# Número de Waring en Cuerpos Finitos

Zahir Mejias
Jean-Karlo Accetta

Sujeta a cambios, 2010

**Resumen**

El número de Waring es el número mínimo de variables que necesita una ecuación de la forma $x_1^d + x_2^d + ... + x_n^d = \beta$ para que tenga solución en los números naturales para cualquier valor de la constante en los números naturales. Trabajamos en el estudio de generalizaciones de este problema cuando los valores de la constante y las soluciones se definen en cuerpos finitos. Hemos desarrollado un programa para calcular el número de Waring, y con el mismo hemos mejorado en resultados anteriormente publicados.

## 1. Introducción

Un problema importante de la teoría de números es encontrar las propiedades necesarias para que un sistema de ecuaciones tenga solución en un conjunto dado. El problema del número de Waring consiste en hallar el número mínimo de variables necesarias para que la siguiente ecuación tenga soluciones para cualquier constante $\beta$ en los números naturales.

$$x_1^d + x_2^d + ... + x_n^d = \beta. \tag{1}$$

Como referencia principal utilizamos el artículo [2] en el cual se trabaja bajo cuerpos finitos $\mathbb{F}_{p^f}$ donde $p$ es primo, pero nosotros nos enfocamos en cuerpos finitos $\mathbb{Z}_p$. Entonces consideramos la ecuación con constante y soluciones en $\mathbb{Z}_p$. El número de Waring de la ecuación 1 lo denotamos por $\delta(d, p)$.

En este artículo estudiamos teoremas que nos permiten el cálculo del número de Waring para ciertos valores de $p$ y $d$ y construimos una tabla de los números de Waring determinados con los teoremas. Usando programas en C++ calculamos los resultados que faltan para llenar nuestra tabla de números de Waring. Tenemos una segunda tabla en donde usamos el Teorema 4.3 y Remark 5.1 del artículo [2] en donde, dado un valor específico de $d$ con $3 \leq d \leq 12$, se presenta una cota inferior para $p_0$ tal que $\delta(d, p) = 2$ para toda $p \geq p_0$. Para algunos valores de $d$, el valor de $p_0$ conocido no es la cota inferior mínima. Para cada $d$, queremos hallar valores de $p$ menores que esa $p_0$ ya establecida, y poder hallar la cota inferior correspondiente a cada $d$. En la sección de Resultados, presentamos algunas mejoras a las cotas inferiores antes conocidas, incluyendo cotas inferiores mínimas.

# 2. Preliminares

Introducimos teoría que utilizaremos para trabajar en cuerpos finitos y la manipulación de las ecuaciones. Comenzamos definiendo lo que son anillos, luego definimos los cuerpos y finalmente definimos lo que son cuerpos finitos, que es donde estaremos trabajando. Un anillo es un conjunto no-vacío $R$ con dos operaciones, usualmente suma y multiplicación, que satisface los siguientes axiomas:

1. Si $a \in R$ y $b \in R$, entonces $a + b \in R$. (Clausura aditiva)
2. $a + (b + c) = (a + b) + c$ (Suma asociativa)
3. $a + b = b + a$ (Suma conmutativa)
4. $\exists\ 0_R \in R$ tal que $a + 0_R = a = 0_R + a$ (Identidad aditiva)
5. $\forall\ a \in R$, la ecuación $a + x = 0_R$ tiene soluciones en $R$.
6. Si $a \in R$ y $b \in R$, entonces $ab \in R$. (Clausura multiplicativa)
7. $a(bc) = (ab)c$ (Multiplicación asociativa)
8. $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$ (Identidad multiplicativa)

   Si, en adición, el anillo satisface las siguientes propiedades, a la estructura se le llama un cuerpo.

9. $ab = ba \ \forall \ a, b \in R$ (Multiplicación conmutativa)

10. $a1_R = a = 1_R a \ \forall \ a \in R$ (Identidad multiplicativa)

11. Para $a, b \in R$ y $ab = 0_R$, entonces $a = 0_R$ ó $b = 0_R$ (Dominio Integral)

12. Para cada $a \neq 0_R$, las ecuaciónes $ax = 1_R$ y $xa = 1_R$ tienen soluciones en $R$. (Anillo de división)

Un cuerpo finito $\mathbb{F}_q$ es un cuerpo con un número finito de elementos $q = pr$ con $p$ primo y $r \in \mathbb{N}$. Definimos $\mathbb{F}_q^*$ como $\mathbb{F}_q \backslash \{0\} = \{\alpha^0, \alpha^1, ..., \alpha^{q-2}\}$, y llamamos a $\alpha$ una raíz primitiva donde $\alpha$ genera a todos los elementos de $\mathbb{F}_q^*$.

Sea $\mathbb{Z}_p$ un cuerpo con $p$ elementos y las operaciones de suma y multiplicación módulo $p$. Por ejemplo, considere $\mathbb{Z}_5$ y $\alpha = 2$. Note que $\alpha$ es una raí primitva de $\mathbb{Z}_5$ porque $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. Por lo tanto, $\alpha$ genera a $\mathbb{Z}_5$.

**Proposición 1.** *Sea $\alpha$ una raíz primitiva de $\mathbb{F}_q$. Entonces $q - 1$ es el entero menor positivo tal que $\alpha^{q-1} = 1$.*

# 3. Teoremas y Lemas

A continuación, presentamos varios teoremas y lemas estudiados. Las mismas nos facilitan los cálculos de varios resultados; de tal manera, obtenemos números de Waring para ciertos sistemas con ciertas condiciones de tan sólo ver qué teorema le aplica. Comenzamos con los más sencillas y luego desarrollando otras más complejas. Siempre asumimos que $p$ es un número primo y $d$ es un exponente menor que $p$.

**Lema 1.** *Sea $\mathbb{Z}_p$ el cuerpo finito con $p$ elementos y $\alpha \in \mathbb{Z}_p$. Entonces $x^d = \beta$ tiene solución en $\mathbb{Z}_p$ sí y sólo sí $\beta^{q-1/j} = 1$ donde $j = dmc(d, p-1)$.*

*Demostración.* Este teorema es la Proposición 7.1.2 en [5] para cuerpos finitos de orden $p$. □

**Teorema 1.** Teorema Pequeño de Fermat. *Si $p$ es un número primo y $a \in \mathbb{N}$, entonces $a^p \equiv a(mod p)$*

**Teorema 2.** *Sea $p$ primo. Entonces $\delta(d,p) = 1 \iff dmc(d, p-1) = 1$*

*Demostración.* Supongamos que $\delta(d,p) = 1$. Entonces $x^d = \beta$ tiene solución para toda $\beta \in \mathbb{Z}_p$. Por el Lema 1, tenemos que $\beta^{p-1/j} = 1$ para toda $\beta \in \mathbb{Z}_p^*$ donde $j = dmc(d, p-1)$. En particular, si $\beta$ es raíz primitiva de $\mathbb{Z}_p$, entonces $\alpha^{p-1/j} = 1$. Por otro lado, la Proposición 1 dice que $p-1$ es el entero menor positivo tal que lo anterior es cierto. Por lo tanto, $1 = j = dmc(d, p-1)$.

Ahora queremos demostrar que si $j = dmc(d, p-1) = 1$, entonces $\delta(d,p) = 1$. Supongamos que $j = 1 = dmc(d, p-1)$. Sea $\beta \in \mathbb{Z}_p^*$ y $\alpha$ una raíz primita. Entonces $\beta = \alpha^i$ para $1 \leq i \leq (p-1)$. Como $\alpha^{p-1} = 1$, tenemos que $\beta^{p-1} = (\alpha^i)^{p-1} = (\alpha^{p-1})^i = 1^i = 1$. Por lo tanto, $\beta^{(p-1)/j} = \beta^{(p-1)/1} = 1$. Por el Lema 1, $x^d = \beta$ tiene solución para toda $\beta \in \mathbb{Z}_p^*$ y, como $x^d = 0$ tiene solución para $x = 0$, $x^d = \beta$ tiene solución para toda $\beta \in \mathbb{Z}_p$.

□

**Teorema 3.** $\delta(p-1, p) = p-1$

*Demostración.* Por el Teorema 1 tenemos que $\alpha^{p-1} = 1$ para todo $\alpha \in \mathbb{Z}_p^*$. Ahora queremos hallar $\delta(p-1, d)$ con la ecuación $x_1^{p-1} + x_2^{p-1} + .... + x_n^{p-1} = \alpha$. Sabemos que $x_i^{p-1} = 1$ para todo $\alpha \in \mathbb{Z}_p^*$ y para $1 \leq i \leq n$. Para generar el $\alpha$ más grande, $p-1$, necesitaríamos entonces $p-1$ cantidad de variables iguales a 1. Para elementos menores, simplemente se sustituyen las variables necesarias por ceros. Por lo tanto, $\delta(p-1, p) = p-1$. □

**Teorema 4.** $\delta((p-1)/2, p) = (p-1)/2$

*Demostración.* Por el Teorema 1 tenemos que $\alpha^{p-1} = 1$ para $\alpha \in \mathbb{Z}_p^*$. Esto implica que $\alpha^{p-1} - 1 = 0$. Si escribimos esta ecuación de la forma:

$$(\alpha^{p-1/2})^2 - 1 = 0$$

obtenemos una diferencia de cuadrados $(\alpha^{(p-1)/2} + 1)(\alpha^{(p-1)/2} - 1) = 0$ la cual implica que $\alpha^{(p-1)/2} + 1 = 0$ ó $\alpha^{(p-1)/2} - 1 = 0$. De aquí sacamos que $\alpha^{(p-1)/2} = 1$ ó $\alpha^{(p-1)/2} = -1$. Notando que $\alpha^{(p-1)/2} = \pm 1$, podemos redefinir los elementos de $\mathbb{Z}_p$ como $\mathbb{Z}_p = \{0, 1, 2, ..., [(p-1)/2], -[(p-1)/2], ..., -2, -1\}$. Ahora, con $(p-1)/2$ cantidad de variables podemos hallar todos los resultados; para los positivos utilizamos $\alpha^{p-1/2} = 1$, y para los inversos utilizamos $\alpha^{p-1/2} = -1$. Para hallar $(p-1)/2$, utilizamos esa cantidad de variables iguales a 1; para hallar $-[(p-1)/2]$, utilizamos la misma cantidad

de variables iguales a $-1$.Notar que el mínimo de términos ${x_i}^{(p-1)/2}$ para obtener $(p-1)/2$ es $(p-1)/2$. Para el cero, simplemente utilizamos el caso de $0^{(p-1)/2} = 0$.

□

# 4. Problemas

En la siguiente tabla podemos observar los resultados anteriormente publicados que usaremos como referencia. Se observan las cotas inferiores de $p$, fijando la $d$.

Cuadro 1: Resultados Anteriores

| d | $\delta(d,p) \geq 3$ | $\delta(d,p) = 2^*$ |
|---|---|---|
| 3 | $\delta(d,7) = 3$ | $p \geq 13$ |
| 4 | $\delta(d,29) = 3$ | $p \geq 37$ |
| 5 | $\delta(d,61) = 3$ | $p \geq 71$ |
| 6 | $\delta(d,223) = 3$ | $p \geq 229$ |
| 7 | $\delta(d,127) \geq 3$ | $p \geq 196$ |
| 8 | $\delta(d,761) = 3$ | $p \geq 769$ |
| 9 | $\delta(d,307) \geq 3$ | $p \geq 379$ |
| 10 | $\delta(d,p) = ?$ | $p \geq 5171$ |

*Es necesario que $d|(p-1)$

Los problemas a los que queremos contribuir en este artículo son los siguientes:

1. Hallar valor exacto de $\delta(7,127)$ y $\delta(9,307)$.
2. Para $d \geq 10$, hallar valor máximo de $p$ tal que $d|(p-1)$ y $\delta(10,p) \neq 2$.
3. Completar tablas con todos los valores de $\delta(d,p)$ tal que $d \leq 10$ y $p > d$.

# 5. Algoritmo para calcular el Número de Waring

Hemos desarrollado un programa en C++ que implementa los Teoremas anteriormente presentados para poder calcular el número de Waring. Desarrollamos un algoritmo para los casos donde no se cumplen las condiciones de los teoremas. El programa inicialmente le pide al usuario el número primo y también un exponente menor que ese primo. Luego el programa corre de la siguiente manera:

**Paso 1.** *Se verifica la condición del Teorema 2. Si se cumple se devuelve que* $\delta(d,p) = 1$*, si no se cumple se procede al paso 2*

**Paso 2.** *Se verifica la condición del Teorema 3. Si se cumple se devuelve que* $\delta(d,p-1) = p-1$*, si no se cumple se procede al paso 3*

**Paso 3.** *Se verifica la condición del Teorema 4. Si se cumple se devuelve que* $\delta((p-1)/2,p) = (p-1)/2$*, si no se cumple se procede al paso 4*

**Paso 4.** *Algoritmo para hallar los números de Waring que no podamos obtener utilizando los teoremas anteriores.*

*Incluimos, también, un algoritmo que hemos desarrollado para hallar los números de Waring para los cuales los teoremas antes mencionados no nos devuelven resultados concretos. El algoritmo funciona, sin entrar en detalles en cuanto al código del mismo, de la siguiente manera:*

1. *Se hace un listado de los números en* $Z_p$ *, dado el número primo* $p$*. Este será el listado de los resultados.*

2. *Se hace un segundo listado, referido como los resultados originales, de los resultados obtenidos con* $\alpha^d$ *para cada* $\alpha \in Z_p$*. Se marcan estos resultados en el listado de resultados, y si alguno se repite sólo se marca una vez. Si ambas listas son iguales, entonces* $\delta(d,p) = 1$*.*

3. *A cada resultado que esté marcado, se le suma cada resultado original, y este nuevo resultado se marca, también, en la lista de resultados.*

4. *Se repite el paso 3 hasta marcar todos los resultados en la lista, y cada repetición indica una variable adicional a la original en la ecuación. Es decir, la cantidad de repeticiones más 1 es el Número de Waring.*

# 6. Resultados

En la siguiente tabla, presentamos las mejoras de los resultados anteriores mostrados en el Cuadro1, donde hallamos el número de Waring de $\delta(7, 127)$ y $\delta(9, 307)$, y además determinamos la cota mínima $p_0$ de $\delta(10, p) = 2$.

Cuadro 2: Resultados

| d | Anteriores | Nuestros |
|---|---|---|
| 7 | $\delta(7, 127) \geq 3$ | $\delta(7, 127) = 3$ |
| 9 | $\delta(9, 307) \geq 3$ | $\delta(9, 307) = 3$ |
| 10 | $\delta(10, p \geq 5171) = 2$ | $\delta(10, p > 911) = 2$ |

*Es necesario que $d|(p-1)$

**Conjetura 1.** *Sea P un número primo y d un exponente entero. El número de waring de p y d es 1, esto es* $\delta(d, p) = 1$ *cuando* $d = [(p-1)/2] + 1$ *y* $(p-1)/2$ *es un número par.*

**Conjetura 2.** *Sea P un número primo y d un exponente entero. El número de waring de p y d es 1, esto es* $\delta(d, p) = 1$ *cuando* $d = [(p-1)/2] + 2$ *y* $(p-1)/2$ *es un número impar.*

En el Cuadro3 ilustramos todos los resultados que logramos obtener a travéz de nuestra investigación. Cabe recalcar que tomamos en cuenta unicamente los primos tales que $d|(p-1)$

Cuadro 3: tabla de resultados de números de waring

| **d** | **Posibles p** | **# W** | **Referencias** |
|---|---|---|---|
| 3 | 7 | 3 | Res. Anteriores |
| | $\geq 13$ | 2 | Res. Anteriores |
| 4 | 13,17 | 3 | Prog. Comp. |
| | 29 | 3 | Res. Anteriores |
| | $\geq$37 | 2 | Res. Anteriores |

Continuado en la página siguiente.....

Cuadro 3 – Continuado

| **d** | **Posibles p** | **# W** | **Referencias** |
|---|---|---|---|
| 5 | 11 | 5 | Teorema 4 |
| | 31,41 | 3 | Prog. Comp. |
| | 61 | 3 | Res. Anteriores |
| | $\geq$71 | 2 | Res. Anteriores |
| 6 | 13 | 6 | Teorema 4 |
| | 19,31 | 4 | Prog. Comp. |
| | $37 \leq p \leq 67$ | 3 | Prog. Comp. |
| | 109,139 | 3 | Prog. Comp. |
| | 223 | 3 | Res. Anteriores |
| | $71 \leq p \leq 103$<br>127<br>$151 \leq p \leq 211$ | 2 | Prog. Comp. |
| | $p \geq 229$ | 2 | Res. Anteriores |
| 7 | 29,43 | 4 | Prog. Comp. |
| | 71,113,127 | 3 | Prog. Comp. |
| | $p \geq 197$ | 2 | Res. Anteriores |
| 8 | 17 | 8 | Teorema 4 |
| | 41 | 4 | Prog. Com. |
| | $73 \leq p \leq 137$<br>233,257<br>337,761 | 3 | Prog. Comp. |
| | 193,239,241,251<br>$263 \leq p \leq 331$<br>$347 \leq p \leq 757$ | 2 | Prog. Comp. |
| | $p \geq 769$ | 2 | Res. Anteriores |
| 9 | 11 | 1 | Teorema 2 |
| | 19 | 9 | Teorema 4 |
| | 73,109,127<br>163,181,199<br>271,307 | 3 | Prog. Comp. |
| | 13,31<br>$43 \leq p \leq 67$<br>$79 \leq p \leq 103$<br>$139 \leq p \leq 157$ | 2 | Prog. Comp. |

Continuado en la página siguiente.....

Cuadro 3 – Continuado

| **d** | **Posibles p** | **# W** | **Referencias** |
|---|---|---|---|
| | 193<br>$211 \leq p \leq 241$<br>277,283<br>$313 \leq p \leq 349$ | | |
| 10 | 11 | 10 | Teorema 3 |
| | 31 | 5 | Prog. Comp. |
| | 41,61 | 4 | Prog. Comp. |
| | $71 \leq p \leq 491$<br>641<br>911<br>$521 \leq p \leq 631$<br>$661 \leq p \leq 881$ | 3 | Prog. Comp. |
| | $p > 911$ | 2 | |

# Referencias


[1] Castro, F. & Rubio, I. "Solvability of Systems of Two Polynomial Equations Over Finite Fields".

[2] Moreno, O. & Castro, F. "On The Calculation and Estimations of Waring Number for Finite Fields". *Seminaires & Congres*. pp 29-40. November 2005.

[3] Castro, F , Rubio, I. , Guan, P. & Figueroa, R. "On systems of linear and diagonal equation of dregree $p^i + 1$ over finite fields of characteristic $p$".*Finite Fields and Their Applications*. pp 648-657. Received 19 March 2007; revised 24 November 2007.

[4] I. Rubio, "Cyclic Decomposition of Monomial Permutation". *MS Thesis, University of Puerto Rico, Río Piedras*. 1988

[5] k. Ireland & M. I. Rosen, "Elements of Number Theory: including an Introduction to Equations over Finite Fields". *1972, Bogden & Quigley, Inc. Publishers*