Universidad de los Andes

Facultad de Ciencias

Departamento de Matemática

Una Nueva Fórmula de Recurrencia para los Números de Bernoulli

Glauco Alfredo López Díaz

Notas de Matemática

Serie: Pre-Print

No. 213

Mérida - Venezuela

2001

Diseño de Portada: Juan E. Rondón

Notas de Matemática, No. 213
Mérida, 2001.

Una Nueva Fórmula de Recurrencia para los Números de Bernoulli*

Glauco López

Abstract

En estas notas estudiaremos una reciente fórmula de recurrencia para los números de Bernoulli demostrada por **E. Deeba** y **D. Rodríguez** en [**5**] , así como también otra demostración de esta misma fórmula hecha por **F. T. Howard** en [**6**] como aplicación de la fórmula multiplicativa para los polinomios Bernoulli. Por otra parte, como aplicaciones de esta nueva fórmula de recurrencia se presentan nuevas demostraciones de los teoremas clásicos de **Von Staudt-Clausen**, **Carlitz**, **Frobenius**, **Voronoi** y **Ramanujan** acerca de congruencia que involucran a números de Bernoulli.

1 Preliminares

Definición 1.1 *Los polinomios de Bernoulli denotados por $B_m(x)$ se definen de la siguiente manera:*

$$B_m(x) = \frac{x^m}{(m-1)!} + m! \sum_{j=1}^{m} \frac{B_j x^{m-j}}{j!(m-j)!}$$

donde los B_m para todo $m \geq 1$, son los numeros de Bernoulli y estan dados por la siguiente fómula de recurrencia:

$$0 = 1 + \sum_{j=1}^{m-1} \binom{m}{j} B_j \text{ , para todo } m \geq 1 \tag{1.1}$$

Lema 1.2 *Para todo $m \geq 1$ se tiene:*

$$B_m = \sum_{j=1}^{m} \frac{1}{j+1} \cdot \sum_{l=1}^{j} (-1)^l \binom{j}{l} l^m \tag{1.2}$$

* This research was partially supported by CDCHT-ULA under proyect C-677-94-05-E.

Lema 1.3 *Los polinomios de Bernoulli satisfacen la siguiente fórmula:*

$$B_m(x) = \sum_{j=0}^{m} \binom{m}{j} B_j x^{m-j}\,, para\, todo\, m \geq 1 \tag{1.3}$$

Lema 1.4 Fórmula Multiplicativa para los Polinomios de Bernoulli *Para todo $m \geq 1$ el polinomio de Bernoulli $B_m(x)$ satisface la siguiente fórmula multiplicativa:*

$$B_m(kx) = k^{m-1} \sum_{j=0}^{k-1} B_m \left(x + \frac{j}{k} \right)\,, para\, todo\, m \geq 1 \tag{1.4}$$

Lema 1.5 *La siguiente serie de potencias:*

$$\sum_{r=1}^{\infty} (-1)^r \frac{B_r}{r!} z^r,\ con\, B_0 = 1$$

converge uniformemente a la función:

$$\Psi(z) = z \frac{e^z}{e^z - 1}$$

para todo $z \in \mathbb{C}$ con $\left| e^z \right| \neq 1$ y $R_e(z) \neq 0$. En particular,

$$\frac{z}{e^z - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} z^r\,, para\, todo\, z \in \mathbb{C}\, con\, |z| < 2\pi \tag{1.5}$$

2 Una Nueva Fórmula de Recurrencia para Los Números de Bernoulli

Teorema 2.1 (Deeba y Rodríguez) *Para todo $m \geq 1$ los números de Bernoulli satisfacen la siguiente relación:*

$$B_m = \frac{1}{n(1 - n^m)} \sum_{k=0}^{m-1} n^k \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k}\,, con\, n \geq 1 \tag{2.6}$$

Demostración. Por la fórmula multiplicativa de los polinomios de Bernoulli 1.4, se verifica:

$$n^{1-m}B_m(nx) = \sum_{j=0}^{n-1} B_m\left(x + \frac{j}{n}\right)$$

Entonces, para $x = 0$ se cumple:

$$n^{1-m}B_m(0) = \sum_{j=0}^{n-1} B_m\left(\frac{j}{n}\right)$$

y como $B_m(0) = B_m$ para todo $m \geq 1$, se tiene:

$$n^{1-m}B_m = \sum_{j=0}^{n-1} B_m\left(\frac{j}{n}\right)$$

De donde,

$$nB_m = n^m \sum_{j=0}^{n-1} B_m\left(\frac{j}{n}\right) = n^m \left(B_m(0) + \sum_{j=1}^{n-1} B_m\left(\frac{j}{n}\right)\right)$$

$$= n^m B_m + n^m \sum_{j=1}^{n-1} B_m\left(\frac{j}{n}\right)$$

Esto es,

$$nB_m = n^m B_m + n^m \sum_{j=1}^{n-1} B_m\left(\frac{j}{n}\right)$$

A su vez, por la fórmula 1.3 aplicada a $x = \frac{j}{n}$, obtenemos:

$$B_m\left(\frac{j}{n}\right) = \sum_{k=0}^{m} \binom{m}{k} B_k \left(\frac{j}{n}\right)^{m-k}$$

Nótece que si $x \neq 0$ entonces $\frac{j}{n} \neq 0$; es decir, $j \neq 0$; lo cual implica que,

$$nB_m = n^m B_m + n^m \sum_{j=1}^{n-1} \sum_{k=0}^{m} \binom{m}{k} B_k \cdot \left(\frac{j}{n}\right)^{m-k}$$

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

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

En consecuencia,

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

A su vez,

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

$$= \sum_{k=0}^{m-1} n^k \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k} + n^m B_m + n^m B_m \cdot (n-1)$$

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

Así,

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

Luego,

$$B_m = \frac{1}{n(1-n^m)} \sum_{k=0}^{m-1} n^k \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k}$$

Por consiguiente la fórmula 2.6 es cierta para todo $m \geq 1$. ∎

Observación: En el siguiente teorema presentamos una nueva demostración de la fórmula 2.6, hecha por **F.T. Howard** en [**6**] , la cual es una aplicación de la fórmula multiplicativa para los polinomios de Bernoulli 1.4; pero para ello necesitamos algo de notación y un lema previo.

Notación: Dados h y t enteros positivos y p primo denotaremos por $p^h || t$, a la siguiente afirmación:

$$p^h \textit{ divide a } t\textit{, pero } p^{h+1} \textit{ no divide a } t$$

Además, para k y n enteros positivos designamos por $S_k(n)$ a la suma de las k-ésimas potencias de los n primeros enteros positivos, o bien,

$$S_k(n) = 1^k + 2^k + \cdots + n^k \tag{2.7}$$

Lema 2.2 *La función generatriz para $S_k(n)$ está dada por:*

$$F(x,n) = \sum_{k=0}^{\infty} S_k(n)\frac{x^k}{k!} = e^x + e^{2x} + \cdots + e^{nx} = \frac{e^{(n+1)x} - e^x}{e^x - 1} \tag{2.8}$$

para todo $x \neq 0$

Demostración. Por la fórmula 2.7 para k y n enteros positivos resulta:

$$S_k(n)\frac{x^n}{k!} = (1^k + 2^k + \cdots + n^k)\frac{x^k}{k!} = \frac{x^k}{k!} + \frac{(2x)^k}{k!} + \cdots + \frac{(nx)^k}{k!}$$

O sea,

$$S_k(n)\frac{x^n}{k!} = \frac{x^k}{k!} + \frac{(2x)^k}{k!} + \cdots + \frac{(nx)^k}{k!}$$

Por lo cual,

$$F(x,n) = \sum_{k=0}^{\infty} S_k(n)\frac{x^n}{k!} = \sum_{k=0}^{\infty}\left(\frac{x^k}{k!} + \frac{(2x)^k}{k!} + \cdots + \frac{(nx)^k}{k!}\right)$$

$$= \sum_{k=0}^{\infty}\frac{x^k}{k!} + \sum_{k=0}^{\infty}\frac{(2x)^k}{k!} + \cdots + \sum_{k=0}^{\infty}\frac{(nx)^k}{k!} = e^x + e^{2x} + \cdots + e^{nx}$$

Resumiendo, nos queda:

$$F(x,n) = \sum_{k=0}^{\infty} S_k(n)\frac{x^k}{k!} = e^x + e^{2x} + \cdots + e^{nx}$$

Ahora, para $x \neq 0$ se deduce que:

$$e^x + e^{2x} + \cdots + e^{nx} = (e^x + e^{2x} + \cdots + e^{nx})\left(\frac{e^x - 1}{e^x - 1}\right) = \frac{e^{(n+1)x} - e^x}{e^x - 1}$$

Por lo tanto,

$$F(x,n) = \sum_{k=0}^{\infty} S_k(n)\frac{x^k}{k!} = \frac{e^{(n+1)x} - e^x}{e^x - 1}$$

La cual es la fórmula 2.8 para $x \neq 0$. ∎

Teorema 2.3 *Para todo $m \geq 1$ los números de Bernoulli satisfacen la siguiente fórmula de recurrencia:*

$$B_m = \frac{1}{n(1-n^m)} \sum_{k=0}^{m-1} n^k \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k}\, , con\, n \geq 1$$

Demostración. Por la fórmula 1.5 aplicada a $x \in \mathbb{R}$ con $|x| < \pi$ se verifica:

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} B_m \frac{x^m}{m!}$$

Entonces,

$$\sum_{m=0}^{\infty} (n - n^m) B_m \frac{x^m}{m!} = n \sum_{m=0}^{\infty} B_m \frac{x^m}{m!} - \sum_{m=0}^{\infty} B_m \frac{(nx)^m}{m!} = n \frac{x}{e^x - 1} - \frac{nx}{e^{nx} - 1}$$

$$= \frac{nx}{e^{nx} - 1} \cdot \frac{e^{nx} - e^x}{e^x - 1}$$

Esto es,

$$\sum_{m=0}^{\infty} (n - n^m) B_m \frac{x^m}{m!} = \frac{nx}{e^{nx} - 1} \cdot \frac{e^{nx} - e^x}{e^x - 1}$$

Como por la fórmula 2.8 la función generatriz de $S_j(n-1)$ está dada por:

$$F(x, n-1) = \sum_{j=0}^{\infty} S_j(n-1) \frac{x^j}{j!} = \frac{e^{nx} - e^x}{e^x - 1}$$

se cumple que:

$$\frac{nx}{e^{nx} - 1} \cdot \frac{e^{nx} - e^x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{(nx)^k}{k!} \sum_{j=0}^{\infty} S_j(n-1) \frac{x^j}{j!}$$

$$= \sum_{k=0}^{\infty} \frac{n^k B_k x^k}{k!} \sum_{j=0}^{\infty} \frac{S_j(n-1) x^j}{j!}$$

Es decir,

$$\frac{nx}{e^{nx} - 1} \cdot \frac{e^{nx} - e^x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{n^k B_k x^k}{k!} \sum_{j=0}^{\infty} \frac{S_j(n-1) x^j}{j!}$$

De donde,

$$\sum_{m=0}^{\infty}(n-n^m)\frac{B_m}{m!}x^m=\sum_{k=0}^{\infty}\frac{n^kB_kx^k}{k!}\sum_{j=0}^{\infty}\frac{S_j(n-1)x^j}{j!}$$

$$=\sum_{k\geq 0}\sum_{j\geq 0}\frac{n^kB_kx^kS_j(n-1)x^j}{k!j!}=\sum_{j\geq 0}\sum_{k\geq 0}\frac{n^kB_kS_j(n-1)x^{j+k}}{k!j!}$$

Ahora, llamando $j=m-k$ se tiene que $j+k=m$; y además,

$$\sum_{j\geq 0}\sum_{k\geq 0}\frac{n^kB_kS_j(n-1)x^{j+k}}{k!j!}=\sum_{m-k\geq 0}\sum_{k\geq 0}\frac{n^kB_kx^kS_{m-k}(n-1)x^m}{k!(m-k)!}$$

$$=\sum_{m\geq k}\sum_{k\geq 0}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)x^m=\sum_{m=0}^{\infty}\sum_{k=0}^{m}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)x^m$$

En otras palabras,

$$\sum_{k=0}^{\infty}\frac{n^kB_kx^k}{k!}\sum_{j=0}^{\infty}\frac{S_j(n-1)x^j}{j!}=\sum_{m=0}^{\infty}\sum_{k=0}^{m}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)x^m$$

Lo cual implica que,

$$\sum_{m=0}^{\infty}(n-n^m)\frac{B_m}{m!}x^m=\sum_{m=0}^{\infty}\sum_{k=0}^{m}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)x^m$$

Igualando los coeficientes de x^m se tiene:

$$(n-n^m)\frac{B_m}{m!}=\sum_{k=0}^{m}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)$$

En consecuencia,

$$\frac{(n-n^m)}{n(1-n^m)}\frac{B_m}{m!}=\frac{1}{n(1-n^m)}\sum_{k=0}^{m}\left(\frac{n^kB_kS_{m-k}(n-1)}{k!(m-k)!}\right)$$

Por otra parte, como $S_{m-k}(n-1)=\sum_{j=1}^{n-1}j^{m-k}$ resulta:

$$\left(\frac{n-n^{m+1}+n^{m+1}-n^m}{n(1-n^m)}\right)\frac{B_m}{m!}=\frac{1}{n(1-n^m)}\sum_{k=0}^{m}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}$$

O bien,

$$\left(\frac{n(1-n^m)+n^m(n-1)}{n(1-n^m)}\right)\frac{B_m}{m!}=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}$$
$$+\frac{n^mB_m}{n(1-n^m)m!(m-n)!}\sum_{j=1}^{n-1}j^{m-m}$$

Escrito de otra forma, nos queda:

$$\left(1+\frac{n^m(n-1)}{n(1-n^m)}\right)\frac{B_m}{m!}=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}$$
$$+\frac{n^mB_m}{n(1-n^m)m!0!}\sum_{j=1}^{n-1}j^{0}$$

O sea,

$$\frac{B_m}{m!}+\frac{1}{n(1-n^m)}n^m\frac{B_m}{m!}(n-1)$$
$$=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}+\frac{1}{n(1-n^m)}n^m\frac{B_m}{m!}\cdot(n-1)$$

Así,

$$\frac{B_m}{m!}=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}$$

Luego,

$$B_m=\frac{m!}{n(1-n^m)}\sum_{k=0}^{m-1}\frac{n^kB_k}{k!}\cdot\frac{1}{(m-k)!}\sum_{j=1}^{n-1}j^{m-k}$$

Por consiguiente,

$$B_m=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}n^k\cdot\frac{m!}{k!(m-k)!}B_k\sum_{j=1}^{n-1}j^{m-k}$$

Por lo tanto,

$$B_m=\frac{1}{n(1-n^m)}\sum_{k=0}^{m-1}n^k\binom{m}{k}B_k\sum_{j=1}^{n-1}j^{m-k}$$

Con lo cual se concluye que, la fórmula de recurrencia 2.6 es válida para todo $m\geq 1$. ∎

Lema 2.4 *Si p es un número primo y k es un entero no negativo, entonces*

$$S_k(p-1) \equiv \begin{cases} -1 \quad mod\ p \quad si \quad (p-1)|k \\ \ \ 0 \quad mod\ p \quad si \quad (p-1)\not|k \end{cases}$$

Demostración. Si p es un número primo entonces por el Teorema de Fermat se verifica:

$$a^{p-1} \equiv 1\ mod\ p\,, para\,(a,p) = 1$$

Como p es primo se cumple que $(a,p) = 1$ para todo $a = 1, \ldots, p-1$. De donde,

$$a^{p-1} \equiv 1\ mod\ p\,, para\,todo\,a = 1, \ldots, p-1$$

Lo cual implica que,

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p-1 \quad mod\ p$$

A su vez, como $p-1 \equiv -1\ mod\ p$ se tiene:

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1\ mod\ p$$

Ahora, si $(p-1)|k$ entonces $k = q(p-1)$ para algún entero positivo. En consecuencia,

$$\begin{aligned} S_k(p-1) &= 1^k + 2^k + \cdots + (p-1)^k \\ &= 1^{q(p-1)} + 2^{q(p-1)} + \cdots + (p-1)^{q(p-1)} \\ &= \left(1^{(p-1)}\right)^q + \left(2^{(p-1)}\right)^q + \cdots + \left((p-1)^{(p-1)}\right)^q \end{aligned}$$

Esto es,

$$S_k(p-1) = \left(1^{(p-1)}\right)^q + \left(2^{(p-1)}\right)^q + \cdots + \left((p-1)^{(p-1)}\right)^q$$

De nuevo, como $a^{(p-1)} \equiv -1\ mod\ p$ para todo $a = 1, \ldots, p-1$; resulta:

$$(a^{(p-1)})^q \equiv 1\ mod\ p\,, para\,todo\,q = 1, \ldots, p-1$$

Así,

$$(1^{(p-1)})^q + (2^{(p-1)})^q + \cdots + ((p-1)^{(p-1)})^q \equiv (p-1)\ mod\ p$$

Otra vez, como $p-1 \equiv -1\ mod\ p$ tenemos:

$$(1^{(p-1)})^q + (2^{(p-1)})^q + \cdots + ((p-1)^{(p-1)})^q \equiv -1\ mod\ p$$

Es decir,

$$1^k + 2^k + \cdots + (p-1)^k \equiv -1 \ mod \ p$$

Luego,

$$S_k(p-1) \equiv -1 \ mod \ p \, , si \ (p-1)|k$$

Por otra parte, supongamos que $(p-1)\not| k$. Como p es primo la ecuación:

$$x^{p-1} \equiv 1 \ mod \ p$$

tiene $p-1$ raíces, las cuales son $1, 2, \ldots, p-1$. Sea g una raíz primitiva módulo p. Entonces, $g, g^2, \ldots, g^{p-1}$ es una permutación de las raíces $1, 2, \ldots, p-1$ módulo p. De donde,

$$1^k + 2^k + \cdots + (p-1)^k \equiv g^k + (g^2)^k + \cdots + (g^{(p-1)})^k \ mod \ p$$

Por otra lado,

$$g^k + (g^2)^k + \cdots + (g^{(p-1)})^k = g^k + (g^k)^2 + \cdots + (g^k)^{(p-1)}$$

$$= (g^k + (g^k)^2 + \cdots + (g^k)^{(p-1)}) \cdot \frac{(g^k - 1)}{g^k - 1} = \frac{g^k((g^k)^{(p-1)} - 1)}{g^k - 1}$$

Lo cual implica que,

$$g^k + (g^2)^k + \cdots + (g^{(p-1)})^k = \frac{g^k \left((g^k)^{(p-1)} - 1\right)}{g^k - 1}$$

En consecuencia,

$$1^k + 2^k + \cdots + (p-1)^k \equiv \frac{g^k \left((g^k)^{(p-1)} - 1\right)}{g^k - 1} \ mod \ p$$

Como p es primo y $(p-1)\not| k$ obtenemos que $(g^k, p) = 1$ y por lo cual, $(g^k)^{p-1} \equiv 1 \ mod \ p$. Así,

$$\frac{g^k \left((g^k)^{(p-1)} - 1\right)}{g^k - 1} \equiv 0 \ mod \ p$$

Luego, $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \ mod \ p$. Por consiguiente,

$$S_k(p-1) \equiv 0 \ mod \ p \, , si \ (p-1)\not| k$$

Por lo tanto, se infiere el resultado del lema. ∎

Lema 2.5 *Si p es un número primo tal que $p^h \parallel m$ y $k > 2$, entonces*

$$p^k \binom{m}{k} \equiv 0 \ mod \ p^{h+2} \tag{2.9}$$

Si p es impar entonces la congruencia también es válida para $k = 2$, o bien,

$$p^2 \binom{m}{2} \equiv 0 \ mod \ p^{h+2} \tag{2.10}$$

Si $p \geq 5$ y $k \geq 4$ entonces el módulo puede ser elevado a p^{h+4}, o sea,

$$p^k \binom{m}{k} \equiv 0 \ mod \ p^{h+4} \tag{2.11}$$

Demostración. Supongamos primero que p es un número impar y $k = 2$. Entonces,

$$p^2 \binom{m}{2} = p^2 \cdot \frac{m!}{2!(m-2)!} = \frac{p^2 m(m-1)}{2}$$

En otras palabras,

$$p^2 \binom{m}{2} = \frac{p^2 m(m-1)}{2}$$

Como $p^h \parallel m$ se verifica que $p^h | m$ y $p^{h+1} \nmid m$, esto es, $m = p^h r$ para algún r entero positivo. De donde, $p^2 m = p^{h+2} r$. Lo cual implica que $p^{h+2} | p^2 m$. En consecuencia,

$$p^2 m \equiv 0 \ mod \ p^{h+2}$$

Así,

$$\frac{p^2 m(m-1)}{2} \equiv 0 \ mod \ p^{h+2}$$

Luego,

$$p^2 \binom{m}{2} \equiv 0 \ mod \ p^{h+2}$$

Por consiguiente, la congruencia 2.10 es válida para todo p primo impar. Ahora, supongamos que $k > 2$ y $p^w \parallel k$. Entonces,

$$p^k \binom{m}{k} = \frac{p^k m}{k} \frac{(m-1)!}{(k-1)!(m-1-(k-1))!} = \frac{p^k m}{k} \binom{m-1}{k-1}$$

Es decir,

$$p^k \binom{m}{k} = \frac{p^k m}{k} \binom{m-1}{k-1} \tag{2.12}$$

A su vez, como $p^h \parallel m$ se cumple que $p^h | m$ y $p^{h+1} \not| m$. Por otra parte, como $p^w \parallel k$ se tiene que $p^w | k$ y $p^{w+1} \not| k$. De donde, $k = tp^w$, para algún entero positivo t. Escribiendo esto de otra forma nos queda:

$$\frac{1}{k} = \frac{1}{tp^w}$$

Lo cual implica que,

$$\frac{p^k}{k} = \frac{p^k}{tp^w}, \quad \text{o sea,} \quad \frac{tp^k}{k} = p^{k-w}$$

En consecuencia,

$$\frac{tp^k}{k} \binom{m-1}{k-1} = p^{k-w} \binom{m-1}{k-1}$$

Pero, como $\binom{m-1}{k-1}$ es un entero positivo resulta:

$$p^{k-w} \left| \frac{p^k}{k} \binom{m-1}{k-1} \right.$$

Así,

$$p^h p^{k-w} \left| m \frac{p^k}{k} \binom{m-1}{k-1} \right. , ya\, que\, t < k$$

Esto nos dice, por la ecuación 2.12 que

$$p^{h+(k-w)} \left| p^k \binom{m}{k} \right.$$

Luego,

$$p^k \binom{m}{k} \equiv 0 \; mod \; p^{h+(k-w)}$$

Veamos que $k - w \geq 2$. Si $w \geq 2$ entonces para p primos tenemos que $p^w - w \geq 2$. Como $p^w \parallel k$ obtenemos que $k > p^w$. Por consiguiente, $k - w \geq p^w - w \geq 2$. A su vez, como $k > 2$ si $w = 0$ ó $w = 1$ se deduce que $k - w \geq 2$. De donde,

$$p^k \binom{m}{k} \equiv 0 \; mod \; p^{h+(k-w)} \, , con\, k - w \geq 2$$

En particular,

$$p^k \binom{m}{k} \equiv 0 \; mod \; p^{h+2}$$

Lo cual implica que la congruencia 2.9 es cierta para todo p primo tal que $p^h \parallel m$ y $k > 2$. Por último, si $w > 0$ entonces para un primo $p \geq 5$ es cierto que $p^w - w \geq 4$. De nuevo, como $p^w \parallel k$ y $k > 4$ es válido que $k > p^w$. En consecuencia, $k - w \geq p^w - w \geq 4$. Pero, si $w = 0$ entonces $k - 0 \geq 4$. Así,

$$p^k \binom{m}{k} \equiv 0 \; mod \; p^{h+(k-w)}$$

cada vez que $k - w \geq 4$, para $p \geq 5$ y $k \geq 4$. Luego,

$$p^k \binom{m}{k} \equiv 0 \; mod \; p^{h+4}\, , para\, p \geq 5\, y\, k \geq 4$$

Por consiguiente, el módulo de la congruencia 2.9 puede ser elevada a p^{h+4} cuando $p \geq 5$ y $k \geq 4$. Por tanto, la congruencia 2.11 es válida para todo primo $p \geq 5$ y $k \geq 4$. ∎

Definición 2.6 *Sean a, b y m números enteros $m > 1$. Si $(b, m) = 1$ entonces diremos que $\frac{a}{b}$ es un entero módulo m. Además, si $\frac{a}{b}$ y $\frac{c}{d}$ son enteros módulo m diremos que $\frac{a}{b}$ es congruente a $\frac{c}{d}$ módulo m, lo cual denotaremos por:*

$$\frac{a}{b} \equiv \frac{c}{d} \; mod \; m$$

sí y sólo si m divide a $(ad - bc)$; o bien, sí y sólo si $ad \equiv bc \; mod \; m$ en el sentido usual de congruencias sobre los enteros.

En los siguientes dos teoremas enunciamos las propiedades básicas de las congruencias módulo m sobre racionales, las cuales presentamos sin demostración ya que su verificación es muy sencilla.

Teorema 2.7 *Sea m un entero positivo con $m > 1$. Entonces, la relación congruencia módulo m define una relación de equivalencia en el conjunto de los números racionales.*

Teorema 2.8 *Sean* a, b, c, d, e, f, g, h *y* m *enteros positivos con* $m > 1$. *Si* $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ *y* $\frac{g}{h}$ *son enteros módulo* m*, entonces las siguientes propiedades de las congruencias módulo* m *sobre los racionales son válidas:*

1) $\frac{a}{b} \equiv \frac{c}{d}$ *mod* m *y* $\frac{a}{b} - \frac{c}{d} \equiv 0$ *mod* m *son equivalentes.*

2) *Si* $\frac{a}{b} \equiv \frac{c}{d}$ *mod* m *y* $\frac{e}{f} \equiv \frac{g}{h}$ *mod* m*, entonces*

$$\frac{a}{b}x + \frac{e}{f}y \equiv \frac{c}{d}x + \frac{g}{h}y \ mod\ m,$$

para todos los enteros x *e* y.

3) *Si* $\frac{a}{b} \equiv \frac{c}{d}$ *mod* m *y* $\frac{e}{f} \equiv \frac{g}{h}$ *mod* m*, entonces* $\frac{ae}{bf} \equiv \frac{cg}{dh}$ *mod* m

4) *Si* $\frac{a}{b} \equiv \frac{a}{d}$ *mod* m *y* $n|m$ *con* $n > 0$*, entonces* $\frac{a}{b} \equiv \frac{c}{d}$ *mod* n

Teorema 2.9 *Si* p *es un número primo y* $m > 0$ *entonces*

$$pB_{2m} \equiv \begin{cases} -1 & mod\ p \quad si \quad (p-1)|2m \\ 0 & mod\ p \quad si \quad (p-1)\nmid 2m \end{cases}$$

Demostración. Por inducción sobre m. Para $m = 1$ se verifica que $2m = 2$ y
$B_{2m} = B_2 = \frac{1}{6}$. Como el único divisor primo de $2m = 2$ es $p = 2$ se cumple que $p - 1 = 1$ y $1|2$, es decir, $(p-1)|2m$. Entonces, $pB_{2m} = 2B_2 = 2\frac{1}{6} = \frac{1}{3}$.

De donde, $pB_{2m} \equiv -1$ *mod* p. Lo cual implica que,

$$pB_{2m} \equiv -1 \ mod\ p\,, si\,(p-1)|2m\, para\, m = 1$$

En consecuencia, el enunciado del teorema es cierto para $m = 1$.

Supongamos que $(p-1)\nmid 2k$ para todo $k = 1, \ldots, m-1$; y supongamos, como hipótesis de inducción, que el enunciado del teorema es válido para $k = 2, \ldots, m-1$. Así, por la fórmula 2.6, se tiene:

$$n(1 - n^m)B_m = \sum_{k=0}^{m-1} n^n \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k} = n^0 \binom{m}{0} B_0 \sum_{j=1}^{m-1} j^{m-0}$$

$$+\sum_{k=1}^{m-1} n^k \binom{m}{k} B_k \sum_{j=1}^{n-1} j^{m-k} = S_m(n-1) + \sum_{k=1}^{m-1} n^k \binom{m}{k} B_k S_{m-k}(n-1)$$

Luego, para $n = p$ resulta:

$$p(1-p^m)B_m = S_m(p-1) + \sum_{k=1}^{m-1} p^k \binom{m}{p} B_k S_{m-k}(p-1)$$

Evaluando en $2m$ nos queda:

$$p(1-p^{2m})B_{2m} = S_{2m}(p-1) + \sum_{k=1}^{2m-1} p^k \binom{2m}{k} B_k S_{2m-k}(p-1)$$

$$= S_{2m}(p-1) + p^1 \binom{2m}{1} B_1 S_{2m-1}(p-1) + \sum_{k=2}^{2m-1} p^k \binom{2m}{k} B_k S_{2m-k}(p-1)$$

A su vez, como $B_1 = -\dfrac{1}{2}$ y $B_{2k+1} = 0$ para todo $k \geq 1$, tenemos:

$$p(1-p^{2m})B_{2m}$$

$$= S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1) \qquad (2.13)$$

O sea,

$$pB_{2m} - \left(S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1)\right)$$

$$= P^{2m+1} B_{2m}$$

Por consiguiente,

$$p^{2m+1} \Big| pB_{2m} - \left(S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1)\right)$$

Entonces, como para todo $p | p^{2m+1}$ obtenemos:

$$p \Big| pB_{2m} - \left(S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1)\right)$$

De donde,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1) \ mod \ p$$

Por otra parte, si $(p-1)\not|\,2k$ para $k = 1, \ldots, m-1$, entonces por hipótesis de inducción se deduce que:

$$pB_{2k} \equiv 0 \ mod \ p \,, para\, todo\, k = 1, \ldots, m-1$$

Lo cual implica que,

$$p^{2k}B_{2k} \equiv 0 \ mod \ p \,, para\, todo\, k = 1, \ldots, m-1$$

En consecuencia,

$$p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1) \equiv 0 \ mod \ p, \quad \text{para todo} \quad k = 1, \ldots, m-1$$

Así,

$$\sum_{k=1}^{m-1} p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1) \equiv 0 \ mod \ p$$

Luego,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1) \ mod \ p$$

Ahora, como $p \equiv 0 \ mod \ p$ y m, $S_{2m-1}(p-1)$ son enteros positivos, se verifica:

$$-mpS_{2m-1}(p-1) \equiv 0 \ mod \ p$$

Por consiguiente, $pB_{2m} \equiv S_{2m}(p-1) \ mod \ p$. Por último, como

$$S_{2m}(p-1) \equiv \begin{cases} -1 \quad mod \ p & \text{si} \quad (p-1)|2m \\ \ \ 0 \quad mod \ p & \text{si} \quad (p-1)\not|\,2m \end{cases}$$

por el lema 2.4, se cumple:

$$pB_{2m} \equiv \begin{cases} -1 \quad mod \ p & \text{si} \quad (p-1)|2m \\ \ \ 0 \quad mod \ p & \text{si} \quad (p-1)\not|\,2m \end{cases}$$

Por lo tanto, el enunciado es cierto para todo $m \geq 1$. ∎

Teorema 2.10 (Von Staudt - Clausen) *Para* $m \geq 1$,

$$B_{2m} = G_{2m} - \sum_{(p-1)|2m} \frac{1}{p}$$

donde G_{2m} *es un entero y la suma esta tomada sobre todos los primos* p *tales que* $(p-1)$ *divide a* $2m$.

Demostración. Para demostrar este teorema veamos que es equivalente al teorema 2.9. En primer lugar veamos que el teorema 2.10 implica al teorema 2.9. Sea m un entero positivo cualquiera y sea q un número primo arbitrario. Entonces, por el teorema 2.10 se verifica:

$$B_{2m} = G_{2m} - \sum_{(p-1)|2m} \frac{1}{p}$$

donde G_{2m} es un entero y la suma esta tomada sobre todos los primos p tales que $(p-1)$ divide a $2m$. De donde,

$$qB_{2m} = qG_{2m} - \sum_{(p-1)|2m} \frac{q}{p}$$

Si $(p-1)|2m$ entonces,

$$qB_{2m} = qG_{2m} - \sum_{\substack{(p-1)|2m \\ p\neq q}} \frac{q}{p} - 1 = qG_{2m} - q\left(\sum_{\substack{(p-1)|2m \\ p\neq q}} \frac{1}{p}\right) - 1$$

Esto es,

$$qB_{2m} = qG_{2m} - q\left(\sum_{\substack{(p-1)|2m \\ p\neq q}} \frac{1}{p}\right) - 1$$

Lo cual implica que,

$$qG_{2m} - q\left(\sum_{\substack{(p-1)|2m \\ p\neq q}} \frac{1}{p}\right) - 1 \equiv -1 \ mod \ q$$

En consecuencia, $qB_{2m} \equiv -1 \ mod \ q$. Pero, si $(q-1)\nmid 2m$ entonces

$$qB_{2m} = qG_{2m} - q\sum_{(p-1)|2m} \frac{1}{p}$$

Así,

$$qG_{2m} - q\left(\sum_{(p-1)|2m} \frac{1}{p}\right) \equiv 0 \ mod \ q$$

pues G_{2m} es un entero y $\displaystyle\sum_{(p-1)|2m} \frac{1}{p}$ no contiene a q en el denominador.

Luego, $qB_{2m} \equiv 0 \ mod \ q$. Por consiguiente,

$$qB_{2m} \equiv \begin{cases} -1 & mod \ q \quad \text{si} \quad (p-1)|2m \\ 0 & mod \ q \quad \text{si} \quad (p-1)\nmid 2m \end{cases}$$

Con esto se obtiene el resultado del teorema 2.9. Por lo cual, el teorema 2.10 implica al teorema 2.9.

En segundo lugar veamos que el teorema 2.9 implica al teorema 2.10. Sean $p_1, p_2, \ldots, p_k$ números primos tales que $(p_i - 1)|2m$ para todo $i = 1, \ldots, k$. Como $(p_k - 1)|2m$ por el teorema 2.9 se cumple:

$$p_k B_{2m} \equiv -1 \ mod \ p_k$$

Es decir, $p_k|(p_k B_{2m} + 1)$. En otras palabras, existe $N_k \in \mathbb{Z}$ tal que $p_k B_{2m} = p_k N_k - 1$. Sea $N_{k-1} = p_k N_k - 1$. Entonces, $p_k B_{2m} = N_{k-1}$. A su vez, $N_{k-1} + 1 = p_k N_k$; o bien,

$$N_{k-1} \equiv -1 \ mod \ p_k$$

De donde,

$$p_k B_{2m} \equiv N_{k-1} \ mod \ p_k \, , con \, N_{k-1} \equiv -1 \ mod \ p_k$$

Por otra parte, como $(p_i - 1)|2m$ por el teorema 2.9 para $i = 1, \ldots, k-2$ se tiene:

$$p_i B_{2m} \equiv -1 \ mod \ p_i$$

Ahora, como $(p_i, p_j) = 1$ para todo $j = i+1, \ldots, k$ se resulta que: $(p_i, p_{i+1} \cdots p_k) = 1$. Lo cual implica que,

$$p_i p_{i+1} \cdots p_k B_{2m} \equiv -p_{i+1} \ldots p_k \ mod \ p_i$$

En consecuencia, $p_i|(p_i p_{i+1} \cdots B_{2m} + p_{i+1} \cdots p_k)$. Así, existe $N_i \in \mathbb{Z}$ tal que

$$p_i p_{i+1} \cdots p_k B_{2m} + p_{i+1} \cdots p_k = p_i N_i$$

O sea,

$$p_i p_{i+1} \cdots p_k B_{2m} = p_i N_i - p_{i+1} \cdots p_k$$

Sea

$$N_{i-1} = p_i N_i - p_{i+1} \cdots p_k \tag{2.14}$$

Luego, $p_i p_{i+1} \cdots p_k B_{2m} = N_{i-1}$. Por consiguiente,

$$N_{i-1} + p_{i+1} \cdots p_k = p_i N_i$$

En otras palabras, $p_i | (N_{i-1} + p_{i+1} \cdots p_k)$; es decir,

$$N_{i-1} \equiv -p_{i+1} \cdots p_k \ mod\ p_i$$

Entonces,

$$p_i p_{i+1} \cdots p_k B_{2m} = N_{i-1}\,, con\, N_{i-1} \equiv -p_{i+1} \cdots p_k \ mod\ p_i$$

En particular, para $i = 1$ existe $N_0 \in \mathbb{Z}$ con

$$N_0 \equiv -p_2 p_k \ mod\ p_1$$

tal que, $p_1 p_2 \cdots p_k B_{2m} = N_0$; esto es,

$$B_{2m} = \frac{N_0}{p_1 p_2 \cdots p_k}$$

Como $N_0 = p_1 N_1 - p_2 \cdots p_k$ por la fórmula (2.14) para $i = 1$, tenemos:

$$B_{2m} = \frac{p_1 N_1 - p_2 \cdots p_k}{p_1 p_2 \cdots p_k}$$

De donde,

$$B_{2m} = -\frac{1}{p_1} + \frac{N_1}{p_2 \cdots p_k}\,, con\, N_1 \equiv -p_3 \cdots p_k \ mod\ p_2$$

De nuevo, como $N_1 = p_2 N_2 - p_3 \cdots p_k$ por la fórmula 2.14 para $i = 2$ nos queda:

$$B_{2m} = -\frac{1}{p_1} + \frac{p_2 N_2 - p_3 \cdots p_k}{p_2 \cdots p_k}$$

Lo cual implica que,

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} + \frac{N_2}{p_3 \cdots p_k}\,, con\, N_2 \equiv -p_4 \cdots p_k \ mod\ p_3$$

Continuando con este proceso obtenemos que:

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-2}} + \frac{N_{k-2}}{p_{k-j}p_k}\,, con\, N_{k-2} \equiv p_k \ mod\ p_{k-1}$$

A su vez, como $N_{k-2} = p_{k-1}N_{k-1} - p_k$ por la fórmula 2.14 para $k-1$ se verifica:

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-2}} + \frac{p_{k-1}N_{k-1} - p_k}{p_{k-1}p_k}$$

En consecuencia,

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-2}} - \frac{1}{p_{k-1}} + \frac{N_{k-1}}{p_k}$$

con $N_{k-1} \equiv -1 \ mod\ p_k$. Por otra parte, como $N_{k-1} = p_kN_k - 1$ se cumple:

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-1}} + \frac{p_kN_k - 1}{p_k}$$

Así,

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-1}} - \frac{1}{p_k} + N_k\,, con\, N_k \in \mathbb{Z}$$

Llamando $N_k = G_{2m}$ se tiene:

$$B_{2m} = -\frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_{k-1}} - \frac{1}{p_k} + G_{2m}\,, con\, G_{2m} \in \mathbb{Z}$$

Luego,

$$B_{2m} = G_{2m} - \sum_{(p-1)|2m} \frac{1}{p}\,, con\, G_{2m} \in \mathbb{Z}$$

Por consiguiente, se infiere el resultado del teorema 2.10. Por lo tanto los teoremas 2.9 y 2.10 son equivalentes. ∎

Teorema 2.11 (Carlitz) *Sea $m > 1$. Si p es cualquier primo tal que $(p-1)p^h|2m$, entonces p^h divide al numerador de $B_{2m} + \left(\frac{1}{p}\right) - 1$. Es decir,*

$$pB_{2m} \equiv (p-1) \ mod\ p^{h+1} \tag{2.15}$$

Demostración. Supongamos que $p^h \parallel 2m$, entonces por definición $p^h|2m$ y $p^{h+1}\not|2m$. Como $m>1$ y $p^h|2m$ se verifica que $h>0$ para $p=2$. A su vez, como p es primo y $m>0$ por la fórmula 2.13 se cumple:

$$pB_{2m}-\left(S_{2m}(p-1)-mpS_{2m-1}(p-1)+\sum_{k=1}^{m-1}p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\right)$$

$$=p^{2m+1}B_{2m}$$

De donde,

$$p^{2m+1}\left|pB_{2m}-\left(S_{2m}(p-1)-mpS_{2m-1}(p-1)+\sum_{k=1}^{m-1}p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\right)\right.$$

De nuevo, como $p^h|2m$ se tiene que $p^{h+1}|p^{2m+1}$. Lo cual implica que,

$$p^{h+1}\left|pB_{2m}-\left(S_{2m}(p-1)-mpS_{2m-1}(p-1)+\sum_{k=1}^{m-1}p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\right)\right.$$

En consecuencia,

$$\begin{aligned} pB_{2m}\equiv& S_{2m}(p-1)-mpS_{2m-1}(p-1)\\ &+\sum_{k=1}^{m-1}p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\ mod\ p^{h+1} \end{aligned} \tag{2.16}$$

Por otra parte, como $2k>2$ en la suma anterior y por el lema 2.5 para un primo $p>2$ tal que $p^h \parallel 2m$ resulta:

$$p^{2k}\binom{2m}{2k}\equiv 0\ mod\ p^{h+2}\,, para\, todo\, k=1,\ldots,m-1$$

Pero, como $p^{h+1}|p^{h+2}$ tenemos:

$$p^{2k}\binom{2m}{2k}\equiv 0\ mod\ p^{h+1}\,, para\, todo\, k=1,\ldots,m-1$$

Así,

$$p^{2k}\binom{2m}{2k}B_{2m}\equiv 0\ mod\ p^{h+1}\,, para\, todo\, k=1,\ldots,m-1$$

Por lo cual,

$$p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\equiv 0 \ mod \ p^{h+1}\, , para\, todo\, k=1,\ldots,m-1$$

Luego,

$$\sum_{k=1}^{m-1} p^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(p-1)\equiv 0 \ mod \ p^{h+1}$$

Por consiguiente,

$$pB_{2m}\equiv S_{2m}(p-1)-mpS_{2m-1}(p-1) \ mod \ p^{h+1}$$

Ahora, si $p^h \parallel 2m$ entonces $p^{h+1} \parallel 2mp$ y como $p>2$ se deduce que $p^{h+1} \parallel mp$. En otras palabras,

$$mp\equiv 0 \ mod \ p^{h+1}$$

Por lo tanto,

$$mpS_{2m-1}(p-1)\equiv 0 \ mod \ p^{h+1}$$

De donde,

$$pB_{2m}\equiv S_{2m}(p-1) \ mod \ p^{h+1} \tag{2.17}$$

En particular, para $p=2$ la fórmula 2.16 nos queda en la forma:

$$2B_{2m}\equiv S_{2m}(2-1)-2mS_{2m-1}(2-1)$$

$$+\sum_{k=1}^{m-1} 2^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(2-1) \ mod \ 2^{h+1}, para \ todo \ m>1$$

O bien,

$$2B_{2m}\equiv S_{2m}(1)-2mS_{2m-1}(1)+2^2\binom{2m}{2}B_2S_{2m-2}(1)$$

$$+\sum_{k=2}^{m-1} 2^{k}\binom{2m}{2k}B_{2k}S_{2m-2k}(1) \ mod \ 2^{h+1}\, , para\, todo\, m>1$$

Si $2^h \parallel 2m$ entonces por el lema 2.5 obtenemos que la fórmula 2.16 es válida para $p=2$ y para todo $k=2,\ldots,m-1$. O sea,

$$2^{2k}\binom{2m}{2k}\equiv 0 \ mod \ 2^{h+1}\, , para\, todo\, k=2,\ldots,m-1$$

Lo que implica que,

$$2^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(1) \equiv 0 \ mod\ 2^{h+1}\,, para\, todo\, k = 2, \ldots, m-1$$

En consecuencia,

$$\sum_{k=2}^{m-1} 2^{2k}\binom{2m}{2k}B_{2k}S_{2m-2k}(1) \equiv 0 \ mod\ 2^{h+1}$$

Así,

$$2B_{2m} \equiv S_{2m}(1) - 2mS_{2m-1}(1) + 2^2\binom{2m}{2}B_2S_{2m-1}(1) \ mod\ 2^{h+1},$$

para todo $m > 1$. Escrito de otra forma,

$$2B_{2m} \equiv S_{2m}(1) - 2mS_{2m-1}(1) + 4m(2m-1)B_2S_{2m-2}(1) \ mod\ 2^{h+1}\,,$$

para todo $m>1$. Como $B_2 = \dfrac{1}{6}$ y $S_k(1) = 1$ para todo $k \geq 1$, se verifica:

$$2B_{2m} \equiv 1 - 2m + \left(\frac{1}{3}\right)2m(2m-1) \ mod\ 2^{h+1}\,, para\, todo\, m > 1$$

Por lo cual,

$$2B_{2m} \equiv 1 + \left(\frac{1}{3}\right)2m(2m-4) \ mod\ 2^{h+1}\,, para\, todo\, m > 1$$

De nuevo, como $2^h||2m$ por definición se cumple que $2^h|2m$ y $2^{h+1}\nmid 2m$; pero como $2^h|2m$ y $2|4$ se tiene que $2^h2|2m4$. Esto es,

$$2^{h+1}|2m2my2^{h+1}|2m4$$

Es decir, $2^{h+1}|(2m2m - 2m4)$. En otra palabras, $2^{h+1}|2m(2m-4)$.

Luego,

$$2m(2m-4) \equiv 0 \ mod\ 2^{h+1}\,, para\, todo\, m > 1$$

Por consiguiente,

$$1 + \left(\frac{1}{3}\right)2m(2m-4) \equiv 1 \ mod\ 2^{h+1}\,, para\, todo\, m > 1$$

Y, por transitividad de las congruencias sobre racionales resulta:

$$2B_{2m} \equiv 1 \ mod \ 2^{h+1} \, , para \, todo \, m > 1$$

Con lo cual queda probado el teorema para el caso especial $p = 2$. Por otra parte, si p es un primo impar y $p^h \parallel 2m$ entonces por la fórmula 2.17 obtenemos:

$$pB_{2m} \equiv S_{2m}(p-1) \ mod \ p^{h+1}, \quad \text{para todo } m > 1 \tag{2.18}$$

Además, por la definición de $S_{2m}(p-1)$ nos queda:

$$pB_{2m} \equiv 1^{2m} + 2^{2m} + \cdots + (p-1)^{2m} \ mod \ p^{h+1} \, , para \, todo \, m > 1$$

Ahora, como p es primo se deduce que

$$(a, p) = 1 para \ todo \ a = 1, \ldots, p-1$$

De donde, $(a, p^{h+1}) = 1$ para todo $h > 0$ y para todo $a = 1, \ldots, p-1$. Lo cual implica, por la generalización de Euler del Pequeño Teorema de Fermat, que:

$$a^{\phi(p^{h+1})} \equiv 1 \ mod \ p^{h+1} \, , para \, todo \, a = 1, \ldots, p-1$$

donde $\phi(p^{h+1}) = p^h(p-1)$ y ϕ es la función phi de Euler. En consecuencia,

$$(a^{p^h(p-1)})^r \equiv 1 \ mod \ p^{h+1} \tag{2.19}$$

para todo $r \in \mathbb{Z}$ con $r > 0$ y para todo $a = 1, \ldots, p-1$. Si $p^h(p-1)|2m$ entonces $2m = p^h(p-1)q$ para algún $q \in \mathbb{Z}$ con $q > 0$. Así,

$$1^{2m} + 2^{2m} + \cdots + (p-1)^{2m} = 1^{p^h(p-1)q} + 2^{p^h(p-1)q} + \cdots + (p-1)^{p^h(p-1)}$$

$$= (1^{p^h(p-1)})^q + (2^{p^h(p-1)})^q + \cdots + ((p-1)^{p^h(p-1)})^q$$

O bien,

$$1^{2m} + 2^{2m} + \cdots + (p-1)^{2m} = (1^{p^h(p-1)})^q + (2^{p^h(p-1)})^q + \cdots + ((p-1)^{p^h(p-1)})^q$$

Por la fórmula (2.19) obtenemos que:

$$(1^{p^h(p-1)})^q + (2^{p^h(p-1)})^q + ... + ((p-1)^{p^h(p-1)})^q \equiv \underbrace{1 + 1 + \cdots + 1}_{(p-1)-veces} \ mod \ p^{h+1}$$

Por lo cual,

$$1^{2m}+2^{2m}+\cdots+(p-1)^{2m} \equiv (p-1) \ mod \ P^{h+1} \, , para \, todo \, m > 1$$

Luego,

$$pB_{2m} \equiv (p-1) \ mod \ p^{h+1} \, , para \, todo \, m > 1$$

Por consiguiente,

$$B_{2m} \equiv 1 - \frac{1}{p} \ mod \ p^{h+1} \, , para \, todo \, m > 1$$

Por otra lado, como $p^h | p^{h+1}$ por el teorema 2.8 parte 4), se verifica:

$$B_{2m} \equiv 1 - \frac{1}{p} \ mod \ p^{h} \, , para \, todo \, m > 1$$

Por lo tanto, p^h divide al numerador de $B_{2m} + \frac{1}{p} - 1$ para todo $m > 1$.∎

Observación: Si $p \geq 5$ entonces por el lema 2.5 se cumple:

$$p^{2k}\binom{2m}{2k} \equiv 0 \ mod \ p^{h+2} \, , para \, todo \, k = 1, \ldots, m-1$$

O sea,

$$p^{2k}\binom{2m}{2k} B_{2k} \equiv 0 \ mod \ p^{h+2} \, , para \, todo \, k = 1, \ldots, m-1$$

Esto nos dice que el módulo en la fórmula 2.18 puede ser elevado a p^{h+2}. Además, en el siguiente teorema se generaliza la fórmula 2.17.

Teorema 2.12 *Sea p un número primo con $p \geq 5$. Si $p^h \parallel 2m$ y $p-1$ no divide a $2m-2$, entonces*

$$pB_{2m} \equiv S_{2m}(p-1) \ mod \ p^{h+3} \, , para \, todo \, m > 1$$

Demostración. Para $m > 1$ y para el primo p por la fórmula 2.13 se verifica:

$$pB_{2m} - \left(S_{2m}(p-1) - mpS_{2m-1}(p-1) + \sum_{k=1}^{m-1} p^{2k}\binom{2m}{2k} B_{2k} S_{2m-2k}(p-1) \right)$$
$$= p^{2m+1}B_{2m}$$

De donde,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1)$$
$$+\sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1) \ mod \ p^{2m+1}$$

Como $2m+1 \geq h+3$ (lo cual se prueba fácilmente por inducción) se cumple que $p^{h+3} | p^{2m+1}$. Lo cual implica, por el teorema 2.8 parte 4), que:

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1)$$
$$+\sum_{k=1}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1) \ mod \ p^{h+3}$$

Esto es,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1) + p^2 \binom{2m}{2} B_2 S_{2m-2}(p-1)$$
$$+ \sum_{k=2}^{m-1} p^{2k} \binom{2m}{2k} B_{2k} S_{2m-2k}(p-1) \ mod \ p^{h+3}$$

A su vez, como $p \geq 5$ y $p^h \parallel 2m$ por el lema 2.5 se tiene:

$$p^{2k} \binom{2m}{2k} \equiv 0 \ mod \ p^{h+4}, para\, todo\, k = 2, \ldots, m-1$$

Por otra parte, como $p^{h+3} | p^{h+4}$ para todo $h > 0$ por el teorema 2.8 parte 4) resulta:

$$p^{2k} \binom{2m}{2k} \equiv 0 \ mod \ p^{h+3}, para\, todo\, k = 2, \ldots, m-1$$

En consecuencia,

$$p^{2k} \binom{2m}{2k} B_{2m} S_{2m-2k}(p-1) \equiv 0 \ mod \ p^{h+3}, \quad \text{para todo} \quad k = 2, \ldots, m-1$$

Así,

$$\sum_{k=2}^{m-1} p^{2k} \binom{2m}{2k} B_{2m} S_{2m-2k}(p-1) \equiv 0 \ mod \ p^{h+3}$$

Por lo cual,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1)$$
$$+p^2 \binom{2m}{2} B_2 S_{2m-2}(p-1) \ mod \ p^{h+3}$$

Sustituyendo $B_2 = \dfrac{1}{6}$ tenemos:

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1)$$
$$+ \left(\frac{1}{6}\right) p^2 m(2m-1) S_{2m-2}(p-1) \ mod \ p^{h+3}$$

Por otro lado, como $p-1$ no divide a $2m-2$ por el lema 2.4 obtenemos

$$S_{2m-2}(p-1) \equiv 0 \ mod \ p \qquad (2.20)$$

Es decir, $p|S_{2m-2}(p-1)$. Luego, como $p^h|2m$ se deduce que

$$p^{h+1}|2mS_{2m-2}(p-1)$$

Por consiguiente,

$$p^{h+3} \Big| p^2 2mS_{2m-2}(p-1)$$

Es decir, $p^2 2mS_{2m-2}(p-1) \equiv 0 \ mod \ p^{h+3}$. Por lo tanto,

$$pB_{2m} \equiv S_{2m}(p-1) - mpS_{2m-1}(p-1) \ mod \ p^{h+3} \qquad (2.21)$$

Ahora, reemplazando a m por $2m-1$ y n por p en la fórmula 2.14 nos queda:

$$B_{2m-1} = \frac{1}{p(1-p^{2m-1})} \sum_{k=0}^{2m-1-1} p^k \binom{2m-1}{k} B_k \sum_{j=1}^{p-1} j^{2m-1-k}$$

Y por la fórmula 2.7 se verifica

$$B_{2m-1} = \frac{1}{p(1-p^{2m-1})} \sum_{k=0}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1)$$

Pero, como $B_{2m-1} = 0$ para todo $m \geq 2$ se cumple:

$$0 = \sum_{k=0}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1)$$

De otra manera,

$$0 = B_0 S_{2m-1}(p-1) + \sum_{k=1}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1)$$

Entonces, como $B_0 = 1$ se tiene:

$$S_{2m-1}(p-1) = -\sum_{k=1}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1)$$

O bien,

$$\begin{aligned} & S_{2m-1}(p-1) \\ = & -p^1 \binom{2m-1}{1} B_1 S_{2m-1-1}(p-1) - \sum_{k=2}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1) \end{aligned} \tag{2.22}$$

A su vez, como

$$p^k \equiv 0 \ mod \ p^2 \, , para \, todo \, k \geq 2$$

resulta:

$$-p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1) \equiv 0 \ mod \ p^2 \, , para \, todo \, k = 2, \ldots, 2k-2$$

De donde,

$$-\sum_{k=2}^{2m-2} p^k \binom{2m-1}{k} B_k S_{2m-1-k}(p-1) \equiv 0 \ mod \ p^2$$

Reduciendo a congruencias módulo p^2 la igualdad 2.22 tenemos:

$$S_{2m-1}(p-1) \equiv -p \binom{2m-1}{1} B_1 S_{2m-2}(p-1) \ mod \ p^2$$

O sea,

$$S_{2m-1}(p-1) \equiv -p(2m-1) B_1 S_{2m-2}(p-1) \ mod \ p^2$$

Por otra parte, como $B_1 = -\dfrac{1}{2}$ obtenemos:

$$S_{2m-1}(p-1) \equiv \frac{1}{2} p(2m-1) S_{2m-2}(p-1) \ mod \ p^2$$

Utilizando la congruencia 2.20, ya que $p-1$ no divide a $2m-2$ se deduce que

$$p^2 | pS_{2m-2}(p-1)$$

Lo cual implica,

$$\frac{1}{2}p(2m-1)S_{2m-2}(p-1) \equiv 0 \ mod \ p^2$$

En consecuencia, por transitividad de las congruencias sobre racionales

$$S_{2m-1}(p-1) \equiv 0 \ mod \ p^2$$

Luego,

$$p^2 | S_{2m-1}(p-1)$$

Y así,

$$p^3 | pS_{2m-1}(p-1)$$

Por último, como $p \geq 5$ y $p^h | 2m$ es válido que $p^h | m$. Por lo cual,

$$p^{h+3} | pmS_{2m-1}(p-1)$$

Por consiguiente,

$$pmS_{2m-1}(p-1) \equiv 0 \ mod \ p^{h+3}$$

Sustituyendo este resultado en la congruencia 2.21 nos queda:

$$pB_{2m} \equiv S_{2m}(p-1) \ mod \ p^{h+3}$$

Por lo tanto, se infiere el resultado del teorema. ∎

Teorema 2.13 (Frobenius) *Si $m > 2$, entonces 16 divide al numerador de $B_{2m} - \frac{1}{2} + 6m$. Esto es, $2B_{2m} \equiv 1 - 12m \ mod \ 32$*

Demostración. Por la fórmula 2.14 aplicada a $2m$ y $n = 2$ se verifica:

$$2(1-2^{2m})B_{2m} = \sum_{k=0}^{2m-1} 2^k \binom{2m}{k} B_k \sum_{j=1}^{1} j^{2m-k}$$

Es decir,

$$2(1-2^{2m})B_{2m} = \sum_{k=0}^{2m-1} 2^k \binom{2m}{k} B_k$$

Como $B_{2k+1} = 0$ para todo $k \geq 1$ se cumple:

$$2(1-2^{2m})B_{2m} = B_0 + 4mB_1 + \sum_{k=1}^{m} 2^{2k} \binom{2m}{2k} B_{2k}$$

A su vez, como $B_0 = 1$ y $B_1 = -\dfrac{1}{2}$ se tiene:

$$2(1-2^{2m})B_{2m} = 1 - 2m + \sum_{k=1}^{m} 2^{2k} \binom{2m}{2k} B_{2m}$$

Por otra parte, para todo $j = 1, \ldots, m$ resulta:

$$2(1-2^{2m})B_{2m} - \left(1 - 2m + \sum_{k=1}^{j} 2^{2k} \binom{2m}{2k} B_{2m}\right) = \sum_{k=1}^{m} 2^{2k} \binom{2m}{2k} B_{2k}$$

$$-\sum_{k=1}^{j} 2^{2k} \binom{2m}{2k} B_{2k} = \sum_{k=j+1}^{m} 2^{2k} \binom{2m}{2k} B_{2k}$$

O bien,

$$2(1-2^{2m})B_{2m} - \left(1 - 2m + \sum_{k=1}^{j} 2^{2k} \binom{2m}{2k} B_{2m}\right) = \sum_{k=j+1}^{m} 2^{2k} \binom{2m}{2k} B_{2k}$$

para todo $j = 1, \ldots, m$. Ahora, como

$$2^{2j+1} \Big| \sum_{k=j+1}^{m} 2^{2k} \binom{2m}{2k} B_{2k}$$

para todo $j = 1, \ldots, m$; tenemos:

$$2^{2j+1} \Big| 2(1-2^{2m})B_{2m} - \left(1 - 2m + \sum_{k=1}^{j} 2^{2k} \binom{2m}{2k} B_{2k}\right)$$

De donde,

$$2(1-2^{2m})B_{2m} \equiv 1 - 2m + \sum_{k=1}^{j} 2^{2k} \binom{2m}{2k} B_{2m} \; mod \; 2^{2j+1}$$

para todo $j = 1, \ldots, m$. Pero, si $j = 2$ para $m > 2$ obtenemos:

$$2(1 - 2^{2m})B_{2m} \equiv 1 - 2m + 2^2 \binom{2m}{2} B_2 + 2^4 \binom{2m}{4} B_4 \; mod \; 2^5$$

Sabiendo que $B_2 = \frac{1}{6}$ y $B_4 = -\frac{1}{30}$, nos queda:

$$2B_{2m} - 2^{2m+1}B_{2m} \equiv 1 - 2m + \frac{2}{3}\binom{2m}{2} - \frac{8}{15}\binom{2m}{4} B_4 \; mod \; 32$$

Por otro lado, como $m > 2$ se deduce que

$$2^{2m+1} \equiv 0 \; mod \; 32$$

que $2m + 1 > 5$, o sea,

$$2^{2m+1}B_{2m} \equiv 0 \; mod \; 32$$

Lo cual implica que,

$$2B_{2m} \equiv 1 - 2m + \frac{2}{3}\binom{2m}{2} - \frac{8}{15}\binom{2m}{4} \; mod \; 32$$

Estudiando el segundo miembro de esta congruencia, notamos que:

$$1 - 2m + \frac{2}{3}\binom{2m}{2} - \frac{8}{15}\binom{2m}{4} = \frac{-16m^4 + 48m^3 + 16m^2 - 108m + 45}{45}$$

En consecuencia,

$$2B_{2m} \equiv \frac{-16m^4 + 48m^3 + 16m^2 - 108m + 45}{45} \; mod \; 32$$

Como $32 \equiv 0 \; mod \; 32$ es válido que $-32 \cdot 23 \equiv 0 \; mod \; 32$, esto es,

$$-736 \equiv 0 \; mod \; 32$$

A su vez, como $-736 = -720 - 16$ se satisface $16 \equiv -720 \; mod \; 32$. Por otra parte, como $720 = 45 \cdot 16$ se verifica:

$$\frac{16}{45} \equiv -16 \; mod \; 32$$

Así,

$$\frac{16}{45}m^2 \equiv -16m^2 \; mod \; 32$$

De nuevo, como $32 \equiv 0 \; mod \; 32$ se cumple $-32 \cdot 9 \equiv 0 \; mod \; 32$, es decir, $-288 \equiv 0 \; mod \; 32$; y como $-288 = -108 - 180$ se tiene $-108 \equiv 180 \; mod \; 32$. Por consiguiente, siendo $180 = 45 \cdot 4$ resulta:

$$-\frac{108}{45} \equiv 4 \; mod \; 32$$

Por lo cual,

$$-\frac{108}{45} m \equiv 4m \; mod \; 32$$

Sólo resta probar que:

$$\frac{-16m^4 + 48m^3}{45} \equiv 0 \; mod \; 32$$

Lo cual es cierto, pues $-16m^4 + 48m^3 = 16m^3(-m+3)$; y además,

$$16m^3(-m+3) \equiv 0 \; mod \; 32$$

ya que $m^3(-m+3)$ es par para todo $m > 2$. Luego,

$$2B_{2m} \equiv 1 - 12m \; mod \; 32 \, , para \, todo \, m > 2$$

Pero, como $16|32$ por el teorema 2.8 parte 4) nos queda:

$$2B_{2m} \equiv 1 - 12m \; mod \; 16 \, , para \, todo \, m > 2$$

Por consiguiente,

$$B_{2m} \equiv \frac{1}{2} - 6m \; mod \; 16 \, , para \, todo \, m > 2$$

Por lo tanto, 16 divide al numerador de $B_{2m} - \dfrac{1}{2} + 6m$ para todo $m > 2$.
∎

Teorema 2.14 *Sea* $B_{2m} = \dfrac{P_{2m}}{Q_{2m}}$ *con* P_{2m} *y* Q_{2m} *enteros,* $Q_{2m} \neq 0$ *y* $(P_{2m}, Q_{2m}) = 1$. *Entonces, para todos los enteros positivos m y n se satisface la siguiente congruencia:*

$$\left(1^{2m} + 2^{2m} + \cdots + (n-1)^{2m}\right) Q_{2m} \equiv n P_{2m} \; mod \; n^2 \tag{2.23}$$

Demostración. Por la fórmula 2.14 aplicada a $2m$, se verifica:

$$n(1-n^{2m})B_{2m} = \sum_{k=0}^{2m-1} n^k \binom{2m}{k} B_k \sum_{j=1}^{n-1} j^{2m-k}$$

A su vez, por la fórmula 2.15 se cumple:

$$n(1-n^{2m})B_{2m} = \sum_{k=0}^{2m-1} n^k \binom{2m}{k} B_k S_{2m-k}(n-1)$$

Como $B_{2m} = \dfrac{P_{2m}}{Q_{2m}}$ con P_{2m} y Q_{2m} enteros y $Q_{2m} \neq 0$ para todo $m \geq 1$ se tiene:

$$n(1-n^{2m})\frac{P_{2m}}{Q_{2m}} = \sum_{k=0}^{2m-1} n^k \binom{2m}{k} B_k S_{2m-k}(n-1) nP_{2m} + n^{2m+1}P_{2m}$$

$$= B_0 S_{2m}(n-1)Q_{2m} + n2mS_{2m-1}(n-1)Q_{2m}$$

$$+ \left(\sum_{k=2}^{2m-1} n^k \binom{2m}{k} B_k S_{2m-k}(n-1) \right) Q_{2m}$$

Por otra parte, como $n^2 | n^k$ para todo $k \geq 2$ resulta:

$$n^k \equiv 0 \; mod \; n^2 \, , para \, todo \, k \geq 2$$

De donde,

$$n^k B_k \binom{2m}{k} S_{2m-k}(n-1) \equiv 0 \; mod \; n^2 \, , para \, todo \, k \geq 2$$

Lo cual implica que,

$$\sum_{k=2}^{2m-1} n^k B_k \binom{2m}{k} S_{2m-k}(n-1) \equiv 0 \; mod \; n^2$$

En consecuencia,

$$\left(\sum_{k=2}^{2m-1} n^k B_k \binom{2m}{k} S_{2m-k}(n-1) \right) Q_{2m} \equiv 0 \; mod \; n^2$$

Por otro lado, como $n^2|n^{2m+1}$ tenemos que $n^{2m+1} \equiv 0 \ mod \ n^2$. Así,

$$n^{2m+1}P_{2m} \equiv 0 \ mod \ n^2$$

Por lo cual,

$$nP_{2m} \equiv B_0 S_{2m}(n-1)Q_{2m} + 2nmB_1 S_{2m-1}(n-1)Q_{2m} \ mod \ n^2$$

Por otra parte, como $B_0 = 1$ y $B_1 = -\frac{1}{2}$ nos queda:

$$nP_{2m} \equiv S_{2m}(n-1)Q_{2m} + nmS_{2m-1}(n-1)Q_{2m} \ mod \ n^2 \tag{2.24}$$

De nuevo, por la fórmula 2.14 aplicada a $2m-1$, obtenemos:

$$B_{2m-1} = \frac{1}{n(1-n^{2m-1})} \sum_{k=0}^{2m-2} n^k \binom{2m-1}{k} B_k \sum_{j=1}^{n-1} j^{2m-1-k}$$

Por la fórmula 2.15 se deduce que:

$$B_{2m-1} = \frac{1}{n(1-n^{2m-1})} \sum_{k=0}^{2m-2} n^k \binom{2m-1}{k} B_k S_{2m-1-k}(n-1)$$

Como $B_{2m-1} = 0$, para todo $m \geq 2$ es cierto que:

$$0 = \sum_{k=0}^{2m-2} n^k \binom{2m-1}{k} B_k S_{2m-1-k}(n-1)$$

Esto es,

$$S_{2m-1}(n-1) = -\sum_{k=1}^{2m-2} n^k \binom{2m-1}{k} B_k S_{2m-1-k}(n-1)$$

Sustituyendo la expresión de $S_{2m-1}(n-1)$ en la fórmula 2.24 se satisface:

$$nP_{2m} \equiv S_{2m}(n-1)Q_{2m}$$

$$+nmQ_{2m} \sum_{k=1}^{2m-2} n^k \binom{2m-1}{k} B_k S_{2m-1-k}(n-1) \ mod \ n^2$$

Es decir,

$$nP_{2m} \equiv S_{2m}(n-1)Q_{2m}$$

$$+mQ_{2m}\sum_{k=1}^{2m-2} n^{k+1}\binom{2m-1}{k}B_kS_{2m-1-k}(n-1)\ mod\ n^2$$

Ahora, como $n^2|n^{k+1}$ para todo $k\geq 1$ es válido que $n^{k+1}\equiv 0\ mod\ n^2$, para todo$k\geq 1$. Luego,

$$n^{k+1}\binom{2m-1}{k}B_kS_{2m-1-k}(n-1)\equiv 0\ mod\ n^2\ , para\, todo\, k\geq 1$$

Por consiguiente,

$$\sum_{k=1}^{2m-2} n^{k+1}\binom{2m-1}{k}B_kS_{2m-1-k}(n-1)\equiv 0\ mod\ n^2$$

Además,

$$nQ_{2m}\sum_{k=1}^{2m-1} n^{k+1}\binom{2m-1}{k}B_kS_{2m-1-k}(n-1)\equiv 0\ mod\ n^2$$

O bien, $nmQ_{2m}S_{2m-1}(n-1)\equiv 0\ mod\ n^2$; o sea,

$$nP_{2m}\equiv S_{2m}(n-1)Q_{2m}\ mod\ n^2$$

Por lo tanto,

$$\left(1^{2m}+2^{2m}+\cdots+(n-1)^{2m}\right)Q_{2m}\equiv nP_{2m}\ mod\ n^2$$

Congruencia esta que se satisface para todos los enteros positivos m y n. ∎

Teorema 2.15 (Voronoi) *Sea* $B_{2m}=\dfrac{P_{2m}}{Q_{2m}}$ *con* P_{2m} *y* Q_{2m} *enteros,* $Q_{2m}\neq 0$ *y* $(P_{2m},Q_{2m})=1$*. Si* a *y* n *son enteros positivos tales que* $(a,n)=1$*, entonces*

$$(a^{2m}-1)P_{2m}\equiv 2ma^{2m-1}Q_{2m}\sum_{j=1}^{n-1} j^{2m-1}\left[\frac{ja}{n}\right]\ mod\ n$$

donde $[\alpha]$ *denota la parte entera de* α *que se define como el único entero* j *tal que* $j\leq\alpha<j+1$*.*

Demostración. Sean a y n enteros positivos tales que $(a,n)=1$, por el algoritmo de la división de Euclides se verifica:

Para todo $k=1,\dots,n-1$ existen enteros únicos q_k y r_k tales que $ka=q_kn+r_k\,,con\,0\leq r_k<n$. Como $(a,n)=1$ se cumple:

$$\left[\frac{ka}{n}\right]=q_k\,,para\,todo\,k=1,\dots,n-1. \tag{2.25}$$

De donde, los conjuntos $\{1,2,\dots,n-1\}$ y $\{r_1,r_2,\dots,r_{n-1}\}$ son iguales.

A su vez, elevando ka a la $2m$ se tiene:

$$(ka)^{2m}=(q_kn+r_k)^{2m}\,,para\,todo\,k=1,\dots,n-1$$

Usando el Teorema Binomial resulta:

$$(q_kn+r_k)^{2m}=\sum_{j=0}^{2m}\binom{2m}{j}(q_kn)^{2m-j}r_k^j\,,para\,todo\,k=1,\dots,n-1$$

Lo cual implica que,

$$k^{2m}a^{2m}=\sum_{j=0}^{2m}\binom{2m}{j}q_k^{2m-j}n^{2m-j}r_k^j\,,para\,todo\,k=1,\dots,n-1$$

Reduciendo a congruencias módulo n^2 tenemos:

$$k^{2m}a^{2m}\equiv\binom{2m}{2m-1}q_k^{2m-(2m-1)}n^{2m-(2m-1)}r_k^{2m-1}$$

$$+\binom{2m}{2m}q_k^{2m-2m}n^{2m-2m}r_k^{2m}\ mod\ n^2$$

para todo $k=1,\dots,n-1$. Esto es,

$$k^{2m}a^{2m}\equiv 2mq_knr^{2m-1}+r_k^{2m}\ mod\ n^2,\quad \text{para todo } k=1,...,n-1$$

Sustituyendo la fórmula 2.25 nos queda:

$$k^{2m}a^{2m}\equiv r_k^{2m}+2mnr_k^{2m-1}\left[\frac{ka}{n}\right]\ mod\ n^2\,,para\,todo\,k=1,\dots,n-1$$

Por otro lado, como $r_k\equiv ka\ mod\ n$ para todo $k=1,\dots,n-1$ se deduce que:

$$r_k^{2m-1}\equiv(ka)^{2m-1}\ mod\ n\,,para\,todo\,k=1,\dots,n-1$$

En consecuencia,

$$2mnr_k^{2m-1}\left[\frac{ka}{n}\right] \equiv 2mn(ka)^{2m-1}\left[\frac{ka}{n}\right] \; mod\ n^2\,, para\, todo\, k=1,\ldots,n-1$$

Así,

$$r_k^{2m} + 2mnr_k^{2m-1}\left[\frac{ka}{n}\right] \equiv r_k^{2m} + 2mnk^{2m-1}a^{2m-1}\left[\frac{ka}{n}\right] \; mod\ n^2$$

para todo $k = 1, \ldots, n-1$. Por transitividad de las congruencias módulo n sobre enteros obtenemos:

$$k^{2m}a^{2m} \equiv r_k^{2m} + ma^{2m-1}n\left[\frac{ka}{n}\right]k^{2m-1} \; mod\ n^2\,, para\, todo\, k=1,\ldots,n-1$$

Sumando miembro a miembro cada una de estas congruencias se verifica:

$$(1^{2m}+2^{2m}+\cdots+(n-1)^{2m})a^{2m} \equiv (r_1^{2m}+r_2^{2m}+\cdots+r_{n-1}^{2m})$$

$$+2ma^{2m-1}n\left(\left[\frac{1a}{n}\right]1^{2m-1}+\left[\frac{2a}{n}\right]2^{2m-1}+\cdots+\left[\frac{(n-1)a}{n}\right](n-1)^{2m-1}\right) mod\ n^2$$

Por otra parte, como $\{r_1, r_2, \ldots, r_{n-1}\} = \{1, 2, \ldots, n-1\}$ se cumple:

$$r_1^{2m} + r_2^{2m} + \cdots + r_{n-1}^{2m} = 1^{2m} + 2^{2m} + \cdots + (n-1)^{2m}$$

Luego,

$$(1^{2m}+2^{2m}+\cdots+(n-1)^{2m})a^{2m} \equiv (1^{2m}+2^{2m}+\cdots+(n-1)^{2m})$$

$$+2ma^{2m-1}n\left(\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]j^{2m-1}\right) \; mod\ n^2$$

Ahora, usando la fórmula 2.15 se tiene:

$$(a^{2m}-1)S_{2m}(n-1) \equiv 2ma^{2m-1}n\left(\sum_{j=1}^{n-1} j^{2m-1}\left[\frac{ja}{n}\right]\right) \; mod\ n^2$$

Usando la fórmula 2.23 resulta $S_{2m}(n-1) \equiv n\dfrac{P_{2m}}{Q_{2m}}\ mod\ n^2$. Por lo cual,

$$(a^{2m}-1)S_{2m}(n-1) \equiv (a^{2m}-1)n\frac{P_{2m}}{Q_{2m}} \; mod\ n^2$$

Luego

$$(a^{2m}-1)n\frac{P_{2m}}{Q_{2m}} \equiv (a^{2m}-1)S_{2m}(n-1) \ mod \ n^2$$

Por la transitividad de las congruencias módulo n sobre los racionales tenemos:

$$(a^{2m}-1)n\frac{P_{2m}}{Q_{2m}} \equiv 2ma^{2m-1}n\left(\sum_{j=1}^{n-1} j^{2m-1}\left[\frac{ja}{n}\right]\right) \ mod \ n^2$$

Por consiguiente,

$$(a^{2m}-1)P_{2m} \equiv 2ma^{2m-1}Q_{2m}\left(\sum_{j=1}^{n-1} j^{2m-1}\left[\frac{ja}{n}\right]\right) \ mod \ n^2$$

Entonces, como $n|n^2$ por el teorema 2.8 parte 4) se deduce que:

$$(a^{2m}-1)P_{2m} \equiv 2ma^{2m-1}Q_{2m}\left(\sum_{j=1}^{n-1} j^{2m-1}\left[\frac{ja}{n}\right]\right) \ mod \ n$$

Por lo tanto, se infiere el resultado del teorema. ∎

Teorema 2.16 (Ramanujan) *Si* 4 *divide a* m *entonces* 200 *divide al numerador de* $B_{4m}+\frac{1}{30}$*, esto es,* $30B_{4m} \equiv -1 \ mod \ 200$*. Además,* 5 *divide al numerador de* $\frac{B_{4m+2}}{4m+2}-\frac{1}{12}$*; es decir,* $\frac{B_{4m+2}}{4m+2} \equiv \frac{1}{12} \ mod \ 5$*.*

Demostración. Usando el teorema 2.11 **(Carlitz)** para $p=2$ y $h=2$ se verifica:

$$2B_{4m} \equiv 1 \ mod \ 8$$

De donde, $30B_{4m} \equiv 15 \ mod \ 8$. A su vez, como $16 \equiv 0 \ mod \ 8$ se cumple que $15 \equiv -1 \ mod \ 8$. Por la transitividad de las congruencias módulo m sobre los racionales se tiene:

$$30B_{4m} \equiv -1 \ mod \ 8 \tag{2.26}$$

Ahora, si $p=5$ entonces $p-1=4$; y como $(p-1)\not|(4m-2)$ ya que $4\not|(4m-2)$ para todo $m>3$, por la fórmula 2.26 resulta:

$$5B_{4m} \equiv S_{4m}(4) \ mod \ 5^{h+3}\text{, para todo } h>0$$

En particular, para $h = 1$ nos queda $5B_{4m} \equiv S_{4m}(4)\ mod\ 5^4$. Por otra parte, como $5^2|5^4$ por el teorema 2.8 parte 4), se deduce que

$$5B_{4m} \equiv S_{4m}(4)\ mod\ 25$$

Usando por la fórmula 2.15 tenemos:

$$S_{4m}(4) = 1^{4m} + 2^{4m} + 3^{4m} + 4^{4m} = 1 + 16^m + 81^m + 256^m$$

$$= 1 + 16^m + (75 + 6)^m + (250 + 6)^m$$

O bien,

$$S_{4m}(4) = 1 + 16^m + (75 + 6)^m + (250 + 6)^m$$

Reduciendo a congruencias módulo 25 obtenemos:

$$1 + 16^m + (75 + 6)^m + (250 + 6)^m \equiv 1 + 16^m + 6^m + 6^m\ mod\ 25$$

Lo que implica que,

$$S_{4m}(4) \equiv 1 + 16^m + 6^m + 6^m\ mod\ 25$$

Además,

$$1 + 16^m + 6^m + 6^m = 1 + (1 + 15)^m + (1 + 5)^m + (1 + 5)^m$$

De nuevo, reduciendo a congruencias módulo 25 se verifica:

$$1 + (1 + 15)^m + (1 + 5)^m + (1 + 5)^m$$

$$\equiv 1 + (1 + 15m) + (1 + 5m) + (1 + 5m)\ mod\ 25$$

O sea,

$$1 + (1 + 15)^m + (1 + 5)^m + (1 + 5)^m \equiv 4 + 25m\ mod\ 25$$

En consecuencia,

$$1 + (1 + 15)^m + (1 + 5)^m + (1 + 5)^m \equiv 4\ mod\ 25$$

Así, $S_{4m}(4) \equiv 4\ mod\ 25$. Luego, $5B_{4m} \equiv 4\ mod\ 25$. Por otra parte, como $(6, 25) = 1$ se cumple $30B_{4m} \equiv 24\ mod\ 25$. A su vez, como $25 \equiv 0\ mod\ 25$ se tiene que $24 \equiv -1\ mod\ 25$ y por transitividad de las congruencias sobre los racionales resulta:

$$30B_{4m} \equiv -1\ mod\ 25 \tag{2.27}$$

De las fórmulas 2.26 y 2.27, como $(8,25)=1$ por el Teorema Chino del Resto se deduce que $30B_{4m} \equiv -1 \; mod \; 200$.

Por consiguiente, $B_{4m} \equiv -\frac{1}{30} \; mod \; 200$. Esto nos dice que 200 divide al numerador de $B_{4m} + \frac{1}{30}$.

Ahora, supongamos que $5^h \parallel (4m+2)$ (por supuesto esto es cierto para $p=1$ y $m=2$). Por la fórmula 2.25 y por la observación del teorema 2.11 tenemos:

$$5B_{4m+2} \equiv S_{4m+2}(4) \; mod \; 5^{h+2} \,, para \, todo \, m > 1$$

Por otro lado, de la fórmula 2.15 obtenemos:

$$\begin{aligned} S_{4m+2}(4) &= 1^{4m+2} + 2^{4m+2} + 3^{4m+2} + 4^{4m+2} \\ &= 1 + 4^{2m+1} + 9^{2m+1} + 16^{2m+1} \\ &= 1 + (5-1)^{2m+1} + (10-1)^{2m+1} + (15+1)^{2m+1} \end{aligned}$$

En otras palabras,

$$S_{4m+2}(4) = 1 + (5-1)^{2m+1} + (10-1)^{2m+1} + (15+1)^{2m+1}$$

De donde,

$$5B_{4m+2} \equiv 1 + (5-1)^{2m+1} + (10-1)^{2m+1} + (15+1)^{2m+1} \; mod \; 5^{h+2}$$

Reduciendo módulo 5^{h+2} nos queda:

$$\begin{aligned} &1 + (5-1)^{2m+1} + (10-1)^{2m+1} + (15+1)^{2m+1} \\ &\equiv 1 + (-1 + (2m+1)5) + (-1 + (2m+1)10) \\ &\quad +(1 + (2m+1)15) \; mod \; 5^{h+2} \end{aligned}$$

Desarrollando el segundo miembro de esta congruencia se tiene:

$$\begin{aligned} &1 + (-1 + (2m+1)5) + (-1 + (2m+1)10) + (1 + (2m+1)15) \\ &= 60m + 30 = 30(2m+1) \end{aligned}$$

Lo cual implica que,

$$\begin{aligned} &1 + (-1 + (2m+1)5) + (-1 + (2m+1)10) + (1 + (2m+1)15) \\ &= 30(2m+1) \end{aligned}$$

En consecuencia,

$$1+(5-1)^{2m+1}+(10-1)^{2m+1}+(15+1)^{2m+1}\equiv 30(2m+1)\ mod\ 5^{h+1}$$

Así, $5B_{4m+2}\equiv 30(2m+1)\ mod\ 5^{h+2}$. De otra manera,

$$5B_{4m+2}\equiv 15(4m+2)\ mod\ 5^{h+2}$$

Luego,

$$\frac{B_{4m+2}}{4m+2}\equiv 3\ mod\ 5^{h+2}$$

Por otra parte, como $5|5^{h+2}$ para todo $h>0$ por el teorema 2.8 parte 4) se deduce que:

$$\frac{B_{4m+2}}{4m+2}\equiv 3\ mod\ 5$$

Y como $35\equiv 0\ mod\ 5$ resulta que

$$36\equiv 1\ mod\ 5$$

Por consiguiente, $3\equiv\dfrac{1}{12}\ mod\ 5$. De nuevo, por la transitividad de las congruencias módulo m sobre los racionales tenemos:

$$\frac{B_{4m+2}}{4m+2}\equiv\frac{1}{12}\ mod\ 5$$

Lo cual nos dice que 5 divide al numerador de $\dfrac{B_{4m+2}}{4m+2}-\dfrac{1}{12}$.

Por lo tanto, se infieren los resultados del teorema. ∎

Referencias

[**1**] **L. Carlitz**, Some Congruences for the Bernoulli Numbers, The American Journal of Mathematics 75 (1953), pp. 163-172.
[**2**] **L. Carlitz**, A note on the Staudt-Clausen Theorem, The American Mathematical Monthly 64 (1957), pp. 19-21.
[**3**] **L. Carlitz**, A Property of the Bernoulli Numbers, The American Mathematical Monthly 66 (1959), pp. 714-715.
[**4**] **L. Carlitz**, A Property of the Bernoulli Numbers, The American Mathematical Monthly 67 (1960), pp. 1011-1012.

[**5**] **E. Deeba and D. Rodríguez**, Stirling's Series and Bernoulli Numbers, The American Mathematical Monthly 98 (1991), pp. 423-429.
[**6**] **F. T. Howard**, Applications of a Recurrence for the Bernoulli Numbers, Journal of Number Theory 52, pp. 157-172 (1995).
[**7**] **G. López**, Notas de Matemáticas N 211, Mérida, Venezuela, 2000.
[**8**] **G. López**, Notas de Matemáticas N 212, Mérida, Venezuela, 2000.
[**9**] **S. Ramanujan**, Collected Papers, Chelsea, New York, 1962.
[**10**] **H. S. Vandiver**, Fermat's Last Theorem, The American Mathematical Monthly 53 (1946), pp. 553-578.

Departamento de Matemáticas.
Facultad de Ciencias.
Universidad de Los Andes.
Mérida 5101.
Venezuela
e-mail address: glauco@ciens.ula.ve