Revista

de

Matemáticas Elementales

VOLUMEN III. FASCICULO 5

Tarifa Postal Reducida. — Licencia Nº 1993 del Ministerio de Correos y Telégrafos.

SOBRE LOS CRITERIOS DE DIVISIBILIDAD I.

Por Carlo Federici Casa

0) Sean a y b dos (números) naturales (Nt) y tales que $a > b$. Para establecer la verdad de la proposición *"a es divisible por b" basta* ejecutar la división de a por b: si la división indicada tiene residuo nulo la proposición es verdadera, de otra manera es falsa.

Se dijo *"basta* ejecutar la división de a por b", pero no se ha afirmado que esto se necesite.

Ahora bien, pueden presentarse casos en que ejecutar la división se presente como una fatiga inútil, por ejemplo, cuando lo que interesa es la verdad o falsedad de dicha proposición y no el conocimiento del cuociente de la división de a por b, y entonces se buscará todo medio para evitar semejante fatiga. Se deberá, entonces, buscar condiciones necesarias y suficientes que permitan establecer la verdad o falsedad de la proposición *"a es divisible por b"* sin tener que ejecutar la división y, naturalmente, con la mayor sencillez.

Los enunciados de estas condiciones (¡necesarias y suficientes!) se llaman *"criterios o caracteres de divisibilidad"*.

1) Se puede afirmar que el más antiguo criterio de divisibilidad, conocido por nosotros, es el citado en el Talmud.

Pero una búsqueda verdadera y amplia de criterios sólo puede hacerse remontar a Pascal, quien enuncia un criterio al cual se pueden reducir muchos de uso más común, y esta búsqueda prosigue con D'Alembert, Gergonne,...

Mas quien ojee una lista de criterios no deja de extrañarse al advertir el hecho de que ellos, si bien enunciados por autores dife-

rentes y en diferentes épocas pero con un fin común, se presentan desligados y esto no obstante se sepa que todos se apoyan sobre una base única, aunque demasiado amplia para que pueda evidenciar, si es posible, los ligámenes comunes.

Además uno se sorprende de que exista un verdadero florecimiento de criterios de divisibilidad, más o menos generales, cuando en la práctica sólo se conocen los muy particulares relativos a $b = 2^d, 5^c, 3, 9, 11$ que se deducen del criterio de PASCAL ya nombrado.

Es bastante natural, entonces, que se quiera encontrar un criterio al cual puedan reducirse todos los demás como simples casos particulares, criterio que sí podrá llamarse general y que servirá para poner en evidencia los nexos muy estrechos que existen entre criterio y criterio.

2) Para desarrollar esta búsqueda es conveniente introducir el concepto de "congruencia" que se encuentra, por primera vez, en la monumental obra del matemático alemán C. F. GAUSS (1777-1855) "Disquisitiones Arithmeticae", Leipzig, 1801.

"Dos (números) enteros (*Et*) *a,b* se llaman congruentes entre sí y con respecto al módulo *m*, siendo *m* un Et diferente de cero, si la diferencia *a-b* es un múltiplo de *m*, es decir, si el módulo (o valor absoluto) de *a-b* es divisible por el módulo de *m*". Para indicar que "*a* es congruente a *b*, módulo *m*" sería conveniente emplear la escritura "$a \overset{m}{=} b$", llamando toda escritura de ese tipo una *congruencia* (aritmética) pero, teniendo en cuenta las inevitables dificultades tipográficas, adoptaremos la escritura "$a = b \ md \ m$".

Tenemos por lo tanto la definición fundamental
2.0) "Si *a,b,m* son *Et* y $m \neq 0$, entonces, decir: $a = b \ md \ m$, es lo mismo que decir: existe un k tal que k es *Et*, et, $a - b = k.\ m$". (Usaremos en este artículo la palabra "et" en vez de "y" por ser costumbre en la lógica matemática y para evitar posibles confusiones).

De la definición 2.0 de congruencia se deducen fácilmente los siguientes teoremas

2.1) "$a = a \ md \ m$"

2.2) "$a = b \ md \ m$, implica que, $b = a \ md \ m$"

2.3) "$a = b \ md \ m$, et, $b = c \ md \ m$,, implica que, $a = c \ md \ m$"

que muestran que la congruencia goza de las propiedades de reflexividad, simetricidad y transitividad.

Por cumplir estas tres condiciones la "congruencia con respecto a un determinado módulo" pertenece a la clase de las relaciones ecualiformes o equivalencias, clase de relaciones fundamental tanto en matemática como en física y, en general, en teoría del conocimiento.

Veamos las demostraciones.

En primer lugar sabemos que $a - a = 0.\ m$ de manera que resulta $a \underline{=} a\ md\ m$.

En segundo lugar de $a \underline{=} b\ md\ m$, se deduce que existe un k tal que $a - b = k.\ m$ y por lo tanto que $b - a = (-k).\ m$ así que $b \underline{=} a\ md\ m$.

En tercer lugar de $a \underline{=} b\ md\ m$, et, $b \underline{=} c\ md\ m$ se deduce que existen k y k' tales que $a - b = k.m$, et, $b - c = k'.m$, de donde sumando miembro a miembro se deduce que $a - c = (k + k').\ m$, es decir, que $a \underline{=} c\ md\ m$.

Es igualmente fácil demostrar que

0) "$a \underline{=} b\ md\ m$, et, $a' \underline{=} b'\ md\ m$,, implica que, $a + a' \underline{=} (b + b')\ md\ m$".

En efecto, de $a \underline{=} b\ md\ m$, et, $a' \underline{=} b'\ md\ m$ se deduce que existen k y k' tales que $a - b = k.\ m$, et, $a' - b' = k'.\ m$ de donde sumando miembro a miembro se deduce que $(a + a') - (b + b') = (k + k').\ m$ es decir que $a + a' \underline{=} b + b'\ md\ m$.

De este teorema y de la propiedad reflexiva de la congruencia se deduce que

"$a \underline{=} b\ md\ m$, implica que, $a + c \underline{=} b + c\ md\ m$"

1) "$a \underline{=} b\ md\ m$, et, $a' \underline{=} b'\ md\ m$,, implica que

$a - a' \underline{=} b - b'\ md\ m$".

En efecto, de $a \underline{=} b\ md\ m$, et, $a' \underline{=} b'\ md\ m$ se deduce que existen k y k' tales que $a - b = k.\ m$, et, $a' - b' = k'.\ m$, de donde,

restando miembro a miembro, se deduce que $(a - a') - (b - b') = (k - k')$. m es decir que $a - a' \equiv b - b' \ md \ m$.

De este teorema y de la propiedad reflexiva de la congruencia se deduce que

"$a \equiv b \ md \ m$, implica que, $a - c \equiv b - c \ md \ m$"

2) "$a \equiv b \ md \ m$, et, $a' \equiv b' \ md \ m'$„ implica que,

$aa' \equiv bb' \ md \ m$".

En efecto, de $a \equiv b \ md \ m$, et, $a' \equiv b' \ md \ m$ se deduce que existen k y k' tales que $a - b = k$. m, et, $a' - b' = k'$. m es decir que $a = k$. $m + b$, et, $a' = k'$. $m + b'$ de donde, multiplicando miembro a miembro, se deduce que $aa' = (kb' + k'b + mkk')$ $m + bb'$ o también que $aa' - bb' = (kb' + k'b + mkk')m$ es decir que $aa' \equiv bb' \ md \ m$.

De este teorema y de la propiedad reflexiva de la congruencia se deduce que

"$a \equiv b \ md \ m$, implica que, $a. c \equiv b. c \ md \ m$".

Como ejercicio demuestre el lector: "$a \equiv b \ md \ m$, et, $c \neq 0$„ implica que, $a.c \equiv b.c \ md \ m.c$".

3) "$a \equiv b \ md \ m$, et, $a' \equiv b' \ md \ m$, et, $a \equiv 0 \ md \ a'$, et, $b \equiv 0 \ md \ b'$, et, $dm \ (a', m) = dm \ (b', m) = 1$„ implica que $a/a' \equiv b/b' \ md \ m$, en donde $dm \ (x, y)$ designa el máximo común divisor de x e y".

En efecto, de $a \equiv 0 \ md \ a'$, et, $b \equiv 0 \ md \ b'$ se deduce que existen a'' y b'' tales que $a = a''. a'$, et, $b = b''. b'$, y de $a \equiv b \ md \ m$ se deduce que existe k tal que $a - b = k. m$ y, por lo tanto, que $a''. a' - b''. b' = k. m$. Además de $a' \equiv b' \ md \ m$ se deduce que existe k' tal que $a' - b' = k'. m$ es decir que $a' = b' + k' m$ y por lo tanto se tiene que $a'' (b' + k' m) - b''. b' = k. m$ de donde se deduce que $(a'' - b''). b' = (k - a'' k'). m$ es decir que $a'' - b'' = (k - a'' k'). m/b'$ y como $dm \ (b', m) = 1$ se deduce que $k - a'' k' \equiv 0 \ md \ b'$ así que $a'' - b'' = [(k - a'' k')/b']. m$ es decir que $a'' \equiv b'' \ md \ m$ de donde recordando el significado de a'' y b'' se deduce por fin que $a/a' \equiv b/b' \ md \ m$.

De este teorema y de la propiedad reflexiva de la congruencia se deduce que

"$a \equiv b \ md \ m$, et, $a \equiv 0 \ md \ c$, et, $b \equiv 0 \ md \ c$, et, $dm \ (c, m) = 1$,,

implica que, $a/c \equiv b/c \ md \ m$".

Vamos a demostrar también que

"$a.c \equiv b.c \ md \ m$, et, $d = dm \ (c, m)$,, implica que,

$a \equiv b \ md \ (m/d)$".

En efecto, de $ac \equiv bc \ md \ m$ se deduce que existe k tal que $ac - bc = k.m$ es decir que $a - b = k.m/c$ o también por ser d igual al $dm \ (c, m)$ se deduce que $a - b = k \ (m/d)/(c/d)$ y como m/d y c/d son primos entre sí se deduce que $a - b = [k/(c/d)].(m/d)$ es decir que $a \equiv b \ md \ (m/d)$.

Resulta también obvio que

"$a \equiv b \ md \ m$, et, $m \equiv 0 \ md \ n$,, implica que, $a \equiv b \ md \ n$".

Dejamos al lector la demostración.

4) "$a \equiv b \ md \ m$, implica que, $a^p \equiv b^p \ md \ m$" (en donde p es un Et no negativo).

En efecto, de $a \equiv b \ md \ m$ se deduce que existe un k tal que $a - b = k.m$ o también que $a = b + k.m$ y por lo tanto que $a^p = (b + k.m)^p$ de donde, recordando la fórmula [llamada erroneamente de Newton y que se encuentra en Chu Shi Ki (1303), Stifel (1544), Tartaglia (1556)...]

$$(a + b)^p = a^p + p\,a^{p-1}\,b + \ldots + p\,a\,b^{p-1} + b^p$$

se deduce que

$$a^p = b^p + p\,b^{p-1}\,k.m + \ldots + p\,b\,k^{p-1}\,m^{p-1} + k^p\,m^p$$

es decir que

$$a^p - b^p = (p\,b^{p-1} + \ldots + p\,b\,k^{p-2}\,m^{p-2} + k^{p-1}\,m^{p-1})\,k.m$$

y por lo tanto que $a^p \equiv b^p \ md \ m$.

De los teoremas que preceden, y más precisamente de 0) y 2) se deduce con facilidad que

"Si $c,d,\ldots$ son $Et_{,,}$ et$_{,,}$ $p,q,\ldots$ son Et no negativos$_{,,}$ et,

$$fn\, x = c\, x^{p} + d\, x^{q} + \ldots, \text{ et, } a \underline{=} b \ md \ m_{,,,}$$

entonces $fn\, a \underline{=} fn\, b \ md \ m$".

Dejamos al lector la demostración detallada.

Por fin queremos demostrar que

"$a \underline{=} b \ md \ m'$, et, $a \underline{=} b \ md \ m''$, et, $m = MM\ (m', m'')_{,,}$ implica que, $a \underline{=} b \ md \ m$" en donde $MM\ (x, y)$ designa el mínimo común múltiplo de x e y.

En efecto, de $m = MM\ (m', m'')$ se deduce que existen d' y d'' tales que $m = m'd'$, et, $m = m''d''$, et, $1 = dm\ (d', d'')$ y en virtud de esta última relación existen δ' y δ'' tales que (Véase Revista de Matemáticas Elementales Vol. 1, Fs. 4-5, pp. 76-77: *Números Primos,* por J. Horváth) $d'\,\delta' + d''\,\delta'' = 1$. Además, de $a \underline{=} b \ md \ m'$, et, $a \underline{=} b \ md \ m''$ se deduce que existen k' y k'' tales que $a - b = k'.\, m'$, et, $a - b = k''.\, m''$ es decir que $(a - b)\, d' = k'\, m'\, d' = k'.\, m$, et, $(a - b)\, d'' = k''\, m''\, d'' = k''\, m$ de donde, multiplicando la primera por δ' y la segunda por δ'' y sumando ordenadamente se deduce que $(a - b)\ (d'\,\delta' + d''\,\delta'') = (k'\,\delta' + k''\,\delta'')\ m$; recordando que $d'\,\delta' + d''\,\delta'' = 1$ se deduce que $a - b = (k'\,\delta' + + k''\,\delta'')\ m$ y por fin que $a \underline{=} b \ md \ m$.