La Ecuación $x_1^2 + x_2^2 + \cdots + x_n^2 \equiv k \, mod \, p$

J. L. Aguado - J. O. Araujo

Introducción

Existe una fórmula general sobre el número C_F de soluciones en Z_n de una ecuación de congruencia del tipo:

$$F(x_1, \ldots, x_m) \equiv 0 \, mod \, n$$

donde la función F es polinómica. Esta fórmula se expresa habitualmente de la siguiente manera:

$$C_F = \frac{1}{n} \sum_{a=0}^{n-1} \sum_{(x_1,\ldots,x_m) \in Z_n^m} \exp\left(\frac{2\pi i a}{n} F(x_1, \ldots, x_m)\right)$$

Ver por ejemplo [4] y [7].

Sin embargo, debido a su carácter formal, esta expresión es poco práctica para ser aplicada en forma directa en casos concretos.

En este trabajo presentamos una expresión más explícita para el caso de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv k \, mod \, p$$

donde k es un número entero y p es un número primo.

Para $n = 1$ se establece la ley de reciprocidad cuadrática, que brinda un mecanismo práctico para decidir si un número dado es o no residuo cuadrático, hecho fundamental en la resolución de ecuaciones cuadrátricas de congruencias.

Para $n > 1$, se observa que la ecuación siempre tiene solución y se calcula el número de soluciones como el número de ceros de una forma cuadrática en Z_p^n. En otras palabras, se obtiene el número de puntos que tiene una "esfera finita" sobre Z_p.

Con la intención de presentar el material en forma autocontenida se esbozan los elementos de congruencias necesarios para tal fin.

1. Congruencias

Al estudiar la existencia de soluciones enteras de una ecuación algebraica con coeficientes enteros es natural utilizar argumentos de divisibilidad. Este enfoque, además de ser estimulante, es, en muchos casos, suficiente para determinar el problema.

Por ejemplo la ecuación:

$$x^5 - x^3 + 7x - 3 = 0$$

expresada como:

$$x\,(x^4 - x^2 + 7) = 3$$

nos dice que las posibles soluciones enteras sólo pueden ser divisores de 3, como lo establece el conocido criterio de Gauss. Los divisores de 3 son ± 1 ± 3. Una cuenta permite verificar que $\pm 1, \pm 3$ no son solución. Por tanto la ecuación no tiene solución entera.

En la ecuación:

$$x^3 + 2y^3 + 4z^3 - 6xyz = 0 \tag{1}$$

si (x, y, z) es solución entera, entonces x es par, y observando que (1) puede ponerse como:

$$2\left(y^3 + 2z^3 + 4\left(\frac{x}{2}\right)^3 - 6\left(\frac{x}{2}\right)yz\right) = 0$$

vemos que la terna $(y, z, x/2)$ es también solución. Si iteramos el siguiente proceso:

$$\begin{aligned} x &\rightarrow y \\ y &\rightarrow z \\ z &\rightarrow \tfrac{x}{2} \end{aligned}$$

obtenemos las ternas $(z, y/2, x/2)$ y $\frac{1}{2}(x, y, z)$ como nuevas soluciones enteras. En general, tendremos que:

si (x, y, z) *es solución entera de* (1) *entonces* $\frac{1}{2^n}(x, y, z)$ *es solución entera de* (1) *para cada número natural* n.

Esto permite concluir: La única solución entera de (1) es

$$x = 0, y = 0 \quad \text{y} \quad z = 0.$$

En la ecuación:

$$x^2 + 4y = 95 \tag{2}$$

debe ser x impar. Escribimos $x = 4k + r$, donde $r = 1$ ó $r = 3$ y tenemos:

$$16k^2 + 8kr + r^2 + 4y = 4 \times 23 + 3$$

lo que implica que $r^2 - 3$ debe ser múltiplo de 4. Como $r^2 - 3$ es -1 ó 6. Esto es una contradicción que determina la inexistencia de soluciones enteras para (2).

El cálculo del resto de la división por un número entero n de una expresión algebraica, puede ser tratado usando la siguiente propiedad:

los enteros a *y* $a + k\,n$ $(k \in \boldsymbol{Z})$, *tienen el mismo resto al dividirlos por* n

Las congruencias, más que una notación, brindan un modo sistemático para reducir el cálculo de restos de expresiones algebraicas mediante mecanismos que nos son muy familiares.

Definición 1. Fijado un número entero n, diremos que los número a y b en $\boldsymbol{Z}$ son *congruentes módulo* n, o que a *es congruente con* b *módulo* n, si n divide a $a - b$.

La notación utilizada para indicar esta situación es:

$$a \equiv b \, mod \, n$$

La relación a es congruente con b módulo n resulta una relación de equivalencia en $\boldsymbol{Z}$, y se comprueban sin mayor dificultad las siguientes propiedades básicas:

i) Si $a \equiv b \, mod \, n$ *y* $c \equiv d \, mod \, n$ *entonces*:

$$a + c \equiv b + d \, mod \, n \quad y \quad ac \equiv bd \, mod \, n$$

Es decir la congruencia módulo n es una relación de equivalencia compatible con las operaciones de anillo en Z. Esto nos permite afirmar que el cociente $Z_n = Z/\equiv$ es también un anillo conmutativo con las operaciones:

$$[a] + [b] = [a + b] \quad y \quad [a]\,[b] = [a\,b]$$

Siendo $[a]$ la clase de equivalencia de $a \; mod\, n$. Además, no es difícil ver que Z_n es un cuerpo si, y sólo si, n es primo.

Aquí utilizaremos los representantes canónicos: $0, 1, \ldots, n-1$ para describir los elementos de Z_n, aunque, en el caso n impar puede resultar más conveniente utilizar el sitema de representantes $0, \pm 1, \ldots, \pm\frac{n-1}{2}$.

Para un tratamiento más detallado sobre estas estructuras puede consultarse [3].

2. La Ley de Reciprocidad Cuadrática

Sea p un número primo, k un entero. El problema es averiguar si la ecuación:

$$x^2 \equiv k \, mod\, p \tag{3}$$

tiene solución.

Como es el caso $p = 2$ siempre existe solución, en lo que sigue supondremos que p es un primo impar.

Por ejemplo, consideremos la ecuación:

$$x^2 \equiv 139 \; mod\, 11 \tag{4}$$

dado que:

$$139 \equiv 7 \; mod\, 11$$

y que

$$(x + h\,11)^2 = x^2 + 22xh + 121h^2 \equiv x^2 \, mod\, 11$$

vemos que estudiar la existencia de soluciones de la ecuación (4) equivale a estudiar la existencia de soluciones de la *ecuación reducida*:

$$x^2 \equiv 7 mod\, 11 \tag{5}$$

Esta observación es válida en el caso general, es decir, en (3) tanto k como x pueden suponerse recorriendo un sistema de representantes módulo 11.
A partir de la tabla de cuadrados $mod\, 11$:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1

vemos que la ecuación (5) no tiene solución y sólo tendrán solución las ecuaciones para los valores $k = 0, 1, 4, 9, 5$.
No es casual que la tabla anterior, con la exclusión de 0, es simétrica. La razón es que: $10 \equiv -1\ mod 11$, $9 \equiv -2\ mod 11$, etc. Es decir que pudimos haber escrito:

x	0	1	2	3	4	5	-5	-4	-3	-2	-1
x^2	0	1	4	9	5	3	3	5	9	4	1

O bien:

x	0	± 1	± 2	± 3	± 4	± 5
x^2	0	1	4	9	5	3

Definición 2. Un elemento $k \in Z$ se dirá un *cuadrado módulo* p, si la ecuación (3) tiene solución, en caso contrario, se dirá que k es un *no cuadrado módulo* p.

Como ya observamos antes, k puede reemplazarse por cualquier elemento de su clase módulo p. De ahora en más p es un primo impar.
La función $x \to x^2$ de Z_p en Z_p toma un mismo valor en exactamente $\pm x$,

puesto que si recordamos que p es primo tendremos:

$$\begin{aligned} x^2 \equiv y^2 mod\, p &\Leftrightarrow p \mid (x-y)(x+y) \\ &\Leftrightarrow p \mid (x-y) \acute{o} p \mid (x+y) \\ &\Leftrightarrow x \equiv \pm y \, mod\, p \end{aligned}$$

Entonces, el número de cuadrados no nulos en $\boldsymbol{Z}_p$ es $\frac{p-1}{2}$ por ser p impar.
Se sigue que hay $\frac{p-1}{2}+1 = \frac{p+1}{2}$ cuadrados en $\boldsymbol{Z}_p$, y $\frac{p-1}{2}$ no cuadrados en $\boldsymbol{Z}_p$.
Es claro que el producto de cuadrados es un cuadrado, y que el inverso multiplicativo de un cuadrado no nulo es también un cuadrado.
Designemos con $\mathcal{C}$ el conjunto de cuadrados no nulos de $\boldsymbol{Z}_p$ y $\mathcal{N}$ el conjunto de no cuadrados de $\boldsymbol{Z}_p$. Observar que $\boldsymbol{Z}_p = \{0\} \cup \mathcal{C} \cup \mathcal{N}$ y esta unión es disjunta. Además

$$|\mathcal{C}| = |\mathcal{N}| = \frac{p-1}{2} \tag{6}$$

Supongamos $k \neq 0$ en $\boldsymbol{Z}_p$. La aplicación $f_k(x) = k \cdot x$ es una biyección de $\boldsymbol{Z}_p$, en particular inyectiva. Si $k \in \boldsymbol{Z}_p$ y $x \in \mathcal{C}$, entonces la identidad

$$k = (k\,x)(x^{-1})$$

muestra que $k\,x \in \mathcal{C}$, si, y sólo si, $k \in \mathcal{C}$ Consecuentemente $k\,x \notin \mathcal{C}$,si, y sólo si, $k \notin \mathcal{C}$, si, y sólo si, $k \in \mathcal{N}$ (pues $k \neq 0$).
Como f_k es inyectiva y $f_k(0) = 0$, podemos establecer:

$$\begin{aligned} f_k(\mathcal{C}) = \mathcal{C} \quad &\text{y} \quad f_k(\mathcal{N}) = \mathcal{N} \quad \text{si } k \in \mathcal{C} \\ f_k(\mathcal{C}) = \mathcal{N} \quad &\text{y} \quad f_k(\mathcal{N}) = \mathcal{C} \quad \text{si } k \in \mathcal{N} \end{aligned} \tag{7}$$

Supongamos entonces dado k no nulo en $\boldsymbol{Z}_p$, $k = p_1 p_2 \cdots p_s$ donde los p_i son números primos. Entonces, $k \in \mathcal{C}$ si, y sólo si, el número de índices i tales que $p_i \in \mathcal{N}$ es par. En efecto, $f_k = f_{p_1} \circ f_{p_2} \circ \cdots \circ f_{p_s}$, luego:

$$k \in \mathcal{C} \Leftrightarrow \mathcal{C} = f_k(\mathcal{C}) = f_{p_1} \circ f_{p_2} \circ \cdots \circ f_{p_s}(\mathcal{C})$$

En virtud de (7), el número de cambios en la sucesión:

$$\mathcal{C}, f_{p_s}(\mathcal{C}), f_{p_{s-1}}(f_{p_s}(\mathcal{C})), ..., f_{p_1}(f_{p_2}(\cdots(f_{p_s}(\mathcal{C})...)$$

debe ser par.

El problema de determinar si k es un cuadrado en Z_p se reduce a decidir si un número primo $q < p$ es o no un cuadrado en Z_p, este caso será tratado a continuación, luego de efectuar una serie de consideraciones previas.

Los siguientes teoremas inician el camino hacia nuestro propósito:

Teorema 1: *Teorema de Wilson. Si p es un primo, entonces*

$$(p-1)! \equiv -1 mod\, p$$

Corolario 1:

$$c \equiv (-1)^{\frac{p+1}{2}} mod\, p \text{ y, } n \equiv -c \, mod\, p$$

Demostración:

$$-1 \equiv (p-1)! \equiv \prod_{1 \leq i \leq \frac{p-1}{2}} (-i)\, i \equiv (-1)^{\frac{p-1}{2}} \prod_{1 \leq i \leq \frac{p-1}{2}} i^2 \equiv (-1)^{\frac{p-1}{2}} c mod\, p$$

de donde:

$$c \equiv (-1)^{\frac{p+1}{2}} mod\, p$$

Además:

$$c^2 \equiv 1 \, mod\, p$$

Por otra parte, de la identidad:

$$c\, n \equiv (p-1)! \equiv -1$$

resulta:

$$n \equiv c^2\, n \equiv -c \;\; mod\, p$$

□

Teorema 2: *Criterio de Euler*

$$k \in \mathcal{C} \Leftrightarrow k^{\frac{p-1}{2}} \equiv 1 \, mod\, p$$

Demostración:

$$k \in \mathcal{C} \quad \Leftrightarrow f_k(\mathcal{C}) = \mathcal{C} \Leftrightarrow \prod_{x \in \mathcal{C}} (k.x) \equiv c \; mod\, p$$
$$\Leftrightarrow k^{\frac{p-1}{2}}\, c \equiv c \, mod\, p \Leftrightarrow k^{\frac{p-1}{2}} \equiv 1 \; mod\, p$$

□

Como consecuencia del Criterio de Euler se tiene:

Corolario 2:

i) Sea p un primo impar, entonces, $-1 \in \mathcal{C}$ si y sólo si p es de la forma $4m+1$.

ii) Sea p de la forma $4m+3$, si $a^2 + b^2 \equiv 0 \; mod\, p$, entonces $a \equiv 0 \equiv b \, mod\, p$.

Demostración:

i) es consecuencia directa del Teorema 2. Para *ii)*, si $a \not\equiv 0 \, mod\, p$ entonces:

$$\left(\frac{b}{a}\right)^2 \equiv -1 \; mod\, p$$

en contradicción con *i)*.□

Teorema 3: *Lema de Gauss*

Considerando el sistema de restos $\left\{\pm i, 1 \leq i \leq \frac{p-1}{2}\right\}$ y $k \neq 0$ en $\mathbf{Z}_p$, sea:

$$s = |\{i > 0 \,/\, k\, i \equiv -j \; mod\, p, \text{ con } j > 0\}|$$

entonces:

$$k^{\frac{p-1}{2}} \equiv (-1)^s \; mod\, p$$

Demostración:

$$k^{\frac{p-1}{2}} \, (\frac{p-1}{2})! \equiv \prod_{1 \leq i \leq \frac{p-1}{2}} (k\, i) \equiv (-1)^s \, (\frac{p-1}{2})! \, mod\, p$$

En efecto, sólo hay que observar que, salvo signos, la sucesión $k\, i \; mod\, p$, para $i = 1, \ldots, \frac{p-1}{2}$, recorre todos los restos positivos $1, \ldots, \frac{p-1}{2}$. Esto está bien, pues si $k\, i \equiv \pm k\, j \; mod\, p$ para algún par i, j de restos positivos, se tendría $i \equiv \pm j$ lo que sólo es posible si $i = j$.□

Definición 3. Definimos el *símbolo de Legendre* $\left(\frac{k}{p}\right)$ como:

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & si \quad k \in \mathcal{C} \\ -1 & si \quad k \in \mathcal{N} \end{cases}$$

Las siguientes identidades pueden establecerse sin mayor dificultad:

$$\begin{array}{lll} i) & \left(\frac{kl}{p}\right) & = \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) \\ ii) & \left(\frac{kl^2}{p}\right) & = \left(\frac{k}{p}\right) \end{array}$$

A partir del lema de Gauss es posible obtener una expresión más explícita para el símbolo de Legendre. En efecto, sean k y x en $\mathbb{Z}$ tales que $p \nmid k$ y $1 \leq x \leq \frac{p-1}{2}$.
Ponemos:

$$k\,x = m\,p + r \quad con\ 1 \leq r < p$$

entonces tenemos:

$$\left[\frac{2kx}{p}\right] = \left[\frac{2mp + 2r}{p}\right] = 2m + \left[\frac{2r}{p}\right]$$

Ahora observamos que:

$$\left[\frac{2r}{p}\right] = \begin{cases} 0 & si \quad 0 < r < \frac{p}{2} \\ \\ 1 & si \quad \frac{p}{2} < r < p \end{cases}$$

Luego $\left[\frac{2kx}{p}\right]$ es par si $0 < r < \frac{p}{2}$ e impar si $\frac{p}{2} < r < p$
De este modo se tiene:

$$\left(\frac{k}{p}\right) \equiv (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2kx}{p}\right]} \quad mod\, p \tag{8}$$

Conservando las notaciones precedentes vamos a establecer el siguiente resultado comocido como *ley de reciprocidad cuadrática.*

Teorema 4:

Si p y q son números primos impares, se tiene:

$$\begin{array}{lrcl} i) & \left(\frac{2}{p}\right) & = & (-1)^{\frac{p^2-1}{8}} \\ ii) & \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) & = & (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}} \end{array}$$

3. Caso $n = 2$

En general, si c_k es el número de soluciones de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv k \mod p$$

resulta $c_k = c_h$ si $h, k \in \mathcal{C}$, ó si $h, k \in \mathcal{N}$, dado que en ambos casos:

$$h = a^2\, k$$

puesto que $(a\, x_1, a\, x_2, .., a\, x_n)$ recorre el conjunto de soluciones de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv h \mod p$$

cuando $(x_1, x_2, ..., x_n)$ recorre el conjunto de soluciones de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv k \mod p$$

Veamos que si $n \geq 2$, la ecuación precedente siempre tiene solución. Esto es claro si $k \in \mathcal{C}$ ó $k = 0$. Por otra parte, la suma de dos cuadrados no puede ser siempre un cuadrado, ya que en tal caso, $2 = 1 + 1 \in \mathcal{C}$, $3 = 2 + 1 \in \mathcal{C}$, etcétera, daría que $\mathbb{Z}_p \subseteq \mathcal{C} \cup \{0\}$. Se sigue que existe $h \in \mathcal{N}$ que es suma de dos cuadrados, o sea:

$$h = a^2 + b^2 = a^2 + b^2 + 0^2 + \cdots + 0^2$$

En consecuencia, si $n \geq 2$ se tiene $c_k \neq 0$ para todo $k \in \mathcal{N}$.

Consideremos la ecuación:

$$x^2 + y^2 \equiv k \mod p$$

Si $k = 0$, tenemos:

$$x^2 \equiv (-1)\ y^2 \mod p$$

Si $p \equiv 3 \mod 4$ se sigue que $(0,0)$ es la única solución. Si $p \equiv 1 \mod 4$, entonces $-1 \in C$ y podemos poner $a^2 \equiv -1 \mod p$, luego:

$$x^2 + y^2 \equiv x^2 - a^2\ y^2 \equiv (x - a\ y)\ (x + a\ y) \equiv 0 \mod p$$

Es decir (ay, y) y $(-ay, y)$ con $y \in Z_p$ son todas las soluciones, totalizando $2\ (p-1) + 1 = 2p - 1$ soluciones.
Sea $k \in \mathcal{N}$, $a^2 + b^2 \equiv k \mod p$. A cada solución (x, y) de la ecuación:

$$x^2 + y^2 \equiv 1 \mod p$$

le asociamos el par:

$$x' = a\ x - b\ y \ \ , \ \ y' = b\ x + a\ y$$

Dado que:

$$\det \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a^2 + b^2 \equiv k \not\equiv 0 \mod p$$

la aplicación $(x, y) \to (x', y')$ es inyectiva, y de la identidad:

$$x'^2 + y'^2 = (x^2 + y^2)\ (a^2 + b^2) \equiv k \mod p$$

se tiene $c_1 \leq c_k$. Ahora si $c^2 + d^2 \equiv k^{-1} \mod p$, razonando como antes, si:

$$x' = c\ x - d\ y \ \ , \ \ y' = d\ x + c\ y$$

se tiene:

$$x'^2 + y'^2 \equiv 1 \mod p \ \ si\ x^2 + y^2 \equiv k \mod p$$

luego $c_k \leq c_1$. En conclusión, si $n = 2$, $c_k = c_1$ para todo $k \neq 0$. Teniendo en cuenta que hay p^2 elementos en Z_p^2, obtenemos:

$$p^2 = c_0 + c_1\,(p-1)$$

y se sigue que:

$$c_1 = \begin{cases} p+1 & si \quad p \equiv 3\, mod\, 4 \\ \\ p-1 & si \quad p \equiv 1\, mod\, 4 \end{cases}$$

4. El caso general

Sea ζ la raíz $p-$ésima primitiva de la unidad:

$$\zeta = \cos(\frac{2\pi}{p}) + i\ sen(\frac{2\pi}{p})$$

y consideremos:

$$\alpha = \sum_{x=1}^{p-1} \zeta^{x^2}$$

Se tiene:

$$\begin{aligned} \alpha^2 &= \sum_{x=1}^{p-1}\sum_{y=1}^{p-1} \zeta^{x^2+y^2} = \sum_{x^2+y^2\equiv 0} 1 + \sum_{x^2+y^2\in\mathcal{C}} \zeta^{x^2+y^2} + \sum_{x^2+y^2\in\mathcal{N}} \zeta^{x^2+y^2} \\ &= c_0 + c_1 \sum_{k\in\mathcal{C}} \zeta^k + c_1 \sum_{k\in\mathcal{N}} \zeta^k = c_0 + c_1 \sum_{k\neq 0} \zeta^k \\ &= c_0 - c_1 \end{aligned}$$

y teniendo en cuenta que:

$$c_0 - c_1 = \begin{cases} 1-(p+1) = -p & si \quad p \equiv 3\, mod\, 4 \\ \\ 2p-1-(p-1) = p & si \quad p \equiv 1\, mod\, 4 \end{cases}$$

resulta:

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p$$

Observar que α es un número complejo que verifica $\alpha^2 = \pm p$, es decir α no es racional y además, para $h \in N$:

$$\alpha^{2h} = (-1)^{\frac{(p-1)}{2}h} p^h \quad y \quad \alpha^{2h+1} = (-1)^{\frac{(p-1)}{2}h} p^h \alpha \tag{9}$$

es decir, α^n es entero si n es par, y es α multiplicado por entero cuando n es impar.

Por otra parte:

$$\begin{aligned}
\alpha^n &= \sum_{(x_1,\ldots,x_n)\in Z_p^n} \zeta^{x_1^2+\cdots+x_n^2} \\
&= \sum_{x_1^2+\cdots+x_n^2=0} 1 + \sum_{x_1^2+\cdots+x_n^2\in C} \zeta^{x_1^2+\cdots+x_n^2} + \sum_{x_1^2+\cdots+x_n^2\in \mathcal{N}} \zeta^{x_1^2+\cdots+x_n^2} \\
&= c_0(n) + c_1(n) \sum_{k\in C} \zeta^k + c_g(n) \sum_{k\in \mathcal{N}} \zeta^k \\
&= c_0(n) - c_g(n) + (c_1(n) - c_g(n)) \sum_{k\in C} \zeta^k
\end{aligned}$$

donde $c_0(n), c_1(n)$ y $c_g(n)$ denotan el número de soluciones de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_n^2 \equiv k \ mod\, p$$

para $k = 0, 1, g$ respectivamente siendo g un elemento de $\mathcal{N}$. Así mismo notemos que:

$$\alpha = \sum_{x=1}^{p-1} \zeta^{x^2} = 1 + 2 \sum_{k\in C} \zeta^k$$

es decir:

$$\sum_{k\in C} \zeta^k = \frac{\alpha - 1}{2}$$

Luego:

$$\begin{aligned}
\alpha^n &= c_0(n) - c_g(n) + (c_1(n) - c_g(n)) \left(\tfrac{\alpha-1}{2}\right) \\
&= c_1(n) - c_g(n) 2\,\alpha + 2\,c_0(n) - c_1(n) - c_g(n) 2
\end{aligned}$$

y a partir de (9) se tiene:

$$\begin{array}{l}\text{si } n \text{ es par} \\ c_1(n) - c_g(n) = 0 \qquad \text{y} \quad 2\,c_0(n) - c_1(n) - c_g(n) = 2\left((-1)^{\frac{p-1}{2}}.p\right)^{\frac{n}{2}} \\ \text{si } n \text{ es impar} \\ 2\,c_0(n) - c_1(n) - c_g(n) = 0 \quad \text{y} \quad c_1(n) - c_g(n) = 2\left((-1)^{\frac{p-1}{2}}.p\right)^{\frac{n-1}{2}}\end{array} \tag{10}$$

Por otra parte, clasificando los elementos de $\boldsymbol{Z}_p^n$ según los valores de:

$$x_1^2 + x_2^2 + \cdots + x_n^2$$

y teniendo en cuenta (6) se tiene:

$$p^n = c_0(n) + \frac{p-1}{2}\,c_1(n) + \frac{p-1}{2}\,c_g(n) \tag{11}$$

A partir de (10) y (11) tenemos los sistemas lineales:

$$\begin{bmatrix} 0 & 1 & -1 \\ 2 & -1 & -1 \\ 2 & p-1 & p-1 \end{bmatrix} \begin{bmatrix} c_0(n) \\ c_1(n) \\ c_g(n) \end{bmatrix} = \begin{bmatrix} 0 \\ 2\left((-1)^{\frac{p-1}{2}}.p\right)^{\frac{n}{2}} \\ 2p^n \end{bmatrix} \quad \text{si } n \text{ es par}$$

$$\begin{bmatrix} 0 & 1 & -1 \\ 2 & -1 & -1 \\ 2 & p-1 & p-1 \end{bmatrix} \begin{bmatrix} c_0(n) \\ c_1(n) \\ c_g(n) \end{bmatrix} = \begin{bmatrix} 2\left((-1)^{\frac{p-1}{2}}.p\right)^{\frac{n-1}{2}} \\ 0 \\ 2p^n \end{bmatrix} \quad \text{si } n \text{ es impar}$$

resolviendo estos sistemas podemos establecer el siguiente resultado:

Teorema 5:

si n es par:

$$c_0(n) = (-1)^{\frac{(p-1)\,n}{4}}(p-1)\,p^{\frac{n-2}{2}} + p^{n-1}$$

$$c_g(n) = c_1(n) = (-1)^{\frac{(p-1)\,n}{4}+1}\,p^{\frac{n-2}{2}} + p^{n-1}$$

si n es impar:

$$c_0(n) = p^{n-1}$$

$$c_1(n) = (-1)^{\frac{(p-1)(n-1)}{4}} p^{\frac{n-1}{2}} + p^{n-1}$$

$$c_g(n) = (-1)^{\frac{(p-1)(n-1)}{4}+1} p^{\frac{n-1}{2}} + p^{n-1}$$

Referencias:

[1] Apostol, T. M. *Introducción a la Teoría de Analítica de Números.* Editorial Reverté, 1980.

[2] Gavrilov, G. P., Sapozhenko, A. A. *Problemas de Matemática Discreta.* Editorial MIR, 1980.

[3] Le Veque, W. J. *Teoría Elemental de los Números.* Herrero Hnos. Mexico. 1968.

[4] Narkiewicz, W. *Number Theory.* World Scientific Publishing Co. 1983.

[5] Riesel, Hans. *Prime Numbers and Computer Methods for Factorization.* Birkhäuser Boston, inc. Progress in Mathematics Vol. 57, 1985.

[6] Samuel, Pierre. *Teoría Algebraica de Números.* Ediciones Omega, Barcelona, 1972.

[7] Vinogradov, I. *Fundamentos de la Teoría de los Números.* Editorial MIR, 1977.

Facultad de Ciencias Exactas. Universidad Nacional del Centro de la Provincia de Buenos Aires. Campus Universitario. Paraje Arroyo seco. Tandil.