SOBRE EL INDICE DE IRREGULARIDAD DE LOS NUMEROS PRIMOS

por

PILAR BÁYER
(en Regensburg)

INTRODUCCIÓN

Un primo $p \geqslant 3$ es llamado *regular* si y sólo si no divide al numerador de ningún número de Bernoulli B_{2m}, siendo $1 \leqslant m \leqslant (p-3)/2$. La sencillez de tales primos estriba en que Kummer probó que para los exponentes primos regulares la ecuación de Fermat $x^p + y^p = z^p$ carece de soluciones enteras no triviales. En general, dado un primo p, un par $(p, 2m)$ se llama irregular si p divide al numerador de B_{2m}. El número δ de pares irregulares que un primo presenta en el intervalo $1 \leqslant m \leqslant (p-3)/2$ se llama el *índice de irregularidad* de p.

Sea $\zeta_{p^{n+1}}$ una raíz primitiva p^{n+1}-ésima de la unidad. Designemos por h_n el número de clases del cuerpo ciclotómico $\mathbf{Q}(\zeta_{p^{n+1}})$ y por $p^{e(n)}$ la máxima potencia de p que divide a h_n. Una conocida fórmula debida a Iwasawa afirma que, para todo n suficientemente grande,

$$e(n) = \mu p^n + \lambda n + \nu ,$$

en donde $\mu \geqslant 0$, $\lambda \geqslant 0$ y ν, enteros independientes de n, son los llamados *invariantes ciclotómicos* de p. Se verifica que $\lambda = \mu = \nu = 0$ si y sólo si p es regular. Los invariantes ciclotómicos han sido calculados para todos los primos $p < 10^5$ (véase [4] y [8]), obteniéndose en todos los casos que $\mu = 0$ y $\lambda = \nu = \delta$. Un reciente teorema de B. Ferrero y L. C. Washington prueba que $\mu = 0$ para todo primo p.

En esta nota nos ocupamos de la igualdad $\lambda = \delta$. Proveniente de la descomposición $h_n = h_n^+ \, h_n^-$, en donde h_n^+ es el número de clases

del cuerpo real maximal de $\mathbf{Q}(\zeta_{p^{n+1}})$ y h_n^- es un entero, el invariante λ descompone en la forma $\lambda = \lambda^+ + \lambda^-$. Un conocido criterio dado por Mestänkylä ([6], [7]) afirma que la igualdad $\lambda = \delta$ tiene lugar si y sólo si $\lambda^+ = 0$ y para cada par irregular $(p, 2m)$, $1 \leqslant m \leqslant (p-3)/2$, se cumple que

$$\frac{B_{2m}}{2m} \equiv \frac{B_{2m+p-1}}{2m+p-1} \mod p^2.$$

Es sabido (congruencia de Kummer) que tales cocientes son siempre congruentes módulo p.

Ofrecemos aquí una nueva demostración del criterio anterior, basada en la fórmula explícita de las funciones zeta p-ádicas hallada por Washington [9].

1. Funciones zeta p-ádicas

La función zeta de Riemann toma sobre los enteros negativos valores racionales:

$$\zeta(1-n) = -\frac{B_n}{n} \quad (n \geqslant 1),$$

en donde B_n designa el n-ésimo número de Bernoulli. Como es sabido, tales números se definen a partir del desarrollo

$$\frac{te^t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!},$$

y son nulos, para $n > 1$, si y sólo si n es impar.

Kubota y Leopoldt probaron en 1964 la existencia de funciones contínuas p-ádicas que interpolaban los anteriores valores. Tal interpolación, sin embargo, no puede hacerse por medio de una única función p-ádica, sino que requiere una partición de los enteros n en clases de restos módulo $p-1$.

En lo sucesivo supondremos siempre que p es distinto de dos. Sea $\mathbf{Z}_p^*$ el grupo multiplicativo de las unidades p-ádicas, $U_p = 1 + pZ_p$ el subgrupo de las unidades principales y $V_{p-1} \subseteq \mathbf{Z}_p^*$ el grupo cíclico de orden $p-1$ formado por las raíces $(p-1)$-ésimas de la unidad. Se tiene que $\mathbf{Z}_p^* = V_{p-1} \times U_p$ y de acuerdo con esta

descomposición, cada elemento $a \in \mathbf{Z}_p^*$ se escribe de manera única en la forma

$$a = \omega(a)\,\langle a\rangle, \quad \text{siendo} \quad \omega(a) \in V_{p-1}, \quad \langle a\rangle \in U_p.$$

Si $a \in \mathbf{Z}$ es divisible por p, definamos $\omega(a) = 0$. La aplicación

$$\begin{aligned} \mathbf{Z} &\to V_{p-1} \\ a &\to \omega(a) \end{aligned}$$

se identifica entonces con un carácter de Dirichlet de conductor p. Según Kubota y Leopoldt (véase [3], §3), para cada entero i $(1 \leqslant i \leqslant p-1)$, existe una única función contínua

$$\zeta_p(\omega^i, \ ) : \mathbf{Z}_p - \{1\} \to \mathbf{Q}_p,$$

tal que sobre los enteros $n \geqslant 1$, $n \equiv i \bmod (p-1)$, satisface la igualdad

$$\zeta_p(\omega^i, 1-n) = (1 - p^{n-1})\,\zeta(1-n).$$

La función $\zeta_p(\omega^i, \ )$ es idénticamente nula si y sólo si i es impar. Claramente para todo entero $n \geqslant 1$

$$v_p(\zeta_p(\omega^n, 1-n)) = v_p(\zeta(1-n)),$$

en donde por v_p designamos la valoración de $\mathbf{Q}_p$ asociada a p.

Si $B_{2m} = P_{2m}/Q_{2m}$ es la representación racional de un número de Bernoulli en su forma irreducible, por el teorema de von Staudt-Clausen ([1], Cap. V) sabemos que un número primo p divide a Q_{2m} si y sólo si $(p-1) \mid 2m$. En consecuencia, si $1 \leqslant m \leqslant (p-3)/2$,

$$v_p(\zeta_p(\omega^{2m}, 1-2m)) = v_p(P_{2m}),$$

y con ello el carácter irregular de un primo puede «leerse» a través de los valores tomados por las funciones zeta p-ádicas.

Designemos por Ω_p una clausura algebraica de $\mathbf{Q}_p$ y sea

$$D = \{s \in \Omega_p \mid \ |s| < p^{(p-2)/(p-1)}\}$$

en donde $|\ |$ denota el valor absoluto p-ádico normalizado por $|p| = p^{-1}$ La función $\zeta_p(\omega^i, s)$ se extiende a una función meromorfa en D (de

hecho analítica si $i \neq 0$), que viene dada por la siguiente fórmula debido a Washington [9]:

$$\zeta_p(\omega^i, s) = \frac{1}{s-1}\frac{1}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}(-1)^j\binom{1-s}{j}\left(\frac{p}{a}\right)^j B_j .$$

2. Relación con los invariantes ciclotómicos de Iwasawa

En lo sucesivo supondremos siempre que i es par. La función $\zeta_p(\omega^i, s)$ tiene entonces únicamente un número finito de ceros en D. En efecto, por un teorema debido a Iwasawa (véase [3], §6), sabemos que existe una serie formal $f_i(T) \in \mathbf{Z}_p[[T]]$ tal que

$$\zeta_p(\omega^0, s) = \frac{f_0(q^s-1)}{q^s-1} \quad , \quad \text{si} \quad i \equiv 0 \bmod (p-1),$$
$$\zeta_p(\omega^i, s) = f_i(q^s-1) \quad , \quad \text{si} \quad i \not\equiv 0 \bmod (p-1),$$

para todo $s \in D$, siendo $q = 1 + p$. Por el teorema de preparación de Weierstraß, la serie $f_i(T)$ descompone en la forma

$$f_i(T) = p^{\mu_i}\, g_i(T)\, u_i(T), \qquad (*)$$

en donde μ_i es un entero no negativo, $g_p(T) \in \mathbf{Z}_p[T]$ es un polinomio de Weierstraß, es decir, es mónico y verifica que

$$g_i(T) \equiv T^{\lambda_i} \bmod p$$

y $u_i(T)$ es una unidad de $\mathbf{Z}_p[[T]]$. Ferrero y Washington [2] han demostrado que, en las series que nos ocupan, μ_i es igual a cero.

Sea $\zeta_{p^{n+1}}$ una raíz primitiva p^{n+1}-ésima de la unidad. Sea h_n el número de clases del cuerpo ciclotómico $\mathbf{Q}(\zeta_{p^{n+1}})$ y h_n^+ el de su cuerpo real maximal $\mathbf{Q}(\zeta_{p^{n+1}} + \zeta_{p^{n+1}}^{-1})$.
Es sabido que $h_n^+ | h_n$. Definamos h_n^- por la igualdad

$$h_n = h_n^+ h_n^- .$$

Sea $p^{e(n)}$ (resp. $p^{e^-(n)}$) la máxima potencia de p que divide a h_n resp. a h_n^-). Iwasawa demostró (cf. [3], §7) que existen enteros $\lambda \geqslant 0$, $\mu \geqslant 0$, ν (resp. $\lambda^- \geqslant 0$, $\mu^- \geqslant 0$, ν^-), tales que, para todo n suficientemente grande,

$$e(n) = \mu p^n + \lambda n + \nu ,$$

$$e^-(n) = \mu^- p^n + \lambda^- n + \nu^- .$$

Además tales enteros son «calculables» a partir de las funciones de Kubota y Leopoldt. Concretamente:

$$\mu^- = \sum_{i=2}^{p-1} \mu_i \quad , \quad \lambda^- = \sum_{i=2}^{p-1} \lambda_i \quad \text{(i par)}.$$

Con ello $\mu^- = 0$ (y ello implica $\mu = 0$) según el teorema de Ferrero-Washington.

Claramente $\lambda \geqslant \lambda^-$. Definamos λ^+ por la igualdad $\lambda = \lambda^+ + \lambda^-$ y sea

$$f_i(T) = \sum_{j=0}^{\infty} a_j^{(i)} T^j \quad , \quad a_j^{(i)} \in \mathbf{Z}_p ,$$

la serie (*). Deducimos ahora que $p | a_0^{(i)}$ si y sólo si el polinomio de Weierstraß $g_i(T)$ es distinto de 1. Es decir

$$p | a_0^{(i)} \Leftrightarrow \lambda_i \geqslant 1 .$$

Sea $2 \leqslant i \leqslant p - 3$ (recordemos que i es par). De la igualdad

$$v_p \left(\sum_{j=0}^{\infty} a_j^{(i)} (q^{1-i} - 1)^j \right) = v_p(\zeta_p(\omega^i, 1 - i)) = v_p(B_i)$$

se sigue que

$\lambda_i \geqslant 1 \Leftrightarrow (p, i)$ es un par irregular.

En consecuencia

$$\lambda \geqslant \lambda^- \geqslant \delta,$$

siendo δ el índice de irregularidad de p. Consideremos ahora el índice λ_{p-1}. Por el teorema de von Staudt-Clausen sabemos que $v_p(B_{p-1}) = -1$; ello implica que la serie $f_{p-1}(T)$ debe ser un elemento unitario de $\mathbf{Z}_p[[T]]$; es decir $\lambda_{p-1} = 0$. Obtenemos así la siguiente

Proposición. Dado un primo p (> 3), la igualdad $\lambda = \delta$ se verifica si y sólo si $\lambda^+ = 0$ y $\lambda_i = 1$ para todo par irregular (p, i), $2 \leqslant i \leqslant p - 3$, i par.

En tal caso, las funciones $\zeta_p(\omega^i, s)$, i par, tienen a lo sumo un cero simple en $\mathbf{Z}_p$.

Nota. Una célebre conjetura debida a Vandiver afirma que $p \nmid h_0^+$. Si $p \nmid h_0^+$, entonces $p \nmid h_n^+$ para todo $n \geqslant 0$, con lo cual $\lambda^+ = 0$ para este valor de p. La conjetura de Vandiver es cierta para todo primo $p < 10^5$.

3. Estudio de la condición $\lambda_i = 1$

La congruencia

$$f_i(T) = \sum_{j=0}^{\infty} a_j^{(i)} T^j \equiv T^{\lambda_i} u_i(T) \mod p$$

nos dice que el valor de λ_i puede reconocerse como el índice del primero de los coeficientes de la serie $f_i(T)$ que no es múltiplo de p. Es decir, se tiene que

$$a_j^{(i)} \equiv 0 \mod p \text{ , para } 0 \leqslant j < \lambda_i ,$$
$$a_{\lambda_i}^{(i)} \not\equiv 0 \mod p .$$

Supondremos en lo sucesivo que es $i \leqslant p - 3$. Asimismo, puesto que estamos interesados únicamente en los valores de i para los cuales (p, i) es un par irregular, podemos suponer que $p > 3$ y que $i > 2$.

De la igualdad $\zeta_p(\omega^i, s) = \sum_{j=0}^{\infty} a_j^{(i)} (q^s - 1)^j$ se obtiene

$$\zeta'_p(\omega^i, 0) = a_1^{(i)} \log q$$

en donde $'$ indica la derivada respecto a s y log designa la función logaritmo p-ádico. Por tanto

$$a_1^{(i)} \not\equiv 0 \mod p \Leftrightarrow v_p(\zeta'_p(\omega^i, 0)) = 1 .$$

Estudiaremos ahora esta última condición a partir de la fórmula de Washington. Sea

$$T(s) : = \frac{1}{p} \sum_{a=1}^{p} \omega^i(a) \langle a \rangle^{1-s} \sum_{j=0}^{\infty} (-1)^j \binom{1-s}{j} \left(\frac{p}{a}\right)^j B_j .$$

Debemos pues calcular

$$-\zeta'_p(\omega^i, 0) = T(0) + T'(0)$$

módulo p^2. Puesto que $\langle a \rangle^{p^2} \equiv 1 \mod p^3$, para todo $a \in \mathbf{Z}_p^*$, se tiene que $a^{p^2} \equiv \omega(a) \mod p^3$. Por tanto

$$\begin{aligned} T(0) &= \frac{1}{p} \sum_{a=1}^{p} \omega^i(a) \langle a \rangle - \frac{1}{2} \sum_{a=1}^{p} \omega^{i-1}(a) \\ &= \frac{1}{p} \sum_{a=1}^{p} \omega^{i-1}(a)\, a \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^{p^2(i-1)+1} \\ &= \frac{1}{p} S_{p^2(i-1)+1}(p) \qquad \mod p^2 , \end{aligned}$$

en donde si k, $n \geqslant 1$ son enteros arbitrarios

$$S_k(n) : = \sum_{a=1}^{n-1} a^k .$$

Es sabido que las sumas de potencias de números naturales están ligadas a los números de Bernoulli. Así para $k \geqslant 1$

$$S_k(n) = \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} n^{k+1-j} B_j$$

(véase [1], Ch. V). Sea $0 \leqslant r \leqslant i$ un entero; haciendo $k = p^2(i-r)+r$ y $n = p$ en la fórmula anterior, se obtiene la congruencia

$$S_{p^2(i-r)+r} \equiv p\, B_{p^2(i-r)+r} \mod p^3 .$$

Con ello

$$T(0) \equiv B_{p^2(i-1)+1} \mod p^2 .$$

Escribamos ahora $T'(s) = T_1(s) + T_2(s)$, en donde

$$T_1(s) := -\frac{1}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^{1-s}\log\langle a\rangle\sum_{j=0}^{\infty}(-1)^j\binom{1-s}{j}\left(\frac{p}{a}\right)^j B_j$$

y

$$T_2(s) := -\frac{1}{2}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^{1-s}a^{-1} - \frac{1}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^{1-s}\sum_{j=2}^{\infty}\frac{1}{j(j-1)}\left(\frac{p}{a}\right)^j B_j .$$

Teniendo en cuenta que $\log\langle a\rangle \equiv \langle a\rangle - 1 - \frac{(\langle a\rangle - 1)^2}{2} \bmod p^3$, deducimos

$$\begin{aligned}
T_1(0) &= -\frac{1}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle\log\langle a\rangle + \frac{1}{2}\sum_{a=1}^{p}\omega^{i-1}(a)\log\langle a\rangle \\
&\equiv \frac{1}{2p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^3 - \frac{2}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle^2 + \\
&\quad + \frac{3}{2p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle + \frac{1}{2}\sum_{a=1}^{p}\omega^{i-1}(a)\langle a\rangle \\
&\equiv \frac{1}{2p}S_{p^2(i-3)+3}(p) - \frac{2}{p}S_{p^2(i-2)+2}(p) + \\
&\quad + \frac{3}{2p}S_{p^2(i-1)+1}(p) + \frac{1}{2}S_{p^2(i-2)+1} \\
&\equiv +\frac{1}{2}B_{p^2(i-3)+3} - 2B_{p^2(i-2)+2} + \frac{3}{2}B_{p^2(i-1)+1} \bmod p^2 .
\end{aligned}$$

En cuanto al término $T_2(0)$ tenemos

$$\begin{aligned}
T_2(0) &= -\frac{1}{p}\sum_{a=1}^{p}\omega^i(a)\langle a\rangle\left\{\frac{p^2}{12a^2} + p^3\sum_{j=4}^{\infty}\frac{p^{j-4}}{a^j}\frac{1}{j(j-1)}pB_j\right\} \\
&\equiv -\frac{p}{12}\sum_{a=1}^{p}\omega^{i-1}(a)a^{-1} \equiv -\frac{p}{12}\sum_{a=1}^{p}\omega^{i-2}(a) = 0 \bmod p^2 .
\end{aligned}$$

Reuniendo las congruencias obtenidas resulta

$$-2\zeta'_p(\omega^i, 0) \equiv B_{p^2(i-3)+3} - 4B_{p^2(i-2)+2} + 5B_{p^2(i-1)+1} \bmod p^2 .$$

Esta expresión puede ahora simplificarse por medio de las congruencias de Kummer. Para ello, dado un entero $t \geqslant 0$, definimos

$$A_t = \frac{B_{i+t(p-1)}}{i+t(p-1)};$$

entonces (véase por ejemplo [5])

$$A_t \equiv A_0 \bmod p$$
$$A_t - 2\,A_{t+1} + A_{t+2} \equiv 0 \bmod p^2.$$

Sustituyendo se obtiene que

$$\begin{aligned} -2\,\zeta'_p(\omega^i, 0) &\equiv 3\,A_{p(i-3)+i-3} - 8\,A_{p(i-2)+i-2} + 5\,A_{p(i-1)+i-1} \\ &\equiv -A_{p(i-3)+i-3} + A_{p(i-2)+i-2} \\ &\equiv (p+1)\,(A_1 - A_0) \bmod p^2. \end{aligned}$$

Por tanto, si (p, i) es un par irregular

$$2\,\zeta'_p(\omega^i, 0) \equiv \frac{B_i}{i} - \frac{B_{i+p-1}}{i+p-1} \bmod p^2$$

y

$$v_p(\zeta'_p(\omega^i, 0)) = 1 \Leftrightarrow \frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \bmod p^2.$$

Con ello se obtiene el siguiente

Teorema. Sea (p, i) un par irregular $(2 \leqslant i \leqslant p-3)$; la igualdad $\lambda_i = 1$ se cumple si y sólo si

$$\frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \bmod p^2.$$

Corolario. El invariante ciclotómico de Iwasawa λ^- coincide con el índice de irregularidad de p si y sólo si $\frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \bmod p^2$, siempre que $p|B_i$ $(2 \leqslant i \leqslant p-3)$, i par.

BIBLIOGRAFIA

[1] BOREVITCH, Z. I., SHAFAREVITCH, I.R.: *Théorie des nombres*. Paris: Gauthier-Villars, 1967.

[2] FERRERO, B., WASHINGTON, L.C.: *The Iwasawa invariant* μ_p vanishes for abelian number fields. Ann of Math. *109*, 377-395 (1979).

[3] IWASAWA, K.: *Lectures on p-adic L-functions*. Annals of Math. Studies. Princeton University Press, 1972.

[4] JOHNSON, W.: *Irregular primes and cyclotomic invariants*. Math. Comp. *29*, 113-120 (1975).

[5] JOHNSON, W.: *p-adic proofs on congruences for the Bernoulli, Numbers*. J. Number Theory *7*, 251-256 (1975).

[6] METSÄNKYLÄ, T.: *On the cyclotomic invariants of Iwasawa*. Math. Scand. *37*, 61-75 (1975).

[7] METSÄNKYLÄ, T.: *Iwasawa invariants and Kummer congruences*. J. Number Theory *10*, 510-522 (1978).

[8] WAGSTAFF, S. S.: *The irregular primes to 125.000*. Math. Comp. *32*, 583-591 (1978).

[9] WASHINGTON, L. C.: *A note on p-adic L-functions*. J. Number Theory *8*, 245-250 (1976).

Pilar Báyer