EL MÉTODO POLINOMIAL EN TEORÍA DE NÚMEROS ADITIVA

SANDRA PATRICIA BUITRÓN CAICEDO
ALEXANDER CRUZ FAJARDO

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Popayán
Septiembre de 2009

EL MÉTODO POLINOMIAL EN TEORÍA DE NÚMEROS ADITIVA

SANDRA PATRICIA BUITRÓN CAICEDO
ALEXANDER CRUZ FAJARDO

Trabajo de grado presentado como requisito
parcial para optar al título de Matemático

Director:
Dr. CARLOS ALBERTO TRUJILLO SOLARTE

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Popayán
Septiembre de 2009

Agradecimientos

A Dios, a la Universidad, especialmente a nuestro director Dr. Carlos Alberto Trujillo, por su apoyo, consejos, comprensión y su valiosa colaboración que hizo posible alcanzar este propósito. Al Magister Carlos Arturo Rodriguez por sus importantes aportes y observaciones, al comité de seguimiento conformado por los profesores Luz Victoria de la Pava y Favián Arenas por su apoyo y colaboración en el desarrollo de nuestro trabajo.

A Dios por ser la luz de mi vida, a mis Padres Felisa y Roger Antonio, mil gracias por su gran apoyo, sus consejos y por ser el soporte que me ayudó a salir adelante. A mi hermana Lorena por su incondicional apoyo y su valiosa amistad, a mis amigos.

Sandra Patricia

A Dios, en quien depositè mi confianza y siempre me dio fuerzas para seguir adelante, a mis Padres Aquilina y Esteban por ese gran apoyo moral y a mis demás familiares y amigos que me apuraban con su pregunta ¿Cuándo terminas?

Alexander

Introducción

Uno de los propósitos de la Teoría de Números Aditiva es estudiar la cardinalidad de ciertos conjuntos suma con y sin restricciones. Por ejemplo uno de los problemas clásicos en dicha teoría es la conjetura, hoy teorema, de Erdös-Heilbronn la cual establece que si p es un número primo y $A \subseteq \mathbb{Z}p$, $A \neq \emptyset$ entonces

$$|A\hat{+}A| \geq \text{mín}\{p, 2|A| - 3\},$$

donde, $A\hat{+}A = \{x + y : x, y \in A, x \neq y\}$. Esta conjetura fue formulada en los años sesenta, treinta años despúes es demostrada por Días da Silva y Hamidoune; pero es en 1995 que esta conjetura es probada por Alon, Nathanson y Ruzsa utilizando uno de los métodos elementales más importantes: El Método Polinomial.

El Método Polinomial es una técnica que se utiliza para estimar el tamaño de conjuntos suma, es de gran importancia ya que muchos de los resultados de Teoría de Números Aditiva y algunas de sus nuevas extensiones se prueban de una manera elemental utilizando el Método Polinomial. Un ejemplo de ello es el caso de la Conjetura de Erdös-Heilbronn.

Nuestro principal interés es dar a conocer esta técnica, que consiste en resolver problemas ubicándolos en el dominio de los polinomios sobre un campo y utilizando las propiedades elementales de los mismos. Esto se hace asociando un polinomio al conjunto suma (Por ejemplo un polinomio cuyo conjunto de raíces contiene a dicho conjunto.) y luego se utilizan todas las herramientas conocidas de los polinomios para dar solución al problema en cuestión.
El éxito que ha tenido el Método Polinomial en la prueba de varios resultados y su carácter elemental constituyen la razón fundamental que nos motivó a estudiarlo, entenderlo y sobretodo a divulgarlo.

El presente trabajo aborda lo referente a dicho método y algunas de sus aplicaciones, se divide en tres capítulos y un apéndice.

El primero de ellos consigna algunos resultados sobre el cardinal de conjuntos suma, conjuntos diferencia y conjuntos asociados; empezamos estudiando estos conjuntos en los enteros y posteriormente en subconjuntos de $\mathbb{Z}_p$ con p primo, y llegamos a dos resultados importantes como lo son la prueba de la conjetura de Erdös-Heilbronn y el Teorema de Cauchy - Davenport los cuales nos permiten desarrollar en plenitud el

Método Polinomial.

Los resultados obtenidos en el capítulo uno y algunas de sus aplicaciones se generalizan en el segundo capítulo, se presentan además ejemplos que son de gran utilidad para la asimilación de los mismos.
En el tercer capítulo, presentamos algunos resultados asociados a nuestro tema, que no se prueban utilizando directamente el Método Polinomial.
Por último tenemos el apéndice, en el cual compilamos algunas definiciones y demostraciones de teoremas utilizados en el desarrollo de este trabajo.

Índice general

Capítulo 1

El Método Polinomial en dos variables

1.1. Notación y Ejemplos

Sean $\langle G, + \rangle$ un grupo conmutativo, notado aditivamente y A,B subconjuntos finitos no vacíos de G y $g \in G$.
En Teoría de Números Aditiva estamos interesados en estudiar el cardinal de conjuntos suma $A + B$, conjuntos diferencia $A - B$ y conjuntos asociados, en relación con el cardinal de los conjuntos A y B..

Empezamos definiendo los siguientes conjuntos:
El conjunto suma de A y B es:

$$A + B := \{x + y : x \in A,\, y \in B\}.$$

El conjunto suma estricta de A y B es:

$$A \hat{+} B := \{x + y : x \in A,\, y \in B,\, x \neq y\}.$$

En particular cuando $A = B$, usamos la siguiente notación:

$$A + A := \{x + y : x, y \in A\},$$

$$A \hat{+} A := \{x + y : x, y \in A,\, x \neq y\}.$$

El conjunto diferencia de A y B es:

$$A - B := \{x - y : x \in A,\, y \in B\}.$$

Definimos la suma de n veces el conjunto A así:

$$nA = \{a_0 + \cdots + a_{n-1} : a_i \in A\}$$

$$\hat{n}A = \{a_0 + \cdots + a_{n-1} : a_i \in A \text{ y } a_i \neq a_j \text{ para todo } i \neq j\},$$

También definimos:

$$-A := \{-x : x \in A\}.$$

$$A + g = A + \{g\} := \{a + g : a \in A\}.$$

Si X es un conjunto, usamos $|X|$ para representar su cardinal.

Ejemplo 1. Sean $G = \mathbb{Z}$, $A = \{-7, -3, 4, 8, 30\}$ y $B = \{-5, 0, 4, 12, 30, 31\}$.

+	-7	-3	4	8	30
-5	-12	-8	-1	3	25
0	-7	-3	4	8	30
4	-3	1	8	12	34
12	5	9	16	20	42
30	23	27	34	38	60
31	24	28	35	39	61

$$A + B = \{-12, -8, -7, -3, -1, 1, 3, 4, 5, 8, 9, 12, 16, 20$$
$$23, 24, 25, 27, 28, 30, 34, 35, 38, 39, 42, 60, 61\}.$$

$$A\hat{+}B = \{-12, -8, -7, -3, -1, 1, 3, 4, 5, 8, 9, 12, 16, 20$$
$$23, 24, 25, 27, 28, 30, 34, 35, 38, 39, 42, 61\}.$$

+	-7	-3	4	8	30
-7	-14	-10	-3	1	23
-3		-6	1	5	27
4			8	12	34
8				16	38
30					60

$$A + A = \{-14, -10, -6, -3, 1, 5, 8, 12, 16, 23, 27, 34, 38, 60\}.$$

$$A\hat{+}A = \{-10, -3, 1, 5, 12, 23, 27, 34, 38\}.$$

Ejemplo 2. Sean $G = \mathbb{Z}_{11}$, $A = \{0, 3, 7, 8, 10\}$ y $B = \{1, 2, 4, 8\}$.

+	0	3	7	8	10
1	1	4	8	9	0
2	2	5	9	10	1
4	4	7	0	1	3
8	8	0	4	5	7

$$A + B = \{0, 1, 2, 3, 4, 5, 7, 8, 9, 10\}.$$

$$A \hat{+} B = \{0, 1, 2, 3, 4, 5, 7, 8, 9, 10\}.$$

+	0	3	7	8	10
0	0	3	7	8	10
3		6	10	0	2
7			3	4	6
8				5	7
10					9

$$A + A = \{0, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

$$A \hat{+} A = \{0, 2, 3, 4, 6, 7, 8, 10\}.$$

Proposición 1.1. *Sean A y B subconjuntos finitos no vacíos de un grupo conmutativo $\langle G, + \rangle$ y $g \in G$. Tenemos:*

1. $|A| = |A + g| = |-A|$.
2. $\text{máx}\{|A|, |B|\} \leq |A + B| \leq |A||B|$.
3. $\text{máx}\{|A|, |B|\} \leq |A - B| \leq |A||B|$.

Demostración. Numeral 1.
Esta afirmación se prueba de manera inmediata ya que existe una función biyectiva $f : A \longrightarrow A + g$ definida como $f(a) = a + g$, para todo $a \in A$.

Sean $a, a' \in A$ tal que $f(a) = f(a')$, entonces

$$a + g = a' + g,$$

por lo tanto $a = a'$. De ahí que f es inyectiva.

Sea $c \in A + g$, luego existe $a \in A$ tal que $c = a + g$, de este modo $f(a) = a + g = c$, así f es sobreyectiva.

Por lo tanto f es biyectiva, es decir, $|A+g| = |A|$.

La segunda igualdad se prueba de manera similar definiendo una función $g : A \longrightarrow -A$ definida como $g(a) = -a$. □

Demostración. Numeral 2.
Sean $|A| = \text{máx}\{|A|, |B|\}$ y $b \in B$.
Como $A + b \subseteq A + B$ y además por la Proposición 1.1 Numeral 1,

$$|A + b| = |A|$$

entonces tenemos que,

$$\text{máx}\{|A|, |B|\} \leq |A + B|.$$

La segunda desigualdad es clara ya que $|A||B|$ es el máximo número posible de sumas distintas en $A + B$. Notemos que la igualdad se da en el caso en que todas las sumas sean distintas. □

Demostración. Numeral 3.
Si hacemos $A - B = A + (-B)$ y usando la Proposición 1.1 Numeral 2, obtenemos el resultado deseado. □

Proposición 1.2. *Sea A un subconjunto finito no vacío de un grupo conmutativo $\langle G, + \rangle$. Entonces,*

1. $|A| \leq |A + A| \leq \frac{|A|(|A|+1)}{2} = \binom{|A|+1}{2}$.
2. $|A| \leq |A - A| \leq |A|(|A| - 1) + 1$.

Demostración. Numeral 1.
Por la Proposición 1.1 Numeral 2, tenemos que

$$|A| \leq |A + A|.$$

Como

$$A + A = (A \hat{+} A) \cup (2.A),$$

donde $2.A = \{a + a : a \in A\}$, entonces

$$\begin{aligned} |A + A| &\leq |A \hat{+} A| + |2.A| \\ &\leq \binom{|A|}{2} + |A| = \binom{|A| + 1}{2}. \end{aligned}$$

□

Demostración. Numeral 2.
La primera desigualdad se da por la Proposición 1.1 Numeral 2.
Como

$$A - A = (A\hat{-}A) \cup \{0\},$$

donde $A\hat{-}A = \{a - b : a, b \in A,\ a \neq b\}$, entonces

$$\begin{aligned} |A - A| &\leq |A\hat{-}A| + |\{0\}| \\ &\leq 2\binom{|A|}{2} + 1 = |A|(|A| - 1) + 1. \end{aligned}$$

□

Cuando $G = \mathbb{Z}$, se obtienen ligeras mejoras en las cotas inferiores.

Proposición 1.3. *Sean A, B subconjuntos finitos no vacíos de $\mathbb{Z}$.*

1. $|A| + |B| - 1 \leq |A + B|$.
2. $2|A| - 1 \leq |A + A|$.
3. $2|A| - 1 \leq |A - A|$.
4. $2|A| - 3 \leq |A\hat{+}A|$.

Demostración. Numeral 1.
Sean $A, B \subseteq \mathbb{Z}$ finitos, abusando de la notación los ordenamos como:

$$A = \{a_1 < a_2 < a_3 < \cdots < a_k\}, \text{ donde } |A| = k,$$

y

$$B = \{b_1 < b_2 < b_3 < \cdots < b_l\}, \text{ donde } |B| = l.$$

Definamos

$$A + b_1 := \{a + b_1 : a \in A\} \subseteq A + B$$

y

$$a_k + B := \{a_k + b : b \in B\} \subseteq A + B,$$

donde por la Proposición 1.1 Numeral 1,

$$|A + b_1| = |A| = k \quad y \quad |a_k + B| = |B| = l.$$

Ahora probemos que:

$$(A + b_1) \cap (a_k + B) = \{a_k + b_1\}.$$

Sea $x \in (A + b_1) \cap (a_k + B)$, entonces existen $a \in A \ y \ b \in B$ tales que

$$x = a + b_1 = a_k + b,$$

entonces

$$a - a_k = b - b_1,$$

es decir,

$$a - a_k = b - b_1 = 0$$

así

$$a = a_k \ \text{y} \ b = b_1$$

luego por ordenamiento obtenemos que

$$a \leq a_k \ y \ b \geq b_1,$$

entonces

$$a - a_k \leq 0 \ \ y \ \ b - b_1 \geq 0,$$

de donde

$$a = a_k \ \ y \ \ b = b_1$$

y así

$$x = a_k + b_1.$$

Por lo tanto,

$$\begin{aligned} |(A + b_1) \cup (a_k + B)| \ &= \ |(A + b_1)| + |(a_k + B)| \ - \ |(A + b_1) \cap (a_k + B)| \\ &= \ |A| + |B| - 1. \end{aligned}$$

Y como

$$(A + b_1) \cup (a_k + B) \subseteq A + B,$$

entonces tenemos que

$$|A| + |B| - 1 \ \leq \ |A + B|.$$

□

Demostración. Numeral 2.
Basta con tomar $A = B$ en la Proposición 1.3 Numeral 1.
Por lo tanto, $2|A| - 1 \ \leq \ |A + A|$. □

Demostración. Numeral 3.
Basta con tomar $B = -A$ en la Proposición 1.3 Numeral 1.
Por lo tanto, $2|A| - 1 \ \leq \ |A + B| = |A + (-A)| = |A - A|$. □

Demostración. Numeral 4.
Sean $A \subseteq \mathbb{Z}$ finito, abusando de la notación lo ordenamos como:

$$A = \{a_1 < a_2 < a_3 < \cdots < a_k\}, \text{ donde } |A| = k.$$

Definamos

$$a_1 \hat{+} A = (a_1 + A) \backslash \{a_1 + a_1\} \subset A \hat{+} A.$$

De igual forma tenemos

$$a_k \hat{+} A = (a_k + A) \backslash \{a_k + a_k\} \subset A \hat{+} A.$$

Luego,

$$|a_1 \hat{+} A| = |A| - 1$$
$$|a_k \hat{+} A| = |A| - 1.$$

Así,

$$a_k \hat{+} A \cap a_1 \hat{+} A = a_1 + a_k.$$

Observemos que esta intersección consta de un solo elemento. Así

$$\begin{aligned} |a_1 \hat{+} A \cup a_k \hat{+} A| &= |a_1 \hat{+} A| + |a_k \hat{+} A| - |a_k \hat{+} A \cap a_1 \hat{+} A| \\ &= (|A| - 1) + (|A| - 1) - 1 \\ &= 2|A| - 3. \end{aligned}$$

□

Veamos por ejemplo, cómo se comporta la cardinalidad del conjunto suma de dos subconjuntos finitos no vacíos de $\mathbb{Z}$.

Ejemplo 3. Sean $A = \{1, 2, 3, 4, 5, 6\}$ *y* $B = \{1, 2, 3, 4, 5\}$.

+	1	2	3	4	5	6
1	**2**	**3**	**4**	**5**	**6**	**7**
2		4	5	6	7	**8**
3			6	7	8	**9**
4				8	9	**10**
5					10	**11**

$A + B$ está dado por {2,3,4,5,6,7,8,9,10,11}, en este caso tenemos la igualdad que es la mínima cardinalidad que expresamos en la Proposición 1.3 Numeral 1, esto es,

$$|A| + |B| - 1 = |A + B| = 10.$$

Ejemplo 4. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{6, 11, 16, 21\}$, veamos que el conjunto suma $A + B$ tiene la máxima cardinalidad expresada en la Proposición 1.3 Numeral 1.

+	1	2	3	4	5
6	7	8	9	10	11
11	12	13	14	15	16
16	17	18	19	20	21
21	22	23	24	25	26

En este caso, $A+B = \{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26\}$. Observemos que el conjunto suma $A + B$ tiene la máxima cardinalidad expresada en la Proposición 1.3 Numeral 1, es decir,

$$|A + B| = |A||B| = (5)(4) = 20.$$

Ejemplo 5. Sea $A = \{1, 2, 3, 4, 5\}$.

+	1	2	3	4	5
1	2	3	4	5	6
2		4	5	6	7
3			6	7	8
4				8	9
5					10

En este caso $A + A = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$, satisface el enunciado expresado en la Proposición 1.3 Numeral 2, el cual tiene la mínima cardinalidad, esto es,

$$2|A| - 1 = |A + A| = 9.$$

Ejemplo 6. Presentamos ahora un ejemplo en el cual la cardinalidad de $A + A$ es máxima.
Sea $A = \{1, 2, 4, 8, 13, 23, 31\}$.

+	1	2	4	8	13	23	31
1	2	3	5	9	14	24	32
2		4	6	10	15	25	33
4			8	12	17	27	35
8				16	21	31	39
13					26	36	44
23						46	54
31							62

En este caso el conjunto suma $A + A$ está dado por:
$\{2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 17, 21, 24, 25, 26, 27, 31, 32, 33, 35, 36, 39, 44, 46, 54, 62\}$,
el cual tiene la máxima cardinalidad expresada en la Proposición 1.3 Numeral 2, es decir,

$$2|A| - 1 = 13 \leq |A + A| = 28.$$

A continuación presentamos dos resultados importantes (1.4) y (1.5) que nos sirven para demostrar el Teorema 1.6 el cual nos permite usar en plenitud el Método Polinomial.
Recordemos que en cualquier campo el número de raíces de un polinomio no nulo, no puede exceder su grado.
Una extensión en dos variables de este resultado es el siguiente teorema.

Teorema 1.4. *(Alon - Tarsi) Sean A y B subconjuntos no vacíos de un campo F con $|A| = k$ y $|B| = l$. Sea $f(x, y)$ un polinomio con coeficientes en F y de grado a lo sumo $k - 1$ en x y $l - 1$ en y. Si $f(a, b) = 0$ para todo $a \in A$ y para todo $b \in B$, entonces $f(x, y)$ es idénticamente cero.*

Demostración. Sabemos que en cualquier campo si un polinomio no cero, $p(x) \in F[x]$ es de grado a lo más $k - 1$, entonces no puede tener k raíces distintas en F. Luego si un polinomio de grado n es superado por el número de sus raíces, entonces éste es el polinomio idénticamente cero. Utilicemos este hecho en un polinomio con dos variables $f(x, y)$.
Escribamos el polinomio $f(x, y)$ de la siguiente forma:

$$f(x,y) = \sum_{i=0}^{k-1}\sum_{j=0}^{l-1} f_{i,j}x^i y^j = \sum_{i=0}^{k-1} v_i(y)x^i, \qquad \text{donde} \qquad v_i(y) = \sum_{j=0}^{l-1} f_{i,j}y^j.$$

Es claro que $v_i(y)$ es un polinomio de grado a lo más $l - 1$ en y.
Ahora fijemos $b \in B$, tomemos

$$u(x) = f(x, b) = \sum_{i=0}^{k-1} v_i(b)x^i,$$

así que $u(x)$ es un polinomio de grado a lo más $k - 1$ en x, tal que $u(a) = f(a, b) = 0$, para todo $a \in A$. Como $u(x)$ tiene por lo menos k raíces distintas, $u(x)$ es el polinomio cero y así $v_i(b) = 0$, para todo $i = 0, \cdots, k - 1$ y y para todo $b \in B$. Como

$$grad(v_i) = l - 1$$

y $|B| = l$, entonces $v_i(y)$ es el polinomio cero para todo $i = 0, \cdots, k - 1$.
Por lo tanto $f_{i,j} = 0$ para todo i, j, y así $f(x, y)$ es idénticamente cero. □

Lema 1.5. *Sea A un subconjunto finito de un campo F, y sea $|A| = k$. Para todo $m \geq 0$ existe un polinomio $r_m(x) \in F[x]$ de grado a lo más $k-1$, tal que $r_m(a) = a^m$ para todo $a \in A$.*

En esta prueba se utiliza el algoritmo de la división para polinomios.

Demostración. Sean $A = \{a_0, a_1, a_2, ..., a_{k-1}\}$ y

$$t(x) = \prod_{j=0}^{k-1}(x - a_j).$$

Entonces $t(x) \in F[x]$ y $grad(t) = k$, además $t(a) = 0$ para todo $a \in A$.
Por el algoritmo de la división para polinomios sobre un campo (Ver Apéndice A.1), tenemos que para todo $m \geq 0$ existen polinomios $q_m(x)$ y $r_m(x)$ tal que

$$x^m = t(x)q_m(x) + r_m(x) \quad \text{donde} \quad 0 \leq grad(r_m) < grad(t) = k,$$

luego,

$$a_i^m = t(a_i)q_m(a_i) + r_m(a_i) = r_m(a_i),$$

para todo $a_i \in A$.
Por lo tanto $r_m(x)$ es el polinomio buscado. □

Ejemplo 7. Sean $F = \mathbb{Z}_{11}$, $A = \{1, 3, 5, 7\}$, $k = |A| = 4$ y $m = 5$.
Sea

$$\begin{aligned} t(x) &= (x-1)(x-3)(x-5)(x-7) \\ &= x^4 - 5x^3 + 9x^2 + 6. \end{aligned}$$

Al realizar la división del polinomio x^5 entre el polinomio $t(x)$ obtenemos como residuo el polinomio $r(x) = 5x^3 + 10x^2 + 5x + 3$ de grado 3. Luego tenemos

$$r_5(1) = 1 = 1^5$$
$$r_5(3) = 1 = 3^5$$
$$r_5(5) = 1 = 5^5$$
$$r_5(7) = 10 = 7^5.$$

Observación 1. *Otra forma de demostrar el Lema 1.5 es utilizando el determinante de Vandermonde (Ver Apéndice A.2.2). Presentamos dicha demostración.*

Demostración. Sea $A = \{a_0, a_1, a_2, ..., a_{k-1}\}$. Probemos que existe un polinomio

$$r_m(x) = z_0 + z_1 x + z_2 x^2 + ... + z_{k-1} x^{k-1} \in F[x],$$

tal que,

$$r_m(a_i) = z_0 + z_1 a_i + z_2 a_i^2 + ... + z_{k-1} a_i^{k-1} = a_i^m.$$

para todo $i = 0, ..., k-1$. Este es un sistema de k ecuaciones lineales con k indeterminadas $z_0, z_1, z_2, ..., z_{k-1}$, y tiene solución si el determinante de los coeficientes de las indeterminadas es no cero. El lema se sigue inmediatamente de la observación que este determinante es el determinante de Vandermonde,

$$\begin{vmatrix} 1 & a_0 & a_0^2 \dots & a_0^{k-1} \\ 1 & a_1 & a_1^2 \dots & a_1^{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & a_{k-1} & a_{k-1}^2 \dots & a_{k-1}^{k-1} \end{vmatrix}$$

$$= \prod_{0 \le i < j \le k-1} (a_j - a_i) \neq 0,$$

luego el sistema tiene solución única y por lo tanto $r_m(x)$ es el polinomio pedido. □

Ejemplo 8. Sean $F = \mathbb{Z}_{11}$, $A = \{1, 3, 5, 7\}$, $k = |A| = 4$ y $m = 5$.
Hagamos la construcción de $r_5(x)$.

$$r_5(x) = z_0 + z_1 x + z_2 x^2 + z_3 x^3$$
$$r_5(1) = z_0 + z_1 + z_2 + z_3 = 1^5 = 1$$
$$r_5(3) = z_0 + 3z_1 + 9z_2 + 5z_3 = 3^5 = 1$$
$$r_5(5) = z_0 + 5z_1 + 3z_2 + 4z_3 = 5^5 = 1$$
$$r_5(7) = z_0 + 7z_1 + 5z_2 + 2z_3 = 7^5 = 10.$$

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 9 & 5 & 1 \\ 1 & 5 & 3 & 4 & 1 \\ 1 & 7 & 5 & 2 & 10 \end{array}\right]$$

Realizando operaciones elementales obtenemos la siguiente matriz.

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 8 & 4 & 0 \\ 0 & 0 & 2 & 0 & 9 \\ 0 & 0 & 0 & 6 & 8 \end{array}\right]$$

Así, la solución al sistema anterior es:

$$6z_3 = 8 \rightarrow z_3 = 5.$$

$$2z_2 = 9 \rightarrow z_2 = 10$$

$$2z_1 + 8z_2 + 4z_3 = 0 \rightarrow z_1 = 5$$

$$z_0 + z_1 + z_2 + z_3 = 1 \rightarrow z_0 = 3$$

Por lo tanto $r_5(x) = 5x^3 + 10x^2 + 5x + 3$

Observación 2. *Observemos que en el Lema 1.5 el polinomio $r_m(x)$ es único.*

Demostración. Sean $|A| = k$, $A = \{a_0, a_1, a_2, ..., a_{k-1}\}$ y $m \geq 0$. Supongamos que existen dos polinomios $r_m(x)$ y $r'_m(x)$, ambos de grado menor o igual que $k-1$, tal que

$$r_m(a_i) = r'_m(a_i) = a_i^m$$

para todo $i = 0, 1, ..., k-1$.
La diferencia $d(x) = r_m(x) - r'_m(x)$ tiene grado

$$grad(d) = max\{grad(r), grad(r')\} \leq k-1$$

y además $d(a_i) = 0$, para $i = 0, 1, ..., k-1$, es decir, d tiene mas raíces que su grado, por lo tanto d es el polinomio nulo, así $r_m(x) = r'_m(x)$.

□

Teorema 1.6. *Si p es un número primo y $F = \mathbb{Z}_p$, A y B subconjuntos no vacíos del campo F tales que $|A| \neq |B|$, entonces*

$$|A \hat{+} B| \geq \text{mín}\{p, |A| + |B| - 2\}.$$

Demostración. Sean $E = A \hat{+} B$, $|A| = k$ y $|B| = l$.
Sin pérdida de generalidad, supongamos que $1 \leq l < k \leq p$.

1. Supongamos además que $p \geq k+l-2$; debemos probar que $|E| \geq k+l-2$ o equivalentemente $|E| > k+l-3$.
Procedamos por contradicción.
Supongamos que $|E| \leq k+l-3$.
Escogemos $w \in \mathbb{Z}^+ \cup \{0\}$ tal que, $w+|E| = k+l-3$. Ahora construimos tres polinomios f_0, f_1 y f en $F[x,y]$ de la siguiente forma:

$$f_0(x,y) = \prod_{e \in E}(x+y-e),$$

entonces tenemos que

$$grad(f_0) = |E| \leq k+l-3 \text{ y } f_0(a,b) = 0,$$

para todo $a \in A$ y para todo $b \in B$, $a \neq b$.
El segundo polinomio es de la forma:

$$f_1(x,y) = (x-y)f_0(x,y),$$

de aquí obtenemos que,

$$grad(f_1) = 1+|E| \leq k+l-2 \text{ y } f_1(a,b) = 0,$$

para todo $a \in A$ y para todo $b \in B$.

Finalmente multiplicando

$$f_1 \text{ por } (x+y)^w,$$

obtenemos el tercer polinomio

$$f(x,y) = (x-y)(x+y)^w \prod_{e \in E}(x+y-e),$$

donde

$$grad(f) \text{ es } |E|+w+1 = k+l-2 \quad \text{y} \quad f(a,b) = 0,$$

para todo $a \in A$ y para todo $b \in B$.
El polinomio $f(x,y)$ es de la forma:

$$f(x,y) = \sum_{i+j \leq k+l-2} f_{i,j}x^i y^j \quad \text{donde} \quad i,j \geq 0$$

$$= (x-y)(x+y)^{k+l-3} + \text{los términos de orden inferior.}$$

Puesto que

$$1 \leq l < k \leq p \quad \text{y} \quad 1 \leq k+l-3 \leq p-1,$$

se sigue que el coeficiente $f_{k-1,l-1}$ del monomio $x^{k-1}y^{l-1}$ en $f(x,y)$ está dado por:

$$x(x+y)^{k+l-3} - y(x+y)^{k+l-3},$$

luego por el desarrollo binomial de Newton tenemos

$$\binom{k+l-3}{k-2} - \binom{k+l-3}{k-1} = \frac{(k-l)(k+l-3)!}{(k-1)!(l-1)!} \not\equiv 0 \pmod{p}.$$

Por el Lema 1.5, para todo $m \geq k$ existe un polinomio $r_m(x)$ de grado a lo más $k-1$ tal que

$$r_m(a) = a^m \text{ para todo } a \in A,$$

y para todo $n \geq l$ existe un polinomio $s_n(y)$ de grado a lo más $l-1$ tal que

$$s_n(b) = b^n \text{ para todo } b \in B.$$

Usamos los polinomios $r_m(x)$ y $s_n(y)$ para construir un nuevo polinomio $f^*(x,y)$ a partir de $f(x,y)$ como sigue:

Si $x^m y^n$ es un monomio en $f(x,y)$ con $m \geq k$, entonces reemplazamos

$$x^m y^n \text{ por } r_m(x)y^n.$$

Como

$$grad(f) = k + l - 2,$$

y si $m \geq k$, entonces $m - k \geq 0$, luego

$$m + n \leq k + l - 2,$$

así

$$0 \leq m - k \leq -n + l - 2,$$

por lo tanto $n \leq l - 2$.

De este modo no es necesario reemplazar el término y^n por $s_n(y)$ y así $r_m(x)y^n$ es una suma de monomios $x^i y^j$ con $i \leq k-1$ y $j \leq l-2$.

Similarmente, si $x^m y^n$ es un monomio en $f(x,y)$ con $n \geq l$, entonces reemplazamos

$$x^m y^n \text{ por } x^m s_n(y).$$

Como

$$grad(f) = k + l - 2 \quad \text{y} \quad n \geq l,$$

entonces $n - l \geq 0$, luego

$$m + n \leq k + l - 2,$$

así

$$0 \leq n - l \leq -m + k - 2,$$

por lo tanto $m \leq k - 2$. Luego no es necesario reemplazar

$$x^m \text{ por } r_m(x)$$

y así $x^m s_n(y)$ es una suma de monomios $x^i y^j$ con $i \leq k-1$ y $j \leq l-1$, lo anterior determina un nuevo polinomio $f^*(x, y)$ de grado a lo más $k-1$ en x y $l-1$ en y.

El polinomio $f^*(x, y)$ lo construimos a partir del polinomio $f(x, y)$, pero el coeficiente $f_{k-1,l-1}$ del monomio $x^{k-1}y^{l-1}$ en $f(x, y)$ no se modificó en $f^*(x, y)$ ya que solo se modificaron los términos x^m, y^n tales que $m > k-1$, $n > l-1$.

De otro modo

$$f^*(a, b) = f(a, b) = 0 \text{ para todo } a \in A, \quad \text{para todo } b \in B,$$

ya que por la construcción de $f^*(x, y)$ tenemos que si $x^m y^n$ es un término de $f(x, y)$, al evaluar (a, b) en éste, obtenemos el término $a^m b^n$.
Si $m > k-1$, $x^m y^n$ lo reemplazamos por $r_m(x)y^n$ y al evaluarlo en (a, b) obtenemos

$$r_m(a)y^n = a^m b^n$$

luego

$$f(a, b) = f^*(a, b) \text{ para todo } (a, b) \in A \times B.$$

Similarmente, se hace si $n > l - 1$.

Luego tenemos que $f^*(x, y)$ es un polinomio con coeficientes en $\mathbb{Z}_p$, tal que su grado en x es $k-1$ y su grado en y es $l-1$, además $f^*(a, b) = 0$ para todo $(a, b) \in A \times B$ donde $A, B \subseteq \mathbb{Z}_p$ y $|A| = k$, $|B| = l$ luego por el Lema 2.1 se sigue inmediatamente que el polinomio $f^*(x, y)$ es idénticamente cero, lo cual contradice el hecho de que el coeficiente

$$f_{k-1,l-1} \text{ de } x^{k-1}y^{l-1} \text{ en } f(x, y)$$

es no cero, puesto que este coeficiente es también coeficiente en $f^*(x, y)$.
Por lo tanto $|E| > k + l - 2$.

2. Si $k+l-2>p$, entonces $l>p-k+2$.
   Sea $l'=p-k+2$ y sea $B'\subseteq B$ tal que $|B'|=l'$, luego

$$2\leq l'<l<k \quad \text{y} \quad p=l'+k-2,$$

   y definamos:

$$E'=\{a+b' : a\in A, b'\in B', a\neq b'\},$$

   entonces $E'\subseteq E$, luego $|E|\geq|E'|$.
   Además A, B', E' son tales que $|A|=k, |B'|=l',$ donde

$$k+l'-2=p=\text{mín}\{p, k+l-2\}$$

   luego se tiene que

$$|E|\geq|E'|\geq k+l-2.$$

   Por lo tanto

$$|E|\geq k+l-2,$$

   que es lo que queríamos demostrar.

□

Ejemplo 9. Sean $F=\mathbb{Z}_{11}$, $A=\{0,1,2,10\}$, $B=\{0,1,2\}$. El conjunto suma $A\hat{+}B$ esta dado por:

+	0	1	2	10
0		1	2	10
1	1		3	0
2	2	3		1

$A\hat{+}B=\{0,1,2,3,10\}$, es decir, $|A\hat{+}B|=5=|A|+|B|-2$.

1.2. Teorema de Erdös-Heilbronn

Esta conjetura, hoy teorema, fue formulada en 1964 y probada 30 años después por Dias da Silva y Hamidoune, quienes utilizan Teoría de Representaciones y Algebra lineal para demostrar una generalización de la conjetura. Más adelante Nathanson simplifica el método de Dias da Silva y Hamidoune reemplazando la teoría de representaciones por algunas propiedades del Ballot Numbers (ver [6] sección 3.8). Finalmente en 1995 Alon, Nathanson y Ruzsa dan una prueba de éste teorema utilizando el Método Polinomial (ver [1]), en la cual la muestran como un caso particular de 1.6, donde se aprecia el uso del Método Polinomial.

Teorema 1.7. *(Dias da Silva-Hamidoune) Si p es un número primo, $F = \mathbb{Z}_p$ y $A \subseteq F$ con $|A| = k \geq 2$, entonces*

$$|A\hat{+}A| \geq \text{mín}\{p,\, 2k-3\}.$$

Demostración. Sea $A \subseteq F$, $|A| = k \geq 2$.
Escojamos $a \in A$ y sea $B = A - \{a\}$ entonces $|B| = |A| - 1$.
Definamos $E = A\hat{+}B$, dado que $|A| \neq |B|$ además $E \subseteq A\hat{+}A$, luego por Teorema 1.6,

$$|A\hat{+}A| \geq |E| \geq \text{mín}\{p, |A| + |B| - 2\} = \text{mín}\{p, 2|A| - 3\}.$$

Esto completa la prueba de la conjetura de Erdös y Heilbronn. □

A continuación presentamos algunos ejemplos de este resultado.

Ejemplo 10. Sean $F = \mathbb{Z}_{17}$, $A = \{4, 7, 10, 16\}$. El conjunto suma $A\hat{+}A$ está dado por:

+	4	7	10	16
4		11	14	3
7	11		0	6
10	14	0		9
16	3	6	9	

$A\hat{+}A = \{0, 3, 6, 9, 11, 14\}$ y $|A\hat{+}A| = 6 \geq |A| + |A| - 3 = 5$.

Ejemplo 11. Sean $F = \mathbb{Z}_{11}$, $A = \{1, 4, 5, 6, 7, 8, 10\}$. El conjunto suma $A\hat{+}A$ está dado por:

+	1	4	5	6	7	8	10
1		5	6	7	8	9	0
4			9	10	0	1	3
5				0	1	2	4
6					2	3	5
7						4	6
8							7
10							

$A\hat{+}A = \mathbb{Z}_{11}$, y entonces $|A\hat{+}A| \geq \text{mín}\{p, |A| + |A| - 3\} = p = 11$.

1.3. Teorema de Cauchy-Davenport

Otro de los resultados importantes es el Teorema de Cauchy-Davenport, el cual tiene numerosas aplicaciones en Teoría de Números Aditiva y puede ser redemostrado utilizando el Método Polinomial, cabe anotar que este teorema fue probado por Cauchy

en 1813 y redescubierto por Davenport en 1935, una forma de enunciarlo es la siguiente.

Teorema 1.8. *(Cauchy-Davenport) Si p es un número primo y $F = \mathbb{Z}_p$, A y B subconjuntos no vacíos del campo F, entonces*

$$|A + B| \geq \text{mín}\{p, |A| + |B| - 1\}.$$

Demostración. Sea $|A| = k$, $|B| = l$. Supongamos que $k + l - 1 \leq p$.
Si $|A+B| \leq k+l-2$. Escojamos un w para que $w+|A+B| = k+l-2$ y consideremos el polinomio

$$f(x, y) = (x + y)^w \prod_{c \in (A+B)} (x + y - c),$$

entonces $f(a, b) = 0$ para todo $a \in A$ y para todo $b \in B$. El grado total del polinomio es $k + l - 2$ y el coeficiente del monomio $x^{k-1}y^{l-1}$ es exactamente

$$\binom{k+l-2}{k-1} \not\equiv 0 \pmod{p}.$$

La prueba de este resultado continua exactamente como la prueba del Teorema 1.6. □

Veamos algunos ejemplos de este teorema.

Ejemplo 12. Sean $F = \mathbb{Z}_{17}$, $A = \{3, 4, 5, 6, 7\}$, $B = \{0, 1, 15, 16, \}$. El conjunto suma $A + B$ esta dado por:

+	3	4	5	6	7
0	3	4	5	6	7
1	4	5	6	7	8
15	1	2	3	4	5
16	2	3	4	5	6

$A + B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, es decir,

$$|A + B| = |A| + |B| - 1 = 8.$$

Ejemplo 13. Sean $F = \mathbb{Z}_{17}$, $A = \{3, 4, 5, 6, 7\}$, $B = \{0, 5, 10, 15, \}$. El conjunto suma $A + B$ esta dado por:

+	3	4	5	6	7
0	3	4	5	6	7
5	8	9	10	11	12
10	13	14	15	16	0
15	1	2	3	4	5

$A + B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, \}$, es decir,

$$|A + B| = 17 \geq |A| + |B| - 1 = 8.$$

Otra de las aplicaciones del método polinomial es el siguiente teorema.

Teorema 1.9. *Sean A y B subconjuntos no vacíos de un campo F, $F = \mathbb{Z}_p$ y sea*

$$C = \{a + b : a \in A,\, b \in B, a \cdot b \neq 1\}.$$

Si $|A| = k$ y $|B| = l$, entonces

$$|C| \geq \text{mín}\{p,\, k + l - 3\}.$$

Demostración. Si $k + l - 3 > p$.
Sea $l' = p - k + 3$, entonces $3 \leq l' < l$. Escojamos $B' \subseteq B$ tal que $|B'| = l'$ y sea

$$C' = \{a + b' : a \in A,\, b' \in B', a \cdot b' \neq 1\}.$$

Así $C' \subseteq C$.
Esto es suficiente para probar que $|C'| \geq k + l' - 3$.
De forma similar supongamos que $k + l - 3 \leq p$, y probemos que $|C| \geq k + l - 3$. Supongamos que $|C| \leq k + l - 4$, escojamos un w para que $w + |C| = k + l - 4$ y consideremos el polinomio

$$f(x, y) = (xy - y)(x + y)^w \prod_{c \in C}(x + y - c),$$

entonces $f(a, b) = 0$ para todo $a \in A$ y para todo $b \in B$.
El grado total del polinomio es $k + l - 2$, y el coeficiente del monomio $x^{k-1}y^{l-1}$ es exactamente

$$\binom{k + l - 4}{k - 2} \not\equiv 0 \pmod{p}.$$

La prueba continua exactamente como la prueba del Teorema 1.6.

□

Ejemplo 14. Sean $F = \mathbb{Z}_{17}$, $A = \{1, 2, 3, 4\}$ y $B = \{1, 6, 9, 16\}$. El conjunto suma $C = \{a + b : a \in A,\, b \in B, a \cdot b \neq 1\}$, esta dado por:

+	1	2	3	4
1		3	4	5
6	7	8		10
9	10		12	13
16	0	1	2	3

$C = \{0, 1, 2, 3, 4, 5, 7, 8, 10, 12, 13\}$.
Observemos que $|C| \geq \text{mín}\{p,\, k + l - 3\} = \text{mín}\{17,\, 5\}$, por lo tanto $|C| \geq \{k + l - 3\}$.

Capítulo 2

Generalización

En el presente capítulo mostramos la generalización de los resultados presentados en el capítulo anterior.

2.1. El Método Polinomial General

Recordemos que en cualquier campo el número de raíces de un polinomio no nulo, no puede exceder el grado del polinomio, de manera general este resultado se tiene en el siguiente teorema.

Teorema 2.1. *(Alon - Tarsi) Sea $f = f(x_0, \cdots, x_k)$ un polinomio en $k+1$ variables $x_0, \cdots, x_k$ sobre un campo arbitrario F. Supongamos que para todo $i = 0, \cdots, k$ el grado de f como un polinomio en x_i es a lo más c_i y A_i es un subconjunto de F de cardinalidad $c_i + 1$. Si $f(a_0, \cdots, a_k) = 0$ para toda $(k+1) - tupla\,(a_0, \cdots, a_k) \in A_0 \times \cdots \times A_k$, entonces f es el polinomio cero.*

Demostración. En la prueba se usa inducción sobre k.

- Para $k = 0$, tenemos que $f = f(x_0)$ es un polinomio en x_0 de grado c_0 y $A_0 \subset F$ tal que $|A_0| = c_0 + 1$, luego como $f(a_0) = 0$ para todo $a_0 \in A_0$, entonces f tiene $c_0 + 1$ raíces y por lo tanto f es el polinomio cero.

- Sea $k \geq 1$ y supongamos que el enunciado se cumple para polinomios con a lo sumo k variables. Dado el polinomio $f = f(x_0, \ldots, x_k)$ y los conjuntos $A_0, \ldots, A_k$ que satisfacen las hipótesis del teorema, escribamos f como un polinomio en la variable x_k así;

$$f = \sum_{i=0}^{c_k} f_i(x_0, \ldots, x_{k-1}) x_k^i \,,$$

donde cada $f_i(x_0, \ldots, x_{k-1})$ es un polinomio en k variables $x_0, \ldots, x_{k-1}$ y de grado a lo más c_j en cada variable x_j, para $0 \leq j \leq k-1$.
Fijando la k-tupla $(a_0, \ldots, a_{k-1}) \in A_0 \times \cdots \times A_{k-1}$, el polinomio

$$g(x_k) = \sum_{i=0}^{c_k} f_i(a_0, \ldots, a_{k-1}) x_k^i,$$

tiene grado a lo más c_k en x_k y es tal que $g(a_k) = f(a_0, \ldots, a_{k-1}, a_k) = 0$ para todo $a_k \in A_k$. Como $g(x_k)$ tiene a lo más c_k raíces y $|A_k| = c_k + 1$, entonces $g(x_k)$ es el polinomio cero y así

$$f_i(a_0, \ldots, a_{k-1}) = 0 \text{ para todo } (a_0, \ldots, a_{k-1}) \in A_0 \times \cdots \times A_{k-1},$$

luego por hipótesis de inducción tenemos que $f_i(x_0, \ldots, x_{k-1}) = 0$ para todo i y por lo tanto el polinomio f es el polinomio cero.

□

El resultado anterior es de gran importancia para el desarrollo de nuestra monografía, ya que nos permite demostrar el Teorema 2.2, el cual tiene diversas aplicaciones en Teoría de Números Aditiva y fue formulado por Noga Alon, Melvyn Nathanson e Imre Ruzsa en [1] y [2] para subconjuntos en el campo $\mathbb{Z}_p$. En estos artículos se afirma que el resultado es válido para cualquier otro campo distinto de $\mathbb{Z}_p$.
A continuación mostramos una prueba, la cual es válida para cualquier campo arbitrario.

Teorema 2.2. *(Teorema General) Sean $A_0, \ldots, A_k$ subconjuntos de un campo arbitrario F con $|A_i| = c_i + 1$ para $i = 0, \ldots, k$.*
Sea $h = h(x_0, \ldots, x_k)$ un polinomio no nulo en $F[x_0, \cdots, x_k]$ y definamos

$$m = \sum_{i=0}^{k} c_i - grad(h).$$

Si el coeficiente de $x_0^{c_0} \cdots x_k^{c_k}$ en el polinomio

$$(x_0 + \cdots + x_k)^m h(x_0, \ldots, x_k)$$

es distinto de cero, entonces

$$|\{a_0 + \cdots + a_k : a_i \in A_i \text{ y } h(a_0, \ldots, a_k) \neq 0\}| \geq m + 1.$$

Demostración. Supongamos que la afirmación es falsa y sean

$$E = \{a_0 + \cdots + a_k : a_i \in A_i \text{ y } h(a_0, \ldots, a_k) \neq 0\},$$

y E' un conjunto de m elementos de F tal que, $E \subseteq E'$.
Sea $Q = Q(x_0, \ldots, x_k)$ el polinomio definido de la siguiente manera

$$Q = h(x_0, \ldots, x_k) \prod_{e \in E'} (x_0 + \cdots + x_k - e).$$

Observemos que:

1. $Q(a_0, \ldots, a_k) = 0$ para toda $(k+1)$-tupla $(a_0, \ldots, a_k) \in A_0 \times \cdots \times A_k$, ya que $h(a_0, \ldots, a_k) = 0$ ó $a_0 + \cdots + a_k \in E'$.

2. $grad(Q) = m + grad(h) = \sum_{i=0}^{k} c_i$.

3. El coeficiente del monomio $x_0^{c_0} \cdots x_k^{c_k}$ en Q es el mismo que el coeficiente de éste en el polinomio

   $$(x_0 + \cdots + x_k)^m h(x_0, \ldots, x_k),$$

   ya que $Q(x_0, \ldots, x_k) = h(x_0, \ldots, x_k)(x_0 + \cdots + x_k)^m +$términos de menor orden.

4. El $grad(Q)$ en cada variable x_i es a lo más $grad(h) + m = \sum_{i=0}^{k} c_i$.

Ahora, para cada i, con $0 \leq i \leq k$ definamos el polinomio

$$g_i(x_i) = \prod_{a \in Ai} (x_i - a),$$

cuyo grado es $c_i + 1$, luego para cada x_i^t en Q, existen polinomios $q_{it}(x_i)$ y $r_{it}(x_i)$ tales que

$$x_i^t = q_{it}(x_i) g_i(x_i) + r_{it}(x_i) \quad \text{con} \quad 0 \leq grad(r_{it}(x_i)) < grad(g_i(x_i)) = c_i + 1.$$

Construyamos un nuevo polinomio $\overline{Q}(x_0, \ldots, x_k)$ a partir del polinomio $Q(x_0, \ldots, x_k)$ reemplazando cada ocurrencia de x_i^t por $r_{it}(x_i)$. Notemos que:

1. En la construcción de $\overline{Q}(x_0, \ldots, x_k)$ no se modifica el coeficiente del monomio $x_0^{c_0} \cdots x_k^{c_k}$ ya que éste no ocurre en ninguno de los monomios $x_0^{c_0} \cdots x_i^t \cdots x_k^{c_k}$ para todo $t > grad(g_i(x_i)) = c_i + 1$, es decir, $x_0^{c_0} \cdots x_i^t \cdots x_k^{c_k}$ no está en Q, por que su grado es:

   $$\begin{aligned} c_0 + \cdots + t + \cdots + c_k &> c_0 + \cdots + grad(g_i(x_i)) + \cdots + c_k \\ &= \sum_{i=0}^{k} c_i + 1 > grad(Q). \end{aligned}$$

2. Para cada $a_i \in A_i$, $r_{it}(a_i) = a_i^t$ y por lo tanto

$$\overline{Q}(a_0, \ldots, a_k) = Q(a_0, \ldots, a_k) = 0 \text{ para toda } (a_0, \ldots, a_k) \in A_0 \times \cdots \times A_k.$$

3. El grado de $\overline{Q}$ en cada variable x_i es a lo más c_i, ya que $grad(r_{it}(x_i))$ es a lo más c_i.

De la observación anterior $\overline{Q}$ cumple las hipótesis del Teorema 2.1 y por lo tanto $\overline{Q}(x_0, \ldots, x_k)$ es el polinomio cero. Así el coeficiente de $x_0^{c_0} \cdots x_k^{c_k}$ en $\overline{Q}$ es cero. Lo cual es una contradicción. □

Ejemplo 15. Sea $F = \mathbb{Z}_7,\ A_0 = \{1, 2\},\ A_1 = \{1, 2, 6\},\ A_2 = \{2, 3, 5, 6\}$.
Definamos $h(x_0, x_1, x_2) = (x_0 + 5)(x_1 + 5)(x_2 + 5)$ y así

$$m = \sum_{i=0}^{k} c_i - grad(h) = 3.$$

Veamos el coeficiente de $x_0 x_1^2 x_2^3$ en $(x_0 + x_1 + x_2)^3 h(x_0, x_1, x_2)$.

$$\begin{aligned}(x_0 + x_1 + x_2)^3 h(x_0, x_1, x_2) &= (x_0 + x_1 + x_2)^3 (x_0 + 5)(x_1 + 5)(x_2 + 5) \\ &= [x_0^3 + 3x_0^2 x_1 + 3x_0^2 x_2 + 3x_0 x_1^2 + 6x_0 x_1 x_2 + 3x_0 x_2^2 + x_1^3 + 3x_1^2 x_2 + \\ &3x_1 x_2^2 + x_2^3][x_0 x_1 x_2 + 5x_0 x_2 + 5x_1 x_2 + 4x_2 + 5x_0 x_1 + 4x_0 + 4x_1 + 6].\end{aligned}$$

Luego el coeficiente del monomio en cuestión es $3 \not\equiv 0 \pmod 7$.
Veamos los elementos del conjunto $E = \{a_0 + a_1 + a_2 : a_i \in A_i \text{ y } h(a_0, a_1, a_2) \neq 0\}$.

(x_0, x_1, x_2)	$h(x_0, x_1, x_2)$	$a_0 + a_1 + a_2$
(1,1,3)	1	5
(1,1,5)	3	0
(1,1,6)	4	1
(1,6,3)	3	3
(1,6,5)	2	5
(1,6,6)	5	6

Luego $E = \{0, 1, 3, 5, 6\}$, así $|E| = 5 \geq m + 1 = 4$.

Ejemplo 16. En el Teorema 2.2 una particularidad es que los subconjuntos que escogemos son subconjuntos de un campo arbitrario F, en este sentido surge de manera inmediata la siguiente pregunta.
¿Es posible que pueda reemplazarse la estructura de campo?, es decir, ¿el Teorema 2.2

sigue siendo válido si sustituimos el campo F por un anillo R?
El siguiente ejemplo ilustra que el resultado del teorema no siempre se tiene.

Sean $F = \mathbb{Z}_8$, $A_0 = \{1, 3\}$, $A_1 = \{1, 3, 5\}$, $A_2 = \{2, 3, 6, 7\}$.
Definamos $h(x_0, x_1, x_2) = (x_0 + 5)(x_1 + 5)(x_2 + 5)$ y así

$$m = \sum_{i=0}^{k} c_i - grad(h) = 3.$$

Veamos el coeficiente de $x_0x_1^2x_2^3$ en $(x_0 + x_1 + x_2)^3 h(x_0, x_1, x_2)$.

$(x_0 + x_1 + x_2)^3 h(x_0, x_1, x_2) = (x_0 + x_1 + x_2)^3(x_0 + 5)(x_1 + 5)(x_2 + 5)$
$= [x_0^3 + 3x_0^2x_1 + 3x_0^2x_2 + 3x_0x_1^2 + 6x_0x_1x_2 + 3x_0x_2^2 + x_1^3 + 3x_1^2x_2$
$+3x_1x_2^2 + x_2^3][x_0x_1x_2 + 5x_0x_2 + 5x_1x_2 + x_2 + 5x_0x_1 + x_0 + x_1 + 5]$.
Así el coeficiente del monomio en cuestión es $3 \not\equiv 0 \pmod 8$.
Veamos los elementos del conjunto $E = \{a_0 + a_1 + a_2 : a_i \in A_i \text{ y } h(a_0, a_1, a_2) \neq 0\}$.

(x_0, x_1, x_2)	$h(x_0, x_1, x_2)$	$a_0 + a_1 + a_2$
(1,1,2)	4	**4**
(1,1,6)	4	0
(1,1,7)	0	**1**
(1,5,2)	4	0
(1,5,6)	4	**4**
(1,5,7)	0	5

Luego $E = \{0, 4\}$, así $|E| = 2 < m + 1 = 4$, es decir, si se reemplaza la estructura de campo por la de anillo, en general el teorema no siempre es cierto.

2.2. Teorema de Cauchy-Davenport y su generalización

Otra manera de demostrar el Teorema de Cauchy-Davenport es reemplazando $h = 1$, $k = 1$, $A_0 = A$, $A_1 = B$, y $m = |A| + |B| - 2$ en el Teorema 2.2. Veamos:

Demostración. Si $|A| + |B| \leq p + 1$ apliquemos el Teorema 2.2 con $h = 1$, $k = 1$, $A_0 = A$, $A_1 = B$, y $m = |A| + |B| - 2$, entonces $|A| = c_0 + 1$, $|B| = c_1 + 1$, y el coeficiente relevante es

$$\binom{m}{c_0} \not\equiv 0 \pmod p.$$

Si $|A|+|B| > p+1$ reemplazamos B por un subconjunto B' de cardinalidad $p+1-|A|$ y se aplica el resultado sobre A y B', para concluir en este caso $|A|+|B| \geq |A+B'| = p$.

□

Presentamos el siguiente lema, el cual es utilizado para demostrar la generalización del Teorema de Cauchy-Davenport.

Lema 2.3. *Sea $C_0, \ldots, C_k$, enteros no negativos supongamos que $\sum_{i=0}^{k} c_i = m + \binom{k+1}{2}$, donde m es un entero no negativo, entonces el coeficiente de $\prod_{i=0}^{k} x_i^{c_i}$ en el polinomio*

$$(x_0 + x_1 + \cdots + x_k)^m \prod_{k \geq i > j \geq 0} (x_i - x_j)$$

es

$$\frac{m!}{c_0! c_1! \cdots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j).$$

Demostración. El producto $\prod_{k \geq i > j \geq 0}(x_i - x_j)$ es precisamente el determinante de Vandermonde (Ver Apéndice A.2.2) $det(x_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$ el cual es igual a la suma

$$\sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} \prod_{i=0}^{k} x_i^{\sigma(i)},$$

donde S_{k+1} denota el conjunto de todas las permutaciones de los $k+1$ símbolos desde $0, \ldots, k$. Así se sigue que el coeficiente requerido, el cual denotaremos por C, esta dado por

$$C = \sum_{\sigma \in S_{k+1}} (-1)^{sign(\sigma)} \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \ldots (c_k - \sigma(k))!}.$$

Similarmente, el producto $\prod_{k \geq i > j \geq 0}(c_i - c_j)$ es el determinante de Vandermonde $det(c_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$.

Para dos enteros $r \geq 1$ y s, $(s)_r$ denota el producto $s(s-1)\cdots(s-r+1)$ y definimos también $(s)_0 = 1$ para todo s.

Observe que la matriz $((c_i)_j)_{0 \leq i \leq k, 0 \leq j \leq k}$ puede obtenerse de la matriz $(c_i^j)_{0 \leq i \leq k, 0 \leq j \leq k}$ restando apropiadamente combinaciones lineales de las columnas con índices menores que j desde la columna indizada por j, para cada $j = k, k-1, \ldots, 1$.

Por lo tanto esas dos matrices tienen el mismo determinante. De esto deducimos que,

$$\begin{aligned}
&\frac{m!}{c_0! c_1! \cdots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j) \\
&= \frac{m!}{c_0! c_1! \cdots c_k!} det((c_i)_j)_{0 \leq i \leq k, 0 \leq j \leq k} \\
&= \frac{m!}{c_0! c_1! \cdots c_k!} \sum_{\sigma \in S_{k+1}} sign(\sigma)(c_0)_{\sigma_0}(c_1)_{\sigma_1} \cdots (c_k)_{\sigma_k}
\end{aligned}$$

$$= \sum_{\sigma \in S_{k+1}} sign(\sigma) \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \dots (c_k - \sigma(k))!} = C,$$

completando la prueba. □

El Teorema de Cauchy-Davenport generalizado es el siguiente.

Teorema 2.4. *(Cauchy-Davenport genaralizado) Sean p un número primo, $A_0, \dots, A_k$ subconjuntos no vacíos de $\mathbb{Z}p$. Si $|A_i| \neq |A_j|$ para todo $0 \leq i < j \leq k$ y*

$$\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1,$$

entonces

$$|\{a_0 + \dots + a_k : a_i \in A_i, a_i \neq a_j \text{ para todo } i \neq j\}| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Demostración. Definamos,

$$h(x_0, \dots, x_k) = \prod_{k \geq i > j \geq 0} (x_i - x_j).$$

Notemos que,

$$\{a_0 + \dots + a_k : a_i \in A_i, a_i \neq a_j \ \forall \ i \neq j\} = \{a_0 + \dots + a_k : a_i \in A_i, h(a_0, \dots, a_k) \neq 0\}.$$

Supongamos que $|A_i| = c_i + 1$, donde los c_i son enteros no negativos distintos dos a dos y hagamos $m = \sum_{i=0}^{k} c_i - grad(h)$, luego

$$\begin{aligned} m &= \sum_{i=0}^{k} (|A_i| - 1) - \binom{k+1}{2} \\ &= \sum_{i=0}^{k} |A_i| - (k+1) - \binom{k+1}{2} \\ &= \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} \leq p - 1 < p. \end{aligned}$$

Ahora, como del Lema 2.3, el coeficiente del monomio $x_0^{c_0} \cdots x_k^{c_k}$ en el polinomio

$$(x_0 + \dots + x_k)^m \prod_{k \geq i > j \geq 0} (x_i - x_j),$$

es

$$C = \frac{m!}{c_0! \cdots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j)$$

y dado que $m < p$ y los c_i son distintos dos a dos, entonces

$$C \not\equiv 0 \pmod{p}$$

y por lo tanto del Teorema 2.2 tenemos que:

$$|\{a_0 + \cdots + a_k : a_i \in A_i; a_i \neq a_j \text{ para todo } i \neq j\}| \geq m + 1 = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

□

2.3. Teorema de Erdös - Heilbronn y su generalización

Notemos que un caso especial del Teorema 2.4 está dado cuando $k = 1$, $A_0 = A$, $A_1 = A - \{a\}$, para un elemento arbitrario $a \in A$ lo cual implica que si $A \subseteq \mathbb{Z}p$ y $2|A| - 1 \leq p + 2$ entonces el número de sumas $a_1 + a_2$ con $a_1, a_2 \in A$ y $a_1 \neq a_2$ es por lo menos $2|A| - 3$.

Esto implica otra forma de probar el Teorema conjeturado por Erdös y Heilbronn en 1964 y probado recientemente por Dias Da Silva y Hamidoune, usando algunas herramientas del Algebra Lineal y la Teoría de representaciones de los grupos simétricos. Veamos:

Demostración. Apliquemos el Teorema 2.4 con $k = 1$, $A_0 = A$ y $A_1 = A \setminus \{a\}$ para $a \in A$ fijo. Como $A \subseteq \mathbb{Z}p$ y $|A_0| \neq |A_1|$, entonces:
Si

$$|A_0| + |A_1| \leq p + \binom{3}{2} - 1,$$

lo cual es equivalente a

$$2|A| - 3 \leq p$$

y dado que

$$\{a_i + a_j : a_i \in A_0, a_j \in A_1, a_i \neq a_j \text{ para todo } i \neq j\} = \{a + a' : a, a' \in A, a \neq a'\},$$

entonces

$$\{a + a' : a, a' \in A, a \neq a'\} \geq |A_0| + |A_1| - \binom{3}{2} + 1 = 2|A| - 3.$$

Además, si $2|A| - 3 > p$, es decir, $|A_0| + |A_1| - 2 > p$, escogemos $A_1' \subseteq A_1$ tal que $|A_0| + |A_1'| - 2 = p$ y por lo tanto el teorema se cumple para A_0 y A_1, luego como

$$\{a_i + a_j : a_i \in A_0, a_j \in A_1', a_i \neq a_j \ \forall\ i \neq j\} \subseteq \{a_i + a_j : a_i \in A_0, a_j \in A_1 \ \forall\ i \neq j\},$$

entonces

$$|\{a_i + a_j : a_i \in A_0, a_j \in A_1 \ \forall\ i \neq j\}| \geq |\{a_i + a_j : a_i \in A_0, a_j \in A_1', a_i \neq a_j \ \forall\ i \neq j\}| > p.$$

Por lo tanto

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geq \text{mín}\{p, 2|A| - 3\}.$$

□

Otra manera de obtener el Teorema de Erdös-Heilbronn), es a partir de la generalización formulada por Dias da Silva y Hamidoune, en éste trabajo dicha generalización corresponde al Teorema 2.6, aquí presentamos la prueba apoyados en el siguiente teorema.

Teorema 2.5. *Sea p un número primo y sean $A_0, \ldots, A_k$ subconjuntos no vacíos de $\mathbb{Z}_p$, donde $|A_i| = b_i$. Supongamos que $b_0 \geq \ldots \geq b_k$ y definamos $b_0', \cdots, b_k'$ por*

$$b_0' = b_0 \text{ y } b_i' = \text{mín}\{b_{i-1}' - 1, b_i\} \text{ para } 1 \leq i \leq k.$$

Si $b_k' > 0$, entonces

$$|\{a_0 + \cdots + a_k : a_i \in A_i \text{ y } a_i \neq a_j \text{ para todo } i \neq j\}| \geq \text{mín}\left\{p, \sum_{i=0}^{k} b_i' - \binom{k+2}{2} + 1\right\},$$

mas aún, la estimación es la mejor para todos los valores posibles de $p \geq b_0 \geq \cdots \geq b_k$.

Demostración. Si $b_i' \leq 0$ para algún i entonces $b_k' \leq 0$ lo cual no es posible, por lo tanto $b_i' > 0$ para todo i.
Sea A_i' un subconjunto arbitrario de A_i tal que $|A_i'| = b_i$ para cada i, $1 \leq i \leq k$, entonces $|A_i'| \neq |A_j'|$ para cada $i \neq j$.

Si

$$\sum_{i=0}^{k} b_i' \leq p + \binom{k+2}{2} - 1,$$

entonces del Teorema 2.4 tenemos que:

$$\{a_0 + \cdots + a_k : a_i \in A_i', a_i \neq a_j \ \forall\ i \neq j\} \geq \sum_{i=0}^{k} b_i' - \binom{k+2}{2} + 1,$$

además, como

$$\{a_0 + \cdots + a_k : a_i \in A'_i, a_i \neq a_j \ \forall\ i \neq j\} \subseteq \{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \forall\ i \neq j\},$$

entonces

$$|\{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \forall\ i \neq j\}| \geq |\{a_0 + \cdots + a_k : a_i \in A'_i, a_i \neq a_j \ \forall\ i \neq j\}|,$$

de ahí que

$$|\{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \forall\ i \neq j\}| \geq \sum_{i=0}^{k} b'_i - \binom{k+2}{2} + 1.$$

Por otro lado, afirmamos que existen naturales $b''_0 > \cdots > b''_k \geq 1$ tales que $b''_i \leq b'_i$ y

$$\sum_{i=0}^{k} b''_i = p + \binom{k+2}{2} - 1,$$

en efecto consideremos el operador T que envía secuencias de enteros $(d_0, \ldots, d_k)$ con $d_0 > \cdots > d_k \geq 1$ en secuencias del mismo tipo, y T definido de la siguiente manera:

La secuencia $(k+1, k, \ldots, 1)$ se envía en sí misma. Para cualquier otra secuencia $(d_0, \ldots, d_k)$, sea j el mayor índice para el cual $d_j > k + 1 - j$ y definamos

$$T(d_0, \ldots, d_k) = (d_0, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_k).$$

Claramente, la suma de los elementos de $T(D)$ es uno menos, que la suma de los elementos de D para toda secuencia D distinta de $(k+1, k, \ldots, 1)$.
Así aplicando repetidamente T a nuestra secuencia $(b'_0, \ldots, b'_k)$ obtenemos la secuencia deseada $(b''_0, \ldots, b''_k)$.

Ahora, retomando la demostración en el caso en que

$$\sum_{i=0}^{k} b'_i > p + \binom{k+2}{2} - 1,$$

sean b''_i como en la afirmación anterior y consideremos los subconjuntos $A''_i \subseteq A'_i$ tales que $|A''_i| = b''_i$, por lo tanto el teorema se cumple para los A''_i, esto es:

$$|\{a_0 + \cdots + a_k : a_i \in A''_i, a_i \neq a_j \ \forall\ i \neq j\}| \geq \sum_{i=0}^{k} b''_i - \binom{k+2}{2} + 1 = p,$$

además como

$$\{a_0 + \cdots + a_k : a_i \in A_i'', a_i \neq a_j \ \forall\ i \neq j\} \subseteq \{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \forall\ i \neq j\},$$

tenemos que

$$|\{a_0+\cdots+a_k : a_i \in A_i, a_i \neq a_j \ \forall\, i \neq j\}| \geq |\{a_0+\cdots+a_k : a_i \in A_i'', a_i \neq a_j \ \forall\, i \neq j\}| > p,$$

y por lo tanto

$$\{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \ \forall\ i \neq j\} \geq \text{mín}\{p, \sum_{i=0}^{k} b_i - \binom{k+2}{2} + 1\}.$$

□

Teorema 2.6. *(Erdös - Heilbronn generalizado) Sean p es un número primo, A un subconjunto no vacío de $\mathbb{Z}_p$, y $\hat{n}A$ el conjunto de todas las sumas de n elementos distintos de A, entonces*

$$|\hat{n}A| \geq \text{mín}\{p, n|A| - n^2 + 1\}.$$

Demostración. Observemos que si $|A| < n$ no tenemos nada que probar, ya que no tiene sentido hablar del conjunto $\hat{n}A$.
Si $|A| \geq n$, tomemos $n = k+1$ y apliquemos la Proposición 2.5 con $A_i = A$, $b_i' = |A| - i$ para todo i, $0 \leq i \leq k$. Como $b_k' = |A| - n + 1 \geq n - n + 1 = 1 > 0$ y además $\hat{n}A = \{a_0 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \text{ para todo } i \neq j\}$, entonces

$$\begin{aligned}
|\hat{n}A| &\geq \text{mín}\{p, \sum_{i=0}^{k} b_i' - \binom{k+2}{2} + 1\} \\
&= \text{mín}\{p, \sum_{i=0}^{k} (|A| - i) - \frac{(k+1)(k+2)}{2} + 1\} \\
&= \text{mín}\{p, \sum_{i=0}^{k} |A| - \frac{k(k+1)}{2} - \frac{(k+1)(k+2)}{2} + 1\} \\
&= \text{mín}\{p, (k+1)|A| - (k+1)^2 + 1\} \\
&= \text{mín}\{p, n|A| - n^2 + 1\},
\end{aligned}$$

luego

$$|\hat{n}A| \geq \text{mín}\{p, n|A| - n^2 + 1\}.$$

□

2.4. Otras aplicaciones del Método Polinomial

En los últimos 15 años el método polinomial ha sido una herramienta muy utilizada en el estudio de problemas que tienen que ver con el cardinal de conjuntos suma con restricciones. Algunos ejemplos particulares de este tipo de problemas se presentan en ([1],[2],[5],[7]).Veamos por ejemplo, los siguientes.

Proposición 2.7. *Sean p un número primo, A, B subconjuntos no vacíos de $\mathbb{Z}_p$, entonces*

$$|\{a+b : a \in A, b \in B \text{ y } ab \neq 1\}| \geq \text{mín}\{p, |A|+|B|-3\}.$$

Demostración. Definamos $h(x_0, x_1) = x_0x_1 - 1$. Sean $A_0 = A$, $A_1 = B$, $c_0 = |A| - 1$, $c_1 = |B| - 1$ y $m = c_0 + c_1 - grad(h) = |A| + |B| - 4$.
Como

$$\{a+b : a \in A, b \in B \text{ y } ab \neq 1\} = \{a_0 + a_1 : a_i \in A_i \text{ y } h(a_0, a_1) \neq 0\},$$

y dado que el coeficiente del monomio $x_0^{c_0}x_i^{c_1}$ en el polinomio

$$(x_0 + x_1)^{|A|+|B|-4}(x_0x_1 - 1)$$

es

$$C = \binom{|A|+|B|-4}{|B|-2} = \frac{(|A|+|B|-4)!}{(|B|-2)!(|A|-2)!},$$

entonces si $|A|+|B|-4 < p$, es decir, si $|A|+|B|-3 \leq p$ tenemos que $C \not\equiv 0 \pmod{p}$ y por lo tanto del Teorema 2.2,

$$|\{a+b : a \in A, b \in B \text{ y } ab \neq 1\}| \geq m+1 = |A|+|B|-3.$$

Por otro lado, si $|A|+|B|-4 \geq p$, es decir, si $|A|+|B|-3 > p$ escogemos B' subconjunto de B tal que $|A| + |B'| - 3 = p$ y así el teorema se cumple para A y B', luego

$$|\{a+b : a \in A, b \in B' \text{ y } ab \neq 1\}| \geq |A| + |B'| - 3 = p,$$

además, ya que

$$\{a+b : a \in A, b \in B' \text{ y } ab \neq 1\} \subseteq \{a+b : a \in A, b \in B \text{ y } ab \neq 1\},$$

entonces

$$|\{a+b : a \in A, b \in B \text{ y } ab \neq 1\}| \geq |\{a+b : a \in A, b \in B' \text{ y } ab \neq 1\}| \geq p,$$

y por lo tanto podemos concluir que

$$|\{a+b : a \in A, b \in B \text{ y } ab \neq 1\}| \geq \text{mín}\{p, |A|+|B|-3\}.$$

□

Proposición 2.8. *Sean p un número primo y $A_0, \ldots, A_k$ subconjuntos no vacíos de $\mathbb{Z}_p$, entonces para cada $g \in \mathbb{Z}_p$,*

$$|\{a_0 + \cdots + a_k : a_i \in A_i, \prod_{i=0}^{k} a_i \neq g\}| \geq \text{mín}\{p, \sum_{i=0}^{k} |A_i| - 2k - 1\}.$$

Demostración. Si $g = 0$ el resultado se sigue del Teorema de Cauchy Davenport.
Sea $g \neq 0$. En primer lugar supongamos que $|A_i| > 1$ para todo i.
Si $\sum_{i=0}^{k} |A_i| - 2k - 2 < p$ y aplicando el Teorema 2.2 con

$$h = \prod_{i=0}^{k} x_i - g \quad \text{y} \quad m = \sum_{i=0}^{k} |A_i| - 2k - 2.$$

Aquí $c_i = |A_i| = 1$ y el coeficiente de

$$\prod_{i=0}^{k} x_i^{c_i} \quad \text{en} \quad h.(x_0 + \cdots + x_k)^m$$

es

$$\frac{m!}{\prod(c_{i-1})!} \not\equiv 0 \pmod{p}.$$

lo que implica el resultado deseado. En otro caso, reemplazamos algunos de los conjuntos A_i por subconjuntos no vacíos A_i' de forma que se cumpla $|A_i'| > 1$ y

$$\sum_{i=0}^{k} |A_i'| = p + 2k + 1$$

y aplicamos el resultado a los conjuntos A_i'.
Cuando $|A_i| = 1$ para varios conjuntos A_i, el resultado se deduce aplicando el caso previo a los conjuntos A_j de cardinalidad mayor que 1 modificando el valor de g apropiadamente. □

Capítulo 3

Algunas limitaciones del Método Polinomial

Este capítulo, muestra algunos resultados para los cuales el Método Polinomial no se aplica directamente.

3.1. Suma de subconjuntos con restricciones polinomiales

Teorema 3.1. *Sean k, m, n enteros positivos con $k > m(n-1)$, y F un campo de característica p, donde p es cero o es mayor que $K = (k-1)n - (m+1)\binom{n}{2}$.*
Sean $A_1, ..., A_n$ subconjuntos de F para el cual

$$|A_n| = k \quad y \quad |A_{i+1}| - |A_i| \in \{0, 1\} \quad y \text{ para } \quad i = 1, ..., n-1.$$

Sean $P_1(x), ..., P_n(x) \in F[x]$ mónicos y de grado m. Entonces tenemos,
$|\{a_1 + \cdots + a_n : a_i \in A_i, \quad y \quad P_i(a_i) \neq P(a_j) + b_j \quad si \quad i \neq j\}| \geq K + 1.$

Demostración. Para $1 \leq i \leq n$ se tiene $|A_n| - |A_i| \leq n - 1$, así podemos escoger $A_i' \subseteq A_i$ luego $|A_i'| = k - n + i$.
Sin pérdida de generalidad podemos asumir que $A_i' = A_i$, esto es, $k_i = |A_i| = k - n + i$ para $i = 1, ..., n$. Como el caso $K < 0$ o $n = 1$ es claro, supongamos $K \geq 0$ y $n \geq 2$ donde e denota la identidad multiplicativa del campo F.
Sea

$$f(x_1, ..., x_n) = \prod_{1 \leq i < j \leq n} (P_j(x_j) - P_i(x_i)).$$

Claramente,

$$\sum_{i=1}^{n} (k_i - 1) - grad(f) = (k-1)n - \binom{n}{2} - grad(f) = K,$$

y

$$[x_1^{k_1-1}\cdots x_n^{k_n-1}](x_1+\cdots+x_n)^K f(x_1,...,x_n)=hc^{\binom{n}{2}},$$

donde h es el coeficiente de $x_1^{k-n}\cdots x_n^{k-1}$ en el polinomio

$$g(x_1,...,x_n)=(x_1+\cdots+x_n)^K\prod_{1\le i<i<j\le n}(x_j^m-x_i^m)\in\mathbb{Z}[x_i,...,x_n].$$

Luego por el determinante de Vandermonde (Ver Apéndice A.2.2) y el Teorema del coeficiente multinomial, $g(x_1,...,x_n)$ coincide con

$$\sum_{\sigma\in S_n} sign(\sigma)x_1^{m(\sigma(1)-1)}\sum_{j_1,...,j_n\ge 0}\frac{K!}{j_1!j_2!\cdots j_n!}(x_1^{j_1}...x_n^{j_n})=K.$$

donde $j_1+\cdots+j_n=K$.
Así,

$$\begin{aligned}h&=K!\sum_{\sigma\in S_n} sign(\sigma)\frac{(k-1-(\sigma(1)-1)m)_{n-1})}{(k-1-(\sigma(1)-1)m)!}\\&\qquad\times...\times\frac{(k-1-(\sigma(n)-1)m)_0)}{(k-1-(\sigma(n)-1)m)!}\\&=\frac{K!(-1)^{\binom{n}{2}}}{\prod_{i=1}^n(k-1-(i-1)m)!}\det\|(k-1-im)_j\|_{0\le i,j\le n-1}.\end{aligned}$$

Es bien conocido que

$$x^j=(x)_j+\sum_{0\le r<j}S(j,r)(x)_r,$$

donde $S(j,r)$, $(0\le r<j)$, son números de Stirling de segunda clase.
Así,

$$\begin{aligned}&\det\|(k-1-im)_j\|_{0\le i,j\le n-1}\\&=\det\|(k-1-im)^j\|_{0\le i,j\le n-1}\\&=(-1)^{\binom{n}{2}}\prod_{0\le i<j<n}(k-1-im-(k-1-jm))\ (Vandermonde).\end{aligned}$$

Como

$$(-1)^{\binom{n}{2}}\det\|(k-1-im)_j\|_{0\le i,j\le n-1},$$

divide

$$\prod_{i=0}^{n-1}(k-1-im)!,$$

entonces tenemos $h\mid K!$ y por lo tanto $p\nmid h$, ahora es suficiente aplicar el Lema 2.2 para obtener el resultado deseado. □

Ejemplo 17. Sean $F = \mathbb{Z}_7,\ k = 5,\ m = 3,\ n = 2$.
La característica de F es 7, luego,

$$7 > K = (k-1)n - (m+1)\binom{n}{2} = 4.$$

Sean $P_1(x) = P_2(x) = x^3, \quad A_1 = \{1,3,4,5,6\}, \quad A_2 = \{1,2,4,6\}$.
Veamos el conjunto $S = \{a_1 + a_2 : a_1 \in A_1, a_2 \in A_2, a_1^3 \neq a_2^3\}$.

a_i	1	2	3	4	5	6
$P(a_i)$	1	1	6	1	1	6

Luego, $S = \{0,1,4,5,6\}$, es decir, $|S| = 5 \geq K + 1 = 5$.

3.2. Una cota inferior para $|\{a+b : a \in A,\ b \in B,\ P(a,b) \neq 0\}|$

Un resultado con un alcance mayor nos lo presenta Jian-Xin Liu y Zhi-Wei Sun en [5]. A continuación damos algunas definiciones que nos permiten demostrar dichos resultados.

Definiciones

1. A lo largo de este documento, cada uno de los intervalos $(k,l), [k,l), (k,l], [k,l]$ representarán el conjunto de enteros sobre éstos, con $k, l \in \mathbb{Z}$.

2. Para un polinomio $P(x_1, ..., x_n)$ sobre un campo, sea $\hat{P}(i_1, ..., i_n)$ el coeficiente de $x_1^{i_1} ... x_n^{i_n}$ en $P(x_1, ..., x_n)$.

3. Sea E un campo cerrado algebraicamente y $P(x)$ un polinomio sobre E. Para $\alpha \in E$, si $(x-\alpha)^m \mid P(x)$ pero $(x-\alpha)^{m+1} \nmid P(x)$, entonces llamamos a m la multiplicidad de α con respecto a $P(x)$ y la denotamos por $m_p(\alpha)$.

4. Para algún entero positivo q el conjunto

$$N_q(p) = q|\{\alpha \in E^\times : m_p(\alpha) \geq q\}| - \sum_{\alpha \in E^\times} \{m_p(\alpha)_q\},$$

donde $\{m\}_q$ denota el mínimo residuo no negativo de $m \in \mathbb{Z}$ módulo q y

$$E^\times = E \backslash \{0\}.$$

Note que $N_1(P)$ es el número de raíces distintas de en $E^\times$ de la ecuación $P(x) = 0$.

5. Sea p la característica de E y

$$\wp(p) = \begin{cases} \{1, p, p^{2,\cdots}\} & \text{si } p < \infty \\ \{1\} & \text{en otro caso.} \end{cases}$$

6. Definimos

$$N(P) = \max_{q \in \wp(p)} q|\{\alpha \in E^{\times} \backslash \{-1\} : m_p(\alpha) \geq q\}|.$$

A continuación presentamos un teorema para el cual los alcances del Método Polinomial no son suficientes para su demostración, ya que las restricciones en este caso son polinómicas.

Teorema 3.2. *Sean F un campo de característica p, A y B dos subconjuntos finitos no vacíos de F, $P(x, y)$ un polinomio sobre F de grado $d = grad(P)$, tal que para algún $i \in [0, |A| - 1]$ y $j \in [0, |B| - 1]$ tenemos que,*

$$\hat{P}(i, d - i) \neq 0 \quad y \quad \hat{P}(d - j, j) \neq 0.$$

Definamos $P_0(x, y)$ el polinomio homogéneo de grado d tal que,

$$P(x, y) = P_0(x, y) + R(x, y),$$

para algún $R(x, y) \in F[x, y]$ con $grad(R) < d$, y $P^*(x) = P_0(x, 1)$.
Entonces para el conjunto $C = \{a + b : a \in A, b \in B \text{ y } P(a, b) \neq 0\}$ tenemos,

$$|C| \geq \text{mín}\{p - m_{p^*}(-1),\ |A| + |B| - 1 - d - N(P^*)\}. \tag{3.1}$$

Para demostrar este teorema es necesario conocer el siguiente resultado:

Lema 3.3. *Sea $P(x)$ un polinomio sobre el campo F de característica p. Supongamos que existen enteros no negativos $k < l$ tal que $\hat{P}(i) = 0$ para todo $i \in (k, l)$. Entonces $x^l \mid P(x)$, ó $grad(P) \leq k$, ó $N_q(P) \geq l - k$ para algún $q \in \wp(p)$.*

Demostración. (Teorema 3.2) Sean $k_1 = |A| - 1$ y $k_2 = |B| - 1$.
Si hacemos $|C| \geq k_1 + k_2 - d + 1$ obtenemos 3.1.
Supongamos que $|C| \leq k_1 + k_2 - d$ y $\delta = k_1 + k_2 - d - |C|$.
Dado que $\hat{P}(d - j, j) \neq 0$ para algún $j \in [0, k_2]$,

$$Q(x, y) = P(x, y) / \prod_{b \in B} (y - b) \notin F[x, y].$$

De otro modo $\hat{P}(d-j, j)$ es cero, porque es igual al coeficiente de $x^{d-j}y^j$ en $y^{|B|}Q(x, y)$.
Así existe un $b_0 \in B$ tal que $P(x, b_0)$ no es idénticamente cero, es decir,

$$P(a, b_0) = 0$$

para a lo más d elementos $a \in F$.
Por lo tanto,

$$|C| \geq |\{a + b_0 : a \in A \text{ y } P(a, b_0) \neq 0\}| \geq |A| - d,$$

y así $\delta < k_2$.
Similarmente, tenemos $\delta < k_1$. Colocamos

$$f(x, y) = P(x, y) \prod_{c \in C} (x + y - c) \quad \text{y} \quad f_0(x, y) = P_0(x, y)(x + y)^{|C|}.$$

Observemos que $grad(f) = grad(f_0) = d + |C| = k_1 + k_2 - \delta$.
Sea $k_1 \in [k_1 - \delta, k_1]$.
Entonces $k_2 = k_1 + k_2 - \delta - k_1 \in (0, k_2]$.
Como $k_1 + k_2 = grad(f)$ y $f(x, y)$ desaparece sobre el producto cartesiano $A \times B$, $\hat{f}(k_1, k_2) = 0$ por [[4] A. Teorema 1.2].
Dado que,

$$\widehat{P^*}(i) = \hat{P}_0(i, d - i) = \hat{P}(i, d - i) \neq 0,$$

para algún $i \in [0, k_1]$. Luego tenemos $m_{p^*}(0) \leq k_1$.
Similarmente,
$\widehat{P^*}(d - j) \neq 0$ para algún $j \in [0, k_2]$ y por lo tanto $grad(P^*) \geq d - k_2$.
El conjunto $f^*(x) = f_0(x, 1) = P^*(x)(x + 1)^{|C|}$. Recordemos que,

$$\hat{f^*}(k) = \hat{f}(k, k_1 + k_2 - \delta - k) = 0,$$

para $k \in [k_1 - \delta, k_1]$.
Puesto que,

$$x^{k_1+1} \nmid f^*(x) \quad \text{y} \quad grad(f^*) = |C| + grad(P^*) \geq |C| + d - k_2 = k_1 - \delta,$$

por el Lema 3.3 existe un $q \in \wp(p)$ tal que,

$$N_q(f^*) \geq (k_1 + 1) - (k_1 - \delta - 1) = \delta + 2.$$

Si $m_{f^*}(-1) = m_{p^*}(-1) + |C| < p$, entonces

$$N(P^*) = N(f^*) \geq N_q(f^*) - 1 \geq k_1 + k_2 - d - |C| + 1.$$

Por lo tanto,

$$|C| \geq k_1 + k_2 + 1 - d - N(P^*) = |A| + |B| - 1 - d - N(P^*).$$

De esta forma se completa la prueba. □

Demostración. (Lema 3.3) Hagamos inducción sobre el grado de $P(x)$.

1. Cuando $P(x)$ es una constante no hay nada que probar ya que

$$grad(P(x)) = 0 < k$$

.

2. Sea $grad(P(x)) > 0$.
Escribamos $P(x) = x^h Q(x)$ donde $h = m_p(0)$ y $Q(x) \in F[x]$.
Si $h < l$, entonces $h \leq k$ dado que $\hat{P}(i) = 0$ para todo $i \in (k, l)$, por tanto $\hat{Q}(j) = 0$ para todo $j \in (k-h, l-h)$.
Así sin pérdida de generalidad, podemos asumir que $P(0) \neq 0$ y que $P(x)$ es mónico.
Sea E la clausura algebraica del campo F.
Escribamos

$$P(x) = \prod_{j=1}^{n} (x - \alpha_j)^{m_j},$$

donde $\alpha_1, ..., \alpha_n,$ son elementos distintos de $E^\times$ y $m_1, ..., m_n,$ son enteros positivos.

Sea

$$P_j(x) = P(x)/(x - \alpha_j), \quad \text{para} \quad j = 1, ..., n.$$

Como

$$P(x) = P_j(x)(x - \alpha_j) = xP(x) - \alpha_j P_j(x),$$

entonces

$$\hat{P}(i+1) = \hat{P}_j(i) - \alpha_j \hat{P}_j(i+1) \quad \text{para todo} \quad i = 0, 1, 2, ...$$

Notemos que $\hat{P}_j(i) = \alpha_j \hat{P}_j(i+1)$ para todo $i \in [k, l-1)$, ya que $\hat{P}(i+1)$ se hace cero para todo $i \in [k, l-1)$.

Por lo tanto,

$$\hat{P}_j(i) = \alpha_j^{l-1-i} \hat{P}_j(l-1) \quad \text{para todo} \quad i \in [k, l). \tag{3.2}$$

En efecto:

$$\begin{aligned} \hat{P}_j(i) &= \alpha_j \hat{P}_j(i+1) \\ &= \alpha_j \alpha_j \hat{P}_j(i+2) \end{aligned}$$

$$= \alpha_j\alpha_j\alpha_j\hat{P}_j(i+3),$$

$$= \alpha_j^{l-1-i}\hat{P}_j(i+l-1-i)$$
$$= \alpha_j^{l-1-i}\hat{P}_j(l-1).$$

Por otro lado tenemos,

$$P^{'}(x) = \sum_{j=1}^{n} m_j P_j(x),$$

ya que,

$$P(x) = \prod_{j=1}^{n}(x-\alpha_j)^{m_j} = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}...(x-\alpha_n)^{m_n}$$

$$P_j(x) = P(x)/(x-\alpha_j) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}...(x-\alpha_j)^{m_j-1}...(x-\alpha_n)^{m_n},$$

luego,

$$P^{'}(x) = m_1P_1(x) + m_2P_2(x) + \cdots + m_nP_n(x).$$

Así,

$$P^{'}(x) = \sum_{j=1}^{n} m_j P_j(x).$$

Por lo tanto,

$$\sum_{j=1}^{n} m_j\hat{P}_j(i) = 0 \ \text{ para todo } \ i \in [k, l-1), \tag{3.3}$$

puesto que $\hat{P}^{'}(i) = 0$ para todo $i \in [k, l-1)$ debido a que
$\hat{P}(i) = 0$ para todo $i \in (k, l)$.

Combinando las ecuaciones 3.2 y 3.3 encontramos que

$$\sum_{j=1}^{n} m_j\alpha_j^{l-1-i}\hat{P}_j(l-1) = 0 \ \text{ para todo } \ i \in [k, l-1). \tag{3.4}$$

Supongamos que $N_q(P) < l-k$ para cualquier $q \in \wp(p)$. Entonces
$n = N_1(P) \leq l-1-k$, por lo tanto por la ecuación 3.4 tenemos que

$$\sum_{j=1}^{n} \alpha_j^s(m_j\hat{P}_j(l-1)) = 0 \ \text{ para todo } \ s = 1, 2, ..., n,$$

es decir,

$$\begin{gathered}\alpha_1(m_1\hat{P}_1(l-1))+\alpha_2(m_2\hat{P}_2(l-1))+\ldots+\alpha_n(m_n\hat{P}_n(l-1))=0\\ \alpha_1^2(m_1\hat{P}_1(l-1))+\alpha_2^2(m_2\hat{P}_2(l-1))+\ldots+\alpha_n^2(m_n\hat{P}_n(l-1))=0\\ \vdots\\ \alpha_1^n(m_1\hat{P}_1(l-1))+\alpha_2^n(m_2\hat{P}_2(l-1))+\ldots+\alpha_n^n(m_n\hat{P}_n(l-1))=0.\end{gathered}$$

Dado que,

$$\begin{vmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_n^n\end{vmatrix}$$

es el determinante de Vandermonde y no se anula, entonces se tiene que,

$$m_j\hat{P}_j(l-1))=0 \text{ para todo } j=1,2,...,n.$$

Así de la ecuación 3.2 tenemos que

$$m_j\hat{P}_j(i)=0,$$

para algún $i\in[k,l)$ y $j\in[1,n]$.

CASO 1:
$p=\infty$, o $p\nmid m_j$ para algún $j\in[1,n]$.
En este caso hay un $j\in[1,n]$ tal que $\hat{P}_j(i)=0$ para todo $i\in(k-1,l)$.
Luego, $k>0$ ya que

$$\hat{P}_j(0)=P_j(0)\neq 0.$$

También

$$N_1(P_j)\leq n=N_1(P),$$

y

$$N_q(P_j)=N_q(P)+1$$

si $p<\infty$ y $q\in\wp(p)\backslash 1$.

Así $N_q(P_j)\leq N_q(P)+1\leq l-k<l-(k-1)$ para todo $q\in\wp(p)$.
Por la hipótesis de inducción, tendríamos que $grad(P_j)\leq k-1$ y así,

$$grad(P(x))\leq k.$$

CASO 2:
$p<\infty$ y p/m_j para todo $j\in[1,n]$. En este caso,

$$T(x)=\prod_{j=1}^{n}(x-\alpha_j)^{m_j/p}\in E[x]$$

y por lo tanto,

$$P(x) = T(x)^p = (\sum_{i\geq 0})\hat{T}(i)x^i)^p = \sum_{i\geq 0}\hat{T}(i)^p x^{ip}.$$

Para cualquier número real r, sea $\lfloor r \rfloor$ denota el entero más grande que no excede a r, entonces

$$\lfloor k/p \rfloor \leq \lfloor (l-1)/p \rfloor,$$

dado que $k \leq l-1$.

Cuando $i \in (\lfloor k/p \rfloor, \lfloor (l-1)/p \rfloor]$, tenemos que $k < ip < l$ y así

$$\hat{T}(i)^p = \hat{P}(ip) = 0.$$

Si $q \in \wp(p)$, entonces

$$N_q(T) = \frac{N_{pq}(P)}{p} \leq \frac{l-k-1}{p} < \left(1 + \left\lfloor \frac{l-1}{p} \right\rfloor\right) - \left\lfloor \frac{k}{p} \right\rfloor.$$

Por la hipótesis de inducción

$$grad(T) \leq \lfloor k/p \rfloor$$

y así

$$grad(P) = p\, grad(T) \leq k.$$

Así completamos la prueba de inducción.

□

Ejemplo 18. (Lema 3.3) Sean $F = \mathbb{Z}_{11}$, $p = 11$, donde p es la característica de F, $k = 3$, $l = 5$ y sea $p(x) = x^5 + 8x^4 + 9x^3 + 8x^2 + 4x + 3$.
Según el Lema 3.3 debe ocurrir uno de los siguientes casos:

1. $x^l \mid P(x)$.
2. $grad(P) \leq k$.
3. $N_q(P) \geq l - k$ para algún $q \in \wp(p)$.

   Observemos que los casos [1] y [2] no se dan, por ende, debe cumplirse el caso [3], en efecto:

   Para $1 \in \wp(p)$ se cumple que $N_1(P) = 4 \geq l - k = 2$

Corolario 3.4. *Sean F un campo de característica p, A y B dos subconjuntos finitos no vacíos de F, k, m, n enteros no negativos y $Q(x, y) \in F[x, y]$ con grado menor que $k + m + n$.*
Si $|A| > k$ y $|B| > m$, entonces

$$|\{a + b : a \in A, b \in B \text{ y } a^k b^m (a + b)^n \neq Q(a, b)\}|$$

$$\geq \text{mín}\{p - n,\ |A| + |B| - k - m - n - 1\}.$$

Demostración. Para

$$P(x, y) = x^k y^m (x + y)^n - Q(x, y),$$

observemos que,

$$\hat{P}(k,\ m + n) = \hat{P}(k + n,\ m) = 1$$

y

$$P^*(x) = x^k (x + 1)^n.$$

Dado que $N(P^*) = 0$, luego el resultado deseado se obtiene del Teorema 3.2.

□

Corolario 3.5. *Sean F un campo de característica p, A y B subconjuntos no vacíos de F y $\oslash \neq S \subseteq F^\times \times F$ tal que $|S| < \infty$. Entonces*

$$|\{a + b : a \in A, b \in B \text{ y } a + ub \neq v \text{ si } (u, v) \in S\}|$$

$$\geq min\{p - |\{v \in F : (1, v) \in S\}|,\ |A| + |B| - 2|S| - 1\}.$$

Demostración. Solo basta con aplicar el Teorema 3.2 con,

$$P(x, y) = \prod_{(u,v) \in S} (x + uy - v)$$

y notemos que $N(P^*) \leq grad(P^*) = |S|$. □

Apéndice A

Apéndice

En está sección consignaremos algunos resultados que nos permiten demostrar teoremas de gran importancia.

A.1. Algoritmo de la división para Polinomios

Teorema A.1. *(Algoritmo de la división para $F[x]$).*
Sean $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad y \quad g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ *dos elementos de* $F[x]$ *con* a_n *y* b_m *ambos elementos distintos de cero de* F *y* $m \geq 0$*, entonces existen polinomios únicos* $q(x)$ *y* $r(x)$ *en* $F[x]$ *tales que* $f(x) = g(x)q(x)+r(x)$ *donde el grado de* $r(x)$ *es menor que* $m = grad(g(x))$.

Demostración. Se considera el conjunto $S = \{f(x) - g(x)s(x) : s(x) \in F[x]\}$.
Sea $r(x)$ un elemento de grado minimal en S. Entonces $f(x) = g(x)q(x) + r(x)$ para alguna $q(x) \in F[x]$.
Debemos mostrar que el grado de $r(x)$ es menor que m.
Supongamos que $r(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_0$, con $c_j \in F[x]$ y $c_t \neq 0$ *si* $t \neq 0$.
Si $t \geq m$, entonces,

$$f(x) - q(x)g(x) - (c_t \mid b_m)x^{t-m}g(x) = r(x) - (c_t \mid b_m)x^{t-m}g(x), \qquad \text{(A.1)}$$

donde $r(x) - (c_t x^t + \text{términos de grado menor})$, es un polinomio de grado menor que t, que es el grado de $r(x)$.
Sin embargo, el polinomio en la ecuación (A.1) puede escribirse de la forma,

$$f(x) - g(x)[q(x) + (c_t \mid b_m)x^{t-m}],$$

de modo que está en S, contradiciendo el hecho de que $r(x)$ se seleccionó con grado minimal en S.
Así $grad(r(x)) < m = grad(g(x))$.

Para la unicidad, si

$$f(x) = g(x)q_1(x) + r_1(x)$$

y

$$f(x) = g(x)q_2(x) + r_2(x),$$

entonces por sustracción tenemos

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x),$$

como el grado de $r_2(x) - r_1(x)$ es menor que el grado de $g(x)$, lo cual es cierto solo si $q_1(x) - q_2(x) = 0$, es decir , si $q_1(x) = q_2(x)$.
Por lo tanto se tiene que $r_1(x) = r_2(x)$.

□

Ejemplo 19. En $\mathbb{Z}_7[x]$ tomemos los polinomios $f(x) = x^5$ y $g(x) = x^3 + 2x$, para los cuales existen los únicos dos polinomios $q(x) = x^2 + 5$ y $r(x) = 4x$ tal que

$$f(x) = g(x)q(x) + r(x),$$

es decir,

$$x^5 = [x^3 + 2x][x^2 + 5] + 4x.$$

A.2. Determinante de Vandermonde

A.2.1. Matriz de Vandermonde

En álgebra lineal una matriz de Vandermonde de orden n es una matriz cuyas filas están formadas de progresiones geométricas. Esta matriz recibe este nombre en honor al matemático frances Alexandre-Théophile Vandermonde.
Los índices de la matriz de tamaño $n \times n$ están descritos por $V_{i,j} = a_i^{j-1}$ para todos los índices i, j variando de i a n, lo cual se puede describir explícitamente de la forma siguiente:

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}$$

El primer elemento de cada fila es el 1, el segundo elemento es un número arbitrario distinto en cada una de las filas. El tercer elemento es el mismo número arbitrario

elevado al cuadrado. En general, el k-ésimo elemento de cada fila es el mismo número arbitrario elevado a la potencia $k-1$. Así el último elemento de cada fila es el mismo que el segundo elevado a la $n-1$.

A.2.2. Determinante de Vandermonde

Teorema A.2. *El determinante de una matriz de Vandermonde de tamaño $n \times n$ se expresa con la siguiente fórmula general:*

$$|V| = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

Esta fórmula es denominada en algunas oportunidades como el discriminante, pero en general éste se define como el cuadrado de la fórmula anterior.

Demostración. Procedamos por inducción sobre n.
En el caso en que $n = 2$ el resultado es correcto, en efecto:

$$|V| = \begin{vmatrix} 1 & a_1 \\ 1 & a_2 \end{vmatrix} = (a_2 - a_1)$$

Ahora generalizando para el caso $n \times n$, basta con realizar la siguiente operación elemental sobre cada columna $C_i : C_i - (a_i \cdot C_{i-1})$.
Esta operación no afecta el determinante, por lo tanto se obtiene lo siguiente:

$$|V| = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2 - a_1 & a_2(a_2 - a_1) & \cdots & a_2^{n-2}(a_2 - a_1) \\ 1 & a_3 - a_1 & a_3(a_3 - a_1) & \cdots & a_3^{n-2}(a_3 - a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n(a_n - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix}$$

Calculando el determinante, se elimina la primera fila de ceros y la primera columna de unos, quedando entonces el determinante de una matriz de $n-1 \times n-1$.

$$|V| = \begin{vmatrix} a_2 - a_1 & a_2(a_2 - a_1) & \cdots & a_2^{n-2}(a_2 - a_1) \\ a_3 - a_1 & a_3(a_3 - a_1) & \cdots & a_3^{n-2}(a_3 - a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n(a_n - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix}.$$

Siguiendo con el desarrollo del determinante se pueden factorizar los productos de diferencias que son comunes en cada fila y así obtener el siguiente resultado:

$$|V| = (a_2 - a_1)(a_3 - a_1)\cdots(a_n - a_1)\begin{vmatrix} 1 & a_2 & a_2^2 & \cdots & a_2^{n-2} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-2} \\ 1 & a_4 & a_4^2 & \cdots & a_4^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-2} \end{vmatrix}.$$

El proceso se puede repetir continuamente reduciendo el orden de la matriz, quedando así probado el procedimiento por inducción. □

Bibliografía

[1] Alon, Noga; Nathanson, Melvyn B.; Ruzsa, Imre. Adding distinct congruence classes modulo a prime. *Amer. Math. Monthly* **102** (1995), no. 3, 250-255. MR1317846 **(95k:11009)**.

[2] Alon, Noga; Nathanson, Melvyn B.; Ruzsa, Imre. The polynomial method and restricted sums of congruence classes. *J. Number Theory* 56 (1996), no. 2, 404-417.MR1373563 **(96k:11011)**.

[3] Rodriguez C.A. El Método Polinomial.Tésis de Maestría, Universidad de Antioquia, 2007.

[4] Alon, Noga. Combinatorial Nullstellensat. *Combinatorics,Probability and Computing* **8** (1999), 7-29.MR1684621**(2000b:05001)**. (2000), 125-130.MR1760589**(2001b:11019)**

[5] Liu, Jian-Xin; Sun, Zhi-Wei. Sums of subsets with polynomial restrictions. *J. Number Theory* **97** (2002), no. 2, 301-304. MR1942962 **(2004c:11027)**.

[6] Nathanson, Melvyn B. Additive number theory. Inverse problems and the geometry of sumsets. Graduate Texts in Mathematics, 165. *Springer-Verlag*, New York, 1996. xiv+293 pp. ISBN: 0-387-94655-1. MR1477155 **(98f:11011)**.

[7] Pan, Hao; Sun, Zhi-Wei. A lower bound for $|\{a+b : a \in A, b \in B, P(a,b) \neq 0\}|$. *J. Combin. Theory Ser. A* **100** (2002), no. 2, 387-393. MR1940342 **(2003k:11016)**.