CARACTERES SIMULTANEOS DE DIVISIBILIDAD POR GRUPOS DE NUMEROS PRIMOS

por

JOSÉ ANTONIO ESTRUGO

I. Justificación.

La teoría de la divisibilidad por restos potenciales se limita a indicarnos si un número dado, N, es múltiplo del número primo p que se ensaya; pero una vez obtenida esta certeza, los cálculos realizados no sirven para la descomposición factorial de aquél, debiendo, pues, de procederse a la división de N entre p, si se quiere continuar la operación.

Así, por ejemplo, si queremos saber si un número es divisible por 11, siguiendo la regla de restos potenciales, tenemos que sumar sus cifras de lugar par, luego las de lugar impar, restarlas, y si la diferencia es cero ó 11, el número dado lo es. Pero los cálculos realizados, una vez conseguido nuestro objeto, en nada nos facilitan la obtención del cociente por dicho número, que tendrá que ser obtenido por la regla ordinaria.

El presente trabajo, basado en el desarrollo algebraico de una generalización de las reglas de Zbikowski para el número 7, y otra de Folie para el 19, nos permitirá facilitar en gran manera la descomposición factorial (*).

II. Definiciones.

Desde nuestro punto de vista, un grupo de m números primos $(p_1, p_2, \ldots, p_m)$, tiene carácter simultáneo de divisibilidad, siempre que mediante el único resultado obtenido efectuando con un número cualquiera N un conjunto uniforme de operaciones, podamos determinar si dicho número es divisible por algún p_i, por varios, por todos o por ninguno de los que componen el grupo.

La operación a realizar es sumar algebraicamente a las decenas del número N el resultado de multiplicar sus unidades por el *carácter dis-*

(*) Algunos de los teoremas que siguen fueron dados a conocer en nuestro trabajo «Caracteres homogéneos de divisibilidad por grupos de números primos». Anales del Instituto de Actuarios Españoles (1945).

tintivo del grupo, observando si el número resultante —prescindiendo de las unidades de N— es múltiplo de uno, de varios, de todos o de ninguno, en cuyo caso podemos afirmar que el número N es multiplo de ése, de varios, de todos o de ninguno, respectivamente.

En el caso de que el nuevo número formado N_1 tenga gran valor absoluto, podemos operar con él en idéntica forma, y así sucesivamente hasta encontrar otro cuya determinación resulte inmediata.

Denominaremos *capacidad* de un grupo a la potencia en que figuren los números primos que le componen. Así, el grupo $(3^2, 7^2)$ tiene capacidad **2**, teniendo esta misma su carácter distintivo. Si las potencias son las primeras, suprimiremos esta calificación.

III. Casos especiales.

Aunque no encuadrados en la regla general dada, constituyen, sin embargo, caracteres simultáneos de divisibilidad:

a) El grupo de capacidad $n(2^n, 5^n)$, pues basta que las n primeras cifras, a contar de la derecha del número N, sean múltiplos de 2^n, de 5^n, o sean ceros, para saber que el número es divisible por 2^n, por 5^n, o por los dos que componen el grupo.

Este caso trivial no lo consideraremos en lo que sigue, dada la fácil eliminación de dichos factores, además de hacer imposible su inclusión la condición necesaria de que hablaremos seguidamente.

b) El grupo (3,9), pues la *suma* de los valores absolutos de las cifras del número dado nos permite determinar inmediatamente si el número es múltiplo de 3, de 9 o de ninguno.

IV. Condición necesaria y suficiente.

Para que un grupo $(p_1, p_2, \ldots, p_m)$ de números primos tenga carácter distintivo es necesario y suficiente que el producto de dichos números sea de la forma

$$\overset{m}{\underset{1}{\pi}} p_i = 10t + 1, \text{ o bien } \overset{m}{\underset{1}{\pi}} p_i = 10t - 1$$

En estos casos, el carácter distintivo, que expresaremos respectivamente por c y c', quedan definidos por las igualdades

$$c = -\frac{\overset{m}{\underset{1}{\pi}} p_i - 1}{10} = -t, \quad \text{y} \quad c' = \frac{\overset{m}{\underset{1}{\pi}} p_i + 1}{10} = t;$$

teniendo el primero carácter sustractivo y el segundo carácter aditivo. En lo que sigue, al carácter sustractivo le denominaremos $(+1)$ y al aditivo (-1), de acuerdo con que el producto de los números primos termine en 1 o en 9, respectivamente.

Dado un grupo de números primos que no cumplan la condición necesaria, basta introducir dentro del mismo otro número primo del menor valor absoluto, elegido convenientemente para que pueda aplicársele la presente teoría. En general, es suficiente introducir el 3 (..). Otra forma sería aumentar la capacidad en un grado, pero tiene el inconveniente de producir caracteres distintivos más elevados en valor absoluto.

Ejemplos:

1. Calcular el carácter distintivo del grupo (3,7).

Como el producto es 21, pertenece al carácter sustractivo (+ 1) y su valor será:

$$c = -\frac{21 - 1}{10} = -2 \quad .$$

2. Determinar el carácter distintivo del grupo (3,13).

Por ser el producto 39, pertenece al carácter (— 1), siendo su valor

$$c' = \frac{39 + 1}{10} = +4$$

3. Interesa determinar el carácter distintivo mínimo del grupo (7,9).

Como el producto es 63, no cumple la condición necesaria, bastando considerar este otro (3, 7, 9), siendo ahora $\pi p_i = 189$ resulta $c' = 19$.

Si eleváramos la capacidad en un grado, tendríamos el grupo (7^2, 9^2), en donde siendo $\pi p_i = 3969$, se obtendría para $c' = 397$, como puede observarse de mayor valor absoluto que introduciendo el factor 3 dentro del grupo.

V. Demostraciones.

El algoritmo definido en el apartado II, tiene la justificación matemática que sigue:

a) *Carácter* (+ 1).

Sea N el número dado, cuyas unidades representaremos por u_o. Siendo el carácter distintivo del grupo (p_1, p_2 ..., p_m)

$$c = -\frac{\overset{m}{\underset{1}{\pi}} p_i - 1}{10}$$

la operación a efectuar da lugar al nuevo número (teniendo en cuenta que prescindimos de las unidades de N):

$$N_1 = \frac{N - u_o}{10} - \frac{\overset{m}{\underset{1}{\pi}} p_i - 1}{10} u_o = \frac{N - u_o \overset{m}{\underset{1}{\pi}} p_i}{10}$$

(..) En efecto, como el producto de números primos ($\neq$ de 2 y 5) y no incluídos en la condición necesaria presentan la forma $10t + 3$ ó $10t + 7$, se tiene respectivamente $(10t + 3)3 = 30t + 9$ que da un carácter (— 1) y $(10t + 7)3 = 30t + 21 = 10(3t + 2) + 1$, resultando un carácter (+ 1).

y de aquí:

$$N = 10N_1 + u_o \overset{m}{\underset{1}{\pi}} p_i \quad ; \quad (p_i \neq \text{ de } 2 \text{ y } 5) \qquad (1)$$

luego si N_1 es múltiplo de p_i, también lo tendrá que ser N. En general, si N_1 es múltiplo de p_1. p_2 ..., lo será igualmente N de dichos números En el caso de que $N_1 = 0$, entonces N es múltiplo de todos los primos que componen el grupo.

Si N_1 es de gran valor absoluto, podemos efectuar con él idénticas operaciones, obteniéndose un

$$N_2 = \frac{N_1 - u_1}{10} - \frac{\overset{m}{\underset{1}{\pi}} p_i - 1}{10} u_1 = \frac{N_1 - u_1 \overset{m}{\underset{1}{\pi}} p_i}{10}$$

de donde

$$N_1 = 10N_2 + u_1 \overset{m}{\underset{1}{\pi}} p_i \qquad (2)$$

pudiéndose aplicar el mismo razonamiento: Si N_2 es múltiplo de p_1, p_2 ..., lo es N_1, y al serlo éste, en virtud de (1), también lo es N.

Sustituyendo el valor de N_1 en (1) podemos establecer la igualdad:

$$N = 10^2 \cdot N_2 + (10u_1 + u_o) \overset{m}{\underset{1}{\pi}} p_i \qquad (3)$$

habiendo denominado u_1 a las unidades de N_1.

En general, si esta operación se reitera k veces, tendríamos:

$$N = 10^k N_k + (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10u_1 + u_a) \overset{m}{\underset{1}{\pi}} p_i \qquad (4)$$

igualdad esta última que nos será muy útil más adelante.

La operación se dará por terminada al obtener un N_k que cumpla la limitación $O \leqslant N_k < \overset{m}{\pi} p_i$.

b) *Carácter* (— 1).

En este caso, tendremos sucesivamente

$$N_1 = \frac{N - u_o}{10} + \frac{\overset{m}{\underset{1}{\pi}} p_i + 1}{10} u_o = \frac{N + u_o \overset{m}{\underset{1}{\pi}} p_i}{10}$$

y de aquí:

$$N = 10N_1 - u_o \overset{m}{\underset{1}{\pi}} p_i \qquad (5$$

Continuando el algoritmo definido, ahora con N_1,

$$N_2 = \frac{N_1 - u_1}{10} + \frac{\overset{m}{\underset{1}{\pi}} p_i + 1}{10} u_1 = \frac{N_1 + u_1 \overset{m}{\underset{1}{\pi}} p_i}{10}$$

de donde

$$N_1 = 10N_2 - u_1 \overset{m}{\underset{1}{\pi}} p_i$$

Sustituyendo este valor en (5),

$$N = 10^2 N_2 - (10u_1 + u_o) \overset{m}{\underset{1}{\pi}} p_i$$

Y reiterando k veces esta operación obtendríamos por último

$$N = 10^k N_k - (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \dots + 10u_1 + u_o) \overset{m}{\underset{1}{\pi}} p_i \quad (7)$$

siendo válidos los razonamientos anteriores y muy interesante para nuestro estudio la igualdad (7) obtenida. En este caso, N será múltiplo de todos los del grupo si $N_k = \overset{m}{\underset{1}{\pi}} p_i$.

La operación reiterada concluye al obtenerse la limitación

$$o < N_k \leqslant \overset{m}{\underset{1}{\pi}} p_i$$

VI. Ejemplos de aplicación.

1. Determinar si el número 33726 es divisible por alguno del grupo (3, 7, 11).

Como el producto es 231, su carácter es $(+1)$, siendo $c = -23$ y de acuerdo con el algoritmo definido, operaremos como sigue:

$$\begin{array}{rl}
3\ 3\ 7\ 2(6 & \\
-\ 1\ 3\ 8 & = -23 \cdot 6 \\
\hline
3\ 2\ 3(4 & \\
-\ 9\ 2 & = -23 \cdot 4 \\
\hline
2\ 3(1 & \\
-\ 2\ 3 & = -23 \cdot 1 \\
\hline
0 &
\end{array}$$

por tanto, podemos afirmar que 33726 es múltiplo de los tres números que componen el grupo.

2. Hallar por qué número del grupo (13, 17) es divisible 2584. El producto es 221, luego es carácter $(+1)$ siendo $c = -22$

$$\begin{array}{r}
2\ 5\ 8(4 \\
-\ 8\ 8 \\
\hline
1\ 7(0
\end{array}$$

por tanto, 2584 es múltiplo de 17, no siéndolo de 13.

3. Para saber si 79365 es divisible por el grupo (C 3, 11, 13), como $\pi = 429$, será $c' = 43$, basta efectuar las operaciones que siguen:

$$\begin{array}{cccccl}
 & 7 & 9 & 3 & 6 & (5 \\
 & & 2 & 1 & 5 & \\
\cline{2-5}
 & 8 & 1 & 5 & (1 & \\
 & & 4 & 3 & & \\
\cline{2-4}
 & 8 & 5 & (8 & & \\
3 & 4 & 4 & & & \\
\cline{1-3}
4 & 2 & 9 & \multicolumn{3}{l}{= 3 \cdot 11 \cdot 13}
\end{array}$$

luego es divisible por el grupo.

VII. Grupos especiales.

Se nota la necesidad de sistematizar la elección de los grupos de tal manera que resulte sencilla y rápida la investigación de los divisores por los primeros números primos.

Supuesta la eliminación previa de los factores 2 y 5 hasta agotar su capacidad, proponemos la aplicación sistemática de los siguientes grupos:

$$(3, 7, 11) \text{ con } c = -23$$

$$(13, 17) \text{ con } c = -22$$

$$(19, 29) \text{ con } c = -55$$

$$(23, 37) \text{ con } c = -85$$

$$(31, 41) \text{ con } c = -127$$

y para números de gran valor absoluto se puede comenzar por aplicar directamente el grupo

$$(3, 7, 11, 13, 17) \text{ con } c = -5105$$

VIII. Caso de un solo número primo.

Puede ser interesante algunas veces determinar si un número N es divisible por otro p, y exclusivamente por él.

Si p cumple la condición necesaria, formaremos el grupo $(p,1)$ y se aplica el algoritmo definido anteriormente. En caso contrario, se toma el $(p,3)$ y se opera de acuerdo con el carácter distintivo que resulte.

Casos particulares muy notables son los siguientes:

a) El grupo (9,1).

Al ser $c' = 1$, nos indica que a las decenas de N habrá que sumarle las unidades, efectuando idéntica operación para los números que sucesivamente se formen, dando lugar a una regla análoga a la deducida por restos potenciales.

Así, para determinar si 4536 es múltiplo de 9, según nuestro algoritmo sería

$$\begin{array}{llll}
4 & 5 & 3 & (6 \\
 & & 6 & \\
\hline
4 & 5 & (9 & \\
 & 9 & & \\
\hline
5 & (4 & & \\
4 & & & \\
\hline
9 & & &
\end{array}$$

b) *El grupo* (11,1).

Por pertenecer al carácter (+ 1) y ser $c = -1$, habrá que restar a las decenas del número dado sus unidades, y así sucesivamente, coincidiendo con la regla para este número de los restos potenciales. En efecto, suponiendo para fijar ideas que $N = 10^2u_2 + 10u_1 + u_0$, la aplicación del algoritmo para 11 sería

$$N_1 = \frac{10^2u_2 + 10u_1 + u_0 - 11u_0}{10} = 10u_2 + u_1 - u_0$$

$$N_2 = \frac{10u_2 + u_1 - u_0 - 11(u_1 - u_0)}{10} = u_2 - u_1 + u_0$$

confirmándonos lo indicado.

Si el número p cumple la condición necesaria, pueden establecerse criterios de divisibilidad para un solo número.

Así, por ejemplo, si se trata del número 31 ($c = -3$) podríamos enunciar el siguiente teorema: «Un número será divisible por 31 si el resultado de restar a sus decenas tres veces sus unidades es múltiplo de 31 o cero.»

Para el número 29, en que $c' = 3$ se obtendría: «Un número será divisible por 29 si el resultado de sumar a sus decenas tres veces sus unidades es $\dot{29}$.»

IX. El número diagonal: definición.

La idea de recoger el resultado de la aplicación reiterada del algoritmo básico de esta teoría nos ha llevado a plantear las igualdades (4) y (7), que nos permitirán obtener el cociente, una vez comprobado que el número N es divisible por el grupo de números primos dado.

A estos efectos daremos el nombre de «*número diagonal*» *y lo representaremos por* D, *al formado por las unidades sucesivas despreciadas al aplicar el algoritmo inicial y colocadas sus cifras en el orden inverso a como han sido obtenidas.*

Así, en el ejemplo 1 de VI, en el que nos proponíamos averiguar si el número 33726 era divisible por el grupo (3, 7, 11), al aplicar el algoritmo inicial se obtuvo, siendo $c = -23$:

$$\begin{array}{ccccl}
3 & 3 & 7 & 2 & (6 \\
 & 1 & 3 & 8 & \\
\hline
3 & 2 & 3 & (4 & \\
 & 9 & 2 & & \\
\hline
2 & 3 & (1 & & \\
2 & 3 & & & \\
\hline
 & 0 & & &
\end{array}$$

De acuerdo con la definición de número diagonal dada, se tendrá $D = 146$.

En el ejemplo 3 podemos observar que $D = 815$.

X. Teoremas relativos al número diagonal.

Estableceremos a continuación dos teoremas sobre el número diagonal de importancia capital para nuestra teoría, teniendo en cuenta si el carácter distintivo es sustractivo o aditivo.

a) *Carácter* $(+1)$.

Si al aplicar el algoritmo definido a un número N para determinar su divisibilidad por un grupo de números primos $(p_1, p_2, \ldots, p_m)$ *se obtiene un resto cero, el número dado N es igual al producto de los primos que componen el grupo por el número diagonal que resulte; es decir, que* $N = p_1 \cdot p_2 \ldots p_m \cdot D$.

Así, en el ejemplo 1 de VI, que hemos reproducido anteriormente, llegábamos a la evidencia de que 33726 era múltiplo del grupo (3, 7, 11). En virtud de este teorema, conseguimos, además, la descomposición factorial siguiente, habida cuenta de que $D = 146$.

$$33726 = 3 \cdot 7 \cdot 11 \cdot 146 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 73$$

Si el número D no fuera de fácil descomposición, se aplicaría el proceso sistemático indicado en VII.

La demostración de este teorema parte de la igualdad (4):

$$N = 10^k N_k + (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0) \overset{m}{\underset{1}{\pi}} p_i$$

pues haciendo en ella $N_k = 0$, se tiene

$$N = (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0) \overset{m}{\underset{1}{\pi}} p_i \qquad (8)$$

y como lo encerrado entre paréntesis es, según definición, D, tendremos:

$$N = \overset{m}{\underset{1}{\pi}} p_i \cdot D = p_1 \cdot p_2 \cdot p_3 \cdot p_m \cdot D$$

que corrobora nuestro aserto.

b) *Carácter* (—1).

Obteniendo un resto igual al producto de los números que componen el grupo, el número N *es igual al producto de dichos números primos multiplicados por el complemento del número diagonal, que designaremos por* $\overline{D}$; *es decir,* $N = p_1 \cdot p_2 \ldots p_m \cdot \overline{D}$.

En el ejemplo 3 de VI tendremos, haciendo aplicación de lo indicado

$$79365 = 3 \cdot 11 \cdot 13 \cdot \overline{815} = 3 \cdot 11 \cdot 13 \cdot 185$$

Para evidenciar el teorema basta en (7)

$$N = 10^k N_k - (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0) \overset{m}{\underset{1}{\pi}} p_i$$

hacer $N_k = p_1 \cdot p_2 \ldots p_m = \overset{m}{\underset{1}{\pi}} p_i$, con lo cual

$$N = 10^k \overset{m}{\underset{1}{\pi}} p_i - (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0) \overset{m}{\underset{1}{\pi}} p_i =$$

$$= [10^k - (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0)] \overset{m}{\underset{1}{\pi}} p_i \qquad (9)$$

y como lo encerrado entre corchetes es el complemento del número diagonal, $\overline{D}$, tendremos finalmente, como deseábamos:

$$N = p_1 \cdot p_2 \cdot p_3 \ldots p_m \cdot \overline{D}$$

Corolario: Si el número diagonal o su complemento fueran iguales al producto de los números primos, el número N es un cuadrado perfecto, teniendo capacidad 2.

XI. Utilización más extensa del número diagonal.

Es evidente que los teoremas anteriores recogen ambos el caso ideal de que el número dado sea múltiplo de *todos* los que componen el grupo. Es posible, sin embargo, obtener un mayor provecho de las igualdades (4) y (7), bastando que el número sea múltiplo de *uno solo* de los componentes para que pueda ser hallado su cociente.

En efecto, supongamos para fijar ideas que N sea múltiplo de p_1 y de p_2; en este caso de la (4):

$$N = 10^k N_k + (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \ldots + 10 u_1 + u_0) \overset{m}{\underset{1}{\pi}} p_i$$

haciendo $N_k = p_1 \cdot p_2 \cdot c$, nos queda

$$N = 10^k p_1 \cdot p_2 \cdot c + (10^{k-1} u_{k-1} + 10^{k-2} u_{k-2} + \dots + 10 u_1 + u_0) p_1 \cdot p_2 \overset{m}{\underset{3}{\pi}} p_i$$

y de aquí

$$N = p_1 \cdot p_2 \left[10^k c + D \overset{m}{\underset{3}{\pi}} p_i \right] \tag{10}$$

fácil de traducir a regla.

Caso particular notable de (10) lo constituye la investigación de un grupo de dos factores p_1 y p_2, pues suponiendo que N sea múltiplo del primero, tendremos

$$N = p_1 \left[10^k c + D p_2 \right] \tag{11}$$

de cómodo cálculo.

Si el carácter distintivo fuera (—1), el equivalente de (10) resultaría ser

$$N = p_1 \cdot p_2 \left[10^k c - D \overset{m}{\underset{3}{\pi}} p_i \right] \tag{12}$$

y para el caso de investigación de dos factores

$$N = p_1 [10^k c - D \cdot p_2] \tag{13}$$

Al objeto de resaltar su utilidad, resolvamos unos ejemplos sencillos:

1. Descomponer en sus factores primos el número 931.

Consideraremos el grupo (3, 7), en que $c = -2$, tendremos

$$\begin{array}{rrl} 9 & 3 & (1 \\ & -2 & \\ \hline & 9 & (1 \\ -2 & & \\ \hline 7 & & \end{array}$$

El número es múltiplo de 7 solamente, y siendo de acuerdo con (11), $c = 1$ y $D = 11$:

$$931 = 7(10^2 + 3 \cdot 11) = 7 \cdot 133$$

2. Determinar la divisibilidad de 27807 por el grupo (13, 17).

Se tiene $c = -22$; luego

$$\begin{array}{cccl} 2 & 7 & 8 & 0 \; (7 \\ & 1 & 5 & 4 \\ \hline 2 & 6 & 2 & (6 \qquad D = 67 \\ 1 & 3 & 2 & \\ \hline 1 & 3 & 0 & = 13 \cdot 10 \end{array}$$

el número dado es, pues, múltiplo de 13. Si se deseara hallar el cociente para seguir la descomposición factorial, tendríamos aplicando (11):

$$27807 = 13(10^2 \cdot 10 + 67 \cdot 17) = 13 \cdot 2139$$

3. A continuación damos todos los cálculos precisos para determinar la divisibilidad reiterada del grupo (3, 7).

Sea el número 33957. Como se sabe, $c = -2$; por tanto,

$$\begin{array}{lllll} 3 & 3 & 9 & 5 & (7 \\ & & 1 & 4 & \\ \hline 3 & 3 & 8 & (1 & \\ & & 2 & & \\ \hline 3 & 3 & (6 & & \\ 1 & 2 & & & \\ \hline 2 & (1 & & & \\ 2 & & & & \\ \hline 0 & & & & \end{array}$$

$$\begin{array}{llll} 1 & 6 & 1 & (7 \\ - & 1 & 4 & \\ \hline 1 & 4 & (7 & \\ 1 & 4 & & \\ \hline 0 & & & \end{array}$$

$$33957 = 3^2 \cdot 7^2 \cdot 77 = 3^2 \cdot 7^3 \cdot 11$$