/pages/E247.html

[Eul1768] ———, *Remarques sur un beau rapport entre les series des puissances tant directes que reciproques*, Mémoires de l'académie des sciences de Berlin **17** (1768), 83–106.
http://eulerarchive.maa.org/pages/E352.html

[Kah2005] Bruno Kahn, *Algebraic K-theory, algebraic cycles and arithmetic geometry*, Handbook of *K*-theory. Vol. 1, 2, Springer, Berlin, 2005, pp. 351–428. MR2181827
http://www.math.illinois.edu/K-theory/handbook/

[Kat2004] Yitzhak Katznelson, *An introduction to harmonic analysis*, third ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2004. MR2039503
http://dx.doi.org/10.1017/CBO9781139165372

[Lam1847] Gabriel Lamé, *Démonstration générale du théorème de Fermat, sur l'imposibilité, en nombres entiers, de l équation* $x^n + y^n = z^n$, Comptes rendus hebdomadaires des séances de l'Académie des sciences **XXIV** (1847), no. 9, 310–316.
http://gallica.bnf.fr/ark:/12148/bpt6k29812/f310.image

[Mar1977] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977, Universitext. MR0457396

[Neu1999] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859
http://dx.doi.org/10.1007/978-3-662-03983-0

[Rib1979] Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, New York-Heidelberg, 1979. MR551363

[vdP1979] Alfred van der Poorten, *A proof that Euler missed. . .Apéry's proof of the irrationality of* $\zeta(3)$, Math. Intelligencer **1** (1979), no. 4, 195–203, An informal report. MR547748
http://dx.doi.org/10.1007/BF03028234

[Was1997] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575
http://dx.doi.org/10.1007/978-1-4612-1934-7

[Wei2005] Charles Weibel, *Algebraic K-theory of rings of integers in local and global fields*, Handbook of *K*-theory. Vol. 1, 2, Springer, Berlin, 2005, pp. 139–190. MR2181823
http://www.math.illinois.edu/K-theory/handbook/

[Zud2004] Wadim Zudilin, *Arithmetic of linear forms involving odd zeta values*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 251–291. MR2145585
http://jtnb.cedram.org/item?id=JTNB_2004__16_1_251_0