Artículo Original / Original Research

Ciencias Matemáticas, Vol. 38, No. 1, 2024, Pag. 49-59
Recibido (*Received*): 23-06-2024, Revisado (*Reviewed*): 17-07-2024
Aceptado (*Accepted*): 30-10-2024, En línea (*Online*): 26-01-2025

Introducción y solución del problema de los reducidos catalanes

Introduction and solution of the problem of the reduced catalan

Luis Enrique Fernández Machado[1]

Resumen El problema de los reducidos catalanes consiste en la resolución de ecuaciones en congruencia y en la maximización del cardinal del conjunto de soluciones de estas. Para solucionar este problema se desarrolla un novedoso método demostrativo, que se denomina método Bézout-Euler de las potencias, el cual integra teoremas clásicos de la teoría de números como el teorema de Bézout y el teorema de Euler. Para la solución del problema de los reducidos catalanes se obtienen diversos teoremas que demuestran las potencialidades de este proceder demostrativo para conocer la existencia o no de soluciones de una ecuación en congruencia, así como para determinar el número de estas.

Palabras Clave: cardinal, congruencia, ecuación, máximo, potencia.

Abstract *The problem of the reduced Catalans consists of solving equations in congruence and maximizing the cardinal of the set of solutions of these equations. To solve this problem, a novel demonstrative method is developed, called the Bézout-Euler method of powers, which integrates classical theorems of number theory such as Bézout's theorem and Euler's theorem. For the solution of the problem of the reduced Catalans, several theorems are obtained that demonstrate the potential of this demonstrative procedure to know the existence or not of solutions of an equation in congruence, as well as to determine the number of these.*

Keywords: *cardinal, congruence, equation, maximum, power.*

Mathematics Subject Classification: 11, 11A07, 11A15, 11D04.

[1]Departamento de Matemática, Facultad de Matemática y Computación, Universidad de La Habana, La Habana, Cuba. Email: luis.fernandez@matcom.uh.cu.

Editado por (Edited by): Damian Valdés Santiago, Facultad de Matemática y Computación, Universidad de La Habana, La Habana, Cuba.

Citar como: Fernández Machado, L.E. (2024). Introducción y solución del problema de los reducidos catalanes. *Ciencias Matemáticas*, 38(1), 49–59. DOI: https://doi.org/10.5281/zenodo.14744243. Recuperado a partir de https://revistas.uh.cu/rcm/article/view/9749.

Introducción

El interés las ecuaciones en congruencias, conjuntos y expresiones fue suscitado por el siguiente problema, propuesto a los estudiantes del Equipo Nacional de Matemática de Cuba para las Olimpiadas Internacionales [1], y que fue extraído de la Olimpiada Balcánica de Matemáticas de 1999:

Sea p un número primo impar tal que $p \equiv 2 (\mod 3)$. Considere el conjunto:

$$S = \{y^2 - x^3 - 1;\ x, y \in \mathbb{Z}_p\}. \tag{1}$$

Probar que el conjunto S tiene a lo sumo p elementos divisibles por p.

A partir de este problema se obtuvo una generalización significativa, cuya resolución es el objetivo fundamental de esta investigación. Esta generalización del ejercicio olímpico antes presentado se denomina problema de los reducidos catalanes y su enunciado es el siguiente:

Dado m un número natural impar que admite raíces primitivas y sean a, b, c números naturales que cumplen las siguientes condiciones:

- $(a, \varphi(m)) \neq (b, \varphi(m))$.
- Sea p el mayor divisor primo de $\varphi(m)$, entonces
$$\frac{\varphi(m)}{p} \geq \max\{(a, \varphi(m)), (b, \varphi(m))\}.$$
- $(c, m) \in \{1, m\}$.
- Si m no es primo y $m \nmid c$, entonces $\min\{a, b\} \geq \log_p m$.

Se desea determinar el valor máximo posible del cardinal del conjunto $E = \{(x,y) \in (\mathbb{Z}_m \times \mathbb{Z}_m);\ x^a - y^b - c \equiv 0(\text{mod } m)\}$, así como y las condiciones suficientes y necesarias para que a,b y c alcancen ese máximo.

Particularmente, resulta relevante la integración de diversas ideas demostrativas y resultados conocidos de la teoría elemental de números en la solución de este problema generalizado. Esta interrelación de diversos teoremas en un único proceder demostrativo en este artículo, da como resultado un novedoso método de demostración, que se denomina método Bézout-Euler de las potencias, el cual constituye una amplia generalización de las ideas del método Bézout-Fermat [5].

El método Bézout-Euler de las potencias, que recorre transversalmente todo este trabajo, constituye una poderosa herramienta para abordar problemas de este tipo en Olimpiadas de Matemática [5], así como para solucionar casos particulares de la conjetura de Catalan y la ecuación de Catalan-Fermat, donde se utiliza la teoría elemental de números, sin necesidad de recurrir a los tradicionales procedimientos basados en cuerpos ciclotómicos [2, 3, 4].

Relevancia del estudio

La solución del problema de los reducidos catalanes resulta un avance importante para abordar casos significativos de problemas abiertos como la ecuación Catalan-Fermat con herramientas de la teoría elemental de números, sin necesidad de recurrir a técnicas más avanzadas de la teoría algebraica de números. También, el método Bézout-Euler de las potencias, desarrollado para resolver el problema de esta investigación, constituye una metodología valiosa para resolver ecuaciones diofánticas con grado variable del tipo $x^a + y^b = c$, donde los exponentes a,b son también variables. Además, este método demostrativo, por ser una amplia generalización del método Bézout-Fermat, es una poderosa herramienta para la resolución de ejercicios de teoría de números de las Olimpiadas Internacionales de Matemática.

1. Preliminares

Para abordar el problema planteado en esta investigación se usan diversas definiciones, resultados y teoremas de la teoría de números, que se pueden consultar, con sus demostraciones, en [1, 6]. En esta sección se presentan aquellas definiciones y teoremas imprescindibles para comprender este trabajo.

Definición 1 *Dados $a,m,n \in \mathbb{N}$, se dice que m es el orden de a módulo n, si m es el menor número natural para el cual se cumple que $a^m \equiv 1(\text{mod } n)$. Se denota por $ord_n a = m$.*

Definición 2 *La función de Euler es aquella que, para cada $m \in \mathbb{N}$, determina la cantidad de números primos relativos con m menores que m. Se denota por $\varphi(m)$.*

Definición 3 *Dados $r,n \in \mathbb{N}$, se dice que r es raíz primitiva módulo n si y solo si $ord_n r = \varphi(n)$.*

Definición 4 *Sean $a,k,n \in \mathbb{N}$, a es resto de k-ésima potencia en módulo n si y solo si $\exists x \in \mathbb{N};\ x^k \equiv a(\text{mod } n)$.*

Teorema 5 *Sea $m \in \mathbb{N}$, entonces m admite raíces primitivas si y solo si $m = 2,4,p^\alpha,2p^\alpha$ donde $\alpha \in \mathbb{N}$ y p es un número primo impar.*

Teorema 6 *Sean d, k, x números naturales y p un número primo tales que $x^d \equiv 1(\text{mod } p^n)$ y $\varphi(p^n) \equiv 0(\text{mod } d)$. Entonces, existen exactamente d raíces incongruentes de $x^d \equiv 1(\text{mod } p^n)$.*

Teorema 7 *Sean $a,m \in \mathbb{N}$ tales que m admite raíces primtivas y $(a,m) = 1$. Entonces, a es resto de k-ésima potencia módulo m si y solo si:*

$$a^{\frac{\varphi(m)}{d}} \equiv 1(\text{mod } m),\ \text{siendo } d = (k,\varphi(m)).$$

La cantidad de números naturales incongruentes que dejan resto a en módulo m al ser elevados a k es exactamente d.

El teorema 7 se denomina de caracterización de los restos de k-ésimas potencias en módulos que admiten raíces primitivas.

Teorema 8 *Sean $h,j \in \mathbb{N}$ y $d = (h,j)$ entonces:*

$$\exists x,y \in \mathbb{N};\ hx = d + jy.$$

El teorema 8 es una expresión equivalente del teorema de Bézout.

Teorema 9 *Para todos $m,n \in \mathbb{N}$ con $(m,n) = 1$ se cumple que:*

$$m^{\varphi(n)} \equiv 1(\text{mod } n).$$

Este resultado se conoce como teorema de Euler.

2. Desarrollo

El análisis fundamental de esta investigación va dirigido a la siguiente ecuación en congruencia:

$$x^a - y^b - c \equiv 0(\text{mod } m). \tag{2}$$

Como m es un número natural que admite raíces primitivas y es impar, por el teorema 5 se deduce que $m = p^t$, donde p un número primo impar y $t \in \mathbb{N}$. Entonces, se puede notar que m es un número primo ($t = 1$) o m no es un número primo, pero sí una potencia de primo ($t \geq 2$). Para abordar la problemática de esta investigación es necesario dividir el análisis para cada uno de estos dos casos.

2.1 Caso 1: m no primo ($t \geq 2$)

Para este caso se puede notar que:

$$\varphi(m) = p^{t-1}(p-1).$$

Como $(p-1) < p$, sus factores primos son menores que p, por tanto, el mayor divisor primo de $\varphi(m)$ es p. Entonces, al aplicar las condiciones del problema planteado se tiene que:

$$\frac{\varphi(m)}{p} = p^{t-2}(p-1) \geq \text{máx}\{(a,\varphi(m));\ (b,\varphi(m))\}. \quad (3)$$

El interés de la investigación se centra en determinar el número máximo de soluciones $(x,y) \in \mathbb{Z}_m \times \mathbb{Z}_m$ de la ecuación (2). Para ello, primero se analiza el caso en que $c \equiv 0(\text{mod } m)$, y el valor máximo del cardinal de E, así como las condiciones suficientes y necesarias para que se alcance el máximo para este caso.

Luego, bastará probar que $c \equiv 0(\text{mod } m)$ es una condición necesaria para que $|E|$ alcance ese valor, que en el otro caso ($(c,m) = 1$) el máximo valor siempre será menor o igual que el máximo para $c \equiv 0(\text{mod } m)$.

2.1.1 Caso 1.1: $c \equiv 0(\text{mod } m)$

Para este caso, el problema equivale a determinar el valor máximo que puede alcanzar el cardinal del conjunto $E = \{(x,y) \in (\mathbb{Z}_m \times \mathbb{Z}_m);\ x^a - y^b \equiv 0(\text{mod } m)\}$ y la ecuación en congruencia a analizar será:

$$x^a \equiv y^b(\text{mod } m). \quad (4)$$

Hallar el máximo de $|E|$, en este caso, equivale a hallar el número máximo de soluciones (x,y) de la ecuación (4), y las condiciones suficientes y necesarias para alcanzarlo. Intuitivamente, el máximo se alcanzará si se logra que para $x \in \mathbb{Z}_m$ exista la mayor cantidad posible de $y \in \mathbb{Z}_m$ que satisfacen la ecuación (4).

Entonces, basta encontrar condiciones suficientes y necesarias para alcanzar este máximo ideal. Nótese que si $(x,m) = 1$, entonces debe ser $(y,m) = 1$ para satisfacer (4). De modo análogo, si $x \equiv 0(\text{mod } p)$, los valores de $y \in \mathbb{Z}_m$ para los cuales se satisface (4) cumplen que $y \equiv 0(\text{mod } p)$.

Se puede observar que la cantidad máxima de soluciones de la ecuación (4) es la suma de las cantidades máximas de soluciones de esta ecuación cuando $x \equiv 0(\text{mod } p)$ y cuando $(x,m) = 1$.

Por tanto, se puede abordar el problema al hallar las condiciones suficientes y necesarias para que se alcance el máximo en cada caso. A partir de la unión de esas condiciones, se pueden obtener las condiciones suficientes y necesarias para que se alcance el máximo total. Por ello, se divide el análisis en dos subcasos.

Subcaso 1.1.1: $x \equiv 0(\text{mod } p)$. Para este subcaso, se puede notar que:

$$x^a \equiv y^b(\text{mod } m) \Rightarrow y \equiv 0(\text{mod } p). \quad (5)$$

Puede observarse que la máxima cantidad de múltiplos de m se alcanza si se cumple que:

$$x \equiv y \equiv 0(\text{mod } p) \ \Rightarrow x^a \equiv y^b(\text{mod } m). \quad (6)$$

Teorema 10 *La condición planteada en (6) se cumple si y solo si* $\text{mín}\{a,b\} \geq t$.

Demostración. Sea, sin pérdida de generalidad, $\text{mín}\{a,b\} = b$. Entonces, se tiene que:

$$a > b \text{ pues } (a,\varphi(m)) \neq (b,\varphi(m)).$$

- **Suficiencia:** Como $a > b \geq t$, se tiene que:

$$p^a > p^b \geq p^t.$$

Por tanto,

$$x \equiv y \equiv 0(\text{mod } p),$$

$$\Rightarrow x^a \equiv y^b(\text{mod } p^t) \Rightarrow x^a \equiv y^b(\text{mod } m), \text{ pues } m = p^t.$$

- **Necesidad:** Si se cumple la condición (6), se tiene que:

$$x = y = p \equiv 0(\text{mod } p) \Rightarrow x^a = p^a \equiv y^b = p^b(\text{mod } p^t),$$

$$\Rightarrow p^a - p^b = p^b(p^{a-b} - 1) \equiv 0(\text{mod } p^t). \quad (7)$$

Como $a > b$ se obtiene que:

$$(p^{a-b} - 1, p^t) = (p^{a-b} - 1, p) = 1.$$

Por tanto, se tiene que

$$p^b(p^{a-b} - 1) \equiv 0(\text{mod } p^t),$$

$$\Leftrightarrow p^b \equiv 0(\text{mod } p^t),$$

$$\Leftrightarrow \text{mín}\{a,b\} = b \geq t.$$

■

Entonces, basta hallar la cantidad máxima para este subcaso, teniendo como condición suficiente y necesaria que $min\{a,b\} \geq t$ para alcanzarlo.

Teorema 11 *La cantidad máxima de soluciones de la ecuación (4) es* $p^{2(t-1)}$ *y la condición suficiente y necesaria para alcanzar dicha cantidad es* $\text{mín}\{a,b\} \geq t$.

https://doi.org/10.5281/zenodo.14744243 https://revistas.uh.cu/rcm/article/view/9749

Demostración. La condición necesaria y suficiente se demostró en el teorema 10. Como se cumple la condición (6) para tener el número máximo de soluciones, basta hallar la cantidad de $x \in \mathbb{Z}_m$ que son múltiplos de p y elevarla al cuadrado. Sea m_p la cantidad de múltiplos de p menores que m, entonces se tiene que:

$$m_p = \lfloor \frac{m}{p} \rfloor = \lfloor \frac{p^t}{p} \rfloor = p^{t-1}.$$

Entonces, la cantidad máxima es:

$$m_p^2 = (p^{t-1})^2 = p^{2(t-1)}.$$

■

Subcaso 1.1.2: $(x,m) = (y,m) = (y,p) = (x,p) = 1$.

Ahora se realizan dos transformaciones que serán útiles para este subcaso y los posteriores. Por el algoritmo de la división con resto [6] se garantiza que:

$$\exists! q_a, r_a \in \mathbb{N};\ a = \varphi(m)q_a + r_a,\ \varphi(m) > r_a \geq 0, \quad (8)$$

$$\exists! q_b, r_b \in \mathbb{N};\ b = \varphi(m)q_b + r_b,\ \varphi(m) > r_b \geq 0. \quad (9)$$

Lema 12 *El problema de los reducidos catalanes en este subcaso es equivalente a maximizar el cardinal del conjunto* $E' = \{(x,y) \in (\mathbb{Z}_m \times \mathbb{Z}_m);\ x^{r_a} - y^{r_b} \equiv 0 (\text{mod } m)\}$.

Demostración. Se puede notar que las condiciones del problema de los reducidos catalanes no varían al trabajar con r_a y r_b, ya que por las propiedades del máximo común divisor se tiene que:

$$(a, \varphi(m)) = (r_a, \varphi(m)),$$

$$(b, \varphi(m)) = (r_b, \varphi(m)).$$

Al aplicar el Teorema de Euler se tiene que:

$$x^a = x^{\varphi(m)q_a + r_a} = (x^{\varphi(m)})^{q_a} x^{r_a} \equiv x^{r_a} (\text{mod } m),$$

$$y^b = y^{\varphi(m)q_b + r_b} = (y^{\varphi(m)})^{q_b} y^{r_b} \equiv y^{r_b} (\text{mod } m).$$

Por tanto, se obtiene que:

$$(x^a - y^b) \equiv (x^{r_a} - y^{r_b}) (\text{mod } m),$$

$$\Rightarrow |E'| = |E|.$$

■

Entonces, el problema en este subcaso consiste en maximizar el cardinal de E' y determinar las condiciones suficientes y necesarias de r_a, r_b para alcanzarlo.

Sean:

$$d_a = (a, \varphi(m)) = (r_a, \varphi(m)),$$

$$d_b = (b, \varphi(m)) = (r_b, \varphi(m)).$$

Por las condiciones del problema, se puede garantizar sin pérdida de generalidad que:

$$p^{t-2}(p-1) \geq d_a > d_b.$$

Sean $h_a, h_b \in \mathbb{N}$ tales que:

$$\varphi(m) = d_a h_a = d_b h_b.$$

Se puede notar que:

$$h_b > h_a, \text{ pues } d_a > d_b.$$

Teorema 13 *Maximizar el cardinal de* E' *equivale a maximizar el número de soluciones de la ecuación en congruencia:*

$$r^k \equiv 1 (\text{mod } m), \text{ donde } k = (h_a, h_b). \quad (10)$$

Demostración. Obtener el valor máximo del cardinal de E' equivale a determinar el número máximo de $r \in \mathbb{Z}_m$ que satisface que:

$$x^{r_a} \equiv r (\text{mod } m), \quad (11)$$

$$y^{r_b} \equiv r (\text{mod } m). \quad (12)$$

Entonces, basta probar que:

$$x^{r_a} \equiv y^{r_b} \equiv r (\text{mod } m) \Leftrightarrow r^k \equiv 1 (\text{mod } m).$$

- **Suficiencia:** Por el teorema 7 se tiene que las ecuaciones (11) y (12) se cumplen si y solo si:

$$r^{\frac{\varphi(m)}{d_a}} = r^{h_a} \equiv 1 (\text{mod } m), \quad (13)$$

$$r^{\frac{\varphi(m)}{d_b}} = r^{h_b} \equiv 1 (\text{mod } m). \quad (14)$$

Como $k = (h_a, h_b)$, se tiene que:

$$\exists c_a, c_b \in \mathbb{N};\ (c_a, c_b) = 1,\ h_a = k c_a,\ h_b = k c_b. \quad (15)$$

Entonces, se obtiene que:

$$r^k \equiv 1 (\text{mod } m) \Rightarrow r^{k c_a} = r^{h_a} \equiv 1^{c_a} \equiv 1 (\text{mod } m).$$

$$r^k \equiv 1 (\text{mod } m) \Rightarrow r^{k c_b} = r^{h_b} \equiv 1^{c_b} \equiv 1 (\text{mod } m).$$

Por tanto, se tiene que $r^{h_b} \equiv r^{h_a} \equiv 1 (\text{mod } m)$, lo que, por el teorema 7, implica que:

$$x^{r_a} \equiv y^{r_b} \equiv r (\text{mod } m).$$

- **Necesidad:** Por el teorema de Bézout:

$$\exists z, w \in \mathbb{N};\ h_a z = k + h_b w.$$

Por la ecuación (14) se tiene que:

$$(r^{h_b})^w \equiv 1^w \equiv 1 (\text{mod } m).$$

Entonces, a partir de la ecuación (13) se tiene que:

$$r^{h_a z} = r^{k + h_b w} = (r^k) r^{h_b w} = (r^k)(r^{h_b})^w$$

$$\equiv r^k \equiv 1^z \equiv 1 (\text{mod } m).$$

■

Entonces, para resolver el problema de los reducidos catalanes para este subcaso se debe determinar el número máximo de soluciones de la ecuación (10).

Teorema 14 *El valor máximo del cardinal del conjunto E' en este subcaso es $\frac{\varphi(m)^2}{2p}$ y la condición necesaria y suficiente para alcanzarlo es $(\varphi(m), r_b) = \frac{\varphi(m)}{2p}$.*

Demostración. Como k es el máximo común divisor de h_a y h_b, se tiene que:

$$\varphi(m) \equiv 0 (\text{mod } k).$$

De donde, por el teorema 2, el número de $r \in \mathbb{Z}_m$ tal que $(r,m) = 1$ (o lo que es lo mismo, el número de enteros incongruentes módulo m) que satisfacen la ecuación (10) es k. Por tanto, bastaría hallar el máximo valor de $k = (h_a, h_b)$, el cual es claro que es h_a, ya que $h_b > h_a$. Entonces, se tiene que:

$$\exists n \in \mathbb{N};\ h_b = h_a n.$$

Por tanto, aplicando las ecuaciones (13) y (14) se obtiene que:

$$r^{h_a} \equiv 1 (\text{mod } m) \Rightarrow r^{h_b} = (r^{h_a})^n \equiv 1 (\text{mod } m).$$

Se puede concluir que todo resto de r_a-ésima potencia de $x \in \mathbb{Z}_m$ en módulo m también lo es de r_b-ésima potencia en módulo m si $k = h_a$. Para cada valor de $x \in \mathbb{Z}_m$ que genera un resto r de r_a-ésima potencia, existen soluciones $y \in \mathbb{Z}_m$ de la ecuación (12). El número de soluciones de la ecuación (12) que existe por cada $x \in \mathbb{Z}_m$, es d_b por el teorema 3. Entonces, se tiene que el valor máximo de $|E'|$ es:

$$\varphi(m) d_b.$$

Se demuestra por reducción al absurdo que $\frac{\varphi(m)}{2p}$ es el mayor valor que puede alcanzar d_b.

Supongamos que:

$$d_b > \frac{\varphi(m)}{2p}.$$

Se conoce que:

$$\varphi(m) \equiv 0 (\text{mod } d_b).$$

Se puede notar que los divisores de $\varphi(m)$ son de la forma:

$$\frac{\varphi(m)}{d};\ \varphi(m) \equiv 0 (\text{mod } d).$$

Entonces, aplicando las condiciones del ejercicio se tiene que existe un divisor d_1 de $\varphi(m)$ tal que:

$$\frac{\varphi(m)}{p} \geq d_a > d_b = \frac{\varphi(m)}{d_1} > \frac{\varphi(m)}{2p},$$

$$\Rightarrow 2p > d_1 > p.$$

Como no existen múltiplos de p mayores que p y menores que $2p$ se tiene que:

$$(d_1, p) = 1,$$

$$\Rightarrow (d_1, p^{t-1}) = 1,$$

$$\Rightarrow (p-1) \equiv 0 (\text{mod } d_1), \text{ ya que } d_1 \text{ es divisor de } \varphi(m),$$

$$\Rightarrow (p-1) \geq d_1 > p, \text{ absurdo.}$$

Por tanto, el valor máximo de d_b es $\frac{\varphi(m)}{2p}$ y el máximo valor de $|E'|$ para este subcaso:

$$\varphi(m) \left(\frac{\varphi(m)}{2p} \right) = \frac{\varphi(m)^2}{2p} = \frac{p^{2t-3}(p-1)^2}{2}. \qquad (16)$$

Aplicando las condiciones del ejercicio y el valor máximo de d_b demostrado, se obtiene que:

$$d_a = \frac{\varphi(m)}{p} \text{ es el mayor valor que alcanza } d_a.$$

Entonces, bajo estas condiciones de máximo se puede notar:

$$\varphi(m) = d_a h_a = d_b h_b,$$

$$\varphi(m) = \frac{\varphi(m)}{p} h_a = \frac{\varphi(m)}{2p} h_b,$$

$$\Rightarrow h_b = 2h_a.$$

Por lo cual, la condición $d_b = (\varphi(m), r_b) = \frac{\varphi(m)}{2p}$ incluye la condición suficiente y necesaria para maximizar el número de soluciones de la ecuación (10), que equivale a maximizar el cardinal del conjunto E'. ■

Como para alcanzar el valor máximo del cardinal del conjunto E en el Caso 1.1 deben alcanzarse los valores máximos para el Subcaso 1.1.1 y para el Subcaso 1.1.2, entonces deben cumplirse simultáneamente las condiciones necesarias y suficientes para alcanzar dichos valores en cada subcaso. Por tanto, a partir del teorema 11 y el teorema 14 se obtiene el siguiente teorema.

Teorema 15 *El valor máximo del cardinal del conjunto E para el Caso 1.1 es:*

$$p^{2(t-1)} + \frac{\varphi(m)^2}{2p} = \frac{p^{2t-3}(p^2+1)}{2}. \qquad (17)$$

Las condiciones necesarias y suficientes para alcanzar dicho máximo son:

1. $min\{a,b\} \geq t$.
2. $(\varphi(m), b) = (\varphi(m), r_b) = \frac{\varphi(m)}{2p} = \frac{p^{t-2}(p-1)}{2}$.

Para probar que este valor de (17) es el máximo de $|E|$ bajo las condiciones del *"Problema de los reducidos catalanes"*, basta probar que si m no divide a c, el máximo valor que puede alcanzar $|E|$ es menor la expresión en (18). Además, de ello (ya por el caso anterior junto con $c \equiv 0(\text{mod } m)$) se tendrían las condiciones necesarias y suficientes para alcanzar el máximo buscado.

Si m no divide a c, entonces, por la condiciones del problema de los reducidos catalanes, son primos relativos.

2.1.2 Caso 1.2: $(c,m) = 1$

En este caso se debe determinar el valor máximo que puede alcanzar el cardinal del conjunto que se está analizando $E = \{(x,y) \in (\mathbb{Z}_m \times \mathbb{Z}_m);\ x^a - y^b - c \equiv 0(\text{mod } m)\}$, siendo c primo relativo con m. Como este caso es parte del Caso 1 m no es primo y, por las condiciones del problema de los reducidos catalanes, se tiene que

$$(c,m) = 1 \Rightarrow \text{mín}\{a,b\} \geq \log_p m = \log_p p^t = t.$$

Se divide este Caso 1.2 en dos subcasos.

Subcaso 1.2.1: c no es resto de a-ésima potencia en mod p.

Teorema 16 *Para el Subcaso 1.2.1 el valor máximo que puede alcanzar el cardinal de E es:*

$$(\varphi(m) + p^{t-1})d_b = p^t d_b. \tag{18}$$

Además, se cumple que:

$$\frac{\varphi(m)^2}{2p} + p^{2(t-1)} > (\varphi(m) + p^{t-1})d_b. \tag{19}$$

Demostración. Como $a \geq t$, entonces:

$$x \equiv 0(\text{mod } p) \Leftrightarrow x^a \equiv 0(\text{mod } p^t).$$

De ello se deduce que la mayor cantidad de elementos en E cuando $x \equiv 0(\text{mod } p)$, se obtiene cuando $-c$ es un resto de r_b-ésima potencia mod m, pues en otro caso no existirían elementos de E con $x \equiv 0(\text{mod } p)$. Se conoce que la cantidad de múltiplos de p en $\mathbb{Z}_m$ es p^{t-1} y, aplicando el **Teorema 3**, se sabe que:

$$y^b \equiv -c(\text{mod } m), \text{tiene exactamente } d_b \text{soluciones en } \mathbb{Z}_m.$$

Por tanto, la cantidad máxima de elementos de E con $x \equiv 0(\text{mod } p)$ es:

$$p^{t-1}d_b.$$

Si $(x,p) = (x,m) = 1$ y c no es resto de a-ésima potencia en mod p, entonces $(y,p) = (y,m) = 1$ para que existan elementos en E con $(x,m) = 1$. Como $(x,m) = (y,m) = 1$, se puede trabajar con r_a y r_b en vez de con a y b. Luego, el máximo valor de $|E|$ se obtendría si cada valor de $x^{r_a} - c$ es un resto de r_b-ésima potencia en $(\text{mod } m)$, y como $(x,p) = (x,m) = 1$ se tiene que existen $\varphi(m)$ valores generados por $x^{r_a} - c$. Por el teorema 3, por cada uno de esos $\varphi(m)$ valores de x (si siempre generan r_b-ésima potencias en $x^{r_a} - c$) existen exactamente d_b, $y \in \mathbb{Z}_m$ tales que:

$$(x^{r_a} - c) \equiv y^{r_b}(\text{mod } m).$$

Por tanto, la cantidad máxima de elementos en E tales que $(x,m) = (x,p) = 1$ que se puede alcanzar es $\varphi(m)(d_b)$. Entonces, el máximo valor que puede alcanzar $|E|$ es:

$$\varphi(m)(d_b) + p^{t-1}d_b = p^t d_b.$$

Por la demostración desarrollada en el teorema 14 se conoce que:

$$\frac{\varphi(m)}{2p} \geq d_b,$$

$$\Rightarrow \frac{\varphi(m)^2}{2p} \geq \varphi(m)d_b. \tag{20}$$

Aplicando las condiciones del problema, se puede notar que:

$$p^{t-1} > p^{t-2}(p-1) = \frac{\varphi(m)}{p} \geq d_a > d_b.$$

$$\Rightarrow p^{2(t-1)} > p^{t-1}d_b. \tag{21}$$

Por tanto, sumando las desigualdades obtenidas en (20) y (21), se obtiene que:

$$\frac{\varphi(m)^2}{2p} + p^{2(t-1)} > (\varphi(m) + p^{t-1})d_b.$$

■

Subcaso 1.2.2: c es resto de a-ésima potencia en módulo p.

Teorema 17 *Sea $x \in \mathbb{Z}_m$ tal que:*

$$x^a \equiv c(\text{mod } p).$$

Entonces, se tiene que:

$$(x,y) \in E \Rightarrow x^a \equiv c(\text{mod } m).$$

Demostración. Se puede notar que:

$$[x^a \equiv c(\text{mod } p) \wedge (x,y) \in E] \Rightarrow y \equiv 0(\text{mod } p),$$

$$\Rightarrow y^b \equiv 0(\text{mod } m),\ \text{pues } b \geq t,$$

$$\Rightarrow x^a \equiv c(\text{mod } m),\ \text{ya que } (x,y) \in E.$$

■

Teorema 18 *Para el Subcaso 1.2.2 el valor máximo que puede alcanzar el cardinal de E es:*

$$(\varphi(m) - d_a)d_b + (d_a + d_b)p^{t-1}. \tag{22}$$

Demostración. Por el teorema 17, para obtener pares ordenados $(x,y) \in E$ con $x^a \equiv c(\text{mod } p)$, se debe garantizar que c sea resto de a-ésima potencia en módulo m.

Por el teorema 3, la ecuación $x^a \equiv c(\text{mod } m)$ tiene exactamente d_a soluciones en $\mathbb{Z}_m$. Por tanto, la cantidad de pares ordenados $(x,y) \in E$ con $x^a \equiv c(\text{mod } m)$, es:

$$d_a p^{t-1}. \tag{23}$$

Por la demostración del teorema 16, se conoce que la mayor cantidad de pares ordenados $(x,y) \in E$ con $(x,p) = (x,m) = 1$ es:

$$d_b p^{t-1}. \tag{24}$$

Falta maximizar el número de pares ordenados $(x,y) \in E$ con $(x,p) = (x,m) = 1$ y $x^a \not\equiv c(\text{mod } m)$. Para esto, deben ser a y c tales que todos los valores de $x^a - c$, con x bajo las condiciones anteriores, sean restos de r_b-ésimas potencias en $mod(m)$. Aplicando, el teorema 3, se obtiene que existen $\varphi(m) - d_a$ valores de $x \in \mathbb{Z}_m$ tal que:

$$(x,m) = 1, \text{ y } x^a \not\equiv c(\text{mod } m).$$

Por tanto, aplicando razonamientos análogos a los casos anteriores, por el teorema 3 se tiene que el máximo número de pares ordenados de E bajo estas condiciones es:

$$(\varphi(m) - d_a)d_b. \tag{25}$$

Sumando las expresiones (23), (24) y (25) se obtiene que el valor máximo que puede alcanzar el cardinal de E es:

$$(\varphi(m) - d_a)d_b + (d_a + d_b)p^{t-1}.$$

■

Para demostrar que el valor máximo del cardinal de E para este subcaso, planteado en el teorema 18, es menor que el máximo para el Caso 1.1 se demuestra el siguiente lema.

Lema 19 *Si* $\frac{\varphi(m)}{2p} > d_b$, *se cumple que:*

$$\frac{\varphi(m)^2}{2p} - \left(\frac{\varphi(m)}{p}\right) d_a \geq (\varphi(m) - d_a)d_b. \tag{26}$$

Demostración. Se puede notar que:

$$\frac{\varphi(m)^2}{2p} - \left(\frac{\varphi(m)}{p}\right) d_a \geq (\varphi(m) - d_a)d_b.$$

$$\Leftrightarrow \varphi(m)\left(\frac{\varphi(m)}{2p} - d_b\right) \geq d_a\left(\frac{\varphi(m)}{p} - d_b\right). \tag{27}$$

Como se conoce que $\frac{\varphi(m)}{p} \geq d_a$, para demostrar la desigualdad planteada en (27), basta probar que:

$$\varphi(m)\left(\frac{\varphi(m)}{2p} - d_b\right) \geq \frac{\varphi(m)}{p}\left(\frac{\varphi(m)}{p} - d_b\right). \tag{28}$$

Simplificando algebraicamente, se obtiene que la desigualdad expresada en (28), equivale a:

$$\frac{p^{t-2}(p-2)}{2} \geq d_b. \tag{29}$$

Ahora la demostración se dividen tres casos, dependiendo del primo impar p que define a m.

- $p = 3$: Con simples cálculos utilizando las condiciones del problema, se comprueba que si $t = 2$, el valor máximo de $|E|$ planteado en el teorema 18, es menor que el máximo para el Caso 1.1. Por lo cual, se considera $t \geq 3$. Entonces, se tiene que $m = 3^t$. Aplicando razonamientos análogos a los utilizados para probar que $\frac{\varphi(m)}{2p} \geq d_b$, y teniendo en cuenta que en este caso se tiene como condición que $\frac{\varphi(m)}{2p} > d_b$, se obtiene que:

  $$\frac{\varphi(m)}{2p} = 3^{t-2} > d_b \Rightarrow 3^{t-3} \geq d_b.$$

  Pero se puede notar que:

  $$\frac{p^{t-2}(p-2)}{2} = \frac{3^{t-2}}{2} > 3^{t-3} \geq d_b.$$

  Quedando demostrada la desigualdad de (29) para este caso.

- $p \equiv 1(\text{mod } 3)$: Como p es primo, entonces $p \geq 7$. Como $p \equiv 1(\text{mod } 3)$, aplicando razonamientos análogos a los utilizados para probar que $\frac{\varphi(m)}{2p} \geq d_b$, se obtiene que:

  $$\frac{\varphi(m)}{2p} > d_b \Rightarrow \frac{\varphi(m)}{3p} = \frac{p^{t-2}(p-1)}{3} \geq d_b.$$

  Entonces, para demostrar la desigualdad planteada en (29) bastaría probar que:

  $$\frac{p^{t-2}(p-2)}{2} \geq \frac{p^{t-2}(p-1)}{3}.$$

  $$\Leftrightarrow 3(p-2) \geq 2(p-1).$$

  $$\Leftrightarrow p \geq 4.$$

  Quedando así demostrada la desigualdad, pues $p \geq 7$.

- $p \equiv 2(\text{mod } 3)$: Como p es primo, entonces $p \geq 5$. Siendo d el menor divisor de $\frac{\varphi(m)}{p}$, se puede notar que:

  $$\frac{\varphi(m)}{2p} > \frac{\varphi(m)}{3p} > \frac{\varphi(m)}{dp} \geq d_b, \text{ ya que .}$$

  $$d > 3 \text{ por ser } p \equiv 2(\text{mod } 3).$$

Entonces, por la demostración realizada para el caso $p \equiv 1 (\mathrm{mod}\ 3)$, se obtiene que:

$$\frac{p^{t-2}(p-2)}{2} \geq \frac{\varphi(m)}{3p} > d_b.$$

Por tanto, ha quedado demostrada la desigualdad (29) para cada caso posible, la cual es una condición suficiente para que se cumpla (26) como ya se demostró.

■

Teorema 20 *Se cumple que:*

$$\frac{\varphi(m)^2}{2p} + p^{2(t-1)} > (\varphi(m) - d_a)d_b + (d_a + d_b)p^{t-1}. \quad (30)$$

Demostración. Teniendo en cuenta la acotación de d_b, esta demostración se divide en dos partes.

1. $d_b = \frac{\varphi(m)}{2p}$.

   Sea S_m tal que:

   $$S_m = \left(\varphi(m) - \frac{\varphi(m)}{p}\right)\left(\frac{\varphi(m)}{2p}\right) + \left(\frac{\varphi(m)}{p} + \frac{\varphi(m)}{2p}\right)p^{t-1}.$$

   Se conoce que d_a es un divisor de $\varphi(m)$ y que se cumple que:

   $$\frac{\varphi(m}{p} \geq d_a > d_b = \frac{\varphi(m)}{2p}.$$

   Entonces, se tiene que:

   $$d_a = \frac{\varphi(m)}{p}$$

   Por tanto, la desigualdad planteada en (30) se tranforma en:

   $$\frac{\varphi(m)^2}{2p} + p^{2(t-1)} \geq S_m.$$

   Reduciendo algebraicamente, se obtiene que:

   $$\frac{\varphi(m)^2}{2p} + p^{2(t-1)} \geq S_m,$$

   $$\Leftrightarrow p^{t-3}(p-1)^2 + 2p^{t-1} > 3p^{t-2}(p-1),$$

   $$\Leftrightarrow (p-1)^2 + 2p^2 > 3p(p-1),$$

   $$\Leftrightarrow p + 1 > 0.$$

   Quedando así demostrada la desigualdad (30) para este caso.

2. $\frac{\varphi(m)}{2p} > d_b$.

   Como d_b es divisor de $\varphi(m)$, para este caso se obtiene que:

   $$\frac{\varphi(m)}{3p} \geq d_b. \quad (31)$$

   Por el Lema 19 se conoce que:

   $$\frac{\varphi(m)^2}{2p} - \left(\frac{\varphi(m)}{p}\right)d_a \geq (\varphi(m) - d_a)d_b.$$

   Por tanto, para demostrar la desigualdad expresada en (30), basta probar que:

   $$\frac{\varphi(m)}{p}d_a + p^{2(t-1)} \geq (d_a + d_b)p^{t-1}. \quad (32)$$

   Simplificando, se tiene que (32) se cumple si y solo si:

   $$p^t \geq d_a + d_b p. \quad (33)$$

   Se tiene que:

   $$\frac{\varphi(m)}{p} = p^{t-2}(p-1) \geq d_a,$$

   $$\frac{\varphi(m)}{3p} = \frac{p^{t-2}(p-1)}{3} \geq d_b.$$

   Entonces, para demostrar (33), basta probar:

   $p^t \geq p^{t-2}(p-1) + \frac{p^{t-1}(p-1)}{3}$, y esto se cumple si y solo si,

   $$3p^2 \geq (p-1)(p+3),$$

   $$\Leftrightarrow \left(p - \frac{1}{2}\right)^2 \geq -\frac{5}{4}.$$

■

Entonces, se concluye que el máximo valor que puede alcanzar el cardinal del conjunto E en cualquier subcaso del Caso 1.2 es siempre menor que el valor máximo que alcanza en el Caso 1.1. Por lo cual, el problema de los reducidos catalanes ha quedado resuelto cuando m no es primo.

Teorema 21 *El valor máximo del cardinal del conjunto E para el Caso 1 es:*

$$p^{2(t-1)} + \frac{\varphi(m)^2}{2p} = \frac{p^{2t-3}(p^2+1)}{2}. \quad (34)$$

Las condiciones necesarias y suficientes para alcanzar dicho máximo son:

1. $c \equiv 0 (\mathrm{mod}\ m)$.
2. $min\{a,b\} \geq t$.
3. $(\varphi(m), b) = (\varphi(m), r_b) = \frac{\varphi(m)}{2p} = \frac{p^{t-2}(p-1)}{2}$.

2.2 Caso 2: m es primo ($t = 1$)

El caso $m = 3$ se deja como ejercicio al lector. Para el análisis del Caso 2 se utiliza la misma notación que se introdujo en el Caso 1, así como no se desarrollan las demostraciones que sean idénticas o análogas a las realizadas en dicho caso.

Sea $m = q$ y p el mayor divisor primo de $\varphi(m)$. Como m es primo se tiene que:

$$\varphi(m) = \varphi(q) = q - 1.$$

De igual forma que el Caso 1, el Caso 2 se divide en dos casos, pues los valores de máximo para el cardinal de E varían dependiendo del término independiente c.

2.2.1 Caso 2.1: $c \equiv 0 (\mathrm{mod}\ q)$

Definición 22 *Sea q un número primo y p el mayor factor primo de $\varphi(q)$. Se dice que q satisface la condición de máximo si el menor divisor $(d > p)$ de $\varphi(q)$ cumple que:*

$$2p > d. \tag{35}$$

Aplicando razonamientos análogos a los desarrollados en el Caso 1.1, se obtiene la solución para el Caso 2.1.

Teorema 23 *Si el número primo q dado satisface la condición de máximo entonces el mayor valor que puede alcanzar el cardinal de E es:*

$$\frac{\varphi(q)^2}{d} + 1;\ 2p > d > p \text{ y divisor de } \varphi(q). \tag{36}$$

La condición necesaria y suficiente para alcanzar el máximo en este caso es:

1. $d_b = (\varphi(q), b) = \frac{\varphi(q)}{d} = \frac{q-1}{d}$.

En otro caso, el máximo valor del cardinal de E es:

$$\frac{\varphi(q)^2}{2p} + 1. \tag{37}$$

Y la condición necesaria y suficiente para alcanzar el máximo es:

2. $d_b = (\varphi(q), b) = \frac{\varphi(q)}{2p} = \frac{(q-1)}{2p}$.

2.2.2 Caso 2.2: $(c, m) = 1$.

Se demuestra que el máximo valor de $|E|$ es mayor en este caso que en el Caso 2.1, así como se obtienen las condiciones necesarias y suficientes para alcanzar dicho valor, quedando así resuelto el problema de los reducidos catalanes cuando m es primo. Para ello, se divide en dos subcasos el Caso 2.2 de forma análoga a lo realizado para el Caso 1.2.

Subcaso 2.2.1: $x \equiv 0 (\mathrm{mod}\ q)$.

Teorema 24 *Si el número primo q dado satisface la condición de máximo (existe d que satisface (35)), entonces la mayor cantidad de $(x, y) \in E$ para este subcaso es:*

$$\frac{\varphi(q)}{d}. \tag{38}$$

Las condiciones necesarias y suficientes para alcanzar este valor es:

1. *$-c$ es resto de r_b-ésima potencia módulo q.*
2. $d_b = (\varphi(q), b) = \frac{\varphi(q)}{d} = \frac{q-1}{d}$.

En otro caso, el máximo valor es:

$$\frac{\varphi(q)}{2p}. \tag{39}$$

Y las condiciones necesarias y suficientes para alcanzar el máximo es:

3. *$-c$ es resto de r_b-ésima potencia módulo q.*
4. $d_b = (\varphi(q), b) = \frac{\varphi(q)}{2p} = \frac{(q-1)}{2p}$.

Demostración. Se puede notar que si $(x, y) \in E$ en este subcaso, entonces x es cero, ya que $x \in \mathbb{Z}_q$. Para $(x, y) \in E$ en este subcaso, y debe ser primo relativo con q, pues $(c, q) = 1$. Por tanto, análogamente a las demostraciones realizadas previamente, se trabaja con r_b en lugar de b.

El número de $(x, y) \in E$ para este subcaso es igual al número de soluciones de la ecuación en congruencia:

$$y^{r_b} \equiv -c (\mathrm{mod}\ q). \tag{40}$$

Para que la ecuación (40) tenga solución $-c$ debe ser resto de r_b-ésima potencia en módulo q. Por el teorema 3, se tiene que el número de soluciones de la ecuación (40) es d_b y, por tanto, se debe maximizar este valor. Se conoce que si el primo dado q cumple la condición de máximo el mayor valor de d_b es $\frac{\varphi(q)}{d}$, siendo d el menor divisor mayor que p de $\varphi(q)$ que satisface (35). Por tanto, el número máximo de soluciones de la ecuación (40) es $\frac{\varphi(q)}{d}$, con las condiciones necesarias y suficientes dadas en el teorema.

En el caso que el primo dado q no satisface la condición de máximo se demuestra análogamente que el máximo es $\frac{\varphi(q)}{2p}$, con las condiciones suficientes y necesarias análogas para este caso del primo q. ■

Subcaso 2.2.2: $(x, q) = 1$.

Del Caso 1 se conoce que:

$$\frac{\varphi(q)}{d_a} = h_a.$$

Por tanto, por los teoremas 2 y 3, se tiene que el número de restos diferentes de r_a-ésima potencia es h_a, ya que es el número de soluciones de la ecuación en congruencia:

$$z^{\frac{\varphi(q)}{d_a}} = z^{h_a} \equiv 1 (\text{mod } q). \tag{41}$$

Entonces, sea $R = \{r_1, r_2, ..., r_{h_a}\}$ el conjunto de todos los restos de r_a-ésima potencia.

Teorema 25 *El máximo valor del cardinal de E para este subcaso es:*

$$\frac{\varphi(q)^2}{d}. \tag{42}$$

1. *si q satisface la condición de máximo y d el menor divisor mayor que p ($2p > d > p$):*

$$\frac{\varphi(q)^2}{2p}. \tag{43}$$

2. *si q no satisface la condición de máximo.*

Las condiciones necesarias y suficientes para alcanzar el máximo son:

1. *c no es resto de r_a-ésima potencia en* mod *q.*
2. $h_b \equiv 0 (\text{mod ord}_q(r-c)), \forall r \in R.$
3. $d_b = \frac{\varphi(q)}{d}$ *o* $d_b = \frac{\varphi(q)}{2p}$, *dependiendo si q satisface la condición de máximo.*

Demostración. Para realizar la demostración se divide el cálculo del valor máximo del cardinal de E en dos casos.

- c resto de r_a-ésima potencia en mod q.

Por el teorema 3, se tiene que la siguiente ecuación tiene exactamente d_a soluciones en $\mathbb{Z}_q$:

$$x^{r_a} \equiv c (\text{mod } q). \tag{44}$$

Se puede notar que $(x,y) \in E$ con x que satisface (44) si y solo si:

$$y^{r_b} \equiv 0 (\text{mod } q),$$
$$\Leftrightarrow y = 0, \text{pues } y \in \mathbb{Z}_q.$$

Por tanto, se tienen d_a pares ordenados $(x,y) \in E$ con x que satisface (44).

Por otro lado, para maximizar la cantidad de pares ordenados $(x,y) \in E$ con x que no satisface (44), se debe garantizar que la expresión $x^{r_a} - c$ sólo genere restos de r_b-ésima potencia en mod q. Se puede notar que la cantidad de valores de $x \in \mathbb{Z}_q$ que no satisfacen (44) es $\varphi(q) - d_a$, ya que se trabaja dentro del Subcaso 2.2.2. Por tanto, aplicando el teorema 3 se obtiene que la cantidad de pares ordenados $(x,y) \in E$ con x que no satisface (44), es:

$$(\varphi(q) - d_a) d_b.$$

Entonces, el valor máximo de $|E|$ para este primer caso es:

$$(\varphi(q) - d_a) d_b + d_a.$$

Se puede notar que se maximiza para este caso con $d_b > 1$ y que se cumple que:

$$\varphi(q) d_b > (\varphi(q) - d_a) d_b + d_a. \tag{45}$$

- c no es resto de r_a-ésima potencia en mod q.

Se puede notar que el valor máximo de $|E|$ en este segundo caso se alcanza si para cada uno de los $\varphi(q)$ valores de x, se obtiene un resto de r_b-ésima potencia en la expresión algebraica $x^{r_a} - c$. Por tanto, utilizando las propiedades del orden [6] y el teorema 3, se obtiene que la condición 2 es una condición necesaria para alcanzar el máximo. Además, aplicando el teorema 3 se obtiene que el máximo de $|E|$ será:

$$\varphi(q) d_b.$$

Por tanto, a partir de (45) se puede garantizar que el máximo de $|E|$ para el Subcaso 2.2.2, se alcanza cuando c no es resto de r_a-ésima potencia en mod q. Sólo queda maximizar $\varphi(q) d_b$, pero se conoce que su mayor valor es:

$$\frac{\varphi(q)^2}{d}. \tag{46}$$

1. si q satisface la condición de máximo y d el menor divisor mayor que p ($2p > d > p$),

$$\frac{\varphi(q)^2}{2p}. \tag{47}$$

2. si q no satisface la condición de máximo.

■

Se puede notar que:

$$\frac{\varphi(q)^2}{d} + \frac{\varphi(q)}{d} > \frac{\varphi(q)^2}{d} + 1,$$
$$\frac{\varphi(q)^2}{2p} + \frac{\varphi(q)}{2p} > \frac{\varphi(q)^2}{2p} + 1.$$

Entonces, uniendo los teoremas 24 y 25 se obtiene la solución al problema de los reducidos catalanes para el Caso 2.

Teorema 26 *El valor máximo del cardinal del conjunto E para el Caso 2 es:*

$$\frac{\varphi(q)^2}{d}+\frac{\varphi(q)}{d}. \tag{48}$$

1. *si q satisface la condición de máximo y d el menor divisor mayor que p ($2p > d > p$):*

$$\frac{\varphi(q)^2}{2p}+\frac{\varphi(q)}{2p} > \frac{\varphi(q)^2}{2p}+1. \tag{49}$$

2. *si q no satisface la condición de máximo.*

Las condiciones necesarias y suficientes para alcanzar el máximo son:

- $(c,q)=1$.
- $-c$ *resto de* r_b*-ésima potencia* mod q.
- $c \notin R$.
- $h_b \equiv 0(\text{mod ord}_q(r-c)), \forall r \in R$.
- $d_b = \frac{\varphi(q)}{d}$ *o* $d_b = \frac{\varphi(q)}{2p}$*, dependiendo de si q satisface la condición de máximo.*

3. Conclusiones

En este artículo se resolvió el problema de los reducidos catalanes, tanto para m primo como para m no primo. Para la solución se desarrolló un método demostrativo basado en la conexión de resultados de la teoría de números, específicamente, el teorema de Euler, el teorema de Bézout y la caracterización de los restos de k-ésimas potencias en módulos que admiten raíces primitivas. Por tanto, con este método demostrativo, denominado método Bézout-Euler de las potencias, se generalizó el método Bézout-Fermat, lo cual permitió resolver ecuaciones en congruencia más complejas, así como maximizar su cantidad de soluciones incongruentes.

Agradecimientos

A mi esposa y toda mi familia por su apoyo y respaldo en mi pasión por la Matemática. A la profesora Dra. Rita Roldán por contribuir con sus revisiones al desarrollo inicial de esta investigación. A los profesores que despertaron en mí, desde temprana edad, la pasión por la Teoría de Números.

Suplementos

Este artículo no contiene información suplementaria.

Conflictos de interés

Se declara que no existen conflictos de interés.

Referencias

[1] Andreescu, T., D. Andrica y Z. Feng: *104 Number Theory Problems*. Birkhäuser, 2006. https://link.springer.com/book/10.1007/978-0-8176-4561-8.

[2] Cuevas, J.: *Conjetura de Catalan: Inkeri, Mihailescu y Wieferich*. Tesis de Doctorado, 2023. https://www.mat.uc.cl/~natalia.garcia/catalan-mihailescu.pdf.

[3] Mihailescu, P.: *A cyclotomic investigation of the Catalan-Fermat Conjecture*. Arxiv preprint, página 43, 2013. https://arxiv.org/abs/math/0702766.

[4] Mihailescu, P.: *Improved lower bounds for possible solutions in the Second Case of the Fermat Last Theorem and in the Catalan Equation*. Journal of Number Theory, 225:151–173, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0022314X2100055X.

[5] Muniz, A.: *Como Fermat e Bézout podem salvar o dia*. Eureka!, 12:25–30, 2001.

[6] Roldán, R.: *Introducción a la Teoría de Números*. EDUNIV, 2022.