

Escrito 3

Distribución 2-ádica de las unidades módulo b^n :
régimenes, invariante central y casos frontera

Miguel Cerdá Bennassar

Septiembre de 2026

Resumen

Los Escritos 1 y 2 estudiaron, para la base 3, cómo se reparten entre las clases impares módulo 2^k los representantes $1 \leq E < 3^n$ de las unidades módulo 3^n tras la regularización de paridad. Esta nota extiende el estudio a toda base prima impar b . La distribución se organiza en b régimenes posibles y su oscilación nunca supera 2. Solo el régimen central tiene un invariante: el número de clases con el valor central no depende de n , y admite una expresión explícita mediante sumas de Dedekind, con una cota óptima para su desviación respecto del valor medio. Para $b = 3$ se recuperan los resultados del Escrito 2. Los casos frontera, en los que un régimen intermedio tiene oscilación 1, quedan caracterizados exactamente y confinados junto a los bordes de los régimenes, y las bases en las que no aparecen nunca son exactamente los primos de Mersenne; la base 3 es el primero de ellos.

1. Introducción

Sea b un primo impar y $k \geq 4$ con $M := 2^k \geq 4b$. Para cada $n \geq 1$ y cada residuo impar r módulo M se define

$$m_n(r) := \#\{E : 1 \leq E < b^n, b \nmid E, \mathcal{D}_n(E) \equiv r \pmod{M}\},$$
$$\mathcal{D}_n(E) := \begin{cases} E, & E \text{ impar,} \\ E + b^n, & E \text{ par.} \end{cases}$$

Para $b = 3$ esta es la multiplicidad estudiada en los Escritos 1 y 2, donde se obtuvo una clasificación completa en tres régimenes, con oscilación máxima 2 en el régimen central y un número constante $4J_{k-2}$ de clases con valor intermedio. Esta nota muestra que esa estructura es el caso más simple de un fenómeno general. Con base b hay b régimenes posibles; el invariante sobrevive solo en el régimen central; y aparecen casos frontera que en base 3 no existen. Se demuestra que las bases sin casos frontera son exactamente los primos de Mersenne $2^p - 1$, de los que 3 es el primero. Para la motivación de este estudio, véase el Escrito 1.

2. Reducción a un conteo

Proposición 1 (Regularización). $\mathcal{D}_n$ es una biyección entre $\{1 \leq E < b^n : b \nmid E\}$ y $\{1 \leq D < 2b^n : D \text{ impar, } b \nmid D\}$. En consecuencia,

$$m_n(r) = \#\{1 \leq D < 2b^n : D \equiv r \pmod{M}, b \nmid D\}.$$

Demostración. Igual que en el Escrito 1. Los E impares van en sí mismos; los pares van en $E + b^n \in (b^n, 2b^n)$, que es impar; y $b \nmid E$ si y solo si $b \nmid E + b^n$. El único impar de $[1, 2b^n)$ no alcanzado es b^n , que es múltiplo de b . $\square$

Como M es invertible módulo b , para cada r impar con $1 \leq r \leq M-1$ los b levantamientos $r + iM$, $0 \leq i \leq b-1$, recorren todas las clases módulo b , y exactamente uno es múltiplo de b .

Definición 2. Para r impar, $1 \leq r \leq M-1$, sea $\iota(r) \in \{0, \dots, b-1\}$ el índice del levantamiento múltiplo de b :

$$\iota(r) \equiv -r M^{-1} \pmod{b}.$$

Para $n \geq 1$ se definen $u_n := b^{n-1} \pmod{2^{k-1}}$ y $Q_n := \lfloor b^{n-1}/2^{k-1} \rfloor$, y se escribe $h := (b-1)/2$.

Como $2b^n = 2b(2^{k-1}Q_n + u_n) = bM Q_n + 2b u_n$ y $0 < 2b u_n < bM$, el cociente y el resto de $2b^n$ entre bM son Q_n y $R_n = 2b u_n$.

Lema 3 (Conteo). Para todo $n \geq 1$ y todo r impar,

$$m_n(r) = (b-1)Q_n + c_n(r), \quad c_n(r) := \#\{0 \leq i \leq b-1 : i \neq \iota(r), r + iM < 2b u_n\}.$$

Demostración. Cada uno de los Q_n bloques completos de longitud bM contiene un representante de cada una de las $b-1$ clases módulo bM admisibles, y en el resto se cuentan las que quedan por debajo de $R_n = 2b u_n$. $\square$

Corolario 4 (Periodicidad afín). Sea $P := \text{ord}_{2^{k-1}}(b)$. Para todo $n \geq 1$ y todo r impar,

$$m_{n+P}(r) = m_n(r) + \frac{(b-1)b^{n-1}(b^P - 1)}{2^{k-1}}.$$

Sea $e := v_2(b^2 - 1) - 1 \geq 2$. Entonces $P = 2^{k-1-e}$, y los valores de u_n son exactamente los $1 \leq u < 2^{k-1}$ con $u \equiv 1$ o $u \equiv b \pmod{2^{e+1}}$. Para $b \equiv 3, 5 \pmod{8}$ se tiene $e = 2$, y las clases son 1 y b módulo 8.

Demostración. $u_{n+P} = u_n$, luego $c_{n+P} = c_n$, y $Q_{n+P} - Q_n = (b^{n+P-1} - b^{n-1})/2^{k-1}$. Para la segunda, obsérvese primero que $k \geq e+2$: como 2^e divide a $b-1$ o a $b+1$, se tiene $2^{e+2} \leq 4b+4$, y si fuera $2^{e+2} > M \geq 4b$ se tendría $2^{e+2} \geq 2M \geq 8b > 4b+4$. Sea $J := k-1 \geq e+1 \geq 3$. En $(\mathbb{Z}/2^J\mathbb{Z})^\times$, el subgrupo $U := \{u \equiv 1 \pmod{2^{e+1}}\}$ es cíclico de orden 2^{J-e-1} y lo genera cualquier w con $v_2(w-1) = e+1$, pues $v_2(w^{2^i} - 1) = e+1+i$. Como $v_2(b^2 - 1) = e+1$, b^2 genera U . Además $b \notin U$: si $b \equiv 1 \pmod{4}$, entonces $v_2(b-1) = e$; si $b \equiv 3 \pmod{4}$, entonces $v_2(b-1) = 1$. Por tanto $\langle b \rangle = U \cup bU$, de orden $2^{J-e} = 2^{k-1-e}$, formado por las clases $\equiv 1$ y $\equiv b \pmod{2^{e+1}}$. $\square$

3. Los b regímenes

Definición 5. El régimen de n es $j_n := \lfloor 2b u_n / M \rfloor \in \{0, \dots, b-1\}$, y su corte es $t_n := 2b u_n - j_n M \in (0, M)$.

El corte nunca es 0: $2b u_n = jM$ exigiría $b \mid j$, luego $j = 0$ y $u_n = 0$, imposible. Además t_n es par.

Proposición 6 (Valores por régimen). Sea $j = j_n$ y $t = t_n$. Para todo r impar,

$$c_n(r) = \begin{cases} j+1 - \mathbf{1}[\iota(r) \leq j], & r < t, \\ j - \mathbf{1}[\iota(r) \leq j-1], & r \geq t. \end{cases}$$

En particular $c_n(r) \in \{j-1, j, j+1\}$, y la oscilación $\Delta_n := \max_r c_n(r) - \min_r c_n(r)$ nunca supera 2.

Demostración. Los levantamientos con $i \leq j - 1$ cumplen $r + iM < jM < 2bu_n$ y siempre cuentan salvo si $i = \iota(r)$; esto da $j - \mathbf{1}[\iota(r) \leq j - 1]$. El levantamiento $i = j$ cuenta si y solo si $r < t$ e $\iota(r) \neq j$. Los de índice $i \geq j + 1$ nunca cuentan. Sumando ambos casos se obtiene la fórmula. $\square$

Proposición 7 (Regímenes extremos). *Si $j_n = 0$ o $j_n = b - 1$, entonces $\Delta_n = 1$.*

Demostración. Si $j = 0$, $c_n(r) = 1 - \mathbf{1}[\iota(r) = 0]$ para $r < t$ y $c_n(r) = 0$ para $r \geq t$. El valor 1 se alcanza en $r = 1 < t$, pues $\iota(1) \equiv -M^{-1} \not\equiv 0$; el valor 0 se alcanza en el impar $r < M$ con $\iota(r) = 0$ si es menor que t , o en $r = M - 1 \geq t$ en otro caso. Si $j = b - 1$, $c_n(r) = b - 1$ para $r < t$ y $c_n(r) = b - 1 - \mathbf{1}[\iota(r) \leq b - 2]$ para $r \geq t$. El valor $b - 1$ se alcanza en $r = 1$, y el valor $b - 2$ en $r = M - 1 \geq t$, pues $\iota(M - 1) \equiv -1 + M^{-1} \not\equiv b - 1$. $\square$

En los regímenes intermedios, $1 \leq j \leq b - 2$, la oscilación es genéricamente 2; la Sección 7 caracteriza exactamente cuándo no lo es. Para $b = 3$ los regímenes $j = 0, 1, 2$ son los casos (A), (B) y (C) del Escrito 2.

4. El invariante central

El régimen $j = h$ es el *régimen central*. En él, por la Proposición 6, $c_n(r) = h$ si y solo si $r < t$ e $\iota(r) \leq h$, o bien $r \geq t$ e $\iota(r) \geq h$. Para $0 \leq x \leq M$ se define

$$I(x) := \#\{r < x : \iota(r) \leq h\} + \#\{r \geq x : \iota(r) \geq h\},$$

con r recorriendo los impares de $[1, M - 1]$, de modo que el número de clases con valor central en el exponente n es $I(t_n)$.

Lema 8 (Traslación del corte). *Si $0 \leq x$ y $x + 2b \leq M$, entonces $I(x + 2b) = I(x)$.*

Demostración. Los b impares de $[x, x + 2b)$ son consecutivos con diferencia 2, y 2 es invertible módulo b , así que ι toma en ellos cada valor exactamente una vez. Al pasar el corte de x a $x + 2b$, esos b impares pasan del segundo sumando al primero: el primero gana los $h + 1$ que tienen $\iota \leq h$ y el segundo pierde los $h + 1$ que tienen $\iota \geq h$. $\square$

La razón de que solo el régimen central tenga invariante está en este lema. En un régimen j cualquiera, el número de clases con valor j cambia en $(b - j) - (j + 1) = b - 1 - 2j$ al trasladar el corte en $2b$, y esa cantidad solo se anula para $j = h$.

Teorema 9 (Invariante central). *Todos los exponentes del régimen central tienen el mismo número de clases con valor central, a saber*

$$I_{b,k} = 4N_{b,k}, \quad N_{b,k} := \#\{r \text{ impar}, 1 \leq r < 2^{k-2} : \iota(r) \leq h\}.$$

Cuando $\Delta_n = 2$, este es el número de clases con valor intermedio de la distribución normalizada.

Demostración. Paso 1. El corte satisface $t_n \equiv M/2 \pmod{2b}$. En efecto, $2bu_n \equiv 0$ y $-hM = -(b - 1)2^{k-1} = 2^{k-1} - b2^{k-1}$, con $b2^{k-1} \equiv 0 \pmod{2b}$. Como t_n y $M/2$ están en $[0, M]$ y difieren en un múltiplo de $2b$, el Lema 8 da $I(t_n) = I(M/2)$, independiente de n .

Paso 2. La involución $r \mapsto M - r$ intercambia los impares menores y mayores que $M/2$, y cumple $\iota(M - r) \equiv -1 - \iota(r) \equiv 2h - \iota(r) \pmod{b}$; como ambos lados están en $\{0, \dots, 2h\}$, se tiene $\iota(M - r) = 2h - \iota(r)$, que transforma la condición $\iota \leq h$ en $\iota \geq h$. Por tanto los dos sumandos de $I(M/2)$ son iguales, e

$$I(M/2) = 2 \#\{r < M/2 : \iota(r) \leq h\}.$$

Paso 3. La involución $r \mapsto M/2 - r$ de los impares de $(0, M/2)$ cumple

$$\iota(M/2 - r) \equiv -2^{-1} - \iota(r) \equiv h - \iota(r) \pmod{b},$$

pues $2h \equiv -1$. Así envía $\{0, \dots, h\}$ en sí mismo y $\{h+1, \dots, 2h\}$ en sí mismo. Su único punto fijo sería $M/4$, que es par, de modo que empareja los impares de $(0, M/4)$ con los de $(M/4, M/2)$ conservando la condición $\iota \leq h$. Luego $\#\{r < M/2 : \iota(r) \leq h\} = 2N_{b,k}$.

Finalmente, si $\Delta_n = 2$ el mínimo es $h-1$ y el valor intermedio de la distribución normalizada corresponde a $c_n(r) = h$. $\square$

Observación 10 (Relación con el lema de Gauss). Escribiendo $x(r) := r M^{-1} \pmod{b}$, la condición $\iota(r) \leq h$ equivale a $x(r) = 0$ o $x(r) > b/2$. Así, $N_{b,k}$ cuenta cuántos de los múltiplos $r \cdot 2^{-k}$, con r impar menor que 2^{k-2} , caen en 0 o en la mitad superior de $\mathbb{Z}/b\mathbb{Z}$: el mismo tipo de recuento que interviene en el lema de Gauss para el símbolo de Legendre.

Corolario 11 (Base 3). $N_{3,k} = J_{k-2}$, donde J es la sucesión de Jacobsthal, y se recupera $I_{3,k} = 4J_{k-2}$ (Escrito 2).

Demostración. Para $b = 3$, $4N_{3,k}$ es el número de clases con valor intermedio en el régimen central, que es el caso (B) del Escrito 2. El Corolario «El invariante central» del Escrito 2 establece que ese número es $4J_{k-2}$. $\square$

Proposición 12 (Tamaño del invariante). Existe $\delta_{b,k} \in \mathbb{Q}$, que depende de k solo a través de $2^k \pmod{b}$, tal que

$$I_{b,k} = \frac{(b+1)2^k}{4b} + \delta_{b,k}.$$

En particular, $\delta_{b,k}$ es periódica en k con periodo $\text{ord}_b(2)$.

Demostración. Escribáse $M/4 = 2bq + \sigma$ con $0 \leq \sigma < 2b$. Como $M/4$ es par y $2b$ también, σ es par, y queda determinado por $M/4 \pmod{b}$, es decir, por $2^k \pmod{b}$. Por el argumento del Lema 8, cada bloque de $2b$ enteros consecutivos aporta $h+1$ impares con $\iota \leq h$. Además, para $r = 2bq + r'$ se tiene $\iota(r) = \iota(r')$, pues $2bq \equiv 0 \pmod{b}$. Así

$$N_{b,k} = (h+1)q + C, \quad C := \#\{r' \text{ impar}, r' < \sigma : \iota(r') \leq h\},$$

donde C solo depende de σ y de $M^{-1} \pmod{b}$. Sustituyendo $q = (M/4 - \sigma)/(2b)$ y $h+1 = (b+1)/2$ se obtiene $I_{b,k} = 4N_{b,k} = (b+1)M/(4b) + \delta_{b,k}$ con $\delta_{b,k} = 4C - (b+1)\sigma/b$. $\square$

Proposición 13 (Valores extremos de la corrección). Sea $k \geq 4$ con $2^k \geq 4b$. Si $2^{k-1} \equiv \pm 1 \pmod{b}$, entonces

$$\delta_{b,k} = \pm \frac{b^2 - 1}{2b},$$

con el mismo signo. Como $2^{k-1} \equiv 1 \pmod{b}$ para $k-1$ múltiplo de $\text{ord}_b(2)$, este valor se alcanza en todo periodo de k .

Demostración. En la demostración de la Proposición 12, sea $m := \sigma/2 \in \{0, \dots, b-1\}$. Como $\sigma \equiv M/4 \pmod{2b}$, se tiene $m \equiv 2^{k-3} \pmod{b}$, y

$$\delta_{b,k} = 4C - \frac{2(b+1)m}{b}, \quad C = \#\{0 \leq i < m : \iota(2i+1) \leq h\}.$$

Se usa que $-2^{-1} \equiv h$ y $2^{-1} \equiv h+1 \pmod{b}$. Los cuatro casos, con el valor de m y el de C que se obtiene, son:

$2^{k-1} \bmod b$	$b \bmod 4$	m	C
1	3	$(b+1)/4$	m
1	1	$(3b+1)/4$	$h+1$
-1	1	$(b-1)/4$	0
-1	3	$(3b-1)/4$	$m-h$

Caso $2^{k-1} \equiv 1$. Entonces $M^{-1} \equiv 2^{-1}$ e $\iota(2i+1) \equiv -(2i+1)2^{-1} \equiv h-i \pmod{b}$, y $m \equiv 4^{-1} \pmod{b}$. Si $b \equiv 3 \pmod{4}$, $m = (b+1)/4 \leq h+1$; los índices $i < m$ dan $\iota = h-i \in [0, h]$, luego $C = m$ y $\delta_{b,k} = 2m(b-1)/b = (b^2-1)/(2b)$. Si $b \equiv 1 \pmod{4}$, $m = (3b+1)/4$; los índices $0 \leq i \leq h$ dan $\iota = h-i \leq h$, y los índices $h < i < m$ dan $\iota = b+h-i \geq b+h-m+1 = (3b+1)/4 > h$. Así $C = h+1 = (b+1)/2$ y $\delta_{b,k} = 2(b+1)(1 - \frac{3b+1}{4b}) = (b^2-1)/(2b)$.

Caso $2^{k-1} \equiv -1$. Entonces $M^{-1} \equiv -2^{-1}$ e $\iota(2i+1) \equiv (2i+1)2^{-1} \equiv i+h+1 \pmod{b}$, y $m \equiv -4^{-1} \pmod{b}$. Si $b \equiv 1 \pmod{4}$, $m = (b-1)/4 \leq h$; los índices $i < m$ dan $\iota = h+1+i > h$, luego $C = 0$ y $\delta_{b,k} = -2(b+1)m/b = -(b^2-1)/(2b)$. Si $b \equiv 3 \pmod{4}$, $m = (3b-1)/4$; los índices $i < h$ dan $\iota > h$, y los índices $h \leq i < m$ dan $\iota = i-h \leq m-1-h = (b-3)/4 \leq h$. Así $C = m-h = (b+1)/4$ y $\delta_{b,k} = (b+1) - \frac{(b+1)(3b-1)}{2b} = -(b^2-1)/(2b)$. $\square$

Valores del invariante central

$b \backslash k$	6	7	8	9	10	11	12
3	20	44	84	172	340	684	1364
5	20	36	76	156	308	612	1228
7	16	40	72	144	296	584	1168
11	12	36	68	140	276	564	1116
13	20	28	68	140	276	548	1100

La fila $b = 3$ es $4J_{k-2}$. Para $b \geq 5$ no hay una fórmula tan simple, pero el Teorema 14 de la sección siguiente da una expresión explícita en términos de sumas de Dedekind.

5. El invariante central y las sumas de Dedekind

Se usan el diente de sierra $((x)) := x - \lfloor x \rfloor - \frac{1}{2}$ si $x \notin \mathbb{Z}$, $((x)) := 0$ si $x \in \mathbb{Z}$, y la suma de Dedekind

$$s(a, q) := \sum_{j=1}^{q-1} \left(\left(\frac{j}{q} \right) \right) \left(\left(\frac{aj}{q} \right) \right).$$

Es la normalización clásica [5], con $q \geq 1$; la definición se aplica a todo entero a , no solo a los coprimos con q , lo que es necesario más adelante. Se usan las propiedades básicas siguientes: $s(a, q)$ depende de a módulo q ; $s(-a, q) = -s(a, q)$; $s(a', q) = s(a, q)$ si $aa' \equiv 1 \pmod{q}$; y $s(da, dq) = s(a, q)$ para $d \geq 1$, que se obtiene agrupando los índices j módulo q y aplicando la fórmula de multiplicación $\sum_{l=0}^{d-1} ((y + l/d)) = ((dy))$. Además, el Corolario 19 usa la identidad de Petersson–Knopp y la Sección 6 la fórmula de Meyer, ambas citadas en su lugar. Para x entero no divisible por b , $x2^{-1}$ denota el entero $x \cdot 2^{-1} \bmod b$, y x^* su representante impar módulo $2b$, es decir, $x^* \in \{x \bmod b, (x \bmod b) + b\}$ impar.

Teorema 14 (El invariante central en sumas de Dedekind). *Sea $k \geq 4$ con $2^k \geq 4b$. Entonces*

$$\delta_{b,k} = 4 \left[3 s(2^{k-1}, b) - 2 s(2^k, b) - s(2^{k-2}, b) \right],$$

y en consecuencia

$$I_{b,k} = 4N_{b,k} = \frac{(b+1)2^k}{4b} + 4[3s(2^{k-1}, b) - 2s(2^k, b) - s(2^{k-2}, b)].$$

La demostración ocupa los lemas siguientes. Se fija la notación de la Proposición 12: $m := \sigma/2 \equiv 2^{k-3} \pmod{b}$, con $1 \leq m \leq b-1$, y

$$\delta_{b,k} = 4C - \frac{2(b+1)m}{b}, \quad C = \#\{r \text{ impar}, 1 \leq r < 2m : \iota(r) \leq h\}.$$

Sea además $c := -2^{1-k} \pmod{b}$, de modo que $4cm \equiv -1 \pmod{b}$.

Lema 15 (Paridad). *Para r impar, $\iota(r) \leq h$ si y solo si $cr \pmod{b}$ es par.*

Demostración. Para $0 \leq y \leq b-1$, se tiene $y \leq h$ si y solo si $2y \pmod{b} = 2y$, que es par; si $y \geq h+1$, entonces $2y \pmod{b} = 2y-b$, que es impar. Se aplica a $y = \iota(r)$, con $2\iota(r) \equiv -2r \cdot 2^{-k} \equiv cr \pmod{b}$. $\square$

Lema 16 (Ventana de Kronecker).

$$C = \mathbf{1}[2m > b] + \#\left\{1 \leq t \leq h : \left\{\frac{4mt}{b}\right\} \in \left(\frac{1}{2} - \frac{m}{b}, \frac{1}{2}\right) \pmod{1}\right\}.$$

Aquí, un intervalo “módulo 1” denota su imagen en $\mathbb{R}/\mathbb{Z}$: si $m > b/2$, el extremo izquierdo es negativo y el intervalo corresponde a la unión $[0, \frac{1}{2}) \cup (\frac{3}{2} - \frac{m}{b}, 1)$ dentro de $[0, 1)$.

Demostración. Sea c^* el representante impar de c módulo $2b$. Para r impar, c^*r es impar, y su resto módulo $2b$ es v si $v := cr \pmod{b}$ es impar y $v+b$ si v es par. Así, $cr \pmod{b}$ es par si y solo si $c^*r \pmod{2b} \geq b$. La aplicación $r \mapsto y := c^*r \pmod{2b}$ es una biyección de los residuos impares módulo $2b$, con inversa $y \mapsto dy \pmod{2b}$, donde $d := (c^*)^{-1} \pmod{2b}$ cumple $d \equiv c^{-1} \equiv -4m \pmod{b}$. El impar $r = b$ está en $[1, 2m)$ exactamente cuando $2m > b$, va a parar a $y = b$ y cumple la condición, pues $cb \pmod{b} = 0$. Los demás r contados corresponden biyectivamente a los $y = b + 2t$, con $1 \leq t \leq h$, tales que $r = dy \pmod{2b} < 2m$.

Sea $r_t := (-4mt) \pmod{b}$, que no es nulo porque $1 \leq t \leq h$. Como $dy \equiv b + 2dt \pmod{2b}$ y $dt \equiv -4mt \pmod{b}$,

$$dy \pmod{2b} = \begin{cases} b + 2r_t, & r_t < b/2, \\ 2r_t - b, & r_t > b/2. \end{cases}$$

En el primer caso, $dy \pmod{2b} < 2m$ equivale a $r_t/b < m/b - \frac{1}{2}$; en el segundo, a $r_t/b < \frac{1}{2} + m/b$. Juntando ambos, la condición equivale a que r_t/b esté en el arco $(\frac{1}{2}, \frac{1}{2} + \frac{m}{b})$ de $\mathbb{R}/\mathbb{Z}$. Finalmente, como $r_t \neq 0$, se tiene $\{4mt/b\} = 1 - r_t/b$, y la condición es la del enunciado. $\square$

Lema 17 (Dientes de sierra). *Sea $\varphi(n) := ((2mn/b)) - ((mn/b))$, y sea*

$$X := \frac{1}{2} \sum_{j=0}^{b-1} (-1)^j [\varphi(2j+1) - \varphi(2j)].$$

Entonces $\delta_{b,k} = -4X$.

Demostración. Sea K el recuento del Lema 16, con $w := m/b$ y $x_t := 4mt/b$. Para cada t , la condición de la ventana equivale a que haya un entero en $(x_t - \frac{1}{2}, x_t - \frac{1}{2} + w]$, y su indicador es $\lfloor x_t - \frac{1}{2} + w \rfloor - \lfloor x_t - \frac{1}{2} \rfloor$. Ninguno de los dos argumentos es entero, pues sus numeradores sobre $2b$ son $8mt + 2m - b$ y $8mt - b$, impares. Usando $\lfloor y \rfloor = y - \frac{1}{2} - ((y))$ para $y \notin \mathbb{Z}$, y la identidad $((y - \frac{1}{2})) = ((y + \frac{1}{2})) = ((2y)) - ((y))$, válida para todo y real (es

el caso $n = 2$ de la fórmula de multiplicación $\sum_{l=0}^{n-1} ((y + l/n)) = ((ny))$ [5]), se obtiene, con $x_t + w = m(4t + 1)/b$,

$$K = \frac{hm}{b} - \sum_{t=1}^h [\varphi(4t + 1) - \varphi(4t)].$$

La función φ es impar y b -periódica, así que su suma sobre cualquier sistema completo de restos módulo b es nula. Los impares $2j + 1$, $0 \leq j \leq b - 1$, forman un tal sistema, y los que son $\equiv 1$ (mód 4) son los de j par, es decir, los $4t + 1$ con $0 \leq t \leq h$. Por tanto $\sum_{t=0}^h \varphi(4t + 1) = \frac{1}{2} \sum_j (-1)^j \varphi(2j + 1)$, y del mismo modo $\sum_{t=0}^h \varphi(4t) = \frac{1}{2} \sum_j (-1)^j \varphi(2j)$. Como $\varphi(0) = 0$, resulta $K = \frac{hm}{b} + \varphi(1) - X$.

Finalmente, $\varphi(1) = \frac{m}{b} - \mathbf{1}[2m > b]$, de modo que $C = \mathbf{1}[2m > b] + K = \frac{(h+1)m}{b} - X$ y

$$\delta_{b,k} = 4C - \frac{2(b+1)m}{b} = \frac{4(h+1)m - 2(b+1)m}{b} - 4X = -4X. \quad \square$$

Lema 18. *Para y no divisible por b , sea $T(y) := \frac{1}{2} \sum_{j=0}^{b-1} (-1)^j [((y(2j+1)/b)) - ((2yj/b))]$. Entonces*

$$T(y) = 2s(4y, b) - s(2y, b).$$

Demostración. En el primer sumando, la involución $j \mapsto b - 1 - j$ conserva $(-1)^j$, pues $b - 1$ es par, y cambia el signo de $((y(2j+1)/b))$, pues $2(b - 1 - j) + 1 = 2b - (2j + 1)$. Los términos se cancelan por parejas, y el punto fijo $j = h$ aporta $((yb/b)) = 0$. Así, el primer sumando es nulo.

En el segundo, como $2j$ recorre todos los restos módulo b cuando j recorre $0, \dots, b - 1$, y $j \mapsto ((2yj/b))$ es impar, su suma completa es nula; por tanto la suma alternada es el doble de la suma sobre los j pares, que son $j = 2i$ con $0 \leq i \leq h$:

$$\sum_{j=0}^{b-1} (-1)^j ((2yj/b)) = 2 \sum_{i=0}^h ((4yi/b)).$$

Para $1 \leq i \leq b - 1$ se tiene $\mathbf{1}[i \leq h] = \frac{1}{2} - 2((i/b)) + ((2i/b))$: si $i \leq h$, el lado derecho vale $\frac{1}{2} - 2(\frac{i}{b} - \frac{1}{2}) + (\frac{2i}{b} - \frac{1}{2}) = 1$, y si $i > h$, vale $\frac{1}{2} - 2(\frac{i}{b} - \frac{1}{2}) + (\frac{2i}{b} - \frac{3}{2}) = 0$. Aplicándolo a la función impar $F(i) = ((4yi/b))$, cuya suma completa es nula,

$$\sum_{i=1}^h F(i) = -2 \sum_{i=1}^{b-1} F(i)((i/b)) + \sum_{i=1}^{b-1} F(i)((2i/b)) = -2s(4y, b) + s(2y, b),$$

donde en la última suma se ha sustituido $u \equiv 2i$ (mód b), que permuta $\{1, \dots, b - 1\}$ porque 2 es invertible módulo b . Por tanto

$$T(y) = -\frac{1}{2} \cdot 2(-2s(4y, b) + s(2y, b)) = 2s(4y, b) - s(2y, b). \quad \square$$

Demostración del Teorema 14. Por definición, $X = T(2m) - T(m)$. Por el Lema 18,

$$X = 2s(8m, b) - 3s(4m, b) + s(2m, b),$$

y por el Lema 17, $\delta_{b,k} = 4[3s(4m, b) - 2s(8m, b) - s(2m, b)]$. Como $m \equiv 2^{k-3}$ (mód b), se tiene $4m \equiv 2^{k-1}$, $8m \equiv 2^k$ y $2m \equiv 2^{k-2}$ (mód b), y esto es el enunciado. La expresión de $I_{b,k}$ se sigue de la Proposición 12. $\square$

Corolario 19 (Forma corta).

$$\delta_{b,k} = 4 \left[s((2^{k-1})^*, 2b) - s(2^k, b) \right].$$

Demostración. El Teorema 14 no depende de este corolario, que solo reescribe su enunciado. Se usa el caso $n = 2$ de la identidad de Petersson–Knopp [2, 1],

$$\sum_{ad=n} \sum_{\beta \bmod d} s(ah + \beta k, dk) = \sigma(n) s(h, k),$$

válida para enteros cualesquiera h y $k \geq 1$, sin condición de coprimidad [3]. Con $n = 2$, $h = x$ y $k = b$, afirma que

$$s(2x, b) + s(x, 2b) + s(x + b, 2b) = 3s(x, b).$$

De los dos enteros x y $x + b$, uno es x^* y el otro es par, igual a $2g$ con $g \equiv x2^{-1} \pmod{b}$; y $s(2g, 2b) = s(g, b)$. Así,

$$s(x^*, 2b) = 3s(x, b) - s(2x, b) - s(x2^{-1}, b).$$

(Con esta normalización, la igualdad anterior se ha comprobado además numéricamente para todos los primos $5 \leq b < 110$ y todos los x no divisibles por b .) Con $x = 2^{k-1}$ se obtiene $4[s(x^*, 2b) - s(2^k, b)] = 4[3s(2^{k-1}, b) - 2s(2^k, b) - s(2^{k-2}, b)] = \delta_{b,k}$. $\square$

Observación 20. El Teorema 14 da una expresión explícita de $N_{b,k}$ en términos de sumas de Dedekind. Mediante la ley de reciprocidad y el algoritmo de Euclides, las sumas de Dedekind se evalúan en un número de pasos logarítmico en b , así que $N_{b,k}$ se obtiene sin recorrer ningún rango de enteros. Para $b = 3$ se recupera $N_{3,k} = J_{k-2}$. En los casos $2^{k-1} \equiv \pm 1 \pmod{b}$ de la Proposición 13, el Corolario 19 y los valores clásicos $s(1, b) = \frac{(b-1)(b-2)}{12b}$ y $s(2, b) = \frac{(b-1)(b-5)}{24b}$ reproducen $\delta_{b,k} = \pm \frac{b^2-1}{2b}$.

6. La cota óptima

Para $1 \leq a \leq b-1$ con $b \nmid a$, sea $I(a)$ el número de inversiones de la permutación $i \mapsto ai \bmod b$ de $\{1, \dots, b-1\}$, es decir, el número de parejas $i < j$ con $ai \bmod b > aj \bmod b$. Se usa la fórmula de Meyer [4], en la forma enunciada en [6], que con la normalización de la Sección 5 se ha comprobado también numéricamente para todos los primos $5 \leq b < 70$ y todos los a :

$$s(a, b) = \frac{(b-1)(b-2)}{12b} - \frac{I(a)}{3b}.$$

Teorema 21 (Cota óptima). *Para toda unidad x módulo b ,*

$$\left| 3s(x, b) - 2s(2x, b) - s(x2^{-1}, b) \right| \leq \frac{b^2 - 1}{8b},$$

con igualdad si y solo si $x \equiv \pm 1 \pmod{b}$. En particular, para todo $k \geq 4$ con $2^k \geq 4b$,

$$|\delta_{b,k}| \leq \frac{b^2 - 1}{2b},$$

con igualdad si y solo si $2^{k-1} \equiv \pm 1 \pmod{b}$.

Demostración. Para $b = 3$ las unidades son ± 1 y todo se reduce a la Proposición 13; se supone $b \geq 5$. Sea $\pi(u) := xu \bmod b$ en $R := \{1, \dots, b-1\}$. Para un orden total $\prec$ en R , sea $I_\prec$ el número de parejas $u \prec v$ con $\pi(u) > \pi(v)$, y para dos órdenes $\prec, \prec'$ sea $D(\prec, \prec')$ el número de parejas $\{u, v\} \subset R$ que ambos órdenes colocan en sentido contrario.

Tres órdenes. Se consideran el orden natural $<$; el orden

$$2 \prec_1 4 \prec_1 \dots \prec_1 b-1 \prec_1 1 \prec_1 3 \prec_1 \dots \prec_1 b-2,$$

que coloca primero los pares y después los impares, cada grupo en orden creciente; y el orden total $\prec_2$ definido por $u \prec_2 v$ si y solo si $2u \bmod b < 2v \bmod b$, tomando los restos en $\{1, \dots, b-1\}$. Se tiene

$$I(x) = I_{<}, \quad I(2x) = I_{\prec_1}, \quad I(x2^{-1}) = I_{\prec_2}.$$

La primera igualdad es la definición. Para la segunda, $I(2x)$ cuenta las parejas $i < j$ con $\pi(2i) > \pi(2j)$. Al recorrer $i = 1, \dots, h$ el valor $u = 2i \bmod b$ recorre $2, 4, \dots, b-1$, y al recorrer $i = h+1, \dots, b-1$ recorre $1, 3, \dots, b-2$; así, el orden natural de i induce en u el orden $\prec_1$. Para la tercera, $I(x2^{-1})$ cuenta las parejas $i < j$ con $\pi(i2^{-1}) > \pi(j2^{-1})$, y con $u = i \cdot 2^{-1} \bmod b$ se tiene $i = 2u \bmod b$, que es la clave de $\prec_2$.

Comparación de órdenes. Sea $\{u, v\}$ una pareja con $\pi(u) < \pi(v)$. Contribuye a $I_{<}$ si y solo si $v < u$. Si $\prec$ y $\prec'$ la colocan en el mismo sentido, contribuye lo mismo a $I_{\prec}$ y a $I_{\prec'}$; si la colocan en sentido contrario, contribuye a exactamente uno de los dos. Por tanto

$$|I_{\prec} - I_{\prec'}| \leq D(\prec, \prec'),$$

con $I_{\prec} - I_{\prec'} = -D(\prec, \prec')$ si y solo si todas las parejas de desacuerdo contribuyen a $I_{\prec'}$, es decir, si π las ordena como $\prec$.

Desacuerdos. El orden natural y $\prec_1$ discrepan exactamente en las parejas formadas por un impar u y un par v con $u < v$. Para $v = 2k$ hay k impares menores, luego $D(<, \prec_1) = \sum_{k=1}^h k = \frac{h(h+1)}{2}$. El orden natural y $\prec_2$ coinciden en las parejas contenidas en $\{1, \dots, h\}$, donde la clave es $2u$, o en $\{h+1, \dots, b-1\}$, donde es $2u-b$. Para $u \leq h < v$ discrepan si y solo si $2u > 2v-b$, es decir, $v \leq u+h$. Fijado $u \in \{1, \dots, h\}$, los valores admisibles son $v = h+1, \dots, h+u$, en número u , luego $D(<, \prec_2) = \sum_{u=1}^h u = \frac{h(h+1)}{2}$ también. Se escribe $D := \frac{h(h+1)}{2} = \frac{b^2-1}{8}$.

Cota. Como los coeficientes $3, -2, -1$ suman cero, la fórmula de Meyer da

$$3s(x, b) - 2s(2x, b) - s(x2^{-1}, b) = -\frac{Q}{3b}, \quad Q := 2A + B, \quad A := I_{<} - I_{\prec_1}, \quad B := I_{<} - I_{\prec_2}.$$

Por lo anterior,

$$|Q| \leq 2|A| + |B| \leq 3D = \frac{3(b^2-1)}{8},$$

que es la desigualdad del enunciado. La cota para $\delta_{b,k}$ se sigue del Teorema 14 con $x = 2^{k-1}$.

Igualdad. Si $x \equiv \pm 1$, la combinación coincide con $\delta_{b,k}/4$ en los dos casos de la Proposición 13 (con $2^{k-1} \equiv x$), que alcanzan el valor $\pm \frac{b^2-1}{8b}$. Recíprocamente, si $|Q| = 3D$, las dos desigualdades de la cadena anterior son igualdades: $|A| = |B| = D$, y A y B tienen el mismo signo. Si $A = B = D$, se sustituye x por $-x$: como x y u son unidades módulo b , $\pi_{-x}(u) = (-xu) \bmod b = b - \pi_x(u)$, con $\pi_x(u) \neq 0$, lo que invierte todas las comparaciones entre valores de π y cambia A y B por $-A$ y $-B$. Así se puede suponer $A = B = -D$, es decir, que π ordena como el orden natural todas las parejas de desacuerdo:

$$\pi(u) < \pi(v) \quad \text{si } u < v, \text{ } u \text{ impar, } v \text{ par,} \quad \text{y si } u \leq h < v \leq u+h. \quad (*)$$

Supóngase $x \neq 1$, con $2 \leq x \leq b-1$. Como $x(b-1) \geq b$, existe un menor índice i con $x(i+1) \geq b$, y cumple $1 \leq i$ e $i+1 \leq b-1$. Entonces $\pi(j) = xj$ para $1 \leq j \leq i$ y $\pi(i+1) = x(i+1) - b$.

Si i es impar, en la pareja $u = 1 < v = i+1$ el primero es impar y el segundo par, y se tiene $\pi(v) = x(i+1) - b < x$ porque $xi < b$; es decir, $\pi(v) < \pi(u)$. Esto contradice (*).

Si i es par e $i \geq 4$, entonces $i \leq b-3$, porque $b-2$ es impar, e $i+2 \leq b-1$. De $xi < b$ se sigue $x < b/4$, luego $b \leq x(i+2) = xi + 2x < 2b$ y $\pi(i+2) = x(i+2) - b$. La pareja $u = 3 < v = i+2$ tiene u impar y v par, y $\pi(v) = x(i+2) - b < 3x = \pi(u)$ porque $x(i-1) < b$. Esto contradice (*).

Si $i = 2$, entonces $2x < b \leq 3x$. Si x es par, $\pi(h+1) = x(b+1)/2 \pmod{b} = x/2$, y la pareja $u = 1 \leq h < v = h+1 \leq 1+h$ da $\pi(v) = x/2 < x = \pi(u)$. Si x es impar, $\pi(h+1) = (x+b)/2$ y, como $b \leq 3x < 2b$, $\pi(h+2) = (x+b)/2 + x - b = (3x-b)/2$; la pareja $u = 2 \leq h < v = h+2 \leq 2+h$ da $\pi(v) = (3x-b)/2 < 2x = \pi(u)$. En ambos casos se contradice (*).

Por tanto $x = 1$ o, deshaciendo la sustitución, $x = -1$. $\square$

Observación 22. La demostración muestra el origen de la constante: $\frac{b^2-1}{8} = \frac{h(h+1)}{2}$ es el número de parejas en que el orden natural discrepa de cada uno de los órdenes asociados a la multiplicación y a la división por 2 módulo b . La cota es óptima porque la identidad y la inversión son las únicas permutaciones $u \mapsto xu$ que respetan todos esos desacuerdos a la vez.

7. Casos frontera

Para $1 \leq j \leq b-2$ se definen

$$\rho_j := \min\{r \text{ impar} : \iota(r) > j\}, \quad R_j := \max\{r \text{ impar}, r < M : \iota(r) \leq j-1\}.$$

Los b primeros impares $1, 3, \dots, 2b-1$ toman todos los valores de ι , y lo mismo los b últimos, $M-2b+1, \dots, M-1$. Por tanto $\rho_j \leq 2b-1$ y $R_j \geq M-2b+1$, y como $M \geq 4b$, se tiene $\rho_j < R_j$.

Teorema 23 (Caracterización de los casos frontera). *Sea n con régimen intermedio $1 \leq j = j_n \leq b-2$ y corte $t = t_n$. Entonces $\Delta_n \in \{1, 2\}$, y*

$$\Delta_n = 1 \iff t \leq \rho_j \text{ o } t > R_j.$$

Demostración. Por la Proposición 6, $c_n(r) = j+1$ si y solo si $r < t$ e $\iota(r) > j$, y $c_n(r) = j-1$ si y solo si $r \geq t$ e $\iota(r) \leq j-1$. El primer conjunto es vacío exactamente cuando $t \leq \rho_j$, y el segundo exactamente cuando $t > R_j$. Como $\rho_j < R_j$, no pueden ser vacíos a la vez, así que se alcanzan al menos dos valores y $\Delta_n \geq 1$. La oscilación es 2 si y solo si ambos conjuntos son no vacíos. $\square$

Corolario 24 (Localización). *Los casos frontera solo ocurren junto a los bordes de los regímenes: $t \leq \rho_j$ exige $jM/(2b) < u_n < jM/(2b) + 1$, y $t > R_j$ exige $(j+1)M/(2b) - 1 < u_n < (j+1)M/(2b)$. En consecuencia, cada régimen intermedio contiene como mucho dos exponentes excepcionales por periodo, y en total hay como mucho $2(b-2)$.*

Demostración. $t \leq \rho_j < 2b$ equivale a $2bu_n - jM < 2b$, y $t > R_j > M - 2b$ equivale a $(j+1)M - 2bu_n < 2b$. Cada uno de esos intervalos de longitud 1 contiene como mucho un entero, y dentro de un periodo cada valor de u corresponde a un único exponente. $\square$

Proposición 25 (Dependencia de k). *Sea $e = v_2(b^2 - 1) - 1$ como en el Corolario 4. Un entero par $t \in (0, M)$ con $t \equiv -jM \pmod{b}$ es el corte de algún exponente del régimen j si y solo si $t \equiv 2$ o $2b \pmod{2^{e+2}}$. En consecuencia, qué regímenes tienen casos frontera, y en qué borde, depende de k solo a través de $2^k \pmod{b}$, y es periódico en k con periodo $\text{ord}_b(2)$.*

Demostración. Dado t , el único candidato es $u = (t + jM)/(2b)$, que es entero porque t es par y $t + jM \equiv 0 \pmod{b}$, y satisface $1 \leq u < M/2$. Por el Corolario 4, u es un valor de u_n si y solo si $u \equiv 1$ o $b \pmod{2^{e+1}}$, es decir, como $b^2 \equiv 1 \pmod{2^{e+1}}$, si y solo si $bu \equiv b$ o $1 \pmod{2^{e+1}}$. Como $k \geq e+2$, $jM \equiv 0 \pmod{2^{e+2}}$, y de $2bu = t + jM$ se obtiene

$2(bu \bmod 2^{e+1}) \equiv t \pmod{2^{e+2}}$. Por tanto la condición es $t \equiv 2b$ o $2 \pmod{2^{e+2}}$. En ese caso u es un valor u_n , y el exponente n correspondiente tiene régimen j y corte t , porque $2bu_n = jM + t$ con $0 < t < M$. Las condiciones $t \leq \rho_j$ y $t > R_j$ involucran ι , que depende de $M^{-1} \bmod b$, y la distancia de t a 0 o a M . Como $M \equiv 0 \pmod{2^{e+2}}$, todo depende de k solo a través de $2^k \bmod b$. $\square$

Teorema 26 (Bases sin casos frontera). *Sea 2^m la mayor potencia de 2 menor que b , y considérense, como en todo el escrito, los $k \geq 4$ con $2^k \geq 4b$.*

- (a) *Si $b = 2^p - 1$ es un primo de Mersenne, no hay casos frontera para ningún k .*
- (b) *Si b no es un primo de Mersenne, hay casos frontera para todo k que cumpla $2^{-k} \equiv 2^m \pmod{b}$, es decir, $k \equiv -m \pmod{\text{ord}_b(2)}$. Esas soluciones forman una clase módulo $\text{ord}_b(2)$, así que infinitas de ellas cumplen $2^k \geq 4b$.*

En particular, en base $3 = 2^2 - 1$ no hay casos frontera.

Demostración. Se usan la Proposición 25 y el Teorema 23: un caso frontera en el régimen intermedio j exige un corte realizado t con $t \leq \rho_j \leq 2b - 1$ (borde inferior) o con $t > R_j \geq M - 2b + 1$, es decir, $1 \leq M - t \leq 2b - 2$ (borde superior). Recuerdese que $\iota(1) \equiv -M^{-1} \pmod{b}$.

(a) Sea $b = 2^p - 1$. Como $b + 1 = 2^p$ y $b - 1 = 2(2^{p-1} - 1)$ con $2^{p-1} - 1$ impar, se tiene $e = p$. Así, los cortes realizados cumplen $t \equiv 2$ o $t \equiv 2b = 2^{p+1} - 2 \pmod{2^{p+2}}$, y $M \equiv 0 \pmod{2^{p+2}}$ porque $k \geq e + 2 = p + 2$ (Corolario 4).

Borde superior. El número $M - t$ sería congruente con -2 o con $2 - 2^{p+1}$ módulo 2^{p+2} . Los menores enteros positivos de esas clases son $2^{p+2} - 2$ y $2^{p+1} + 2$, ambos mayores que $2b - 2 = 2^{p+1} - 4$. Esto es imposible.

Borde inferior. El único entero positivo $t \leq 2^{p+1} - 3$ en esas clases es $t = 2$. De $t \equiv -jM \pmod{b}$ se sigue $j \equiv -2M^{-1} \equiv 2\iota(1) \pmod{b}$. Como $2^p \equiv 1 \pmod{b}$, se tiene $M^{-1} = 2^{-k} \equiv 2^s \pmod{b}$ para algún $0 \leq s < p - 1$, y como $2^s < b$, resulta $\iota(1) = b - 2^s$. Si $s = p - 1$, entonces $2\iota(1) = 2b - 2^p = b - 1$, luego $j = b - 1$, que es un régimen extremo. Si $s \leq p - 2$, entonces $2^{s+1} < b$ y $j = b - 2^{s+1} < b - 2^s = \iota(1)$; así $\iota(1) > j$, luego $\rho_j = 1 < t = 2$, y por el Teorema 23 tampoco hay caso frontera. En los dos casos, $s = p - 1$ y $s \leq p - 2$, el corte $t = 2$ queda excluido, y con él todo el borde inferior.

(b) Como b no es de la forma $2^{m+1} - 1$, se tiene $2^m \neq h + 1$, y como $b/2 < 2^m < b$, resulta $h + 2 \leq 2^m \leq b - 1$. Sea k con $2^{-k} \equiv 2^m \pmod{b}$, y sean

$$y := \iota(1) = b - 2^m \in [1, h - 1], \quad j := 2y \in [2, b - 3].$$

El régimen j es intermedio. El entero $t := 2$ es par y cumple $t \equiv -jM \pmod{b}$, porque $2^{m+k} \equiv 1 \pmod{b}$ y por tanto $-jM = -2yM \equiv 2^{m+1}M = 2 \cdot 2^{m+k} \equiv 2 \pmod{b}$; además $t \equiv 2 \pmod{2^{e+2}}$; por la Proposición 25 es el corte de un exponente del régimen j . Como $\iota(1) = y \leq j$, el impar $r = 1$ no cumple $\iota(r) > j$, así que $\rho_j \neq 1$, y como ρ_j es impar, $\rho_j \geq 3 > t$. Por el Teorema 23, ese exponente tiene $\Delta_n = 1$. $\square$

Observación 27. El Teorema 26 admite una lectura sencilla: hay casos frontera si y solo si alguna potencia de 2 cae, módulo b , en la franja $[h + 2, b - 1]$ de la mitad superior. Las potencias $1, 2, 4, \dots, 2^m$ menores que b evitan esa franja solo cuando la mayor de ellas es exactamente $h + 1$, y

$$2^m = h + 1 \iff 2^m = \frac{b + 1}{2} \iff b = 2^{m+1} - 1,$$

es decir, cuando b es un primo de Mersenne. La base 3, única base sin casos frontera en los Escritos 1 y 2, resulta ser el primer miembro de esa familia.

Observación 28 (Casos frontera observados). Por ejemplo, para $b = 5$ los casos frontera aparecen en el régimen central para $k = 5, 6, 9, 10$ y no para $k = 7, 8, 11$, reflejando el periodo $\text{ord}_5(2) = 4$ de la Proposición 25. Los de $k = 6$ y $k = 10$ son los del Teorema 26(b), con $2^m = 4$ y $k \equiv -2 \pmod{4}$; los de $k = 5$ y $k = 9$ están en el borde superior. Numéricamente, entre los primos $5 \leq b < 140$ los únicos sin casos frontera son 7, 31 y 127, y también 8191 carece de ellos, como predice el teorema.

8. Observaciones finales

Observación 29. Para $b = 3$, los resultados de esta nota reproducen los del Escrito 2: tres regímenes, oscilación 2 solo en el central, el invariante $4J_{k-2}$ y la ausencia de casos frontera. Lo que en base 3 parecía una coincidencia (que el número de clases intermedias no dependa de n) resulta ser una propiedad exclusiva del régimen central, que para $b = 3$ es el único régimen intermedio.

Observación 30. La generalización planteada en el Problema final del Escrito 2 queda resuelta por los Teoremas 9 y 14: la relación de $N_{b,k}$ con el lema de Gauss se traduce en una combinación de sumas de Dedekind.

Observación 31. La Proposición 25 vale para toda base prima impar, con el módulo 2^{e+2} ; la clase $b \equiv 7 \pmod{8}$ es la que contiene a todos los primos de Mersenne mayores que 3.

Referencias

- [1] L. A. Goldberg, *An elementary proof of the Petersson–Knopp theorem on Dedekind sums*, J. Number Theory **12** (1980), no. 4, 541–542.
- [2] M. I. Knopp, *Hecke operators and an identity for the Dedekind sums*, J. Number Theory **12** (1980), no. 1, 2–9.
- [3] M. Majure, *Algebraic properties of the values of newform Dedekind sums*, arXiv:2208.13060, 2022.
- [4] C. Meyer, *Über einige Anwendungen Dedekindscher Summen*, J. Reine Angew. Math. **198** (1957), 143–203.
- [5] H. Rademacher y E. Grosswald, *Dedekind Sums*, The Carus Mathematical Monographs, No. 16, Mathematical Association of America, Washington, D.C., 1972.
- [6] E. Tsukerman, *Equality of Dedekind sums mod $\mathbb{Z}$, $2\mathbb{Z}$ and $4\mathbb{Z}$* , arXiv:1408.3225.

A. Código de comprobación

Control independiente, no necesario para las demostraciones. Contrasta el Lema 3 con la definición por enumeración directa para bases y exponentes pequeños; comprueba $\Delta_n \leq 2$, el Teorema 9 y el Teorema 23 para $b \in \{3, 5, 7, 11, 13\}$ y $k \in \{6, 7, 8\}$, los Teoremas 14 y 21 (incluido el caso de igualdad) para esas bases y $6 \leq k \leq 11$, y el Teorema 26 para $b \in \{3, 5, 7, 11, 13, 17, 31\}$ recorriendo un periodo completo de k .

```
def m_def(n, r, M, b):
    return sum(1 for E in range(1, b**n) if E % b and
               ((E if E % 2 else E + b**n) - r) % M == 0)

def c(n, r, M, b):
```

```

Q, R = divmod(2 * b**n, b * M)
return sum(1 for i in range(b) if (r + i*M) % b and r + i*M < R)

def m(n, r, M, b):
    return (b - 1) * (2 * b**n // (b * M)) + c(n, r, M, b)

for b in (3, 5, 7):
    for n in range(1, 6):
        assert all(m_def(n, r, 64, b) == m(n, r, 64, b)
                    for r in range(1, 64, 2))

for b in (3, 5, 7, 11, 13):
    h = (b - 1) // 2
    for k in (6, 7, 8):
        M = 2**k; Mi = pow(M, -1, b)
        iota = lambda r: (-r * Mi) % b
        N = sum(1 for r in range(1, M // 4, 2) if iota(r) <= h)
        P = 1
        while pow(b, P, M // 2) != 1: P += 1
        for n in range(1, P + 1):
            u = pow(b, n - 1, M // 2); j = 2*b*u // M; t = 2*b*u - j*M
            v = [c(n, r, M, b) for r in range(1, M, 2)]
            assert max(v) - min(v) <= 2
            if j == h:
                assert v.count(h) == 4 * N
            if 1 <= j <= b - 2:
                rho = min(r for r in range(1, M, 2) if iota(r) > j)
                Rj = max(r for r in range(1, M, 2) if iota(r) <= j - 1)
                pred = 1 if (t <= rho or t > Rj) else 2
                assert max(v) - min(v) == pred
from fractions import Fraction as Fr
def saw(x):
    if x.denominator == 1: return Fr(0)
    return x - (x.numerator // x.denominator) - Fr(1, 2)
def s(a, q):
    return sum(saw(Fr(j, q)) * saw(Fr(a * j, q)) for j in range(1, q))
for b in (3, 5, 7, 11, 13):
    for k in range(6, 12):
        M = 2**k; h = (b - 1) // 2; Mi = pow(M, -1, b)
        N = sum(1 for r in range(1, M // 4, 2) if (-r * Mi) % b <= h)
        d = 4 * (3 * s(2**(k-1) % b, b) - 2 * s(2**k % b, b)
                - s(2**(k-2) % b, b))
        assert 4 * N == Fr((b + 1) * M, 4 * b) + d
        assert abs(d) <= Fr(b * b - 1, 2 * b)
        extremo = abs(d) == Fr(b * b - 1, 2 * b)
        assert extremo == (pow(2, k-1, b) in (1, b-1))
def frontera(b, k):
    # hay algun caso frontera para este k?
    M = 2**k; Mi = pow(M, -1, b); io = lambda r: (-r * Mi) % b
    P = 1
    while pow(b, P, M // 2) != 1: P += 1
    for n in range(P):

```

```

    u = pow(b, n, M // 2); j = 2 * b * u // M; t = 2 * b * u - j * M
    if 1 <= j <= b - 2:
        rho = min(r for r in range(1, M, 2) if io(r) > j)
        Rj = max(r for r in range(1, M, 2) if io(r) <= j - 1)
        if t <= rho or t > Rj: return True
    return False
for b in (3, 5, 7, 11, 13, 17, 31):
    o = 1
    while pow(2, o, b) != 1: o += 1
    k0 = 4
    while 2**k0 < 4 * b: k0 += 1
    hay = any(frontera(b, k) for k in range(k0, k0 + o))
    mersenne = ((b + 1) & b) == 0          # b = 2^p - 1
    assert hay == (not mersenne)
print("OK")

```