Teorema de Clausen–von Staudt. Congruencias de Kummer. Primos irregulares

Alexey Beshenov (cadadr@gmail.com)

7 de Marzo de 2017

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

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

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

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).

Ejemplo.

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

▲

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; 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 $\frac{(-1)^\ell\,\ell!\,\{{k \atop \ell}\}}{\ell+1}$ 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 $\frac{(-1)^\ell\,\ell!\,\{{k \atop \ell}\}}{\ell+1}$ 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 $\frac{(-1)^\ell\,\ell!\,\{{k \atop \ell}\}}{\ell+1}$ 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 la fórmula

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

podemos escribir

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

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 $\frac{(-1)^\ell\,\ell!\,\{{k \atop \ell}\}}{\ell+1}$ es entero.

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

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

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

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

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

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 $\frac{(-1)^\ell\,\ell!\,\{{k \atop \ell}\}}{\ell+1}$ va a contribuir $-\frac{1}{p}$ en el denominador si $p-1 \mid k$, y va a ser entero si $p-1 \nmid k$.

■

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 [Tsuneo Arakawa, Tomoyoshi Ibukiyama, Masanobu Kaneko, *Bernoulli numbers and zeta functions*, §11.3]):

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 $p \nmid k$.

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

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

▲

Para demostrar el teorema, nos va a servir el siguiente

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 $0\leq \ell\leq k$. Ya que $b_\ell \in \mathbb{Z}_{(p)}$, de esta fórmula se deduce que $a_k \in \mathbb{Z}_{(p)}$. Luego,

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

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. 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

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

Aquí hemos usado la función generatriz $\frac{t}{e^t-1} = \frac{t\,e^t}{e^t-1} - t = 1 - \frac{t}{2}\sum_{k\geq 0} B_k\,\frac{t^k}{k!}$. 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 $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p}$. ■

Numeradores de B_k (primos irregulares)

Los primos regulares e irregulares fueron descubiertos por el matemático alemán Ernst Kummer (1810–1893) mientras trabajaba en el **último teorema de Fermat**: *para $n>2$ la ecuación $x^n+y^n=z^n$ no tiene soluciones para x,y,z enteros positivos*. Kummer logró demostrar este teorema para ciertos números primos $n=p$ que él llamó regulares. Como definición, podemos usar la siguiente caracterización:

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

Podemos compilar una lista de los primos irregulares en PARI/GP:

```
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}:

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

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

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

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

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

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

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

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

$$B_{110} = \frac{5 \cdot 157 \cdot 76493 \cdot 150235116317549231 \cdot 369448188741168234283576 91 \cdots}{2 \cdot 3 \cdot 11 \cdot 23}.$$

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

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

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 $p_1, \ldots, p_r$ 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 $p_1, \ldots, p_r$ están en el denominador de B_k, de donde $p \notin \{p_1, \ldots, p_r\}$. 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.

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 [Paulo Ribenboim, *13 lectures on Fermat's last theorem*] (escrito mucho antes de la demostración definitiva del teorema por ANDREW WILES en 1995, pero con buenas explicaciones de los resultados de Kummer).