



Número de Waring en cuerpos finitos

Zahir Mejias, Jean-Karlo Accetta
Departamento de Ciencia de Cómputos
Universidad de Puerto Rico, Recinto de Río Piedras



Resumen

El problema del número de Waring es hallar el número mínimo de variables necesarias para que una ecuación de la forma:

$$x_1^d + x_2^d + \dots + x_n^d = \alpha$$

tenga soluciones en los naturales, $\mathbb{N}$, para cualquier constante $\alpha \in \mathbb{N}$. En nuestro caso, trabajamos con ecuaciones sobre cuerpos finitos F_p , donde p es primo, y denotamos el número de Waring $\delta(d,p)$. Existen teoremas que nos permiten el cálculo del número de Waring para ciertos valores de d y p . Otros teoremas nos dan cotas, dependiendo de d , para valores de p tales que $\delta(d,p) = 2$. En este trabajo, determinamos casos en los cuales el número de Waring no se conoce y usando programas en C++ computamos algunos de estos valores.

Preliminares

Un cuerpo finito es un conjunto finito de elementos que tiene suma y multiplicación, con propiedades similares a los números reales. Nosotros trabajamos con el problema del número de Waring en cuerpos finitos de tamaño p , donde p es primo. De ahora en adelante asumimos que $d \mid (p-1)$.

Ejemplo: Considere:

$$x_1^d + x_2^d + \dots + x_n^d = \alpha \text{ en } \mathbb{Z}_7$$

Note que $x_1^3 + x_2^3 = 2$ no tiene solución en $\mathbb{Z}_7$, pero vemos que $x_1^3 + x_2^3 + x_3^3 = \alpha$ tiene solución para toda $\alpha \in \mathbb{Z}_7$. Por lo tanto $\delta(3,7) = 3$.

Proposición: $\delta(d,p) = 1 \Leftrightarrow d \mid (p-1)$

Proposición: Si $d \mid (p-1)$, entonces $\delta(d,p) \geq 2$.

Lema: $\delta(p-1,p) = p-1$.

Lema: $\delta(\frac{p-1}{2}, p) = \frac{p-1}{2}$

Resultados anteriores

Hay teoremas que nos dan cotas para valores de p tales que $\delta(d,p) = 2$. También se saben algunos valores máximos de p tal que $\delta(d,p) \geq 3$. Con estos resultados podemos construir la siguiente tabla.

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

*Nota: $d \mid (p-1)$

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

Algoritmo

Para resolver estos problemas, desarrollamos un programa en C++ que determina los casos no cubiertos por resultados anteriores y calcula el número de Waring evaluando las ecuaciones directamente:

1. El algoritmo primero verifica si se satisfacen condiciones de lemas o teoremas que nos dan valores de número de Waring.

2. De no satisfacerse ninguna condición:

- Se construyen dos listas: una con las constantes α en $\mathbb{Z}_p$, para marcar cuáles tienen solución; otra para guardar los valores de β^d , $\beta \in \mathbb{Z}_p$
- Se marcan los resultados de β^d en la lista de constantes.
- Se comienza el siguiente ciclo, con $i = 1$, hasta marcar todas las constantes en la lista
 - Por cada repetición, $i = i + 1$
 - Se le suma a cada constante marcada, cada β^d de la segunda lista, y se marca el nuevo resultado en la primera lista
- Cuando hayamos marcado todas las constantes, el resultado es $\delta(d,p) = i$.

Resultados

	Resultados Anteriores	Nuestros resultados
$d=7$	$\delta(7,127) \geq 3$	$\delta(7,127) = 3$
$d=9$	$\delta(9,307) \geq 3$	$\delta(9,307) = 3$
$d=10$	$\delta(10, \geq 5171) = 2$	$\delta(10, \geq 5011) = 2$

Trabajos futuros

1. Seguir llenando tabla de resultados de $\delta(d,p)$
2. Optimizar en C++ el algoritmo de las sumas a las constantes marcadas en $\mathbb{Z}_p$
3. Trabajar con número de Waring para sistemas de ecuaciones
$$x_1^d + x_2^d + \dots + x_n^d = \alpha$$
$$x_1^k + x_2^k + \dots + x_n^k = \beta$$
4. Trabajar con teoremas y lemas para cuerpos de tamaño p^r con $r \geq 2$.

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". Seminares & Congres. pp 29-40. November 2005.
3. Castro, F., Rubio, I., Guan, P. & Figueroa, R. "On systems of linear and diagonal equation of degree $p+1$ 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