DISQUISITIONES ARITHMETICAE.

Sección Primera

DE

LA CONGRUENCIA DE LOS NUMEROS EN GENERAL

Números congruentes, módulos, residuos y no residuos.

1.

Si un número a divide la diferencia de los números b y c, se dice que b y c *son congruentes según el módulo* a; si no lo son, se dice que son *incongruentes*; el número a se llama *módulo*. Ambos números b y c, en el primer caso, son llamados uno *residuo* del otro y, en el segundo caso, *no residuos*.

Tales nociones valen para todos los enteros, tanto positivos como negativos*), y no para las fracciones. Por ejemplo, -9 y $+16$ son congruentes según el módulo 5; -7 es un residuo de $+15$ según el módulo 11; pero no es un residuo según el módulo 3. Dado que cada número divide a cero, todo número puede considerarse congruente consigo mismo, según cualquier módulo.

2.

Todos los residuos de un número dado, a, según el módulo m están comprendidos en la fórmula $a + km$, donde k es un número entero indeterminado. Las proposiciones más fáciles, a las cuales haremos referencia más adelante, pueden demostrarse aquí sin dificultad alguna, y quienquiera podrá comprobar su veracidad con igual facilidad.

*) El módulo debe ser siempre tomado con el valor *absoluto*, a saber: sin ningún signo.

Señalaré la congruencia de los números mediante este símbolo '$\equiv$' y, cuando sea necesario, pondré el módulo entre paréntesis; por ejemplo, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$*).

3.

TEOREMA. *Dados m números enteros sucesivos*

$$a,\ a+1,\ a+2,\ \ldots a+m-1,$$

y dado otro entero A, uno y sólo uno de estos enteros será congruente a A según el módulo m.

Si $\frac{a-A}{m}$ es un entero, entonces $a \equiv A$; si $\frac{a-A}{m}$ es una fracción, sea k el próximo mayor entero positivo (y si es negativo, el próximo menor, sin considerar el signo). $A + km$, que estará entre a y $a + m$, será el número buscado. Es evidente que todos los cocientes $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, y $\frac{a+2-A}{m}$, etc. están ubicados entre $k-1$ y $k+1$; por lo que solo uno de ellos puede ser entero.

Residuos mínimos.

4.

Así, pues, cada número tendrá un residuo, tanto en la sucesión $0, 1, 2, \ldots m-1$, como en $0, -1, -2, \ldots -(m-1)$ a los que llamamos *residuos mínimos.* Es evidente que, a no ser que 0 sea un residuo, siempre se presentan en pares: uno *positivo* y el otro *negativo.* Si son diferentes en magnitud, uno será $< \frac{m}{2}$; de otro modo, cada uno será $= \frac{m}{2}$ sin considerar signos. De donde es evidente que cada número tiene un residuo no mayor que la mitad del módulo, al que se llamará *residuo absolutamente mínimo.*

Por ejemplo: -13 tiene, según el módulo 5, un residuo mínimo positivo que es un residuo absolutamente mínimo; -3 es el residuo mínimo negativo; $+5$ es residuo mínimo positivo de sí mismo, según el módulo 7; -2 es el residuo mínimo negativo, y a la vez, absolutamente mínimo.

*) Adoptamos este símbolo por la gran analogía que se encuentra entre la igualdad y la congruencia. Por la misma razón, el ilustre Legendre, en su tratado, usó el mismo símbolo para la igualdad y la congruencia, lo que nosotros dudamos en imitar para que no se originara ninguna ambigüedad.

Proposiciones elementales sobre congruencias.

5.

Establecidos estos conceptos, reflexionemos sobre las propiedades de los números congruentes que son inmediatamente obvias.

Los números congruentes, según un módulo compuesto, también serán congruentes según cualquier factor de este módulo.

Si varios números son congruentes a un mismo número según un mismo módulo, serán congruentes entre sí (según el mismo módulo).

Esta identidad de módulos se debe sobreentender, también, en lo siguiente:

Los números congruentes poseen los mismos residuos mínimos; los números no congruentes poseen diferentes residuos mínimos.

6.

Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., que son respectivamente congruentes a ellos según un módulo cualquiera, es decir, $A \equiv a$, $B \equiv b$, etc. entonces, $A + B + C +$ etc. $\equiv a + b + c +$ etc.

Si $A \equiv a$, $B \equiv b$, entonces $A - B \equiv a - b$.

7.

Si $A \equiv a$, entonces, también $kA \equiv ka$.

Si k es un número positivo, entonces este es un caso particular del artículo anterior (art. 6), suponiendo que $A = B = C$ etc., y $a = b = c$ etc. Si k es negativo, entonces, $-k$ será positivo, de donde $-kA \equiv -ka$, de tal modo que $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, entonces $AB \equiv ab$, pues $AB \equiv Ab \equiv ab$.

8.

Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., respectivamente congruentes a aquellos, esto es si $A \equiv a$, $B \equiv b$, etc., los productos de cada uno de ellos serán congruentes, ABC etc. $\equiv abc$ etc.

Del artículo anterior, se tiene $AB \equiv ab$, y, por la misma razón, $ABC \equiv abc$, así para cualquier número de factores.

Si todos los números A, B, C, etc. se suponen iguales, y también los correspondientes a, b, c, etc., se tiene este teorema: *Si $A \equiv a$ y k es un entero positivo, entonces $A^k \equiv a^k$.*

9.

Sea X una función algebraica de la indeterminada x, de la forma

$$Ax^a + Bx^b + Cx^c + \text{ etc.}$$

donde A, B, C, etc., son números enteros cualesquiera, y donde a, b, c, etc. son enteros no negativos. Entonces, si se dan valores congruentes a la indeterminada x, según cualquier módulo entero, los valores correspondientes de la función X serán congruentes.

Sean f y g valores congruentes de x. Luego, por el artículo anterior, $f^a \equiv g^a$ y $Af^a \equiv Ag^a$, y del mismo modo $Bf^b \equiv Bg^b$, etc. Entonces,

$$Af^a + Bf^b + Cf^c + \text{ etc.} \equiv Ag^a + Bg^b + Cg^c + \text{ etc.} \qquad \textit{Q. E. D.}$$

Fácilmente se infiere cómo puede ser extendido el teorema a las funciones de varias indeterminadas.

10.

Si se sustituye x por todos los números enteros, consecutivamente, y si se reducen los valores de la función X a los residuos mínimos, entonces éstos formarán una sucesión en la que después de un intervalo de m términos (tomando a m como el módulo) los mismos términos se repetirán de nuevo. Entonces, la serie estará formada por un período de m términos repetido infinitamente. Por ejemplo, sea $X = x^3 - 8x + 6$ y $m = 5$; entonces para $x = 0$, 1, 2, 3, etc. los valores de X producen estos residuos mínimos positivos: 1, 4, 3, 4, 3, 1, 4, etc. donde los primeros cinco números 1, 4, 3, 4, 3 se repiten indefinidamente y, si la sucesión se continúa en el sentido contrario, esto es, si se dan valores negativos a x, el mismo período aparece con los términos en el orden inverso. De donde, resulta evidente que no pueden tener lugar otros términos en cualquier sucesión, excepto aquéllos que constituyen este período.

11.

Por lo tanto, en este ejemplo, X no puede ser ni $\equiv 0$, ni $\equiv 2 \pmod 5$, ni mucho menos $= 0$ ni $= 2$. De donde, se deduce que las ecuaciones $x^3 - 8x + 6 = 0$, y $x^3 - 8x + 4 = 0$ no pueden resolverse con números enteros, y, como se sabe, tampoco con racionales. Más generalmente, es evidente que, cuando X es una función de la incógnita x, de la forma

$$x^n + Ax^{n-1} + Bx^{n-2} + \text{ etc.} + N$$

donde A, B, C, etc. son enteros y n es un entero positivo (en realidad todas las ecuaciones *algebraicas* pueden reducirse a esta forma), la ecuación $X = 0$ no tiene ninguna raíz racional, si la congruencia $X \equiv 0$ no puede satisfacerse para ningún módulo. Aunque este criterio se nos presentó espontáneamente, será tratado más ampliamente en la Sección VIII. A partir de este ejemplo se puede formar alguna idea sobre la utilidad de estas investigaciones.

Algunas aplicaciones.

12.

Muchas cosas que suelen enseñarse en aritmética dependen de los teoremas expuestos en esta sección, e.g., las reglas para averiguar la divisibilidad de un número dado por 9, 11 u otro. *Según el módulo 9* todas las potencias del número 10 son congruentes con la unidad: por eso, si un número dado tiene la forma $a + 10b + 100c +$ etc., entonces dará, según el módulo 9, el mismo residuo mínimo que $a + b + c +$ etc. Así, es evidente que, si los dígitos de un número expresado en decimales se suman uno a uno sin tener en cuenta el lugar que ocupan, esta suma y el número dado presentan los mismos residuos mínimos, de tal modo que éste último puede dividirse entre 9, si aquel es divisible entre 9 y viceversa. Lo mismo es cierto para el divisor 3. Puesto que *según el módulo* 11, $100 \equiv 1$ será, en general $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, y un número de la forma $a + 10b + 100c +$ etc. dará, según el módulo 11, el mismo residuo mínimo que $a - b + c$ etc.; de donde de inmediato se deriva la regla conocida. De este mismo principio, se deducen todas las reglas similares.

De lo anterior se puede inferir el principio de las reglas dadas para la verificación de las operaciones aritméticas. Desde luego, si de los números dados, se derivan otros ya sea por suma, resta, multiplicación o elevación a potencia, se

sustituyen los residuos mínimos en lugar de los números dados, según un módulo arbitrario (por lo general se usan 9 u 11, porque como lo presentamos en nuestro sistema decimal, según éstos, los residuos pueden hallarse con facilidad). Por esto, los resultados deben ser congruentes con los que se derivaron de otros dados; porque si no sucediera así, se concluiría que se ha cometido un error en el cálculo.

Pero, puesto que estos resultados son bastante conocidos y semejantes con los anteriores, sería innecesario detenerse en ellos.