Original

UNA APLICACIÓN DEL TEOREMA DE WILSON

An Aplication of the Wilson Theorem

M. Sc. Andrés Adolfo González-Aguilera, Profesor Asistente, Universidad de Granma, agonzalezl@udg.co.cu, Cuba.

M. Sc. Edubar Oliva-Jaume, Profesor Auxiliar, Universidad de Granma, eoliva@udg.co.cu, Cuba.

Eduardo Renato Moreno-Roque, Profesor Asistente, Universidad de Granma, emorenor@udg.co.cu, Cuba.

Recibido: 3/07/2017 Aceptado: 28 /08/2017

RESUMEN

La aplicación de las Matemáticas a la resolución de problemas de la vida cotidiana constituye uno de los temas que cobran mayor interés en todos los niveles educacionales, es por ello que este artículo tiene como objetivo exponer las herramientas fundamentales de la aritmética modular, útiles para comprender la solución que se ofrece a determinados problemas de la práctica mediante la aplicación de un procedimiento resultante del Teorema de Wilson. Se presenta un ejemplo demostrativo de su aplicación. En la elaboración del trabajo se utilizan como métodos fundamentales el analítico sintético y el inductivo-deductivo. El procedimiento propuesto, a diferencia del teorema de Wilson, da el valor mínimo posible a la solución del problema presentado.

Palabras Clave: Teorema de Wilson, Aritmética modular, Fracciones continuas.

ABSTRACT

The application of the Mathematics to the resolution of problems of the daily life constitutes one of the topics that charge bigger interest in all the educational levels, it is for it that this article has as objective to expose the fundamental tools of the arithmetic to modulate, useful to understand the solution that offers to certain problems of the practice by means of the application of a resulting procedure of the Theorem of Wilson. A demonstrative example of its application is presented. In the elaboration of the work they are used as fundamental methods the analytic

one synthetic and the inductive-deductive one. The proposed procedure, contrary to the theorem of Wilson, he/she gives the minimum value possible to the solution of the presented problem.

Keywords: Wilson's theorem, Modular Arithmetic, Continued Fractions.

INTRODUCCIÓN

A largo de la historia de la humanidad, el hombre se ha enfrentado a disimiles y complejos problemas prácticos y teóricos, siendo capaz de resolverlos con la búsqueda de nuevos conocimientos y métodos de razonamiento, desempeñando un papel fundamental los relacionados con las matemáticas.

La teoría de números [1, 4, 5, 7, 8] es la rama de las matemáticas que estudia las propiedades aritméticas de los números enteros [4], que son todas aquellas que tienen que ver con suma y producto de números. Por ejemplo, dado un número entero *n*, el hallar todos sus divisores es un problema típico de la teoría de números. A propósito de ello, veamos la siguiente situación que pudo darse en cualquier parte:

En una reunión de la directiva nacional de la Sociedad Cubana de Matemática y Computación (COMPUMAT), realizada en La Habana, surgió una inquietud en uno de los miembros: ¿se conoce centralmente la cifra de delegados a los congresos COMPUMAT efectuados a nivel de provincia y a nivel nacional desde que se crea esta sociedad hasta nuestro días?. A la interrogante el presidente respondió: en este preciso instante, no tengo a la mano la cifra exacta, sólo le puedo decir que si los concentramos en grupos de 2, 3, 4 hasta 28 siempre sobra 1, mientras que si los concentramos en grupos de 29 no sobra ninguno. A partir de lo expuesto anteriormente ¿Podría usted determinar la cantidad mínima de participantes que satisfacen las condiciones planteadas por el delegado?

Este artículo pretende dar una solución general al problema anterior, cualquiera sea *p* número primo, por lo que se exponen las herramientas fundamentales de la aritmética modular, útiles para comprender la solución que se ofrece.

POBLACIÓN Y MUESTRA

Uno de los conceptos fundamentales en teoría de números es el de congruencia. Históricamente las congruencias fueron estudiadas primeramente por Fermat, Euler, Lagrange y Legendre. Gauss, en su famosa obra Disquisitiones Arithmeticae [4], es el primer matemático

que hace un estudio coherente y sistemático del tema. Muchos problemas teórico-prácticos pueden simplificarse estudiando el residuo que deja cada entero al ser dividido por un entero fijo. De esta forma, se puede pensar que la teoría de las congruencias es una herramienta poderosa que ayuda a resolver problemas por medio del estudio de residuos.

Como bien se conoce, a cada número entero le corresponde el resto de su división por un número entero m; si a dos enteros a y b les corresponde un mismo resto, éstos se llaman congruentes según el módulo m, o respecto al módulo m o simplemente, congruentes módulo m. En otras palabras, se dice que a es congruente con b en el módulo o el cuerpo m (Zm) si y sólo si existe algún entero k tal que $a-b = km$. De forma general, la congruencia de los números a y b respecto al módulo m se escribe así:

$$a \equiv b \pmod{m}.$$

De la definición de congruencia se sigue fácilmente las siguientes propiedades.

- Propiedad Reflexiva:

  $a \equiv a \pmod{m}, \quad \forall\, a \in Z. \quad (1)$

- Propiedad Simétrica:

  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}, \quad \forall\, a,b \in Z.$

- Propiedad Transitiva:

  Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}, \forall\, a,b,c \in Z.$

- Propiedad Asociativa:

  $[a + (b + c)] \pmod{m} \equiv [(a + b) + c] \pmod{m}, \ \forall\, a,b,c \in Z.$

- Propiedad Conmutativa:

  $(a + b) \pmod{m} \equiv (b + a) \pmod{m},$

  $ab \pmod{m} \equiv ba \pmod{m}, \forall\, a,b \in Z.$

- Propiedad Distributiva:

  $a(b + c) \pmod{m} \equiv (ab + bc) \pmod{m}, \forall\, a,b, \in Z.$

- Existencia de Identidad:

  $(a + 0) \pmod{m} \equiv (0 + a) \pmod{m} \equiv a \pmod{m},$

  $a \cdot 1 \pmod{m} \equiv 1 \cdot a \pmod{m} \equiv a \pmod{m}, \forall\, a \in Z$

  .

- Existencia de Inversos:

$a \cdot a^{-1} \equiv 1 \pmod{m}, \quad si\ (a,m) = 1$

- Reducibilidad:

$(a + b) \pmod{m} \equiv [a \pmod{m} + b \pmod{m}] \pmod{m},$

$ab \pmod{m} \equiv [a \pmod{m}][b \pmod{m}] \pmod{m}, \quad \forall\ a,b \in Z. \qquad (2)$

Definición 1. Sea *m* cualquier entero positivo, se denomina conjunto completo de restos módulo *m* y se denota mediante *CCR* al conjunto

$$Zm = \{0,1,2,...,m-1\},$$

el cual cumple que $\forall\ a \in Z$, $\exists!\ r_i \in CCR$ tal que $a \equiv r_i \pmod{m}$.

Definición 2. Se denomina conjunto reducido de restos módulo *m*, denotado como *CRR*, al subconjunto de *CCR* que son primos relativos con el módulo *m*, es decir

$$CRR = \{x \in CCR : (m, x) = 1\}.$$

Nota. En particular, para un número primo P se tiene $CCR = Z_p \setminus \{0\}$.

Teorema 1. Sea M cualquier entero positivo. Si (a , m) = 1, entonces la congruencia de primer grado $a \cdot x + b \equiv 0 \pmod{m}$ admite solución única módulo m.

A continuación se indicarán dos métodos para determinar la solución única de la congruencia $ax + b \equiv 0 \pmod{m}$, $(a,m) = 1$, uno de ellos basado en la teoría de las fracciones continuas y el otro en el inverso multiplicador.

Desarrollando en fracciones continuas [3, 6, 8] la razón *m/a*,

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots\ q_{n-1} + \cfrac{1}{q_n}}}},$$

se tiene que $x \equiv (-1)^n p_{n-1}\, b \pmod{m}$ [8], donde los p_k cumple con la siguiente relación de recurrencia $p_k = q_k p_{k-1} + p_{k-2}$, con $k = 2,...,n$, siendo $p_0 = 1$ y $p_1 = q_1$. Nótese, que es útil realizar estos cálculos según el esquema siguiente:

$$\begin{array}{cccccccccccc} q_k & & q_1 & q_2 & \cdots & \cdots & \cdots & q_k & \cdots & q_{n-1} & q_n \\ \hline p_k & 1 & q_1 & p_2 & \cdots & p_{k-2} & p_{k-1} & p_k & \cdots & p_{n-1} & m \end{array} \quad (3)$$

Otra de las vías para poder determinar la sólución única de la congruencia $ax+b \equiv 0 \pmod{m}$, $(a,m) = 1$, es multiplicando la misma por el inverso multiplicador de a, esto es, $x \equiv -ba^{\phi(m)-1} \pmod{m}$, donde $\phi(m)$ es la función de Euler [7, 8].

En particular, cuando m es un número primo p, se tiene que $\phi(p) = p-1$, es decir, $x \equiv -ba^{p-2} \pmod{p}$. Precisamente, este resultado se corresponde con el teorema de Fermat, que plantea, si p es primo y a no es divisible por p, se tiene que $aa^{p-2} = a^{p-1} \equiv 1 \pmod{p}$.

ANÁLISIS DE LOS RESULTADOS

Teorema 2 (Wilson). Si p es un número primo se verifica la siguiente congruencia [4, 8]. $(p-1)! + 1 \equiv 0 \pmod{p}$.

Es evidente, que el teorema de Wilson da respuesta inmediata al problema planteado inicialmente, pero la solución dada al mismo no es la mínima, es por ello que a continuación se describe un procedimiento para encontrar dicha solución.

Primeramente, denótese por ρ a los números primos que pertenecen al *CRR* módulo p. De esta manera, el mínimo común múltiplo de los elementos del conjunto $Zp\backslash\{0\}$, viene dado en la forma

$$\prod_{\rho<p-1} \rho^{\left[\frac{\log(p-1)}{\log \rho}\right]}.$$

Corolario 1. Sea p un número primo, entonces existe un único $x \in CRR$ módulo p, tal que

$$x \prod_{\rho<p-1} \rho^{\left[\frac{\log(p-1)}{\log \rho}\right]} + 1 \equiv 0 \pmod{p}, \quad (4)$$

Donde

$$x \equiv \prod_{\rho<p-1} \rho^{-\left[\frac{\log(p-1)}{\log \rho}\right]} (p-1)! \pmod{p}.$$

Demostración.

En efecto, según el teorema de Wilson y las propiedades (1) y (2) se deduce:

$$\left[\prod_{\rho<p-1}\rho^{-\left[\frac{\log(p-1)}{\log\rho}\right]}(p-1)!\ (\mathrm{mod}.\ p)\right]\left[\prod_{\rho<p-1}\rho^{\left[\frac{\log(p-1)}{\log\rho}\right]}\ (\mathrm{mod}.\ p)\right]+1\ \equiv\ 0\ (\mathrm{mod}.\ p)$$

$$\left[\prod_{\rho<p-1}\rho^{-\left[\frac{\log(p-1)}{\log\rho}\right]}(p-1)!\ (\mathrm{mod}.\ p)\right]\prod_{\rho<p-1}\rho^{\left[\frac{\log(p-1)}{\log\rho}\right]}+1\ \equiv\ 0\ (\mathrm{mod}.\ p)$$

,

lo cual coincide con (4).

Ahora bien, sólo queda demostrar que dicho *x* es único. Para ello, basta considerar a (4) como una ecuación de congruencia de primer grado. Evidentemente, existe un único $\varpi\in CRR$ módulo *p* tal que

$$\varpi\equiv\prod_{\rho<p-1}\rho^{\left[\frac{\log(p-1)}{\log\rho}\right]}\ (\mathrm{mod}.\ p).$$

Por tanto, en virtud de la propiedad de reducibilidad (2), la ecuación de congruencia de primer grado (4) es reescribible de la siguiente manera

$$\varpi x+1\equiv 0(\mathrm{mod}.p).$$

Además, como $\varpi\in CRR$ módulo *p*, se tiene que $(\varpi,p)=1$. Por consiguiente, según el teorema (4) la ecuación anterior admite solución única, probándose así la unicidad de *x*. Notése que además, la unicidad de *x* se puede demostrar por reducción al absurdo. □

3.1. Ejemplo.

A continuación se expondrá un ejemplo, donde se da solución al problema planteado inicialmente, pero para el caso donde *p* = 727. Como se podrá comprobar, el mínimo común múltiplo de los elementos del conjunto Z727\{0} es igual a:

133902558048748840062837187475021200348194617248538826576220277271692837327587899723757190971532265636687233614239822997472161769112705863383341699883342362568133492816642809346224675306425533108730918832987442892510905921031384552545532188692934850072848568733390179147950773824539893442979789810656146530528000 (5)

Cuya descomposición en factores primos viene dado por el producto de los números siguientes:

2^9 3^5 5^4 7^3 11^2 13^2 17^2 19^2

23^2 29 31 37 41 43 47 53

59 61 67 71 73 79 83 89

97 101 103 107 109 113 127 131

137 139 149 151 157 163 167 173

179 181 191 193 197 199 211 223

227 229 233 239 241 251 257 263

269 271 277 281 283 293 307 311

313 317 331 337 347 349 353 359

367 373 379 383 389 397 401 409

419 421 431 433 439 443 449 457

461 463 467 479 487 491 499 503

509 521 523 541 547 557 563 569

571 577 587 593 599 601 607 613

617 619 631 641 643 647 653 659

661 673 677 683 691 701 709 719

Obsérvese además, que el valor de $726!/\prod_{\rho<726}\rho^{\left[\frac{\log(726)}{\log\rho}\right]}$ viene dado mediante:

27861980722999417683860195553768367289198741078350159301680526849906468916
08139474617261207306329436214497392803390094200002979020826663385848913542
23493918479596933160526052897291932150055317907077178909098384691449878034
86454652664290371229041329508071619129559817201822550698334270846255069827
97615509149442627337545474009586401909299505523951967579226833433420838659
09222295798861821632827999426840618631412909942007675872752736775456661636
88410710413748877059037348386842986976414461654018532879709304345442048268
37164841994206063350355116817135632933306983291268944798612808305836257347
61093116018197495182389451641527125683403556548914761018300313500986898454
35691652505634098203656066016485524664950945302723281482768506610788414630
17812876267197080727418790009936329574285140457167067052121245808692235713
19961734416373822263082444157341279966944615090288552737953817718976429989

15800761683231733797680010075575776602209033717365856958225818556462648509
56847522490705105454055540586736964251339940356618966495699018548259286179
08199012360909365973952214137964085707799238139114071928935984825153691054
69664291648094676419671845791264461249213846887780847769172495143916076114
71360982252419030797582445247236678823089372940729100385973767975647228830
36336864614993100800000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000 00000000000.

Evidentemente, es mucho más factible y menos tedioso trabajar con [5] que con el número anterior. Se puede comprobar que:

$$\prod_{\rho<726} \rho^{\left[\frac{\log(726)}{\log \rho}\right]} \equiv 282 \pmod{.\ 727}.$$

De esta manera, dar solución al problema planteado inicialmente para p = 727 se reduce a determinar la solución de la ecuación de congruencia de primer grado $282x + 1 \equiv 0$ (mod. 727). Para tal propósito, debe desarrollarse en fracciones continuas la razón 727/282, lo cual viene dado del siguiente modo:

$$\frac{727}{282} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}}}}}.$$

Así, de esta manera, el esquema [3], útil para determinar a los $p_k = q_k p_{k-1} + p_{k-2}$, con $k = 2,...,10$, siendo $p_0 = 1$ y $p_1 = 2$, viene dado mediante:

q_k		2	1	1	2	1	2	2	1	1	2
p_k	1	2	3	5	13	18	49	116	165	281	727

Por tanto, en el caso dado, donde $n = 10$ y $p_{n-1} = 281$, la solución de la ecuación de congruencia de primer grado $282x + 1 \equiv 0 \pmod{727}$ es $x \equiv 281 \pmod{727}$. Otra de las maneras para determinar la solución de la ecuación de congruencia de primer grado $282x + 1 \equiv 0 \pmod{727}$ es tener en cuenta que:

$$\begin{aligned} x &\equiv -282^{725} \pmod{.727} \\ &\equiv -(282)^{2^0}(282)^{2^2}(282)^{2^4}(282)^{2^6}(282)^{2^7}(282)^{2^9} \pmod{.727} \\ &\equiv -446 \pmod{.727} \equiv 281 \pmod{.727}. \end{aligned}$$

Por consiguiente, la solución al problema planteado inicialmente para $p = 727$ es:

$$281 \prod_{\rho<726} \rho^{\left[\frac{\log(726)}{\log \rho}\right]}.$$

CONCLUSIONES

- La aplicación de las Matemáticas a la resolución de problemas de la vida cotidiana constituye uno de los temas que, a pesar de que se ha trabajado con frecuencia, aún no se ha logrado sistematizar en las carreras de perfil económico, en particular el tema relacionado con las ecuaciones modulares.
- El procedimiento propuesto, a diferencia del teorema de Wilson, da el valor mínimo posible a la solución del problema presentado. Constituyendo un procedimiento general, cualquiera sea el valor de *p* primo.

REFERENCIAS BIBLIOGRÁFICAS

1. Adams, W., Goldstein, L. (1976). *Introduction to number theory*, Englewood Cliffs, N.J. Prentice-Hall.
2. Soria-Lorente, A. (2013). *Aritmética de los valores de la función zeta de Riemann en argumentos enteros*, Revista de Investigación, G.I.E, Pensamiento Matemático, accepted.
3. Borwein, J., Van Der Poorten, A. J., Zudilin, W. (2009) Neverending*. Fractions: an Introduction to Continued Fractions*, September 30.
4. Gauss, C. F. (1966). *Disquisitiones Arithmeticae*, Traducida por Arthur A. Clarke New Haven and London, Yale University Press.

5. Ireland, K., Rosen, K. (1990). *A Classical Introduction to Modern Number Theory,* Second edition. Graduate Texts in Mathematics, 84, Springer- Verlag, New York.
6. Jones, W. B., Thron, W. J. (1980). *Continued fractions*, Analytic theory and applications, Encyclopaedia Math. Appl. Section: Analysis, Vol. 11, Addison-Wesley, London.
7. Niven, I., Zuckerman, H. (1966). *Introduction to Number Theory*, New York, Wiley.
8. Vinogrídov, I. (1977). Fundamentos de la teoría de números. Editorial Mir Moscu.