Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

SOLUCIÓN DIRECTA DE LA CONGRUENCIA CUADRÁTICA $x2 \equiv \pm p(mód\ pq)$ CON *p* Y *q* PRIMOS.

A DIRECT SOLUTION OF THE QUADRATIC CONGRUENCE $x2 \equiv \pm p(mód\ pq)$ WITH *p* AND *q* PRIMES.

Orlando Antonio Ruiz Álvarez[1].

RESUMEN

En esta investigación, se propone un procedimiento sencillo para determinar las soluciones de la congruencia cuadrática de módulo compuesto $x^2 \equiv \pm p(\text{mod } pq)$, donde p y q son primos distintos. En el caso de que $q \equiv 3(\text{mód } 4)$ se da una fórmula explicita para las soluciones de la congruencia. Además, se presenta una ilustración del procedimiento a través de ejemplos.

PALABRAS CLAVE: CONGRUENCIAS CUADRÁTICAS, MÓDULO COMPUESTO, TEORÍA DE NÚMEROS.

ABSTRACT

TIn this investigation, a simple procedure is proposed to determine the solutions of the quadratic congruence of composite modulus $x^2 \equiv \pm p(\text{mod } pq)$, donde p y q are different primes. In the case that $q \equiv 3(\text{mód } 4)$ an explicit formula is given for the solutions of the congruence. In addition, an illustration of the procedure is presented through of examples..

KEYWORDS: QUADRATIC CONGRUENCES, COMPOSITE MODULE, THEORY OF NUMBERS.

INTRODUCCIÓN

En secundaria se nos enseña a resolver ecuaciones cuadráticas con una incógnita, es decir, ecuaciones de la forma $a_2\ y^2+a_1\ y+a_0= 0$, $a_2 \neq 0$ tanto en los números enteros como en los reales. Sin embargo, en cursos avanzados de Matemáticas se resuelven ecuaciones semejantes a las que se les denomina congruencias cuadráticas y son de la forma: $a_2\ y^2+a_1y+a_0 \equiv 0\ (\text{mód } m)$, $a_2 \neq 0$ y $m \in Z^+$. Luego de realizar algunas manipulaciones algebraicas y considerando m=p primo en $a_2\ y^2+a_1y+a_0 \equiv 0\ (\text{mód } m)$, la congruencia general se reduce a $x^2 \equiv a\ (\text{mód } p)$, donde $x=2a_2\ y+a_1$ y $a=a_1^2-4a_2a_0$. Existen varios trabajos dedicados a proponer algoritmos para encontrar las soluciones de una ecuación cuadrática módulo primo tales como: Alberto Tonelli (1981), Michele Cipolla (1987), Henry Pocklington (1917), Elwin Berlekamp (1970), Bikashchandra Roy (2018), entre otros. Para el caso de que los módulos no sean primos, es decir, el entero p sea un número compuesto, los estudios se basan en casos particulares como, por ejemplo, Kurt Hensel (1897) y más recientemente *p=2rs* en B. M Roy (2018)..

EGeneralmente el problema de resolver una congruencia cuadrática módulo un número compuesto se reduce a resolver congruencias módulo potencias de primos. Es por ello que en este artículo se propone un procedimiento sencillo para obtener las soluciones de la congruencia

1. Departamento de Matemática Educativa, UNAN-León. Correo electrónico: orlando.ruiz13@fh.unanleon.edu.ni

Recibido: 7 de octubre 2022
Aceptado: 15 de noviembre 2022

Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

cuadrática $x^2 \equiv \pm p \ (\text{mód } pq)$, con p y q primos distintos, en el cual también se justifican cada una de sus propiedades a través de distintas herramientas de la teoría de números, tales como el símbolo de Legendre y el Pequeño Teorema de Fermat.

METODOLOGÍA

Dado lo apremiante del tema y la naturaleza de la composición de la comunidad universitaria de la FAREM-Matagalpa, se decidió hacer un estudio de la percepción del efecto de la pandemia en los miembros de la comunidad universitaria compuesta por estudiantes, docentes y personal administrativo. Para tal efecto se diseñó un cuestionario en el que se caracterizó a los encuestados desde el punto de vista de su afiliación con la universidad, las medidas preventivas tomadas por dichos miembros para prevenir el contagio del Covid-19, y del efecto que la pandemia había tenido en ellos desde su inicio al momento de la encuesta. El efecto se dividió en físico (contagiado / no contagiado), síntomas de la enfermedad y sus secuelas y el efecto multidimensional en el entorno del encuestado.

Para efecto de cumplir los requisitos estadísticos se estimó una muestra pirobalística de la población de aproximadamente 5,000 estudiantes, 220 docentes entre horarios y permanentes y 80 miembros de personal administrativo. Esto resultó en una muestra de 170 y se garantizó de que la información fuera recolectada aleatoriamente para garantizar la representatividad de los resultados. La información fue recolectada durante los meses de septiembre y octubre del 2021. Los datos fueron procesados en el software R y el análisis se centra en la descripción de la información obtenida con algunas extensiones de las implicaciones que dichos resultados indican.

DESARROLLO

Si bien es cierto que el Teorema Chino del Resto (TCR) es una herramienta que se puede usar para determinar las soluciones de la congruencia cuadrática $x^2 \equiv \pm p \ (\text{mód } pq)$, tiene la desventaja de recurrir a solución de un sistema de congruencias lineales, lo cual es muy tedioso y se lleva mucho tiempo Arrufat (2012). En este artículo, resolvemos la congruencia $x^2 \equiv \pm p \ (\text{mód } pq)$, considerando una solución de la forma $x \equiv pt \pm p \ (\text{mód } pq)$, dicha estrategia aún no ha sido considerado en la literatura de Teoría de números.

A continuación, se presenta el resultado principal del artículo:

Proposición

Considere la congruencia:

$$x^2 \equiv \pm p \ (mód \ pq) \quad ①$$

con p, q primos.

i) Posee solución si y sólo sí $\pm p$ es resto cuadrático módulo q (con p y q primos distintos).

ii) $x \equiv \pm y_0 \ p \ (\text{mód } pq)$ es solución de ①, donde y_0 una solución de la congruencia $y^2 \equiv \pm p^{q-2} \ (\text{mód } q)$.

Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

iii) $x \equiv \pm p^{\frac{(q-2)(q+1)}{4}+1} (mód\ pq)$ es solución de ① si q≡3 (mód 4).

Demostración. Supongamos que p,q∈Z^+ son primos distintos y consideremos la ecuación ①.

i).Es bien conocido que si el símbolo de Legendre tiene resultado 1, entonces la congruencia cuadrática tiene solución. Dado que:

$$\left(\pm\frac{p}{pq}\right) = \left(\frac{\pm p}{p}\right)\left(\frac{\pm p}{q}\right) = \left(\frac{\pm p}{q}\right) \quad \text{y} \quad \left(\frac{\pm p}{q}\right) = 1$$ si ±p es resto cuadrático módulo q.

Entonces, la ecuación ① posee solución si y sólo sí ±p es resto cuadrático módulo q. Además, $\left(\pm\frac{p}{pq}\right) = \left(\frac{\pm p}{q}\right) = 1$, si por el Teorema de Lagrange (Koshy (2007)) la congruencia ① tiene exactamente dos soluciones.

ii). Asumamos que la solución de la ecuación ① tiene la forma:

$$x \equiv pt \pm p (mód\ pq) \quad ②,$$

donde, la elección del signo + o - depende del signo de p.

Sustituyendo en ①, se obtiene:

$$(pt \pm p)^2 \equiv \pm p (mód\ pq)$$
$$p^2(t \pm 1)^2 \equiv \pm p\ (mód\ pq)$$
$$p(t \pm 1)^2 \equiv \pm 1\ (mód\ q)$$

Por el Pequeño Teorema de Fermat, al multiplicar por el inverso multiplicativo de *p(mód q)* obtenemos.

$$(t\pm 1)^2 \equiv \pm p^{q-2}\ (mód\ q).$$

Si hacemos y=t±1, entonces $(t\pm 1)^2 \equiv \pm p^{q-2}\ (mód\ q)$ se convierte en

$$y^2 \equiv \pm p^{q-2}\ (mód\ q)$$

Dado que $\left(\pm\frac{p}{q}\right) = 1$, por Koshy (2007) se tiene que $\left(\pm\frac{p^{q-2}}{q}\right) = \left(\pm\frac{p^{-1}}{q}\right) = 1$ lo que indica que $\pm p^{q-2}$ es un resto cuadrático módulo q.

Luego, si y_0 es una solución de $y^2 \equiv \pm p^{q-2}\ (mód\ q)$, entonces

Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

$$t \pm 1 \equiv y\_0 \pmod{q}$$

$$t \equiv y_0 \mp 1 \pmod{q}$$

Sustituyendo en ②,

$$x \equiv p(y_0 \mp 1) \pm p \pmod{pq}$$

$$x \equiv py_0 \pmod{pq} \quad ③$$

Además, como $x \equiv py_0 \pmod{pq}$ es una solución de la congruencia ①, entonces la otra solución es:

$$x \equiv pq - py_0 \ (mód\ pq) \equiv -py_0 \ (mód\ pq).$$

iii). Pockington (1917) demuestra que cuando q sea un primo de la forma $q \equiv 3 \ (mód\ 4)$, las soluciones de $x^2 \equiv a (mód\ q)$ son $x \equiv \pm a^{\frac{q+1}{4}} (mód\ q)$. . Por lo tanto, las soluciones de

$$y^2 \equiv \pm p^{q-2} \pmod{q}$$

están dadas por:

$$y \equiv (\pm p^{q-2})^{\frac{q+1}{4}} (mód\ q),$$

o bien, $y \equiv (\pm p)^{\frac{(q-2)(q+1)}{4}} (mód\ q)$.

Por ③, podemos concluir que las soluciones de la ecuación ①, está dada por:

$$x \equiv \pm p\ (\pm p)^{\frac{(q-2)(q+1)}{4}} (mód\ pq),$$

la cual se puede reescribir de la siguiente manera:

$$x \equiv \pm p^{\frac{(q-2)(q+1)}{4}+1} (mód\ pq).$$

Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

Ilustración de la propuesta

Ejemplo 1

Resolver la congruencia cuadrática $x^2 \equiv 479 (\text{mód } 192\,079)$.

Resolución

Dado que $192\,079 = 401 \cdot 479$ y $x^2 \equiv 479 (\text{mód } 192\,079)$, entonces p=479, q=401. Además,

$$\left(\frac{479}{192\,079}\right) = \left(\frac{479}{401 \cdot 479}\right) = \left(\frac{479}{401}\right)\left(\frac{479}{479}\right) = \left(\frac{479}{401}\right) = \left(\frac{78}{401}\right) = 1,$$

de lo cual concluimos que la ecuación de congruencia dada posee soluciones.

En este caso la ecuación auxiliar, $y^2 \equiv \pm p^{q-2} \pmod{q}$, que obtenemos es:

$$y^2 \equiv 479^{401-2} \pmod{401},$$

$$y^2 \equiv 78^{-1} \pmod{401},$$

o bien,

$$y^2 \equiv 36 (\text{mód } 401)$$

Notemos que una solución de esta última congruencia es:

$$y_0 \equiv 6 (\text{mód } 401).$$

Por lo tanto, las soluciones de $x^2 \equiv 479 (\text{mód } 192\,079)$, son

$$x \equiv \pm (479)(6) \ (\text{mód } 192\,079),$$

$$x \equiv \pm 2874 (\text{mód } 192\,079).$$

Ejemplo 2

Resolver la congruencia cuadrática $x^2 \equiv -13 (\text{mód } 377)$.

Resolución

Dado que $377 = 13 \cdot 29$ y $x^2 \equiv -13 (\text{mód } 377)$, entonces p=13, q=29. Además,

Revista Científica Tecnológica - RECIENTEC
ISSN 2708-7093
Vol. 5. Nº 2, Diciembre 2022/ P. 1-8
URL: https://www.revistarecientec.unan.edu.ni
email: revistarecientec@unan.edu.ni

$$\left(-\frac{13}{377}\right)=\left(-\frac{13}{13\cdot 29}\right)=\left(\frac{13}{13}\right)\left(\frac{-13}{29}\right)=\left(\frac{-13}{29}\right)=1,$$

de lo cual concluimos que la ecuación de congruencia dada posee soluciones.

En este caso la ecuación auxiliar, $y^2\equiv\pm p^{q-2}\ (\text{mód } q)$, que obtenemos es:

$$y^2\equiv -13^{29-2}\ (\text{mód } 29),$$

$$y^2\equiv 78^{27}\ (\text{mód } 29),$$

o bien,

$$y^2\equiv 20(\text{mód } 29)$$

Notemos que una solución de esta última congruencia es:

$$y_0\equiv 7(\text{mód } 29).$$

Por lo tanto, las soluciones de $x^2\equiv -13\ (\text{mód } 377)$,son

$$x\equiv \pm 7\cdot 13\ (\text{mód } 13\cdot 22),$$

$$x\equiv \pm 91\ (\text{mód } 377).$$

Ejemplo 3

Resolver la congruencia cuadrática $x^2\equiv 5(\text{mód } 95)$,

Resolución

Dado que $95=5\cdot 19$, entonces

$$\left(\frac{5}{95}\right)=\left(\frac{5}{5\cdot 19}\right)=\left(\frac{5}{5}\right)\left(\frac{5}{29}\right)=\left(\frac{5}{29}\right)$$

Como $\left(\frac{5}{19}\right)\equiv 1\ (\text{mód } 19)$, se concluye que la ecuación de congruencia dada posee soluciones.

Haciendo $p=5, q=19$, se procede a calcular sus soluciones considerando iii) ya que $19\equiv 3(\text{mód } 4)$:

$$x \equiv \pm 5^{\frac{(19-2)(19+1)}{4}+1}(mód\ 5 \cdot 19)$$

$$x \equiv \pm 5^{86}(mód\ 95)$$

$$x \equiv \pm 85(mód\ 95)$$

CONCLUSIONES

Hemos formulado y verificado mediante tres ejemplos analíticos un nuevo proceso para calcular la solución de la congruencia $x^2 \equiv \pm p$ (mód pq) con p,q primos distintos y demostramos que además de que posee dos soluciones, lleva menos tiempo que el uso de TCR. Consideramos que al utilizar esta fórmula estándar se presenta otro proceso distinto al conocido TCR y, por tanto, podría ser presentada con fines didácticos para su comparación en conjunto con el aula de clases. .

REFERENCIAS

Arrufat González, J. M. (2012). Implementación eficiente del Teorema Chino del Resto. Almería: Máster en informática insdustrial posgrado en informática. Obtenido de http://repositorio.ual.es/bitstream/handle/10835/1869/Trabajo_7036_92.pdf;jsessionid=D49213292618CF44CE1D8F0A08832C6C?sequence=1

Hensel, K. W. (1897). Über eine neue Begründung der Theorie der algebraischen Zahlen. Deutschen Mathematiker-Vereinigung, 84-87. Obtenido de http://www.digizeitschriften.de/dms/img/?PID=PPN37721857X_0006|log2&physid=phys2#navi

Koshy, T. (2007). Elementary Number Theory whith Applications (Segunda ed.). Academic Press is an imprint of Elsevier.

Maheswari, A., & Durairaj, P. (2017). An Algorithm to Find Square Roots of Quadratic Residues Modulo p (p being an odd prime) p≡ 1(mod 4). Global Journal of Pure and Applied Mathematics, XIII(4), 1223-1239. Obtenido de https://www.ripublication.com/gjpam17/gjpamv13n4_09.pdf

Nieto Said, J. H. (2014). Teoría de Números para Olimpiadas de Matemáticas. Caracas, Venezuela: Asociación Venezolana de Competencias Matemáticas. Obtenido de https://acmfiles.s3.amazonaws.com/Libros/TNumerosOlimpiadas.pdf

Piazza, N. (29 de March de 2018). The Chinese Remainder Theorem. Sacred Heart University. Obtenido de https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?article=1217&context=acadfest#:~:text=The%20Chinese%20Remainder%20Theorem%20is,pairwise%20rel%2D%20atively%20prime%20moduli.

Pocklington, H. C. (Febrary de 1917). The Direct Solution of the Quadratic and Cubic Binomial Congruences with prime moduli. Proceedings of the Cambridge Philosophical Society, 19, 57-58. Obtenido de https://ia800301.us.archive.org/25/items/proceedingsofcam1920191721camb/proceedingsofcam1920191721camb_bw.pdf

Roy, B. (2018). Formulation of solutions of some classes of standard quadratic congruence of compositive modulus as a produc of a prime-power integer & two or four. International Journal for Research Trends and Innovarion, 3, 120-122. Obtenido de https://ijrti.org/papers/IJRTI1805023.pdf

Roy, B. (2018). Formulation of solutions of standard quadratic congruence of even compositive modulus. International Journal of Research Science & Management, 99-101. Obtenido de http://www.ijrsm.com/issues%20pdf%20file/Archive-2018/May-2018/13.pdf

Rubiano, G. N., Gordillo, J. E., & Jiménez, L. R. (2004). Teoría de Números (para principiantes) (Segunda ed.). Bogotá, Colombia: Universidad Nacional de Colombia. Obtenido de https://matcris5.files.wordpress.com/2011/08/teoria_de_los_numeros_para_principiantes1.pdf

Wright, S. (Noviembre de 2016). Introducción: Resolviendo la Congruencia Cuadrática General Módulo a Primo. Obtenido de Researchgate: https://www.researchgate.net/publication/310537551_Introduction_Solving_the_General_Quadratic_Congruence_Modulo_a_Prime

AGRADECIMIENTOS

El presente artículo fue realizado bajo la supervisión del Dr. Jony Rojas Rojas a quien se agradece por su paciencia, tiempo y dedicación para que esta investigación saliera de manera exitosa.