Científica
ISSN: 1665-0654
ISSN: 2594-2921
cientifica@ipn.mx
Instituto Politécnico Nacional
México

Ramírez Flores, Mario Antonio; González Medina, Sergio Iván
Aplicaciones de congurencias módulo n y ecuaciones diofantinas
Científica, vol. 27, núm. 1, 2023, Enero-Junio, pp. 1-13
Instituto Politécnico Nacional
Distrito Federal, México

Científica, vol. 27, núm. 1, pp. 01-13, enero-junio 2023, ISSN 2594-2921, Instituto Politécnico Nacional MÉXICO
e270110 | https://doi.org/10.46842/ipn.cien.v27n1a10

ARTICLE

Aplicaciones de congruencias módulo *m* y ecuaciones diofantinas

Congruences Module *m* and its Applications and Diophantine Equations

Mario Antonio **Ramírez Flores**[1]
Sergio Iván **González Medina**[2]

Instituto Politécnico Nacional, MÉXICO
[1] mramirezf@ipn.mx
[2] sigonzalezm@ipn.mx

Recibido 07-07-2022, aceptado 10-01-2023.

Resumen

Se desarrolla un método de análisis de dos tópicos de la teoría de los números: las congruencias modulo m y las ecuaciones diofantinas; las primeras referidas a la divisibilidad entre números, y las segundas a la solución de ecuaciones con coeficientes enteros con solución en números (enteros). Se estudian los números primos y la descomposición de un numero entero en factores primos, a su vez, el conocimiento de divisibilidad y sus propiedades. Asimismo, la aplicación de ambos temas para el encriptado de información en un ejemplo de una palabra con 10 (diez) letras no repetidas, que da lugar a una frase ininteligible, mismo que puede usarse como código de seguridad.

Palabras clave: Teoría de los números, congruencias, ecuaciones diofantinas, encriptado de información.

Abstract

A method of analysis of two topics of the theory of numbers, the congruences modulo m and the Diophantine equations, is developed; the first referred to the divisibility between numbers, and the second to the solution of equations with integer coefficients with solutions in (integer) numbers. Prime numbers and the decomposition of an integer into prime factors are studied, as well as the knowledge of divisibility and its properties. Likewise, the application of both topics for the encryption of information in an example of a word with 10 (ten) non-repeated letters, which gives rise to an unintelligible phrase, which can be used as a security code.

Index terms: Number theory, congruence, Diophantine equations, information encryption.

A LA MEMORIA DE LUIS RF

I. INTRODUCCIÓN

Una pregunta que resulta, además de inocente, desafiante, consiste en cuestionar ¿Qué es un número? La respuesta a semejante inocencia sencillamente es compleja, pues es un concepto fundamental en matemáticas. El concepto de número nació como abstracción de propiedades de conjuntos de objetos con los que el hombre encontraba en su diario quehacer, y ha servido para caracterizar cuantitativamente objetos y procesos. Para proceder a entender, que no significa responder lo incontestable, se recurrirá a la llamada Teoría de los Números, o como decía C.F. Gauss: La Reyna de las Matemáticas.

La teoría de números es la rama de las matemáticas que estudia las propiedades de los números, en particular de los enteros. Gran parte del siglo XIX en la búsqueda del concepto de número, y partiendo de los naturales (N), se obtuvieron clases más amplias y complicadas de números. Se tenía la idea de que un número natural era algo, simple y transparente, que podía ser reducido a un concepto más sencillo. Sin embargo, las cosas se complicaron. En el afán de contextualizar una respuesta alterna que ayude a formar la impresión de número y de sus aplicaciones, se muestra una caracterización de los naturales:

$$\mathbb{N} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \dots\}, \tag{1}$$

cómo se observa están ordenados en una sucesión. Algunas de sus propiedades son:

i) Inicia en un elemento especial, el **0**.
ii) La sucesión no termina ni se ramifica.
iii) La sucesión no se cierra sobre sí misma.
iv) La sucesión no tiene puntos de confluencia (ningún elemento sigue a dos distintos).
v) No hay números intercalados.

La gama de posibilidades para combinar elementos de este conjunto es *grande*, por ende, sus aplicaciones. La razón de este artículo es precisamente indicar algunas aplicaciones de la *teoría en* diferentes áreas, de manera particular se trata, por ejemplo, la *encriptación de información* que además de aumentar la seguridad en la transferencia de esta reduce la posibilidad de ser sustraída.

Haciendo uso de conceptos propios de la teoría de los números para tal fin, se tienen criterios como ***la divisibilidad, ecuaciones diofantinas, congruencias modulo m***, *entre otros*.

A. Los números enteros

En lo sucesivo se considera el conjunto de los números enteros, denotados con la letra mayúscula $\mathbb{Z}$. En este conjunto aparecen los números 0, ±1, ±2,…, es decir:

$$\mathbb{Z} = \{, \dots, -\mathbf{2}, -\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{2}, \dots\}. \tag{2}$$

En el conjunto de los enteros $\mathbb{Z}$ están definidas dos operaciones fundamentales, a saber, la suma (+)**,** $+\mathbf{:}\ \mathbb{Z}\ \mathbf{x}\ \mathbb{Z} \longrightarrow \mathbb{Z}$ y el producto $\mathbf{(\cdot)} \cdot \mathbb{Z}\ \boldsymbol{x}\ \mathbb{Z} \rightarrow \mathbb{Z}$. Lo que exactamente se está diciendo en estas expresiones es que si *a, b son dos números que pertenecen al conjunto de enteros:* $\boldsymbol{a, b} \in \mathbb{Z}$, entonces $\boldsymbol{a} + \boldsymbol{b}$ y $\boldsymbol{a} \cdot \boldsymbol{b}$ están en $\mathbb{Z}$. Dicho sea de paso, el ***cero (0)*** y el ***uno (1)*** son los elementos *neutros* para la *suma y producto respectivamente,* (esto es, $\boldsymbol{a} + \mathbf{0} = \mathbf{0} + \boldsymbol{a} = \boldsymbol{a}$ *y* $\boldsymbol{a} \cdot \mathbf{1} = \mathbf{1} \cdot \boldsymbol{a} = \boldsymbol{a}$ *para todo* $a \in \mathbb{Z}$). Con esto último y otras propiedades, no enunciadas, se dice que el conjunto $\mathbb{Z}$ constituye un anillo conmutativo.

B. Divisibilidad

Un entero $\boldsymbol{a}$ *divide* un entero $\boldsymbol{b}$, y se escribe $(\boldsymbol{a}|\boldsymbol{b})$ con $\boldsymbol{b \neq 0}$, si existe un entero $\boldsymbol{c}$, tal que $\boldsymbol{b = a \cdot c}$ en caso contrario, se dice que $\boldsymbol{a \nmid b}$, ($\boldsymbol{a}$ no divide al entero $\boldsymbol{b}$). La divisibilidad se escribe como:

$$\boldsymbol{a|b \Rightarrow b = a \cdot c.} \tag{3}$$

Propiedades

1. $\boldsymbol{a|b}$ entonces $\boldsymbol{a|b \cdot c}$, para todo $\boldsymbol{c} \in \mathbb{Z}$.
2. Si $\boldsymbol{a|b}$ y $\boldsymbol{b|c}$ entonces $\boldsymbol{a|c}$.
3. Si $\boldsymbol{a|b}$ y $\boldsymbol{a|c}$ entonces $\boldsymbol{a|(bx + cy)}$ para enteros $\boldsymbol{x}$ e $\boldsymbol{y}$.
4. Si $\boldsymbol{a|b}$ y $\boldsymbol{b|a}$ entonces $\boldsymbol{a = \pm b}$.
5. Si $\boldsymbol{a|b}$, $\boldsymbol{a > 0}$ y $\boldsymbol{b > 0}$, entonces $\boldsymbol{a \leq b}$.

Entre otras. Si el entero $\mathbf{a}$ es divisor de $\boldsymbol{b}$ y $\boldsymbol{c}$, entonces $\mathbf{a|b}$ y $\mathbf{a|}\boldsymbol{c}$. Cualquier entero tiene divisores si ocurre que $\boldsymbol{b \neq 0}$ **y** $\boldsymbol{c \neq 0}$.

Si por lo menos uno de $\boldsymbol{b}$ y $\boldsymbol{c}$ no es cero, el mayor entre sus divisores comunes se llama ***máximo común divisor (mcd)*** de $\boldsymbol{b, c,}$ y se denota por $\boldsymbol{(b, c)}$.

Sea $\boldsymbol{g}$ el *mcd* de los números $\boldsymbol{b}$ *y* $\boldsymbol{c}$*:*

$$\boldsymbol{g = (b, c).} \tag{4}$$

Así, existen $\boldsymbol{x_0}$ y $\boldsymbol{y_0}$ enteros tales que:

$$\boldsymbol{g = bx_0 + cy_0.} \tag{5}$$

Propiedades del *mcd de* $\boldsymbol{(a, b)}$.

1. $\boldsymbol{(ma,\ mb) = m(a, b)}$ con $\boldsymbol{m} \in \mathbb{Z}$
2. Si $\boldsymbol{d|a}$ y $\boldsymbol{d|b}$ y $\mathbf{d > 0}$ entonces $(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}\boldsymbol{(a, b)}$.
3. Si $\boldsymbol{(a, b) = g}$ entonces $\left(\frac{a}{g}, \frac{b}{g}\right) = \mathbf{1}$
4. Si $\boldsymbol{(a, b) = 1}$ se dice que $\boldsymbol{a}$ **y** $\boldsymbol{b}$ son primos relativos.

II. LOS NÚMEROS PRIMOS

Se dice que un entero $\boldsymbol{p > 1}$, es un número primo, o simplemente que $\boldsymbol{p}$ es primo, en caso de que no exista divisor $\boldsymbol{d}$ de $\boldsymbol{p}$ que satisfaga $\boldsymbol{1 < d < p}$. Si un entero $\boldsymbol{a > 1}$ no es primo, entonces se dice que es *compuesto*. Vale mencionar dos números enteros son *primos entre sí, o primos relativos,* en caso de no tener otro divisor común que $\boldsymbol{1}$ y $\boldsymbol{-1}$.

Un resultado fundamental dice: todo entero $\boldsymbol{n}$ mayor a $\boldsymbol{1:}$ $(\boldsymbol{n > 1})$, puede expresarse como un producto de primos, es decir.

$$\boldsymbol{n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot, \ldots, \cdot\ p_r^{\alpha r}.} \tag{6}$$

Donde $\boldsymbol{p_1, p_2,\ldots, p_r}$ son primos y $\boldsymbol{\alpha_1, \alpha_2, \ldots, \alpha_r,}$ son enteros positivos.

Ejemplos:

Determinar, y expresar los números dados como producto de primos:

i) $2013 = 3 \cdot 671 = 3 \cdot 11 \cdot 61$, observe que 3,11 y 61 son los factores primos de 2013, y se puede escribir:

$$2013 = (3) \cdot (11) \cdot (61)$$

ii) $72 = 2 \cdot 36 = 2 \cdot 2 \cdot 18 = 2 \cdot 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$ y se escribe:

$$72 = 2^3 \cdot 3^2$$

III. CRITERIOS DE DIVISIBILIDAD.

— *Divisibilidad por **2***

Un número es divisible por 2 si el digito de las unidades de su numeral es par (*0, 2, 4, 6, 8*), o es un número par.

— *Divisibilidad por **3***

Un número es divisible por 3 si la suma de los dígitos de su numeral es divisible por 3.

— *Divisibilidad por **5***

Un número es divisible entre 5 si el último digito de su numeral es 0 o 5.

Es interesante tener presente otros criterios de divisibilidad, por ejemplo, divisibilidad por ***7, 11, 13***, etc.
La experiencia cotidiana indica que pocas veces se practica la aritmética tratando de descomponer un entero como producto de primos, más aún cuando ese entero es del orden de centenas de millar o más. Por ejemplo; el número 62743, no es divisible por 11, y ello significa únicamente que: *no divisible por 11*.

Será interesante averiguar si este número es primo o compuesto: no es divisible por 2, 3, 5, 7, 11; se debe seguir el camino de ensayo error, ahora con el primo 13, 62743/13 no es entero; 62743/17 tampoco es entero. Y así sucesivamente hasta llegar por ejemplo al número 251, pero resulta que 62743/251 no es entero, luego se podría concluir que 62743 es primo. ¿Cuál será el siguiente primo, posterior a 62743?

Como ejemplo de la descomposición de un número en factores primos. Consideré el siguiente: ***6306300***, y tómese la siguiente convención de números primos:

$$\boldsymbol{a = 2, b = 3, c = 5, d = 7,}$$

$$\boldsymbol{e = 11, f = 13, g = 17.}$$

Determinando los factores primos:

$$6306300 = 2 \cdot 3153150 = 2 \cdot 2 \cdot 1576575 = 2 \cdot 2 \cdot 3 \cdot 525525 =$$

$$= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 175175 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 35035 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7007 =$$

$$= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 1001 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 91 =$$

$$= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 7$$

Con los *factores primos* obtenidos, queda establecido que el número ***6306300*** se puede expresar como:

$$\mathbf{6306300} = \mathbf{2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13}.$$

Y de acuerdo con la convención anterior, queda finalmente como:

$$\mathbf{6306300} = \boldsymbol{a^2 \cdot b^2 \cdot c^2 \cdot d^2 \cdot e \cdot f}. \tag{7}$$

¿Se podría imaginar el significado de la "*frase*" $\boldsymbol{a^2b^2c^2d^2ef}$? Y de las posibles combinaciones de estas letras. Así, ***jugando con leyes de los exponentes***, por ejemplo, se podría escribir $\boldsymbol{abcdeabcdf}$ (o muchas otras) sabiendo que *se ha escondido* la cantidad 6306300.

Lo anterior podría considerarse una forma de ocultar información. A manera de ejercicio se propone una nueva convención, por ejemplo, $z = 0, y = 1, x = 2$, …, etc. ¿Cómo se expresaría el número analizado?
En realidad, es poco común el uso y manejo de los números primos, por ello se pueden emplear para ocultar información, usando combinaciones o bien alguna disposición que complique su lectura, esto permitirá decir: *algo oculto subyace* y no será fácil deducir su significado. Se sugiere para aquellos cuya labor es enviar o proteger información contar con una tabla, no pequeña, de números primos para posibles aplicaciones.

IV. ECUACIONES DIOFANTINAS

Una ecuación diofantina es una ecuación lineal con coeficientes enteros, que exige solución entera. Sean $\boldsymbol{a, b, c} \in \mathbb{Z}$. La ecuación lineal $\boldsymbol{ax + by = c}$ tiene solución entera, si y sólo si, el *de* $\boldsymbol{(a, b)|c}$.

Solución Particular
Sean $\boldsymbol{a, b, c}$ tres números enteros y supóngase que los enteros, $\boldsymbol{x_0}$ e $\boldsymbol{y_0}$ son solución de la ecuación $\boldsymbol{ax + by = c}$, es decir, $\boldsymbol{ax_0 + by_0 = c}$. Entonces,

$$\boldsymbol{d = mcd\,(a, b) \Rightarrow d|a} \text{ y } \boldsymbol{d|b \Rightarrow}$$

$$\boldsymbol{d|ax_0 + by_0 \Rightarrow d|c.} \tag{8}$$

Recíprocamente, suponga $\boldsymbol{d = mcd\,(a, b)}$ es divisor de $\boldsymbol{c}$, entonces,

$$\boldsymbol{mcd\,(a, b) \Rightarrow mcd\,(\frac{a}{d}, \frac{b}{d}) = 1.} \tag{9}$$

Por propiedades de divisibilidad,

$$\exists\, \boldsymbol{p, q} \in \mathbb{Z}\text{: } \boldsymbol{\frac{a}{d}p + \frac{b}{d}q = 1,}$$

multiplicando por el entero $\boldsymbol{c}$

$$\Rightarrow \boldsymbol{a\frac{cp}{d} + b\frac{cq}{d} = c},$$

siendo $\boldsymbol{c/d}$ entero puesto que, por hipótesis, $\boldsymbol{d}$ es divisor de $\boldsymbol{c}$. Basta tomar

$$\boldsymbol{x_0 = \frac{cp}{d}\ e\ y_0 = \frac{cq}{d}}, \tag{10}$$

y se tendrá que

$$\boldsymbol{ax_0 + by_0 = c}, \tag{11}$$

es decir, los enteros $\boldsymbol{x_0}$ e $\boldsymbol{y_0}$ son solución de la ecuación y se conoce como *solución particular del sistema*. Debe observarse que este caso asegura la existencia de solución para una ecuación de este tipo y un método de cálculo.

Ejemplo:

Encontrar una solución para la ecuación diofantina:

$$\boldsymbol{525x + 100y = 50}. \tag{12}$$

Solución:

En principio se debe confirmar la existencia de una solución entera para la ecuación. Luego, se requiere calcular el ***mcd*** de $\boldsymbol{525}$ *y* $\boldsymbol{100}$, mediante la descomposición en *factores primos* de estos números:

$$\boldsymbol{525 = 3 \cdot 175 = 3 \cdot 5 \cdot 35 = 3 \cdot 5 \cdot 5 \cdot 7}.$$

Análogamente

$$\boldsymbol{100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5},$$

es decir,

$$\boldsymbol{mcd\ (525, 100) = 25}. \tag{13}$$

Ahora como ***25 divide a 50*** (*y a 100*), se asegura la existencia de soluciones enteras para la ecuación.

A. Cálculo de la solución para la ecuación.

Siguiendo el método se buscan los *coeficientes de la combinación lineal* del *máximo común divisor de 525* y *100*. Este procedimiento es equivalente al *Algoritmo de Euclides*. Si $\boldsymbol{a}$ y $\boldsymbol{b}$ son números enteros, con $\boldsymbol{b > 0}$, entonces existen dos enteros, $\boldsymbol{q}$ y $\boldsymbol{r}$, únicos, tales que $\boldsymbol{a = bq + r}$, con $\boldsymbol{o < r \leq b}$. a los números $\boldsymbol{a, b, q,\ y\ r,}$ se les llama, respectivamente, ***dividendo, divisor, cociente y residuo***.

Una solución puede ser la combinación lineal:

$$\boldsymbol{25 = 525 \cdot 1 + 100 \cdot (-5)},$$

con los valores propuestos, los coeficientes $\boldsymbol{p = 1}$ y $\boldsymbol{q = -5}$, y una solución para la ecuación se obtiene usando:

$$\boldsymbol{x_0 = \frac{cp}{d}\ \ e\ \ y_0 = \frac{cq}{d}.} \tag{14}$$

Donde $\boldsymbol{c}$ es el termino independiente de la ecuación y, ***d,*** el *máximo común divisor* de los coeficientes de $\boldsymbol{x}$ e $\boldsymbol{y}$. En consecuencia,

$$\boldsymbol{x_0 = \frac{50 \cdot 1}{25} = 2,}$$

$$\boldsymbol{y_0 = \frac{50 \cdot (-5)}{25} = -10}.$$

Solución general

Sean $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ *enteros* no nulos, tales que el *máximo común divisor* de $\boldsymbol{a}, \boldsymbol{b}$ divide a $\boldsymbol{c}$. Entonces la solución general de la ecuación $\boldsymbol{ax + by = c}$ es:

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{x_0} + \boldsymbol{k} \cdot \frac{\boldsymbol{b}}{\boldsymbol{d}}, \\ \boldsymbol{y} &= \boldsymbol{y_0} + \boldsymbol{k} \cdot \frac{\boldsymbol{a}}{\boldsymbol{d}}. \end{aligned} \tag{15}$$

Donde $\boldsymbol{x_0}$ e $\boldsymbol{y_0}$ es una solución particular de la misma y $\boldsymbol{k}$ es cualquier entero.

En efecto, sea $\boldsymbol{d}$ el máximo común divisor de $\boldsymbol{a}$ y $\boldsymbol{b}$. Por hipótesis $\boldsymbol{d}$ divide a $\boldsymbol{c}$ luego, existe una solución particular $\boldsymbol{x = x_0}$ e $\boldsymbol{y = y_0}$ para el sistema. Entonces,

$$\boldsymbol{ax_0 + by_0 = c,} \tag{16}$$

dividiendo por $\boldsymbol{d = (a, b)}$, se tiene

$$\frac{\boldsymbol{a}}{\boldsymbol{d}}\boldsymbol{x_0} + \frac{\boldsymbol{b}}{\boldsymbol{d}}\boldsymbol{y_0} = \frac{\boldsymbol{c}}{\boldsymbol{d}}. \tag{17}$$

Siendo $\frac{\boldsymbol{c}}{\boldsymbol{d}}$ entero y $\frac{\boldsymbol{a}}{\boldsymbol{d}}, \frac{\boldsymbol{b}}{\boldsymbol{d}}$ números enteros ***primos entre sí***, luego el *máximo común divisor* de ambos es $\boldsymbol{1}$, y como $\boldsymbol{1}$ divide a $\frac{\boldsymbol{c}}{\boldsymbol{d}}$, se asegura la existencia de una solución particular $\boldsymbol{x_1, y_1}$ para esta ecuación. Esto es,

$$\frac{\boldsymbol{a}}{\boldsymbol{d}}\boldsymbol{x_1} + \frac{\boldsymbol{b}}{\boldsymbol{d}}\boldsymbol{y_1} = \frac{\boldsymbol{c}}{\boldsymbol{d}}. \tag{18}$$

Igualando las ecuaciones anteriores

$$\begin{aligned} \frac{\boldsymbol{a}}{\boldsymbol{d}}\boldsymbol{x_1} + \frac{\boldsymbol{b}}{\boldsymbol{d}}\boldsymbol{y_1} = \frac{\boldsymbol{a}}{\boldsymbol{d}}\boldsymbol{x_0} + \frac{\boldsymbol{b}}{\boldsymbol{d}}\boldsymbol{y_0} \;&\Rightarrow\; \frac{\boldsymbol{a}}{\boldsymbol{d}}(\boldsymbol{x_1 - x_0}) + \frac{\boldsymbol{b}}{\boldsymbol{d}}(\boldsymbol{y_1 - y_0}) = \boldsymbol{0} \\ &\Rightarrow\; \frac{\boldsymbol{a}}{\boldsymbol{d}}(\boldsymbol{x_1 - x_0}) = \frac{\boldsymbol{b}}{\boldsymbol{d}}(\boldsymbol{y_1 - y_0}), \end{aligned}$$

se ve que $\frac{\boldsymbol{b}}{\boldsymbol{d}}$ divide a

$$\Leftrightarrow \frac{\boldsymbol{b}}{\boldsymbol{d}} \Big| \frac{\boldsymbol{a}}{\boldsymbol{d}}(\boldsymbol{x_1 - x_0}),$$

y al ser $\frac{\boldsymbol{b}}{\boldsymbol{d}}$ primo con $\frac{\boldsymbol{a}}{\boldsymbol{d}}$, dividirá a $\boldsymbol{x_1 - x_0}$, luego

$$\frac{\boldsymbol{b}}{\boldsymbol{d}} \Big| \boldsymbol{x_1 - x_0} \Leftrightarrow\; \exists \boldsymbol{k} \in \mathbb{Z} :\; \boldsymbol{x_1 - x_0 = k} \cdot \frac{\boldsymbol{b}}{\boldsymbol{d}} \Rightarrow\; \boldsymbol{x_1 = x_0 + k} \cdot \frac{\boldsymbol{b}}{\boldsymbol{d}},$$

sustituyendo el valor de $\boldsymbol{x_1 - x_0}$ en $\frac{\boldsymbol{a}}{\boldsymbol{d}}(\boldsymbol{x_1 - x_0}) + \frac{\boldsymbol{b}}{\boldsymbol{d}}(\boldsymbol{y_1 - y_0}) = \boldsymbol{0}$ y resulta

$$\frac{\boldsymbol{a}}{\boldsymbol{d}} \cdot (\boldsymbol{k} \cdot \frac{\boldsymbol{b}}{\boldsymbol{d}}) + \frac{\boldsymbol{b}}{\boldsymbol{d}}(\boldsymbol{y_1 - y_0}) = \boldsymbol{0} \Rightarrow \frac{\boldsymbol{a}}{\boldsymbol{d}} \cdot \boldsymbol{k} + \boldsymbol{y_1 - y_0} = \boldsymbol{0} \Rightarrow \boldsymbol{y_1 = y_0 - k} \cdot \frac{\boldsymbol{a}}{\boldsymbol{d}},$$

se ve finalmente que, $\boldsymbol{x_1}$ e $\boldsymbol{y_1}$ es solución de la ecuación $\boldsymbol{ax + by = c}$.

En efecto,

$$\boldsymbol{ax_0 + by_0 = a}\left(\boldsymbol{x_0 + k} \cdot \frac{\boldsymbol{b}}{\boldsymbol{d}}\right) + \boldsymbol{b}\left(\boldsymbol{y_0 + k} \cdot \frac{\boldsymbol{a}}{\boldsymbol{d}}\right)$$

$$= ax_0 + a \cdot k \cdot \frac{b}{d} + by_0 - b \cdot k \cdot \frac{a}{d}$$
$$= ax_0 + by_0 = c\,, \tag{19}$$

luego

$$x = x_0 + k \cdot \tfrac{b}{d} \;\; ; \;\; y = y_0 - k \cdot \tfrac{a}{d}, \tag{20}$$

es solución de la ecuación $ax + by = c$ cualquiera que sea $k \in \mathbb{Z}$, se le denomina solución general de dicha ecuación.

*Nota. En el ejemplo anterior, se llegó a:

$$x_0 = 2 \text{ e } y_0 = -10,$$

era una solución particular para la ecuación:

$$525x + 100y = 50.$$

Luego, una solución general de la misma será:

$$x = 2 + k \cdot \frac{100}{25} = 2 + 4k$$
$$y = -10 - k \cdot \frac{525}{25} = -10 - 21k \tag{21}$$

Siendo k cualquier número entero.

V. CONGRUENCIAS LINEALES

Dentro de los conceptos fundamentales de la teoría de los números se tiene la *divisibilidad*, una aplicación son las ***congruencias.*** Se puede decir que una *congruencia* es una afirmación sobre la divisibilidad, además de ser una *relación de equivalencia*, lo que permite agrupar a los enteros en familias disjuntas de tal manera que dos números son congruentes ***modulo m,*** si y solo si *pertenecen a la misma*. Estas familias se conocen con el nombre de ***Clases Residuales modulo m***, y se designa por $\mathbb{Z}_m$ al conjunto que se forma por ellas. Las *congruencias* tienen propiedades en común con la igualdad y se siguen de acuerdo con:

Teorema. Supóngase que a, b, c, d, x, y y $m > 0$ son enteros. *Se dice que* ***a*** *y* ***b*** *son congruentes* ***módulo m***, si m divide a $a - b$: $m|a - b$, y se escribe:

$$a \equiv b \ (mod\ m) \tag{22}$$

B. Propiedades

1. $a \equiv b \ (mod\ m)$, $b \equiv a (mod\ m)$ y $a - b \equiv 0 \ (mod\ m)$ son proposiciones equivalentes,
2. $a \equiv b \ (mod\ m)$ y $b \equiv c \ (mod\ m)$, entonces $a \equiv c \ (mod\ m)$,
3. $a \equiv b \ (mod\ m)$ y $c \equiv d \ (mod\ m)$, entonces $ax + cy \equiv (bx + dy) \ (mod\ m)$,
4. $a \equiv b \ (mod\ m)$ y $c \equiv d \ (mod\ m)$, entonces $ac \equiv bd \ (mod\ m)$,
5. $a \equiv b \ (mod\ m)$ y $d|m$, entonces $a \equiv b \ (mod\ d)$.
6. Y otras, …

VI. *Ecuación Lineal en Congruencias.*

Ahora una expresión del tipo:

$$\boldsymbol{ax \equiv b\ (mod\ m).} \tag{23}$$

Se dice que es una ecuación lineal en congruencias. Aquí $\boldsymbol{x}$ es una incógnita con valores en $\mathbb{Z}$.
Considere la ecuación

$$\boldsymbol{2x \equiv 1\ (mod\ 5)}, \tag{24}$$

como $\boldsymbol{5|(2x-1)}$ entonces existe un entero $\boldsymbol{k}$ tal que

$$\boldsymbol{2x = 5k + 1,\ y\ \ x = \frac{5k+1}{2}},$$

así, las soluciones son de este tipo.

Nota: al realizar la división se llega a:

$$\boldsymbol{x = 2k + \frac{k+1}{2}},$$

tiene solución para valores de $\boldsymbol{k}$ impares.
Sea la ecuación:

$$\boldsymbol{2x \equiv 1\ (mod\ 4),} \tag{25}$$

entonces $\boldsymbol{2x = 1 + 4k,}$ con $\boldsymbol{k}$ entero, se ve que no hay solución, pues $\boldsymbol{1 + 4k}$ es impar.

Luego la ecuación lineal en congruencias $\boldsymbol{ax \equiv b\ (mod\ m)}$ tiene soluciones cuando y sólo cuando el *mcd* de $\boldsymbol{a\ y\ m}$ es divisible por $\boldsymbol{b}$: $\boldsymbol{(a,m)|b}$.

Si este es el caso, sea $\boldsymbol{d = (a,m),}$ se tienen hasta $\boldsymbol{d}$ soluciones congruentes $\boldsymbol{((mod\ m)}$ y todas congruentes $\boldsymbol{(mod\frac{m}{d})}$.

En efecto, si $\boldsymbol{ax \equiv b\ (mod\ m)}$ tiene por solución $\boldsymbol{c}$, entonces $\boldsymbol{ac \equiv b\ (mod\ m)}$, por lo que $\boldsymbol{ac - b = mk}$, luego $\boldsymbol{b = -mk + ac}$, se observa que $\boldsymbol{d|\ b}$, puesto que $\boldsymbol{d = ac\ + mk}$ es una combinación lineal de $\boldsymbol{a}$ *y* $\boldsymbol{m.}$

Inversamente, si $\boldsymbol{d|\ b}$, entonces, $\boldsymbol{b = dk}$ para alguna $\boldsymbol{k}$, ahora por definición:

$$\boldsymbol{d = ac + mt,\quad \Rightarrow\quad dk = ack + mtk,\ \Rightarrow\quad a(kc) = b\ (mod\ m).}$$

Si $\boldsymbol{d|\ b}$, se tiene que $\boldsymbol{ac = b + mx}$, dividiendo por $\boldsymbol{d}$

$$\boldsymbol{\left(\frac{a}{d}\right)c = \frac{b}{d} + \left(\frac{m}{d}\right)k,\qquad \Rightarrow\qquad \left(\frac{a}{d}\right)c \equiv \frac{b}{d}\ (mod\ \frac{m}{d})}$$

Luego $\boldsymbol{\left(\frac{a}{d},\frac{m}{d}\right) = 1}$, y $\boldsymbol{c}$ existe. Así, cualquier solución de la congruencia $\boldsymbol{ax \equiv b\ (mod\ m)}$ es una solución de la congruencia:

$$\boldsymbol{\left(\frac{a}{d}\right) \equiv \left(\frac{b}{d}\right)\ (mod\frac{m}{d})\ ,} \tag{26}$$

Científica, vol. 27, núm. 1, pp. 01-13, enero-junio 2023, ISSN 2594-2921, Instituto Politécnico Nacional México
DOI: https://doi.org/10.46842/ipn.cien.v27n1a10

Se puede verificar que las soluciones de $\boldsymbol{ax \equiv b\ (mod\ m)}$ son del tipo $\boldsymbol{c + \frac{km}{d}, k \leq d - 1}$.

Ejemplos
:

1. Considere la ecuación $\boldsymbol{5x \equiv 7\ (mod\ 15)}$
$\boldsymbol{d = (5, 15) = 5,\ 5 \nmid 7}$, luego no hay soluciones enteras a la congruencia.

2. Considere la ecuación $\boldsymbol{5x \equiv 10\ (mod\ 20)}$
$\boldsymbol{d = (5, 20) = 5}$ y como $\boldsymbol{5|10}$, luego hay soluciones (***mód 20***).

Obsérvese que al dividir por 5, se tiene que:

$$\boldsymbol{5x \equiv 10\ (mod\ 20)\ \Rightarrow x \equiv\ 2\ (mod\ 4)}, \tag{27}$$

de la última, las soluciones son de tipo $\boldsymbol{4k + 2}$ con $\boldsymbol{0 \leq k \leq 4}$, Es decir, ***2, 6, 10, 14, 18.***

3. Considere la ecuación

$$\boldsymbol{6x \equiv 5\ (mod\ 17)\ ,} \tag{28}$$

$\boldsymbol{d = (6, 17) = 1}$ y como $\boldsymbol{1|5}$, hay soluciones enteras.

Dado que $\boldsymbol{17|(6x - 5)\ \Rightarrow 6x = 5 + 17k\ \Rightarrow\ x = \frac{17k+5}{6}}$, realizando la división se tiene que:

$$\boldsymbol{x = 2k + \frac{5k+5}{6} = 2k + \frac{5(k+1)}{6}.}$$

Nuevamente $\boldsymbol{x}$ es entera si $\boldsymbol{\frac{5(k+1)}{6}}$ es entera. Por ejemplo, si $\boldsymbol{k = 1}$, se tiene:

$$\boldsymbol{x = 2(1) + \frac{5(1+1)}{6} = \frac{22}{6},}$$

que no es un valor entero.

Ahora sea $\boldsymbol{k = 5}$

$$\boldsymbol{x = 2(5) + \frac{5(5+1)}{6} = 15\ \Rightarrow\ 6(15) \equiv 5(mod\ 17).}$$

Verificando

$$\boldsymbol{17|90 - 5\ \Rightarrow\ 17|85\ \Rightarrow 85 = 17(5) = 85.}$$

VII. APLICACIONES

En la teoría *elemental* de números, se estudian los números enteros sin emplear técnicas procedentes de otros campos de las matemáticas. Pertenecen a esta teoría *la divisibilidad, el algoritmo de Euclides, la factorización de los enteros como producto de números primos, la búsqueda de los números perfectos, las congruencias, las ecuaciones Diofantinas*, etc.

Dentro de múltiples y variadas aplicaciones está el desarrollo de técnicas para ocultar información que requiere ser confidencial y poco factible de ser sustraída. Se debe de buscar algún método poco o difícil de vulnerar que impida el *robo* de información, confiable y difícil de violar candados que se impongan.

Se debe *ocultar* el contenido de la información de manera que haga falta una interacción concreta para poder entender ese contenido. Un método para realizar esta acción es la ***encriptación***, es decir, ocultar la información haciendo la conversión del *lenguaje natural* en un texto *codificado o cifrado* que lo haga ilegible e ininteligible.

Dada la complejidad de la teoría de números en cuanto a sus propiedades y puesto que la inmensa mayoría son poco usuales, estos métodos se pueden emplear para obtener procedimientos y encriptar información. Así, si se considera que una población como el universo de estudio, la teoría de números reduce notablemente el tamaño de la misma, y las técnicas más avanzadas la minimizan siendo esto un ingrediente esencial como técnica de seguridad.

Considere una ***ecuación diofantina***, cuya solución permitirá encriptar un mensaje y al mismo tiempo elaborar *la llave* para conocer el contenido.

1. Sea la ecuación:

$$\mathbf{123}\boldsymbol{x}+\mathbf{57}\,\boldsymbol{y}=\mathbf{53}. \tag{29}$$

En principio se debe encontrar el *máximo común divisor* de *123* y *57 (123,57)*. Para ello se descompone cada uno de estos números en sus factores primos:

$$\mathbf{123}=\mathbf{3}\cdot\mathbf{41}\ \ \boldsymbol{y}\ \ \mathbf{57}=\mathbf{3}\cdot\mathbf{19}\ \therefore(\mathbf{123},\mathbf{57})=\mathbf{3}.$$

Como $\mathbf{3}|\mathbf{57}$, la ecuación *tiene soluciones en números enteros*, así la ecuación planteada es *diofantina*.

Si la ecuación original se divide entre $\boldsymbol{3}$:

$$\mathbf{41}\boldsymbol{x}+\mathbf{19}\boldsymbol{y}=\mathbf{177}, \tag{30}$$

despejando $\boldsymbol{y}$,

$$\boldsymbol{y}=\frac{\mathbf{177}-\mathbf{41}\boldsymbol{x}}{\mathbf{19}}=\mathbf{9}-\mathbf{2}\boldsymbol{x}+\frac{\mathbf{6}-\mathbf{3}\boldsymbol{x}}{\mathbf{19}},$$

$\boldsymbol{y}$ es entera si y sólo si $\frac{\mathbf{6}-\mathbf{3}\boldsymbol{x}}{\mathbf{19}}$ lo es. Sea $\boldsymbol{r_1}=\frac{\mathbf{6}-\mathbf{3}\boldsymbol{x}}{\mathbf{19}}$, y supóngase que $\boldsymbol{r_1}\in\mathbb{Z}$. Despejando a $\boldsymbol{x}$ de esta última ecuación

$$\boldsymbol{r_1}\cdot\mathbf{19}=\mathbf{6}-\mathbf{3}\boldsymbol{x}\ \ \Rightarrow\ \ \boldsymbol{x}=\frac{\mathbf{6}-\mathbf{19}\boldsymbol{r_1}}{\mathbf{3}}=\mathbf{2}-\mathbf{6}\boldsymbol{r_1}-\frac{\boldsymbol{r_1}}{\mathbf{3}}.$$

Luego, $\boldsymbol{x}\in\mathbb{Z}$, si $\frac{\boldsymbol{r_1}}{\mathbf{3}}$ también lo es asignando valores a $\boldsymbol{r_1}$ que sean múltiplos de $\boldsymbol{3}$, se tiene:

Si $\boldsymbol{r_1}=\mathbf{3}$, se tiene que $\boldsymbol{x}=\frac{\mathbf{6}-\mathbf{57}}{\mathbf{3}}=-\mathbf{17}$; $\boldsymbol{y}=\mathbf{9}-\mathbf{2}(\mathbf{17})+\frac{\mathbf{6}-\mathbf{3}(-\mathbf{17})}{\mathbf{19}}=\mathbf{46}$

Realizando el mismo proceso para los múltiplos siguientes:

$$\text{Si } \boldsymbol{r_1 = 6;\ x = \frac{6-114}{3} - 36\ ;\ y = 87},$$

$$\text{Si } \boldsymbol{r_1 = 9;\ x = \frac{6-171}{3} - 55\ ;\ y = 128}\ ,$$

$$\text{Si } \boldsymbol{r_1 = 12;\ x = \frac{6-228}{3} - 74\ ;\ y = 169}.$$

Considérese las parejas de valores de $\boldsymbol{x}$ e $\boldsymbol{y}$

-17, 46; -36, 87; -55, 128; -74, 169

Una técnica sencilla para encriptar es usar la asignación de números a letras de una palabra de extensión grande, por ejemplo, ***MURCIELAGO***. Como puede observarse son diez (10) letras distintas.

Se puede convenir la siguiente asignación:

$$\boldsymbol{0 \to M, 1 \to U, 2 \to R, 3 \to C, 4 \to I, 5 \to E, 6 \to L, 7 \to A, 8 \to G, 9 \to O}$$

La ecuación diofantina usada es

$$\boldsymbol{123x + 57\,y = 53}\ , \tag{31}$$

y puede escribirse con el encriptamiento:

$$\boldsymbol{URGx\ + EGy = ECU} \tag{32}$$

La clave para desencriptar es:

$$\boldsymbol{-UA, IL;\ -CL, GA;\ -EE, URG;\ -AI, UAO.}$$

Obsérvese la asignación, de números a letras dada. Claramente un lenguaje poco convencional, y requiere del conocimiento en la solución de ecuaciones diofantinas.

Ahora considérese el caso de una congruencia (***mód m***) para el mismo cometido, *encriptar información*. Sea la ecuación lineal en congruencias.

$$\boldsymbol{15x \equiv 25\ (mod\ 35)} \tag{33}$$

Entonces el ***(15, 35) = 5*** y $\boldsymbol{5|25}$ se tienen $\boldsymbol{\left(\frac{25}{5}\right) = 5}$ soluciones congruentes **(*mód 35*).**

Dividiendo por ***5*** la congruencia, se tiene $\boldsymbol{3x\ =\ 5\ (\mathrm{mod}\ 7)}$, luego $\boldsymbol{3x = 5 + 7k}$

$$\boldsymbol{x = \left(\frac{5+7k}{3}\right) = 1 + 2k + \left(\frac{2+k}{3}\right)},$$

$\boldsymbol{x}$ es entera si, $\left(\frac{\mathbf{2+k}}{\mathbf{3}}\right)$ lo es.

Entonces:

Sea $\boldsymbol{k_1} = \left(\frac{\mathbf{2+k}}{\mathbf{3}}\right)$

1. Si $\boldsymbol{k = 1} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+1}}{\mathbf{3}}\right) = \mathbf{1}$ por lo que si $\boldsymbol{k = 1}$, $\boldsymbol{k_1 = 1}$ y el valor de $\boldsymbol{x = 4}$,
2. Si $\boldsymbol{k = 2} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+2}}{\mathbf{3}}\right) = \frac{\mathbf{4}}{\mathbf{3}} \notin \mathbb{Z}$ no es solución de la congruencia,
3. Si $\boldsymbol{k = 3} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+3}}{\mathbf{3}}\right) = \frac{\mathbf{5}}{\mathbf{3}} \notin \mathbb{Z}$ no es solución de la congruencia,
4. Si $\boldsymbol{k = 4} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+4}}{\mathbf{3}}\right) = \mathbf{2} \in \mathbb{Z}$ por lo que si $\boldsymbol{k = 4}$, $\boldsymbol{k_1 = 2}$ y el valor de $\boldsymbol{x = 11}$,
5. Si $\boldsymbol{k = 5} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+5}}{\mathbf{3}}\right) = \frac{\mathbf{7}}{\mathbf{3}} \notin \mathbb{Z}$ no es solución de la congruencia,
6. Si $\boldsymbol{k = 6} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+6}}{\mathbf{3}}\right) = \frac{\mathbf{8}}{\mathbf{3}} \notin \mathbb{Z}$ no es solución de la congruencia,
7. Si $\boldsymbol{k = 7} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+7}}{\mathbf{3}}\right) = \mathbf{3} \in \mathbb{Z}$ por lo que si $\boldsymbol{k = 7}$, $\boldsymbol{k_1 = 3}$ y el valor de $\boldsymbol{x = 18}$,
8. Si $\boldsymbol{k = 10} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+10}}{\mathbf{3}}\right) = \mathbf{4} \in \mathbb{Z}$ por lo que si $\boldsymbol{k = 10}$, $\boldsymbol{k_1 = 4}$ y el valor de $\boldsymbol{x = 25}$,
9. Si $\boldsymbol{k = 13} \Rightarrow \boldsymbol{k_1} = \left(\frac{\mathbf{2+13}}{\mathbf{3}}\right) = \mathbf{5} \in \mathbb{Z}$ por lo que si $\boldsymbol{k = 13}$, $\boldsymbol{k_1 = 5}$ y el valor de $\boldsymbol{x = 32}$.

Se realizaron operaciones a fin de calcular valores de las constantes y con ellos determinar valores de la incógnita. *Hubo saltos*, y fueron para verificar que algunos valores no son enteros.

Los resultados obtenidos para $\boldsymbol{x}$ son ***4, 11, 18, 25, 32*** y se pueden verificar en la congruencia:

i. $15(\mathbf{4}) \equiv 25(mod\ 35) \Rightarrow 35|60 - 25 = 35 \Rightarrow$
$35|35 = 1$ ***se verifica***,
ii. $15(\mathbf{11}) \equiv 25(mod\ 35) \Rightarrow 35|165 - 25 = 140 \Rightarrow 35|140 = 4$ ***se verifica***,
iii. $15(\mathbf{18}) \equiv 25(mod\ 35) \Rightarrow 35|270 - 25 = 245 \Rightarrow 35|245 = 7$ ***se verifica***,
iv. $15(\mathbf{25}) \equiv 25(mod\ 35) \Rightarrow 35|375 - 25 = 350 \Rightarrow 35|350 = 10$ ***se verifica***,
v. $15(\mathbf{32}) \equiv 25(mod\ 35) \Rightarrow 35|480 - 25 = 455 \Rightarrow 35|455 = 13$ ***se verifica***.

De nueva cuenta considérese que la palabra clave es ***MURCIELAGO*** con la asignación de números a letras establecidos. Como la ecuación en congruencias es:

$$\mathbf{15}\boldsymbol{x} \equiv \mathbf{23}\ (\boldsymbol{mod}\ \mathbf{35})\ , \tag{34}$$

se puede escribir como: (35)

$$\boldsymbol{UEx} \rightarrow \boldsymbol{RE}(\boldsymbol{CE})\ ,$$

así mismo, la clave para desencriptar (los valores de x obtenidos), son

$$\boldsymbol{IUUUGRECR} \rightarrow [4\ 11\ 18\ 25\ 32]$$

Difícil de leer y más aún, con un significado ininteligible. Sin duda contiene información que no será fácil de sustraer. Se pueden emplear palabras de su invención o conocidas del lenguaje común, por ejemplo, ***CENTRIFUGA,*** contiene diez letras que no se repiten y se les puede dar la asignación referida.

Otro ejemplo de aplicación de ecuaciones en congruencias ***modulo m***, es para establecer la relación entre meses del año, días de la semana, horas del día. Así para los meses se tendrá congruencias ***módulo 12***, para los días ***módulo 7*** y para las horas ***módulo 24***.

Algunas personas acostumbran a emplear su fecha de nacimiento, o de algún familiar, como clave de acceso a su información, el uso de congruencias la ocultara dando mayor seguridad. Por ejemplo, una fórmula para determinar el día de la semana en que nació una persona es:

$$d \equiv f + \left[\!\left[\frac{13m-1}{4}\right]\!\right] - 2s + n + \left[\!\left[\frac{s}{4}\right]\!\right] + \left[\!\left[\frac{n}{4}\right]\!\right] (mod\ 7). \tag{36}$$

Dónde: $\boldsymbol{f}$ es la fecha (día del mes), $\boldsymbol{m}$ es el mes, $\boldsymbol{s}$ es el siglo, que, a su vez, es el número de siglos, y $\boldsymbol{n}$ es el año de nacimiento. Dada la complejidad del procedimiento, implica para quien pretendiera acceder a esta información, conocimientos sobre el tema, y si así fuese, demandaría saber la manera en cómo se asignaron números a días, meses y años, empresa que requiere de un gran esfuerzo mental.

Si se busca aumentar la seguridad en el manejo de información, el empleo de congruencias ayudará a este cometido. Por ejemplo, el uso de *números primos*, o empleando el *teorema chino del residuo*, o *congruencias de grado superior*, *etc.*

Se ha mostrado el beneficio que aporta la teoría de números, y en particular las ***Ecuaciones Diofantinas y las Congruencias Modulo m***; la complejidad alcanzada indica que es no fácil su lectura y comprensión.

VIII. Conclusiones

1. Lo visto es sólo un acercamiento a la teoría de los números, se ha pretendido con algunos ejemplos, convencer de los beneficios intelectuales que aporta el estudiarla.
2. La teoría de números es *parte de la estructura matemática y ayuda en la construcción lógica del pensamiento*, pues permite discernir problemas complejos y su solución.
3. La teoría de los números como rama de la matemática, aunque teórica y árida, revela posibles aplicaciones en diferentes áreas de la técnica.
4. El mundo que nos rodea es aritmética, geometría y en particular teoría de los números, a lo largo del tiempo se han puesto de manifiesto su importancia en el desarrollo de otros conocimientos, por ello es importante en el ámbito profesional que se posean este tipo de conocimientos.

Referencias

[1] C. Niven, H. Zuckerman, I*ntroducción a la Teoría de los Números*, 2ª ed., México: Limusa, 1976.
[2] Y. Vinogradov, *Fundamentos de la Teoría de los Números*, URSS: MIR, 1977.
[3] J. Gómez, *Matemáticos, Espías y Piratas Informáticos, Codificación y Criptográficas*, México: RBA, 2010.
[4] L. Cárdenas, et al., *Álgebra Superior*, 2ª ed., México: Trillas, 1990.