UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO CONJUNTO EN CIENCIAS MATEMÁTICAS
UNAM-UMSNH

SUMA DE FRACCIONES Y PRODUCTO DE SUBCONJUNTOS DE INTERVALOS EN CAMPOS PRIMOS

TESIS

QUE PARA OPTAR POR EL GRADO DE DOCTOR EN CIENCIAS MATEMÁTICAS
PRESENTA:

CÉSAR ALFONSO DÍAZ MIJANGOS

ASESOR: DR. MOUBARIZ GARAEV
CENTRO DE CIENCIAS MATEMÁTICAS UNAM

MORELIA, MICHOACÁN, JULIO 2020.

Índice general

Abstract/Resumen I

Introducción 1

1 Congruencias aditivas 11
- 1.1 Sumas trigonométricas y congruencias aditivas 11
- 1.2 Suma y producto de conjuntos 12

2 Suma de fracciones módulo p 15
- 2.1 Planteamiento del problema y nuestros resultados 15
- 2.2 Lemas 17
- 2.3 Demostración del Teorema 2.1 29
- 2.4 Demostración del Teorema 2.2 30
- 2.5 Demostración del Teorema 2.3 33

3 Producto de subconjuntos de intervalos en $\mathbb{F}_p$ 37
- 3.1 Planteamiento del problema y nuestros resultados 37
- 3.2 Lemas 39
  - 3.2.1 Resultante de polinomios 39
  - 3.2.2 Elementos acerca de los enteros algebraicos 43
  - 3.2.3 Elementos de la geometría de números 43
- 3.3 Demostración del Teorema 3.1 44
- 3.4 Demostración del Teorema 3.2 53

4 Conclusión y trabajo a futuro 57

Bibliografía 59

Resumen/Abstract

Abstract. In this thesis we develop two topics, the first one deals with the study of the representability of elements in prime fields as sums of fractions; more precisely, for n a positive integer and $\lambda \in \mathbb{F}_p$ we are interested in the solubility of the congruence

$$\sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p},$$

with $x_i \in \mathcal{I}$ and $y_i \in \mathcal{J}$, for $\mathcal{I} \neq \{0\}$, $\mathcal{J} \neq \{0\}$ short intervals from $\mathbb{F}_p$.

For the second part, we work in obtaining an estimate for the number of solutions to congruences that involve the product of subsets in small intervals modulo a prime; specifically, let $s \in \mathbb{Z}$, h a positive integer and $\mathcal{X} \subset [1, h]$, we are interested in estimate the number $L_4(p, \mathcal{X}, s)$ of solutions to the congruence

$$\prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}.$$

We apply this bound to obtain new results on the number of integer points on exponential curves modulo a prime.

Resumen. En la presente tesis se desarrollan dos temas, el primero concierne al estudio de la representabilidad de elementos en campos primos mediante sumas de fracciones; más precisamente, para n entero positivo y $\lambda \in \mathbb{F}_p$ fijos, nos interesa saber cuándo la congruencia

$$\sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p},$$

admite soluciones con $x_i \in \mathcal{I}$ y $y_i \in \mathcal{J}$, para $\mathcal{I} \neq \{0\}$, $\mathcal{J} \neq \{0\}$ intervalos pequeños de $\mathbb{F}_p$.

El segundo tema trata de la obtención de una estimación fina para el número de

soluciones a congruencias que involucran el producto de subconjuntos en pequeños intervalos módulo primo; de manera concreta, sean $s \in \mathbb{Z}$, h entero positivo y $\mathcal{X} \subset [1, h]$, nos interesa estimar el número $L_4(p, \mathcal{X}, s)$ de soluciones a la congruencia

$$\prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}.$$

Esta estimación encuentra aplicación en la obtención de una cota superior no trivial para el número de puntos enteros sobre curvas exponenciales módulo un primo.

Palabras clave: Campos primos, producto de conjuntos, suma de conjuntos, congruencias multiplicativas, congruencias exponenciales.

Introducción

En el presente trabajo de tesis se desarrollan dos temas, el primero concierne al estudio de la representabilidad de elementos en campos primos mediante sumas de fracciones; más precisamente, para n entero positivo y $\lambda \in \mathbb{F}_p$ fijos, nos interesa saber cuándo la congruencia

$$\sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p},$$

admite soluciones con $x_i \in \mathcal{I}$ y $y_i \in \mathcal{J}$, para $\mathcal{I} \neq \{0\}$, $\mathcal{J} \neq \{0\}$ intervalos de $\mathbb{F}_p$.

El segundo tema trata de la obtención de una estimación fina para el número de soluciones a congruencias que involucran el producto de subconjuntos en pequeños intervalos módulo primo; de manera concreta, sean $s \in \mathbb{Z}$, h entero positivo y $\mathcal{X} \subset [1, h]$, nos interesa estimar el número $L_4(p, \mathcal{X}, s)$ de soluciones a la congruencia

$$\prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}.$$

Esta estimación encuentra aplicación en la obtención de una cota superior no trivial para el número de soluciones (x, y) a la congruencia exponencial

$$x \equiv ag^y \pmod{p},$$

donde a y g son enteros fijos tales que a es primo relativo a p, g tiene orden multiplicativo mayor que h, y (x, y) recorre los puntos enteros de un cuadrado de lado h.

Los resultados de nuestro trabajo en los temas antes mencionados se hallan en los siguientes artículos conjuntos:

I. C. A. Díaz, M. Z. Garaev, *Sums of fractions modulo p*, Arch. Math. 106 (2016), 337-344.

II. C. A. Díaz, M. Z. Garaev, J. Hernández, *Products of subsets of small intervals and points on exponential curves modulo a prime*, Acta Arith. 193 (2020), 309-319.

La tesis consta de tres capítulos. El capítulo uno lo dedicamos a introducir nociones básicas acerca de las congruencias aditivas y su relación con las sumas trigonométricas, así como algunos conceptos elementales sobre la suma y producto de conjuntos en campos primos. El capítulo 2 corresponde a nuestros resultados respecto al problema de sumas de fracciones módulo p. Por último, en el tercer capítulo presentamos nuestro estudio del problema de productos de pequeños intervalos y puntos sobre curvas exponenciales en campos primos. A continuación damos un resumen más detallado del contenido de cada uno de los capítulos.

Resumen al Capítulo 1

En esta parte de la tesis se presentan los conceptos preliminares que serán necesarios en el Capítulo 2. Por ejemplo, se establece la fórmula para el número de soluciones de una congruencia aditiva mediante sumas trigonométricas, y también algunas consideraciones acerca de la suma y producto de conjuntos en $\mathbb{F}_p$.

Dados $X_1, X_2, \ldots, X_n \subset \mathbb{Z}$, $\lambda \in \mathbb{Z}$ y m un entero positivo, una congruencia aditiva es una de la forma

$$\begin{cases} x_1 + x_2 + \ldots + x_n \equiv \lambda \pmod{m}, \\ x_1 \in X_1, x_2 \in X_2, \ldots, x_n \in X_n. \end{cases}$$

El problema principal es determinar cuando una congruencia aditiva tiene solución y, de ser posible, proporcionar una fórmula asintótica para el número de soluciones.

Resumen al Capítulo 2

Las preguntas que involucran suma de fracciones módulo p han sido de interés en el ámbito de las congruencias aditivas. Una de tales cuestiones es el llamado problema de Erdős-Graham el cual busca saber si es verdad que para todo $c > 0$, existe $k_0 = k_0(c)$ tal que para cualquier primo p y $\lambda \in \mathbb{Z}$, existen $k \leq k_0$ enteros $x_i \in [1, p^c]$, $i = 1, 2, \ldots, k$, tales que

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_k} \equiv \lambda \pmod{p}. \tag{1}$$

Si $c > 1/2$ la respuesta afirmativa se sigue de estimaciones clásicas para las sumas de Kloosterman. El caso $c \leq 1/2$ fue resuelto por Shparlinski [21] utilizando estimaciones de Karatsuba para un análogo a las sumas de Kloosterman.

De manera natural uno se puede preguntar por el caso de intervalos no iniciales, es decir, de la forma $[L+1, L+p^c]$. Resulta que si $c \leq 1/2$ es de una dificultad mucho

mayor, donde el principal obstáculo proviene de que ahora no hay control sobre el tamaño de los productos de elementos del intervalo. Si bien esta pregunta permanece abierta, Shparlinski [20] estableció que si en lugar de sumar inversos se consideraban sumas de fracciones, entonces era posible obtener resultados para intervalos arbitrarios con $1/3 < c \leq 1/2$. Ocurre que en su resultado el número de sumandos necesarios es grande cuando c se toma cercano a $1/3$. Más precisamente, utilizando estimaciones de sumas exponenciales con fracciones Shparlinski demostró el siguiente teorema.

Teorema (Shparlinski [20]). *Sean $\mathcal{I}$ y $\mathcal{J}$ dos intervalos en $\mathbb{F}_p$. Entonces el número $R = R(\lambda, \mathcal{I}, \mathcal{J})$ de soluciones a la congruencia*

$$\begin{cases} \frac{x_1}{y_1} + \frac{x_2}{y_2} + \ldots + \frac{x_n}{y_n} \equiv \lambda \pmod{p}, \\ x_1, x_2, \ldots, x_n \in \mathcal{I}, \quad y_1, y_2, \ldots, y_n \in \mathcal{J}, \end{cases} \tag{2}$$

satisface

$$\left| R - \frac{|\mathcal{I}|^n |\mathcal{J}|^n}{p} \right| < |\mathcal{I}||\mathcal{J}| \left(|\mathcal{I}|^{n-2} + (p|\mathcal{J}|)^{\frac{n-2}{2}} \right) p^{o(1)}.$$

De este teorema se sigue que si $n \geq 3$ y $|\mathcal{I}| = |\mathcal{J}| > p^{\frac{n}{3n-2}+\varepsilon}$, entonces la congruencia (2) tiene solución para cualquier $\varepsilon > 0$. Notemos que para que $n/(3n-2) + \varepsilon$ esté cercano a $1/3$ el valor de n debe ser grande.

En nuestro trabajo [9], combinamos herramientas analíticas y combinatorias para obtener la existencia de soluciones a (2) para una cantidad de sumandos menor que la requerida por el teorema de Shparlinski. Los resultados conseguidos son los siguientes.

Teorema (Díaz, Garaev [9]). *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos de $\mathbb{F}_p$ tales que*

$$|\mathcal{I}|^2 |\mathcal{J}| > p^{1+\varepsilon}, \ \ |\mathcal{I}||\mathcal{J}|^2 > p^{1+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\sum_{i=1}^{8} \frac{x_i}{y_i} \equiv \lambda \pmod{p} \tag{3}$$

tiene solución con $x_1, \ldots, x_8 \in \mathcal{I}$ y $y_1, \ldots, y_8 \in \mathcal{J}$.

En particular, de este teorema se sigue que para cualquier $\varepsilon > 0$ existe $\delta = \delta(\varepsilon) > 0$ tal que si $\mathcal{I}$ y $\mathcal{J}$ son intervalos de $\mathbb{F}_p$ con

$$|\mathcal{I}| > p^{\frac{1}{3}+\varepsilon}, \ \ |\mathcal{J}| > p^{\frac{1}{3}-\delta},$$

entonces cualquier elemento $\lambda \in \mathbb{F}_p$ puede ser representado en la forma (3) para algunos $x_1, \dots, x_8 \in \mathcal{I}$ y $y_1, \dots, y_8 \in \mathcal{J}$. Notemos que en este caso (es decir, para $n = 8$) el resultado de Shparlinski garantiza solución cuando $|\mathcal{I}| = |\mathcal{J}| > p^{\frac{4}{11}+\varepsilon}$.

Teorema (Díaz, Garaev [9]). *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos de $\mathbb{F}_p$ tales que*

$$|\mathcal{J}| > p^{\frac{5}{199}}, \ \ |\mathcal{I}||\mathcal{J}|^{\frac{21}{20}} > p^{\frac{3}{4}+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\sum_{i=1}^{12} \frac{x_i}{y_i} \equiv \lambda \pmod{p} \tag{4}$$

tiene solución con $x_1, \dots, x_{12} \in \mathcal{I}$ y $y_1, \dots, y_{12} \in \mathcal{J}$.

De este resultado se sigue que para cualquier $\varepsilon > 0$ existe $\delta = \delta(\varepsilon) > 0$ tal que si $\mathcal{I}$ y $\mathcal{J}$ son intervalos de $\mathbb{F}_p$ con

$$|\mathcal{I}| > p^{\frac{9}{40}+\varepsilon}, \ \ |\mathcal{J}| > p^{\frac{1}{2}-\delta},$$

entonces cualquier elemento $\lambda \in \mathbb{F}_p$ puede ser representado en la forma (4) para algunos $x_1, \dots, x_{12} \in \mathcal{I}$ y $y_1, \dots, y_{12} \in \mathcal{J}$.

Teorema (Díaz, Garaev [9]). *Sean k un entero positivo fijo e $\mathcal{I}$ y $\mathcal{J}$ intervalos de $\mathbb{F}_p$ tales que*

$$|\mathcal{I}||\mathcal{J}|^{\frac{2k}{k+1}} > p^{1+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\sum_{i=1}^{4k} \frac{x_i}{y_i} \equiv \lambda \pmod{p} \tag{5}$$

tiene solución con $x_1, \dots, x_{4k} \in \mathcal{I}$ y $y_1, \dots, y_{4k} \in \mathcal{J}$.

En particular, este teorema implica que para cualquier $\varepsilon > 0$ existe $\delta = \delta(\varepsilon) > 0$, tal que si $\mathcal{I}$ y $\mathcal{J}$ son intervalos de $\mathbb{F}_p$ con

$$|\mathcal{I}| > p^{\frac{1}{k+1}+\varepsilon}, \ \ |\mathcal{J}| > p^{\frac{1}{2}-\delta},$$

entonces cualquier elemento $\lambda \in \mathbb{F}_p$ es representable en la forma

$$\sum_{i=1}^{4k} \frac{x_i}{y_i} \equiv \lambda \pmod{p},$$

para algunos $x_1, \dots, x_{4k} \in \mathcal{I}$ y $y_1, \dots, y_{4k} \in \mathcal{J}$.

Resumen al Capítulo 3

En este capítulo, en primer lugar, estudiaremos congruencias del tipo

$$(x_1 + s) \dots (x_n + s) \equiv (y_1 + s) \dots (y_n + s) \not\equiv 0 \pmod{p},$$

donde p es un número primo, y las variables pertenecen a un intervalo pequeño. Nuestro objetivo es obtener cotas superiores finas para el número de soluciones. Estas cotas serán aplicadas para obtener estimaciones no triviales al número, $J_{a,g}(s;h)$, de soluciones a

$$\begin{cases} x \equiv ag^y \pmod{p}, \\ s+1 \le x, y \le s+h \end{cases} \tag{6}$$

donde $h < p$ es un entero positivo y $g \in \mathbb{F}_p^*$ tiene orden multiplicativo $T > h$; además, $a, s \in \mathbb{Z}$ con $\mathrm{mcd}(a,p) = 1$.

Observando que para $y \in [s+1, s+h]$ fijo hay a lo más un valor de $x \in [s+1, s+h]$ que satisface la congruencia (6), se obtiene la estimación trivial $J_{a,g}(s;h) \le h$.

De la teoría de estimaciones de sumas exponenciales y de caracteres se sabe que si $h < p^{3/4}$, entonces

$$J_{a,g}(s;h) \ll p^{1/2},$$

ver por ejemplo, Vinogradov [22], Montgomery [18] o Garaev [11]. Sin embargo, en el rango $h < p^{1/2}$ esta estimación es peor que la trivial. El problema de obtener cotas no triviales para $J_{a,g}(s;h)$ para todos los rangos de h fue iniciado por Chan y Shparlinski [6], con posteriores refinamientos de Cilleruelo y Garaev [8], y de Bourgain, Garaev, Konyagin y Shparlinski [4, 5]. Más precisamente, para un entero positivo n y un entero $\lambda \not\equiv 0 \pmod{p}$ denotamos con $I_n(s,h,\lambda)$ al número de soluciones de la congruencia

$$(x_1 + s) \dots (x_n + s) \equiv \lambda \pmod{p}, \quad 1 \le x_1, \dots, x_n \le h.$$

Cilleruelo y Garaev [8] mostraron (para el caso $n \in \{2,3\}$), y Bourgain, Garaev, Kon-

yagin y Shparlinski [4] (para cualquier $n \geq 4$), que si $h < p^{1/(n^2-1)}$, entonces se tiene $I_n(s,h,\lambda) \leq h^{o(1)}$. Esto a su vez implica que si $h < p^{1/(n^2-1)}$, entonces

$$J_{a,g}(s;h) \leq h^{1/n+o(1)}.$$

En [5] Bourgain et. al. obtienen nuevas mejoras en el rango de h para $n \in \{2,3\}$. Concretamente, sea $\mathcal{X}$ un subconjunto arbitrario de enteros del intervalo $[1,h]$ con $|\mathcal{X}|$ elementos. Denótese por $L_n(p,\mathcal{X};s)$ al número de soluciones de la congruencia

$$\prod_{i=1}^{n}(x_i+s) \equiv \prod_{j=1}^{n}(y_j+s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}. \tag{7}$$

Bourgain et. al. [5] probaron que si $h^3/|\mathcal{X}| < p$, entonces $L_2(p,\mathcal{X};s) \leq |\mathcal{X}|^2 h^{o(1)}$, y si $h^8/|\mathcal{X}|^4 < p$, entonces $L_3(p,\mathcal{X};s) \leq |\mathcal{X}|^3 h^{o(1)}$. Como una consecuencia de estas estimaciones ellos mostraron que

$$J_{a,g}(s;h) \leq \begin{cases} h^{1/2+o(1)} & \text{si} \quad h < p^{2/5}, \\ h^{1/3+o(1)} & \text{si} \quad h < p^{3/20}. \end{cases} \tag{8}$$

Motivados por los argumentos de [5], obtuvimos una estimación para el número $L_4(p,\mathcal{X};s)$ de soluciones a la congruencia

$$\begin{cases} (x_1+s)\dots(x_4+s) \equiv (y_1+s)\dots(y_4+s) \not\equiv 0 \pmod{p}, \\ x_i, y_j \in \mathcal{X} \subset [1,h]. \end{cases}$$

A partir de la cual conseguimos ampliar el rango de validez de la estimación $J_{a,g}(s;h) \leq h^{1/4+o(1)}$. Nuestros resultados son los siguientes.

Teorema (Díaz, Garaev, Hernandez [10]). *Sea $\mathcal{X} \subseteq [1,h]$ un subconjunto de enteros tal que*

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} < p.$$

Entonces,

$$L_4(p,\mathcal{X};s) \leq |\mathcal{X}|^4 e^{C\frac{\log h}{\log\log h}}$$

para alguna constante absoluta $C > 0$.

Corolario. *Para $h < p^{4/51}$ se cumple que*

$$J_{a,g}(s;h) \leq h^{1/4+o(1)}.$$

Notación

Para un número primo fijo p, denotamos por $\mathbb{F}_p$ al campo de clases residuales módulo p. A los elementos de $\mathbb{F}_p$ los vamos a identificar con los elementos del conjunto $\{0, 1, \ldots, p-1\}$.

Para un conjunto A la cardinalidad de A la estaremos denotando mediante $|A|$. Para $x \in \mathbb{R}$ denotamos por $\|x\|$ a la distancia de x al entero más cercano, es decir, $\|x\| = \min_{n\in\mathbb{Z}}\{|x-n|\}$.

Usaremos la siguiente notación asintótica, escribimos $f(x) \ll g(x)$ para indicar que existe una constante positiva C tal que $|f(x)| \leq Cg(x)$, para x suficientemente grande. En este trabajo, también estaremos utilizando $f(x) = O(g(x))$ de manera equivalente a $f(x) \ll g(x)$. La notación $f(x) = o(g(x))$ significa que $\lim_{x\to\infty} f(x)/g(x) = 0$. Finalmente, para funciones $f, g : (0,\infty) \to \mathbb{R}$ la notación $f(x) = (g(x))^{o(1)}$ indica que para todo $\varepsilon > 0$ existe una constante $c = c(\varepsilon) > 0$ tal que $|f(x)| \leq c\,(g(x))^{\varepsilon}$ para x suficientemente grande.

Por último, para n entero positivo el número de divisores positivos de n lo denotamos por $\tau(n)$, es decir,

$$\tau(n) = \sum_{d|n} 1.$$

Notemos que $\tau(n)$ es el número de soluciones a $d_1 d_2 = n$, en enteros positivos d_1, d_2.

De manera general, para un entero $k \geq 1$, se denota por $\tau_k(n)$ al número de soluciones, en enteros positivos $d_1, \ldots, d_k$, de la ecuación

$$d_1 d_2 \ldots d_k = n.$$

El siguiente resultado clásico lo estaremos utilizando de manera frecuente.

Lema 0.1. *Sea n entero positivo, entonces se cumple que*

$$\tau(n) \leq e^{C\frac{\log n}{\log\log n}},$$

para alguna constante positiva C. En particular, se tiene que $\tau(n) = n^{o(1)}$.

Demostración. Vamos a seguir la demostración presentada en [16]. Sea $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ la descomposición en primos de n. Ya que $\tau(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)$, se tiene

que para cualquier $\delta > 0$ se cumple

$$\frac{\tau(n)}{n^\delta} = \prod_{i=1}^{k} \left(\frac{\alpha_i + 1}{p_i^{\alpha_i \delta}} \right). \tag{9}$$

Como

$$p^{\alpha\delta} \geq 2^{\alpha\delta} = e^{\alpha\delta \log 2} \geq \alpha\delta \log 2,$$

se cumple que

$$\frac{\alpha + 1}{p^{\alpha\delta}} \leq 1 + \frac{1}{\delta \log 2} \leq e^{\frac{1}{\delta \log 2}}.$$

Utilizando esta desigualdad en (9) para los primos menores que $2^{1/\delta}$, se tiene

$$\frac{\tau(n)}{n^\delta} \leq e^{\frac{2^{1/\delta}}{\delta \log 2}} \prod_{p > 2^{1/\delta}} \left(\frac{\alpha_i + 1}{p_i^{\alpha_i \delta}} \right).$$

Por otro lado, si $p \geq 2^{1/\delta}$, entonces

$$p^\delta \geq 2; \quad \frac{\alpha + 1}{p^{\alpha\delta}} \leq \frac{\alpha + 1}{2^\alpha} \leq 1.$$

Por lo tanto,

$$\frac{\tau(n)}{n^\delta} \leq e^{\frac{2^{1/\delta}}{\delta \log 2}}.$$

Tomando

$$\delta = \frac{(1 + \varepsilon) \log 2}{\log \log n},$$

donde $\varepsilon > 0$ es fijo, se sigue que

$$\begin{aligned} \log\left(\frac{\tau(n)}{n^\delta}\right) &\leq \frac{2^{\frac{\log \log n}{(1+\varepsilon) \log 2}} \log \log n}{(1 + \varepsilon) \log^2 2} \\ &= \frac{(\log n)^{\frac{1}{1+\varepsilon}} \log \log n}{(1 + \varepsilon) \log^2 2} \\ &= \frac{(\log n)^{1 - \frac{\varepsilon}{1+\varepsilon}} \log \log n}{(1 + \varepsilon) \log^2 2} \\ &\leq \varepsilon \log 2 \frac{\log n}{\log \log n}, \end{aligned}$$

para n suficientemente grande. Luego

$$\begin{aligned}\log(\tau(n)) &\leq (1+\varepsilon)\log 2\frac{\log n}{\log\log n} + \varepsilon \log 2\frac{\log n}{\log\log n} \\ &= (1+2\varepsilon)\log 2\frac{\log n}{\log\log n}.\end{aligned}$$

Por lo tanto,

$$\tau(n) \leq e^{(1+2\varepsilon)\log 2\frac{\log n}{\log\log n}},$$

para n suficientemente grande. □

Corolario. *Para k entero positivo fijo, se cumple que*

$$\tau_k(n) \leq e^{C\frac{\log n}{\log\log n}},$$

para alguna constante positiva C que solo depende de k.

Demostración. En efecto, notemos que $\tau_k(n)$ es el número de soluciones a

$$d_1 d_2 \ldots d_k = n,$$

en enteros $1 \leq d_1, d_2, \ldots, d_k \leq n$. Ya que cada uno de los d_i es un divisor de n, se sigue que

$$\tau_k(n) \leq (\tau(n))^k.$$

Como k es un entero fijo, el resultado se sigue de la cota para $\tau(n)$. □

Capítulo 1

Congruencias aditivas

1.1 Sumas trigonométricas y congruencias aditivas

Sean m un entero positivo, $\lambda \in \mathbb{Z}$ y $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$ subconjuntos finitos no vacíos de $\mathbb{Z}$. Una congruencia aditiva es una de la forma

$$\begin{cases} x_1 + \cdots + x_n \equiv \lambda \pmod{m}, \\ x_1 \in \mathcal{X}_1, \ldots, x_n \in \mathcal{X}_n. \end{cases} \tag{1.1}$$

El problema general es hallar condiciones bajo las cuales esta congruencia admite solución y obtener, cuando sea posible, una fórmula asintótica para el número de soluciones, cuando $m \to \infty$.

Uno de los métodos utilizados para estudiar el número de soluciones a (1.1) es mediante sumas trigonométricas. El punto de partida para introducir esta herramienta es la siguiente identidad elemental:

$$\frac{1}{m} \sum_{a=0}^{m-1} e^{2\pi i a \frac{x}{m}} = \begin{cases} 1 & \text{si} \quad x \equiv 0 \pmod{m}, \\ 0 & \text{si} \quad x \not\equiv 0 \pmod{m}. \end{cases} \tag{1.2}$$

La cual se sigue a partir de la suma de una progresión geométrica, y del hecho de que $e^{2\pi i \alpha} = 1$ si y sólo si $\alpha \in \mathbb{Z}$.

A partir de la identidad (1.2), al realizar la sustitución $x = x_1 + \cdots + x_n - \lambda$ se obtiene

$$\frac{1}{m} \sum_{a=0}^{m-1} e^{2\pi i a \frac{x_1 + \cdots + x_n - \lambda}{m}} = \begin{cases} 1 & \text{si} \quad x_1 + \cdots + x_n - \lambda \equiv 0 \pmod{m}, \\ 0 & \text{si} \quad x_1 + \cdots + x_n - \lambda \not\equiv 0 \pmod{m}. \end{cases} \tag{1.3}$$

De este modo, vemos que la expresión (1.3) corresponde a la función indicadora del conjunto $\{x_1, \ldots, x_n \in \mathbb{Z} : x_1 + \cdots + x_n \equiv \lambda \pmod{m}\}$. Por lo tanto, si denotamos por J al número de soluciones a (1.1) tenemos que

$$\begin{aligned} J &= \sum_{x_1 \in \mathcal{X}_1} \sum_{x_2 \in \mathcal{X}_2} \cdots \sum_{x_n \in \mathcal{X}_n} \frac{1}{m} \sum_{a=0}^{m-1} e^{2\pi i a \frac{x_1 + \cdots + x_n - \lambda}{m}} \\ &= \frac{1}{m} \sum_{a=0}^{m-1} \sum_{x_1 \in \mathcal{X}_1} \sum_{x_2 \in \mathcal{X}_2} \cdots \sum_{x_n \in \mathcal{X}_n} e^{2\pi i a \frac{x_1 + \cdots + x_n - \lambda}{m}} \end{aligned}$$

Separando el término $a = 0$ se obtiene

$$J = \frac{|\mathcal{X}_1| \ldots |\mathcal{X}_n|}{m} + \text{Error},$$

donde

$$\text{Error} = \frac{1}{m} \sum_{a=1}^{m-1} \sum_{x_1 \in \mathcal{X}_1} \sum_{x_2 \in \mathcal{X}_2} \cdots \sum_{x_n \in \mathcal{X}_n} e^{2\pi i a \frac{x_1 + \cdots + x_n - \lambda}{m}}.$$

El problema de hallar una fórmula asintótica no trivial para J se reduce a investigar bajo qué condiciones se tiene que

$$\text{Error} = o\left(\frac{|\mathcal{X}_1| \ldots |\mathcal{X}_n|}{m}\right).$$

1.2 Suma y producto de conjuntos

Otro método ampliamente utilizado para abordar el problema de la solubilidad de (1.1) es el uso de técnicas combinatorias, concretamente usando resultados de suma y producto de conjuntos en campos primos. En las siguientes líneas presentamos nociones básicas de estos conceptos.

Dados los subconjuntos no vacíos $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n \subset \mathbb{F}_p$, el conjunto suma $\mathcal{X}_1 + \cdots + \mathcal{X}_n$ se define mediante

$$\mathcal{X}_1 + \mathcal{X}_2 + \cdots + \mathcal{X}_n = \{x_1 + \cdots + x_n : x_i \in \mathcal{X}_i, 1 \leq i \leq n\}.$$

Para un entero positivo k y $\mathcal{X} \subset \mathbb{F}_p$ la suma $k-$múltiple de $\mathcal{X}$ se define como

$$k\mathcal{X} = \underbrace{\mathcal{X} + \mathcal{X} + \cdots + \mathcal{X}}_{k \text{ sumandos}} = \{x_1 + \ldots + x_k : x_i \in \mathcal{X}\}.$$

Utilizando la suma de conjuntos el problema de garantizar la existencia de soluciones a (1.1) lo podemos establecer como el problema de demostrar que λ es un elemento de $\mathcal{X}_1 + \cdots + \mathcal{X}_n$.

Análogamente al conjunto suma, el conjunto producto se define por

$$\mathcal{X}_1\mathcal{X}_2 \cdots \mathcal{X}_n = \{x_1x_2 \ldots x_n : x_i \in \mathcal{X}_i, 1 \leq i \leq n\}.$$

También haremos uso de la notación

$$\mathcal{X}^{-1} = \{x^{-1} : x \in \mathcal{X} \setminus \{0\}\}.$$

Sean $\mathcal{X}_1, \ldots, \mathcal{X}_n \subset \mathbb{F}_p$. Para $\lambda \in \mathbb{F}_p$ sea T_λ el número de soluciones a

$$\begin{cases} x_1 + \cdots + x_n \equiv \lambda \pmod{p}, \\ x_i \in \mathcal{X}_i. \end{cases}$$

Haciendo $\mathcal{A} = \{x_1 + \cdots + x_n \pmod{p} : x_i \in \mathcal{X}_i\}$ tenemos que

$$\begin{aligned} \sum_{\lambda \in \mathcal{A}} T_\lambda &= \sum_{\lambda \in \mathcal{A}} |\{(x_1, \ldots, x_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n : x_1 + \cdots + x_n \equiv \lambda \pmod{p}\}| \\ &= |\mathcal{X}_1| \ldots |\mathcal{X}_n|. \end{aligned} \tag{1.4}$$

Y también

$$\begin{aligned} \sum_{\lambda \in \mathcal{A}} T_\lambda^2 &= \sum_{\lambda \in \mathcal{A}} |\{(x_1, \ldots, x_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n : x_1 + \cdots + x_n \equiv \lambda \pmod{p}\}| \times \\ &\quad |\{(y_1, \ldots, y_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n : y_1 + \cdots + y_n \equiv \lambda \pmod{p}\}| \\ &= \sum_{\lambda \in \mathcal{A}} |\{(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n : \\ &\quad x_1 + \cdots + x_n \equiv \lambda \equiv y_1 + \cdots + y_n \pmod{p}\}| \\ &= T, \end{aligned} \tag{1.5}$$

donde T es el número de soluciones a la congruencia simétrica

$$\begin{cases} x_1 + x_2 + \cdots + x_n \equiv y_1 + y_2 + \cdots + y_n \pmod{p}, \\ x_i, y_i \in \mathcal{X}_i. \end{cases}$$

Aplicando la desigualdad de Cauchy-Schwarz a la suma $\sum_{\lambda \in \mathcal{A}} T_\lambda$, y utilizando la

igualdad (1.5) tenemos

$$\sum_{\lambda\in\mathcal{A}} T_\lambda \leq |\mathcal{A}|^{1/2}\left(\sum_{\lambda\in\mathcal{A}} T_\lambda^2\right)^{1/2} = |\mathcal{A}|^{1/2}T^{1/2}.$$

Esta desigualdad junto con (1.4) conducen a una útil relación entre el número de soluciones de una congruencia simétrica y la cardinalidad del conjunto correspondiente, a saber, la siguiente desigualdad

$$|\mathcal{A}| \geq \frac{|\mathcal{X}_1|^2\ldots|\mathcal{X}_n|^2}{T}.$$

Capítulo 2

Suma de fracciones módulo p

2.1 Planteamiento del problema y nuestros resultados

Sean p un número primo, $\lambda \in \mathbb{F}_p$ fijo, e $\mathcal{I}$ y $\mathcal{J}$ dos intervalos en $\mathbb{F}_p$. Vamos a decir que un intervalo $\mathcal{I}$ es *no-cero* si $\mathcal{I} \neq \{0\}$.

Motivados por el trabajo de Shparlinski [20], estudiaremos la siguiente congruencia

$$\begin{cases} \sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p}, \\ x_i \in \mathcal{I}, y_i \in \mathcal{J}, \end{cases} \tag{2.1}$$

donde $\mathcal{I}, \mathcal{J}$ son intervalos no-cero. Usando sumas exponenciales, Shparlinski obtuvo una fórmula asintótica para el número de soluciones a congruencias de la forma $\sum_{i=1}^{n} a_i \frac{x_i}{y_i} \equiv \lambda \pmod{p}$. Para el caso de (2.1), sus resultados implican estimaciones no triviales bajo ciertas condiciones impuestas a los tamaños de $\mathcal{I}$ y $\mathcal{J}$. En particular, si $n \geq 3$ y $|\mathcal{I}| = |\mathcal{J}| > p^{n/(3n-2)+\varepsilon}$, entonces la fórmula asintótica obtenida por Shparlinski resulta ser no trivial para cualquier $\varepsilon > 0$.

En esta parte de la tesis vamos a considerar el problema de la solubilidad de (2.1). La idea principal en la cual descansan nuestros resultados es la de combinar herramientas analíticas y combinatorias. Esta idea nos va a permitir garantizar la existencia de soluciones a (2.1) bajo condiciones más débiles en los tamaños de $\mathcal{I}$ y $\mathcal{J}$. En los enunciados de los teoremas ε siempre denotará una constante positiva fija, y p será un número primo. En seguida presentamos el primer teorema de este capítulo, el cual corresponde a una mejora para el caso $n = 8$.

Teorema 2.1 (Díaz, Garaev [9]). *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos no-cero de $\mathbb{F}_p$ tales que*

$$|\mathcal{I}|^2|\mathcal{J}| > p^{1+\varepsilon}, \quad |\mathcal{I}||\mathcal{J}|^2 > p^{1+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} + \ldots + \frac{x_8}{y_8} \equiv \lambda \pmod{p} \tag{2.2}$$

tiene solución con $(x_1, \ldots, x_8) \in \mathcal{I}^8$ y $(y_1, \ldots, y_8) \in \mathcal{J}^8$.

Del Teorema 2.1 se sigue, en particular, que para cualquier $\varepsilon > 0$ existe un $\delta = \delta(\varepsilon) > 0$ tal que si $|\mathcal{I}| > p^{1/3+\varepsilon}$ y $|\mathcal{J}| > p^{1/3-\delta}$, entonces cualquier elemento $\lambda \in \mathbb{F}_p$ puede ser representado en la forma (2.2) para algunos $(x_1, \ldots, x_8) \in \mathcal{I}^8$ y $(y_1, \ldots, y_8) \in \mathcal{J}^8$. Este resultado representa una mejora respecto a lo obtenido por Shparlinski, pues para este caso de su trabajo se sigue que hay solución cuando $|\mathcal{I}| = |\mathcal{J}| > p^{4/11+\varepsilon}$.

El segundo teorema que enunciaremos corresponde al caso $n = 4k$, para $k \geq 1$.

Teorema 2.2 (Díaz, Garaev [9]). *Sean $k \geq 1$ un entero positivo fijo, $\mathcal{I}$ y $\mathcal{J}$ intervalos no-cero de $\mathbb{F}_p$ tales que*

$$|\mathcal{I}||\mathcal{J}|^{2k/(k+1)} > p^{1+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\sum_{i=1}^{4k} \frac{x_i}{y_i} \equiv \lambda \pmod{p} \tag{2.3}$$

tiene solución con $(x_1, \ldots, x_{4k}) \in \mathcal{I}^{4k}$ y $(y_1, \ldots, y_{4k}) \in \mathcal{J}^{4k}$.

En particular, para cualquier $\varepsilon > 0$ existe $\delta = \delta(\varepsilon, k) > 0$ tal que si $|\mathcal{I}| > p^{1/(k+1)+\varepsilon}$ y $|\mathcal{J}| > p^{1/2-\delta}$, entonces cualquier elemento $\lambda \in \mathbb{F}_p$ es representable en la forma (2.3) para algunos $(x_1, \ldots, x_{4k}) \in \mathcal{I}^{4k}$ y $(y_1, \ldots, y_{4k}) \in \mathcal{J}^{4k}$.

Por último, presentamos un resultado referente al caso $n = 12$.

Teorema 2.3 (Díaz, Garaev [9]). *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos no-cero de $\mathbb{F}_p$ tales que*

$$|\mathcal{J}| > p^{5/199}, \quad |\mathcal{I}||\mathcal{J}|^{21/20} > p^{3/4+\varepsilon}.$$

Entonces para cualquier $\lambda \in \mathbb{F}_p$ la congruencia

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} + \ldots + \frac{x_{12}}{y_{12}} \equiv \lambda \pmod{p} \tag{2.4}$$

tiene solución con $(x_1, \ldots, x_{12}) \in \mathcal{I}^{12}$ *y* $(y_1, \ldots, y_{12}) \in \mathcal{J}^{12}$.

Como una consecuencia del Teorema 2.3 se tiene que para cualquier $\varepsilon > 0$ existe $\delta = \delta(\varepsilon) > 0$ tal que si $|\mathcal{I}| > p^{9/40+\varepsilon}$ y $|\mathcal{J}| > p^{1/2-\delta}$, entonces cualquier $\lambda \in \mathbb{F}_p$ puede ser representado en la forma (2.4) para algunos $(x_1, \ldots, x_{12}) \in \mathcal{I}^{12}$ y $(y_1, \ldots, y_{12}) \in \mathcal{J}^{12}$.

2.2 Lemas

En la obtención de los Teoremas (2.2) y (2.3) se hace uso de la estimación de Weil para las sumas de Kloosterman. Para a, b y $m \geq 1$ enteros, la suma de Kloosterman asociada a estos enteros se define por

$$S(a, b; m) = \sum_{\substack{x \pmod m \\ \mathrm{mcd}(x,m)=1}} e^{2\pi i \frac{ax+bx^{-1}}{m}}.$$

El siguiente lema se encuentra en [15, Corolario 11.12].

Lema 2.1. *Sean* a, b, m *enteros, con* m *positivo. Entonces*

$$|S(a, b; m)| \leq \tau(m) \left(\mathrm{mcd}(a, b, m)\right)^{1/2} m^{1/2}.$$

En particular notamos que en el caso $m = p$ con p primo y $\mathrm{mcd}(a, b, p) = 1$, se tiene $|S(a, b; p)| \leq 2p^{1/2}$.

El resultado del Lema 2.1 lo utilizaremos en conjunción con la siguiente estimación de Vinogradov [23] para una doble suma trigonométrica.

Lema 2.2 (Vinogradov)**.** *Para cualesquier enteros* M, L *con* $M \geq 1$ *se cumple la desigualdad*

$$\sum_{a=1}^{m-1} \left| \sum_{x=L+1}^{L+M} e^{2\pi i \frac{ax}{m}} \right| \leq m \log m.$$

Demostración. Notemos que la suma interior es una suma geométrica la cual se puede calcular como

$$\sum_{x=L+1}^{L+M} e^{2\pi i \frac{ax}{m}} = e^{2\pi i \frac{a(L+1)}{m}} \sum_{x=0}^{M-1} e^{2\pi i \frac{ax}{m}} = e^{2\pi i \frac{a(L+1)}{m}} \left(\frac{e^{2\pi i \frac{aM}{m}} - 1}{e^{2\pi i \frac{a}{m}} - 1} \right).$$

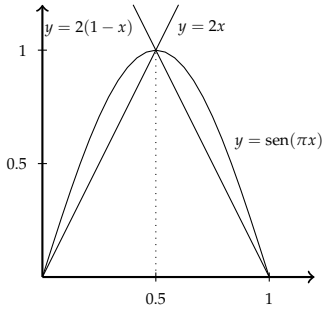

Fig. 2.1

Como

$$\begin{aligned}\frac{e^{2\pi i\frac{aM}{m}}-1}{e^{2\pi i\frac{a}{m}}-1} &= \frac{e^{\pi i\frac{aM}{m}}\left(e^{\pi i\frac{aM}{m}}-e^{-\pi i\frac{aM}{m}}\right)}{e^{\pi i\frac{a}{m}}\left(e^{\pi i\frac{a}{m}}-e^{-\pi i\frac{a}{m}}\right)}\\ &= \frac{e^{\pi i\frac{aM}{m}}}{e^{\pi i\frac{a}{m}}}\left(\frac{\text{sen}\left(\frac{\pi aM}{m}\right)}{\text{sen}\left(\frac{\pi a}{m}\right)}\right),\end{aligned}$$

tenemos que

$$\begin{aligned}\left|\sum_{x=L+1}^{L+M} e^{2\pi i\frac{ax}{m}}\right| &= \left|e^{2\pi i\frac{a(L+1)}{m}}\left(\frac{e^{\pi i\frac{aM}{m}}}{e^{\pi i\frac{a}{m}}}\right)\left(\frac{\text{sen}\left(\frac{\pi aM}{m}\right)}{\text{sen}\left(\frac{\pi a}{m}\right)}\right)\right|\\ &\leq \left|\frac{\text{sen}\left(\frac{\pi aM}{m}\right)}{\text{sen}\left(\frac{\pi a}{m}\right)}\right|\\ &\leq \frac{1}{\left|\text{sen}\left(\frac{\pi a}{m}\right)\right|}.\end{aligned}$$

De la figura (2.1) tenemos que

$$\text{sen}(\pi x) \geq \begin{cases} 2x & \text{si} \quad 0 \leq x \leq 1/2, \\ 2(1-x) & \text{si} \quad 1/2 \leq x \leq 1. \end{cases}$$

Luego $\text{sen}(\pi x) \geq 2\|x\|$ para $0 \leq x \leq 1$. Por lo tanto,

$$\frac{1}{\left|\text{sen}\left(\frac{\pi a}{m}\right)\right|} \leq \frac{1}{2\|\frac{a}{m}\|}.$$

Como $\|x\| = \|1-x\|$ y para $1 \leq a \leq m/2$ se tiene $\|\frac{a}{m}\| = \frac{a}{m}$ se sigue

$$\sum_{a=1}^{m-1} \left| \sum_{x=L+1}^{L+M} e^{2\pi i \frac{ax}{m}} \right| \leq 2 \sum_{a=1}^{m/2} \frac{m}{2a} \leq m \log m. \qquad \square$$

Del trabajo de Glibichuk [14] se sabe que si $|\mathcal{X}||\mathcal{Y}| > 2p$, entonces $8\mathcal{X}\mathcal{Y} = \mathbb{F}_p$. La siguiente versión obtenida por Garaev y García [12] (ver también García [13] para una afirmación más general) será parte importante en la obtención de nuestros resultados.

Lema 2.3 (Garaev-García). *Sean $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ subconjuntos de $\mathbb{F}_p^*$ tales que*

$$|\mathcal{A}||\mathcal{C}| > (2+\sqrt{2})p, \quad |\mathcal{B}||\mathcal{D}| > (2+\sqrt{2})p.$$

Entonces

$$(2\mathcal{A})(2\mathcal{B}) + (2\mathcal{C})(2\mathcal{D}) = \mathbb{F}_p.$$

Demostración. Consideremos el siguiente conjunto

$$\mathcal{H} = \left\{ \frac{d_1+d_2}{b_1+b_2} \pmod p : d_1, d_2 \in \mathcal{D}, b_1, b_2 \in \mathcal{B} \quad \text{y} \quad b_1+b_2 \not\equiv 0 \pmod p \right\}.$$

`Afirmación.` Si $|\mathcal{B}||\mathcal{D}| > p$ entonces $|\mathcal{H}| > p - \frac{p^2}{|\mathcal{B}||\mathcal{D}|-p}$.

En efecto, consideremos el conjunto $R = \mathbb{F}_p \setminus \mathcal{H}$. Sea I el número de soluciones a la congruencia

$$\begin{cases} d_1+d_2 \equiv \lambda(b_1+b_2) \pmod p, \\ d_1, d_2 \in \mathcal{D}, \quad b_1, b_2 \in \mathcal{B}, \quad \lambda \in R. \end{cases}$$

Ya que $\lambda \in R$ se sigue que las únicas posibles soluciones son cuando $b_1+b_2 \equiv 0 \pmod p$, luego también debemos tener que $d_1+d_2 \equiv 0 \pmod p$. De estas consideraciones se sigue que $I \leq |\mathcal{B}||\mathcal{D}||R|$. Por otro lado, expresando a I mediante sumas trigonométricas tenemos que

$$\begin{aligned} I &= \sum_{d_1,d_2 \in \mathcal{D}} \sum_{b_1,b_2 \in \mathcal{B}} \sum_{\lambda \in R} \frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(d_1+d_2-\lambda(b_1+b_2))}{p}} \\ &= \frac{|\mathcal{B}|^2|\mathcal{D}|^2|R|}{p} + \frac{1}{p} \sum_{a=1}^{p-1} \left(\sum_{d \in \mathcal{D}} e^{2\pi i \frac{ad}{p}} \right)^2 \sum_{\lambda \in R} \left(\sum_{b \in \mathcal{B}} e^{-2\pi i \frac{a\lambda b}{p}} \right)^2. \end{aligned}$$

Recordando que $I \leq |\mathcal{B}||\mathcal{D}||R|$, tenemos que

$$\begin{aligned}
\frac{|\mathcal{B}|^2|\mathcal{D}|^2|R|}{p} &\leq |\mathcal{B}||\mathcal{D}||R| + \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{d\in\mathcal{D}} e^{2\pi i\frac{ad}{p}}\right|^2 \sum_{\lambda\in R}\left|\sum_{b\in\mathcal{B}} e^{-2\pi i\frac{a\lambda b}{p}}\right|^2 \\
&\leq |\mathcal{B}||\mathcal{D}||R| + \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{d\in\mathcal{D}} e^{2\pi i\frac{ad}{p}}\right|^2 \sum_{\lambda=0}^{p-1}\left|\sum_{b\in\mathcal{B}} e^{-2\pi i\frac{a\lambda b}{p}}\right|^2 \\
&= |\mathcal{B}||\mathcal{D}||R| + \frac{(p|\mathcal{B}|)}{p}\sum_{a=1}^{p-1}\left|\sum_{d\in\mathcal{D}} e^{2\pi i\frac{ad}{p}}\right|^2 \\
&\leq |\mathcal{B}||\mathcal{D}||R| + |\mathcal{B}|\sum_{a=0}^{p-1}\left|\sum_{d\in\mathcal{D}} e^{2\pi i\frac{ad}{p}}\right|^2 \\
&= |\mathcal{B}||\mathcal{D}||R| + p|\mathcal{B}||\mathcal{D}|.
\end{aligned}$$

De aquí se sigue que $|R|(|\mathcal{B}||\mathcal{D}| - p) \leq p^2$. Ya que $|\mathcal{B}||\mathcal{D}| > p$, tenemos que $|R| \leq \frac{p^2}{|\mathcal{B}||\mathcal{D}|-p}$. De este modo obtenemos que

$$|\mathcal{H}| = p - |R| \geq p - \frac{p^2}{|\mathcal{B}||\mathcal{D}| - p},$$

lo cual demuestra la afirmación.

Continuando con la demostración del lema, denotemos por T al número de soluciones a la congruencia

$$\begin{cases} a + hc \equiv a_1 + hc_1 \pmod{p}, \\ a, a_1 \in \mathcal{A}, \quad c, c_1 \in \mathcal{C}, \quad h \in \mathcal{H}. \end{cases} \tag{2.5}$$

Observemos que si tomamos $c = c_1$ en (2.5), entonces $a = a_1$ y en este caso la congruencia tendrá a lo más $|\mathcal{A}||\mathcal{C}||\mathcal{H}|$ soluciones. Por otro lado, si tomamos $c \neq c_1$ entonces h queda unívocamente determinado y tendremos a lo más $|\mathcal{A}|(|\mathcal{A}| - 1)|\mathcal{C}|(|\mathcal{C}| - 1)$ soluciones. De lo anterior se sigue que $T \leq |\mathcal{A}||\mathcal{C}||\mathcal{H}| + |\mathcal{A}|(|\mathcal{A}| - 1)|\mathcal{C}|(|\mathcal{C}| - 1)$. Luego, existe un $h_0 \in \mathcal{H}$ tal que el número, $T(h_0)$, de soluciones a

$$\begin{cases} a + h_0c \equiv a_1 + h_0c_1 \pmod{p}, \\ a, a_1 \in \mathcal{A}, \quad c, c_1 \in \mathcal{C}, \end{cases}$$

satisface

$$T(h_0) \leq |\mathcal{A}||\mathcal{C}| + \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{H}|}.$$

Recordando la relación entre el número de soluciones a una congruencia simétrica y el tamaño del conjunto correspondiente, tenemos

$$|\mathcal{A} + h_0\mathcal{C}| \geq \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{T(h_0)} \geq \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{A}||\mathcal{C}| + \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{H}|}} = \frac{|\mathcal{A}||\mathcal{C}|}{1 + \frac{|\mathcal{A}||\mathcal{C}|}{|\mathcal{H}|}}.$$

Utilizando el resultado de la afirmación se sigue que

$$|\mathcal{A} + h_0\mathcal{C}| > \frac{p}{2}.$$

Por lo tanto, para cualquier $\lambda \in \mathbb{F}_p$ se cumple que $|\lambda - (\mathcal{A} + h_0\mathcal{C})| > \frac{p}{2}$, de donde $(\mathcal{A} + h_0\mathcal{C}) \cap (\lambda - (\mathcal{A} + h_0\mathcal{C})) \neq \emptyset$. Es decir, para cualquier $\lambda \in \mathbb{F}_p$ existen $a_1, a_2 \in \mathcal{A}$ y $c_1, c_2 \in \mathcal{C}$ tales que

$$a_1 + h_0c_1 \equiv \lambda - a_2 - h_0c_2 \pmod{p}.$$

La demostración termina notando que h_0 es de la forma $h_0 = \frac{d_1+d_2}{b_1+b_2}$ para algunos $d_1, d_2 \in \mathcal{D}$ y $b_1, b_2 \in \mathcal{B}$ con $b_1 + b_2 \not\equiv 0 \pmod{p}$. □

El siguiente resultado se debe a Cilleruelo y Garaev [8].

Lema 2.4 (Cilleruelo-Garaev)**.** *Sean $\mathcal{J}$ un intervalo en $\mathbb{F}_p$, y $\lambda \in \mathbb{F}_p^*$. Entonces el número W_λ de soluciones a la congruencia*

$$xy \equiv \lambda \pmod{p}, \quad x, y \in \mathcal{J},$$

satisface

$$W_\lambda < \frac{|\mathcal{J}|^{3/2+o(1)}}{p^{1/2}} + |\mathcal{J}|^{o(1)}.$$

Demostración. Consideremos el intervalo $\mathcal{J} = \{L+1, L+2, \ldots, L+M\}$ en $\mathbb{F}_p$. Notemos que la congruencia $xy \equiv \lambda \pmod{p}$, $x, y \in \mathcal{J}$ es equivalente a

$$\begin{cases} xy + L(x+y) \equiv \lambda - L^2 \pmod{p}, \\ 1 \leq x, y \leq M. \end{cases} \tag{2.6}$$

Por el principio de las casillas de Dirichlet tenemos que para cada entero positivo $T < p$

existe un entero $1 \leq t \leq T$ y un entero u_0 tal que

$$tL \equiv u_0 \pmod{p}, \quad |u_0| \leq \frac{p}{T}.$$

De (2.6) obtenemos que

$$txy + u_0(x+y) \equiv c \pmod{p}, \quad 1 \leq x, y \leq M,$$

con $c \equiv t(\lambda - L^2) \pmod{p}$ y $0 \leq c < p$. Escribiendo esta congruencia como una ecuación tenemos

$$txy + u_0(x+y) = c - zp, \quad 1 \leq x, y \leq M, \quad z \in \mathbb{Z}. \tag{2.7}$$

Observando el rango en el que varían los términos involucrados en esta igualdad, tenemos

$$|z| = \left| \frac{txy + u_0(x+y) - c}{p} \right| < \frac{TM^2}{p} + \frac{2M}{T} + 1.$$

Por lo tanto, tomando $T \sim \sqrt{\frac{p}{M}}$ se sigue que $z \ll \left(\frac{M^{3/2}}{p^{1/2}} + 1 \right)$.

Notemos que para cada z la ecuación (2.7) es equivalente a

$$(tx + u_0)(ty + u_0) = n_z, \quad 1 \leq x, y \leq M, \tag{2.8}$$

con $n_z = tc + u_0^2 + tpz$. Dado un entero z sea J_z el número de soluciones a (2.8); entonces tenemos que

$$W_\lambda \ll \left(\frac{M^{3/2}}{p^{1/2}} + 1 \right) \max_{z \in \mathbb{Z}} J_z.$$

Si $M > \frac{p^{1/3}}{10}$, para cada z el número de soluciones J_z está acotado por $\tau(n_z)$, el número de divisores de n_z, el cuál es $p^{o(1)} = M^{o(1)}$. Por lo tanto, tenemos $W_\lambda \leq \frac{M^{3/2+o(1)}}{p^{1/2}} + M^{o(1)}$.

Si $M \leq \frac{p^{1/3}}{10}$, en este caso consideremos dos soluciones $(x_0, y_0), (x_1, y_1)$ tales que $\{x_0, y_0\} \cap \{x_1, y_1\} = \emptyset$. Entonces tenemos que

$$L(x_0 + y_0 - x_1 - y_1) \equiv x_1 y_1 - x_0 y_0 \pmod{p},$$

de donde

$$L \equiv ab^{-1} \pmod{p}, \quad 0 < |a| \leq M^2, \quad 0 < |b| \leq 2M.$$

Multiplicando por b a la congruencia (2.6) obtenemos

$$bxy + a(x+y) \equiv b(\lambda - L^2) \pmod{p}.$$

Esta congruencia se puede escribir como

$$bxy + a(x+y) \equiv c_1 \pmod{p}, \tag{2.9}$$

con $c_1 \equiv b(\lambda - L^2) \pmod{p}$ y $|c_1| \leq p/2$. Observando que

$$\begin{aligned} |bxy + a(x+y) - c_1| \leq & 4M^3 + p^{1/2} \\ < & p, \end{aligned}$$

se sigue que la congruencia (2.9) es de hecho una igualdad. Por lo tanto, tenemos

$$bxy + a(x+y) = c_1.$$

Esta igualdad es equivalente a

$$(bx+a)(by+a) = bc_1 + a^2,$$

donde $|bc_1 + a^2| \ll p^{4/3} \ll M^4$. Luego, en este caso el número W_λ de soluciones está acotado por el número de divisores de $bc_1 + a^2$, el cual es $M^{o(1)}$.

Por lo tanto, en cualquier caso tenemos que

$$W_\lambda \leq \frac{|\mathcal{J}|^{3/2+o(1)}}{p^{1/2}} + |\mathcal{J}|^{o(1)}. \qquad \square$$

Consideremos la congruencia $x^{-1} + y^{-1} - \lambda \equiv 0 \pmod{p}$, donde $\lambda \in \mathbb{F}_p^*$. Multiplicando por xy obtenemos que $x + y - \lambda xy \equiv \lambda(x+\lambda^{-1})(y+\lambda^{-1}) - \lambda^{-1} \equiv 0 \pmod{p}$. De aquí se sigue que $(x+\lambda^{-1})(y+\lambda^{-1}) \equiv \lambda^{-2} \pmod{p}$. Y se tiene el siguiente corolario.

Corolario 2.1. *Sean $\mathcal{J}$ un intervalo en $\mathbb{F}_p$, y $\lambda \in \mathbb{F}_p^*$. Entonces el número W_λ de soluciones a la congruencia*

$$x^{-1} + y^{-1} \equiv \lambda \pmod{p}, \quad x, y \in \mathcal{J},$$

satisface

$$W_\lambda < \frac{|\mathcal{J}|^{3/2+o(1)}}{p^{1/2}} + |\mathcal{J}|^{o(1)}. \tag{2.10}$$

Lema 2.5 (Ayyad, Cochrane, Zheng). *Sean $L_1, \dots, L_4$ enteros, y $H_1, \dots, H_4$ enteros positivos. El número J de soluciones a la congruencia*

$$\begin{cases} x_1 x_2 \equiv x_3 x_4 \pmod{p}, \\ L_i + 1 \le x_i \le L_i + H_i, \ i = 1, \dots, 4, \end{cases}$$

satisface

$$J = \frac{|H_1||H_2||H_3||H_4|}{p} + O((|H_1||H_2||H_3||H_4|)^{\frac{1}{2}} \log^2 p)$$

Para la demostración del Teorema 2.2 vamos a necesitar el siguiente resultado de Bourgain y Garaev [3].

Lema 2.6 (Bourgain-Garaev). *Sea $\mathcal{J}$ un intervalo no-cero arbitrario en $\mathbb{F}_p$. Para cualquier entero positivo fijo k, el número T_k de soluciones a la congruencia*

$$\begin{cases} y_1^{-1} + \ldots + y_k^{-1} \equiv y_{k+1}^{-1} + \ldots + y_{2k}^{-1} \pmod{p}, \\ y_1, \dots, y_{2k} \in \mathcal{J}, \end{cases} \tag{2.11}$$

satisface

$$T_k < \left(|\mathcal{J}|^{2k^2/(k+1)} + \frac{|\mathcal{J}|^{2k}}{p} \right) |\mathcal{J}|^{o(1)}. \tag{2.12}$$

Demostración. Sea $\mathcal{J} = \{L+1, L+2, \dots, L+N\}$. Primero consideremos el caso $N < p^{\frac{k+1}{2k}}$. Vamos a ver que en este caso uno obtiene

$$T_k < N^{\frac{2k^2}{k+1} + o(1)}.$$

Sean

$$V = \lfloor N^{(k-1)/(k+1)} \rfloor; \quad Y = \lfloor N^{2/(k+1)} \rfloor; \quad \mathcal{J}_1 = \{L+1, L+2, \dots, L+2N\}.$$

Para un $v \in [0.5V, V]$ dado, definamos la función $\eta_v : \mathcal{J}_1 \to \mathbb{Z}_+$ mediante

$$\eta_v(u) = |\{(u_1, v_1) \in \mathcal{J}_1 \times [0.5V, V] : uv_1 \equiv u_1 v \pmod{p}\}|.$$

Por el Lema 2.5, se sigue que

$$\sum_{u \in \mathcal{J}_1} \sum_{v \in [0.5V, V]} \eta_v(u) < N^{1+o(1)} V.$$

Por lo tanto existe un subconjunto $\mathcal{V} \subset [0.5V, V]$ con $|\mathcal{V}| \sim V$ tal que

$$\sum_{u \in \mathcal{J}_1} \eta_v(u) < N^{1+o(1)} \quad \text{para cualquier} \quad v \in \mathcal{V}. \tag{2.13}$$

Para cualesquiera enteros $y \in \mathcal{Y} = [0.5Y, Y]$ y $v \in \mathcal{V}$ fijos, la cantidad T_k no excede el número de soluciones a la congruencia

$$\frac{1}{u_1 - vy_1} + \cdots + \frac{1}{u_k - vy_k} \equiv \frac{1}{u_{k+1} - vy_{k+1}} + \cdots + \frac{1}{u_{2k} - vy_{2k}} \pmod{p}, \tag{2.14}$$

en enteros $u_i \in \mathcal{J}_1$. Luego, sumando sobre los $y_i \in \mathcal{Y}$ y $v \in \mathcal{V}$ y expresando el número de soluciones a la congruencia (2.14) mediante sumas trigonométricas, obtenemos

$$Y^{2k} V T_k \ll \frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left| \sum_{u \in \mathcal{J}_1} \sum_{y \in \mathcal{Y}} e^{2\pi i \frac{n(u-vy)^{-1}}{p}} \right|^{2k}. \tag{2.15}$$

Para $v \in V$ y B de la forma $B = 2^s < N$, denotemos por

$$S_{v,B} = \{u \in \mathcal{J}_1 : 0.5B \leq \eta_v(u) < B\}.$$

Entonces

$$\mathcal{J}_1 = \bigcup_B S_{v,B},$$

y ya que $v \in \mathcal{V}$, por (2.13) tenemos

$$|S_{v,B}| < \frac{N^{1+o(1)}}{B}. \tag{2.16}$$

De (2.15) se tiene

$$Y^{2k} V T_k \ll \frac{N^{1+o(1)}}{p} \sum_B \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left(\sum_{u \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e^{2\pi i \frac{n(u-vy)^{-1}}{p}} \right| \right)^{2k}.$$

Por lo tanto, de la desigualdad de Hölder y de (2.16), obtenemos para algún B fijo, que

$$Y^{2k} V T_k \ll \frac{N^{o(1)}}{p} \left(\frac{N}{B} \right)^{2k-1} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e^{2\pi i \frac{n(u-vy)^{-1}}{p}} \right|^{2k}. \tag{2.17}$$

La cantidad

$$\frac{1}{p}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\sum_{u\in S_{v,B}}\left|\sum_{y\in\mathcal{Y}}e^{2\pi i\frac{n(u-vy)^{-1}}{p}}\right|^{2k}$$

está acotada por el número de soluciones de la congruencia

$$\begin{cases}\dfrac{1}{u_1-vy_1}+\cdots+\dfrac{1}{u_k-vy_k}\equiv\dfrac{1}{u_{k+1}-vy_{k+1}}+\cdots+\dfrac{1}{u_{2k}-vy_{2k}} \pmod p,\\ v\in\mathcal{V},\quad u\in S_{v,B},\quad y\in\mathcal{Y}.\end{cases}$$

De este modo, se tiene la cota

$$\frac{1}{p}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\sum_{u\in S_{v,B}}\left|\sum_{y\in\mathcal{Y}}e^{2\pi i\frac{n(u-vy)^{-1}}{p}}\right|^{2k}\ll Y^kV\frac{N^{1+o(1)}}{B}+Y^{2k}B.$$

Por lo tanto, de (2.17) se tiene

$$Y^{2k}VT_k\ll N^{2k-1+o(1)}B^{-2k+1}\left(Y^kV\frac{N^{1+o(1)}}{B}+Y^{2k}B\right).$$

Así,

$$T_k<N^{2k+o(1)}Y^{-k}+\frac{N^{2k-1+o(1)}}{V}<N^{\frac{2k^2}{k+1}+o(1)},$$

de donde el resultado es cierto para este caso.

Supongamos ahora que $N>p^{\frac{k+1}{2k}}$. Dividiendo el intervalo $\mathcal{J}=[L+1,L+N]$ en $K\sim Np^{-\frac{k+1}{2k}}$ subintervalos de longitud a lo más $N_1=p^{\frac{k+1}{2k}}$ se tiene que para algunos intervalos $\mathcal{J}_1,\mathcal{J}_2,\ldots,\mathcal{J}_{2k}$ de longitud N_1 se cumple la estimación

$$T_k<K^{2k}R_k\ll\left(\frac{N}{p^{\frac{k+1}{2k}}}\right)^{2k}R_k,$$

donde R_k es el número de soluciones a la congruencia

$$\begin{cases}\dfrac{1}{x_1}+\cdots+\dfrac{1}{x_k}\equiv\dfrac{1}{x_{k+1}}+\cdots+\dfrac{1}{x_{2k}} \pmod p,\\ x_i\in\mathcal{J}_i,\quad i=1,\ldots,2k.\end{cases}$$

Expresando el número de soluciones a esta congruencia mediante sumas trigonométri-

cas, y aplicando la desigualdad de Hölder se llega a

$$R_k \leq \prod_{i=1}^{2k} (R_k(i))^{1/(2k)},$$

donde $R_k(i)$ es el número de soluciones a la congruencia

$$\begin{cases} \dfrac{1}{x_1} + \cdots + \dfrac{1}{x_k} \equiv \dfrac{1}{x_{k+1}} + \cdots + \dfrac{1}{x_{2k}} \pmod{p}, \\ x_1, \ldots, x_{2k} \in \mathcal{J}_i. \end{cases}$$

Por lo tanto, para algún $i = i_0$ se tiene

$$R_k \leq R_k(i_0).$$

Ya que $|\mathcal{J}_{i_0}| < N_1 = p^{\frac{k+1}{2k}}$, tenemos que

$$R_k(i_0) < N_1^{\frac{2k^2}{k+1}+o(1)} = p^k N^{o(1)}.$$

Luego,

$$T_k < \left(\frac{N}{p^{\frac{k+1}{2k}}} \right)^{2k} p^k N^{o(1)} = \frac{N^{2k+o(1)}}{p},$$

y la demostración al Lema (2.6) está completa. □

La demostración al siguiente lema se encuentra en [20, Lemma 7]. Este será utilizado, siguiendo la prueba de Shaprlinski, para obtener una fórmula asintótica al número de soluciones a (2.1).

Lema 2.7 (Shparlinski)**.** *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos de $[0, p-1]$ y sea $\mathcal{W} \subset \mathcal{I} \times \mathcal{J}$ un conjunto convexo arbitrario. Entonces, uniformemente sobre sobre los enteros a primos relativos con p, se cumple*

$$\sum_{(x,y)\in\mathcal{W}} e^{2\pi i a \frac{xy^{-1}}{p}} \ll \left(|\mathcal{I}| + p^{1/2} |\mathcal{J}|^{1/2} \right) p^{o(1)}.$$

El último resultado que se demostrará en esta sección es la fórmula asintótica hallada por Shparlinski [20] para el número de soluciones a (2.1). Esta fórmula la vamos a utilizar en la demostración del Teorema 2.3, concretamente, en el caso de intervalos $\mathcal{J}$ relativamente pequeños.

Lema 2.8 (Shparlinski)**.** *Sean $\mathcal{I}$ y $\mathcal{J}$ intervalos no-cero de $\mathbb{F}_p$. Entonces el número R =*

$R(\lambda, \mathcal{I}, \mathcal{J})$ de soluciones a

$$\sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p},$$

con $x_i \in \mathcal{I}, y_i \in \mathcal{J}$, satisface

$$\left| R - \frac{|\mathcal{I}|^n |\mathcal{J}|^n}{p} \right| < |\mathcal{I}||\mathcal{J}| \left(|\mathcal{I}|^{n-2} + (p|\mathcal{J}|)^{(n-2)/2} \right) p^{o(1)}. \tag{2.18}$$

Demostración. Escribiendo a R mediante sumas exponenciales tenemos que

$$R = \sum_{x_1,\dots,x_n \in \mathcal{I}} \sum_{y_1,\dots,y_n \in \mathcal{J}\setminus\{0\}} \frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i a \frac{(x_1 y_1^{-1} + \cdots + x_n y_n^{-1} - \lambda)}{p}}.$$

Intercambiando el orden de sumación tenemos

$$\begin{aligned} R &= \frac{1}{p} \sum_{a=0}^{p-1} e^{-2\pi i a\lambda} \left(\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}\setminus\{0\}} e^{2\pi i a \frac{(xy^{-1})}{p}} \right)^n \\ &\leq \frac{|\mathcal{I}|^n |\mathcal{J}|^n}{p} + \frac{1}{p} \sum_{a=1}^{p-1} e^{-2\pi i a\lambda} \left(\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}\setminus\{0\}} e^{2\pi i a \frac{(xy^{-1})}{p}} \right)^n. \end{aligned}$$

Para estimar el tamaño de la suma de la derecha, primero aplicamos el Lema 2.7 para obtener una cota superior para la potencia $n-2$ de la doble suma interior, y se obtiene

$$R - \frac{|\mathcal{I}|^n |\mathcal{J}|^n}{p} \leq p^{-1+o(1)} \left(|\mathcal{I}| + p^{1/2} |\mathcal{J}|^{1/2} \right)^{n-2} W, \tag{2.19}$$

donde

$$W = \sum_{a=1}^{p-1} \left| \sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}\setminus\{0\}} e^{2\pi i a \frac{(xy^{-1})}{p}} \right|^2.$$

Para esta última suma tenemos que

$$W = \sum_{a=1}^{p-1} \left| \sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}\setminus\{0\}} e^{2\pi i a \frac{(xy^{-1})}{p}} \right|^2 = \sum_{a=0}^{p-1} \left| \sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}\setminus\{0\}} e^{2\pi i a \frac{(xy^{-1})}{p}} \right|^2 - |\mathcal{I}|^2 |\mathcal{J}|^2. \tag{2.20}$$

Expandiendo el cuadrado e intercambiando el orden de sumación se obtiene

$$\sum_{a=0}^{p-1}\left|\sum_{x\in\mathcal{I}}\sum_{y\in\mathcal{J}\setminus\{0\}}e^{2\pi i a\frac{(xy^{-1})}{p}}\right|^2=\sum_{x_1,x_2\in\mathcal{I}}\sum_{y_1,y_2\in\mathcal{J}\setminus\{0\}}\sum_{a=0}^{p-1}e^{2\pi i a\frac{(x_1y_1^{-1}-x_2y_2^{-1})}{p}}=pT, \qquad (2.21)$$

donde T es el número de soluciones a la congruencia

$$x_1y_2\equiv x_2y_1 \pmod{p}, \quad x_1,x_2\in\mathcal{I}, \quad y_1,y_2\in\mathcal{J}\setminus\{0\}.$$

Por el Lema 2.5 se sigue que

$$T=\frac{|\mathcal{I}|^2|\mathcal{J}|^2}{p}+O\left(|\mathcal{I}||\mathcal{J}|p^{o(1)}\right). \qquad (2.22)$$

De este modo, por (2.20), (2.21) y (2.22) se tiene que

$$W=pT-|\mathcal{I}||\mathcal{J}|\le|\mathcal{I}||\mathcal{J}|p^{1+o(1)}. \qquad (2.23)$$

Por lo tanto, de (2.19) y (2.23) obtenemos

$$R-\frac{|\mathcal{I}|^n|\mathcal{J}|^n}{p}\le|\mathcal{I}||\mathcal{J}|\left(|\mathcal{I}|+p^{1/2}|\mathcal{J}|^{1/2}\right)^{n-2}p^{o(1)}. \qquad (2.24)$$

La demostración termina al observar que para el paréntesis de (2.24) se cumple que

$$\begin{aligned}\left(|\mathcal{I}|+p^{1/2}|\mathcal{J}|^{1/2}\right)^{n-2}&\le 2^{n-2}\,\text{máx}\left\{|\mathcal{I}|,p^{1/2}|\mathcal{J}|^{1/2}\right\}^{n-2}\\&=\text{máx}\left\{|\mathcal{I}|^{n-2},\left(p^{1/2}|\mathcal{J}|^{1/2}\right)^{n-2}\right\}p^{o(1)}\\&=\left(|\mathcal{I}|^{n-2}+(p|\mathcal{J}|)^{\frac{n-2}{2}}\right)p^{o(1)}.\end{aligned}$$

□

2.3 Demostración del Teorema 2.1

Podemos asumir $|\mathcal{I}|>10$, $|\mathcal{J}|>10$. Consideremos un intervalo $\mathcal{I}_0\subset\mathbb{F}_p$ tal que

$$|\mathcal{I}_0|>0.3|\mathcal{I}|, \quad 2\mathcal{I}_0=\mathcal{I}_0+\mathcal{I}_0\subset\mathcal{I}.$$

Es claro que tal intervalo siempre existe. Sea W_λ el número de soluciones a la congruencia

$$\frac{1}{x}+\frac{1}{y}\equiv\lambda \pmod{p}, \quad x,y\in\mathcal{J}\setminus\{0\}.$$

Usando el Corolario 2.1 tenemos que

$$|\mathcal{J}|^2 \ll |\mathcal{J}\setminus\{0\}|^2 = \sum_{\lambda\in\mathcal{J}^{-1}+\mathcal{J}^{-1}} W_\lambda \leq |\mathcal{J}^{-1}+\mathcal{J}^{-1}|\left(\frac{|\mathcal{J}|^{3/2+o(1)}}{p^{1/2}}+|\mathcal{J}|^{o(1)}\right).$$

De aquí se sigue que

$$|\mathcal{J}^{-1}+\mathcal{J}^{-1}| > \text{mín}\left\{|\mathcal{J}|^{2+o(1)}, p^{1/2}|\mathcal{J}|^{1/2+o(1)}\right\}.$$

Denotando por $\mathcal{A}=\mathcal{D}=\mathcal{I}_0\setminus\{0\}$, y por $\mathcal{B}=\mathcal{C}=\left(\mathcal{J}^{-1}+\mathcal{J}^{-1}\right)\setminus\{0\}$. Tenemos que

$$\begin{aligned}|\mathcal{A}||\mathcal{C}| = |\mathcal{B}||\mathcal{D}| &\geq 0.1|\mathcal{I}_0||\mathcal{J}^{-1}+\mathcal{J}^{-1}| \\ &\geq \text{mín}\left\{|\mathcal{I}||\mathcal{J}|^{2+o(1)}, \left(p|\mathcal{I}|^2|\mathcal{J}|\right)^{1/2+o(1)}\right\} \\ &\geq p^{1+0.1\varepsilon} > 4p.\end{aligned}$$

Luego se satisface la condición del Lema 2.3. Por lo tanto, obtenemos

$$(2\mathcal{I}_0)\left(4\mathcal{J}^{-1}\right)+(2\mathcal{I}_0)\left(4\mathcal{J}^{-1}\right)=\mathbb{F}_p.$$

Ya que $2\mathcal{I}_0\subset\mathcal{I}$, la demostración del Teorema 2.1 está completa. □

2.4 Demostración del Teorema 2.2

La demostración consta de dos casos.

Caso 1. $|\mathcal{J}| > p^{(k+1)/2k}$.

Fijemos un elemento $x_0\in\mathcal{I}\setminus\{0\}$, y denotemos por R al número de soluciones a la congruencia

$$\sum_{i=1}^{4k} y_i^{-1}\equiv\lambda x_0^{-1}, \quad y_i\in\mathcal{J}.$$

Basta con mostrar que $R>0$. Denotando por $\mathcal{J}_1=\mathcal{J}\setminus\{0\}$ y expresando R vía

sumas exponenciales tenemos

$$\begin{aligned} R &= \sum_{y_1,\ldots,y_{4k}\in\mathcal{J}_1} \frac{1}{p}\sum_{a=0}^{p-1} e_p\left(a\left(y_1^{-1}+\ldots+y_{4k}^{-1}-\lambda x_0^{-1}\right)\right) \\ &= \frac{|\mathcal{J}_1|^{4k}}{p}+\frac{1}{p}\sum_{a=1}^{p-1}\sum_{y_1,\ldots,y_{4k}\in\mathcal{J}_1} e_p\left(a\left(y_1^{-1}+\ldots+y_{4k}^{-1}\right)e_p\left(-a\lambda x_0^{-1}\right)\right) \\ &= \frac{|\mathcal{J}_1|^{4k}}{p}+\frac{1}{p}\sum_{a=1}^{p-1} e_p\left(-a\lambda x_0^{-1}\right)\left(\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right)^{4k}. \end{aligned}$$

De aquí se sigue que

$$\left|R-\frac{|\mathcal{J}_1|^{4k}}{p}\right| \leq \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right|^{4k}. \tag{2.25}$$

Aquí estamos utilizando la notación $e_p(z) = e^{2\pi iz/p}$. Como una consecuencia de los Lemas 2.1 y 2.2 tenemos

$$\max_{\mathrm{mcd}(a,p)=1}\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right| \leq 3p^{1/2}\log p. \tag{2.26}$$

En efecto, para $\mathrm{mcd}(a,p)=1$ se tiene

$$\begin{aligned} \sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}}{p}} &= \sum_{y\in\mathcal{J}_1}\sum_{x\in\mathcal{J}_1}\frac{1}{p}\sum_{b=0}^{p-1} e^{2\pi i\frac{ay^{-1}}{p}} e^{2\pi i\frac{b(y-x)}{p}} \\ &= \frac{1}{p}\sum_{b=0}^{p-1}\sum_{x\in\mathcal{J}_1} e^{-2\pi i\frac{bx}{p}}\sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}+by}{p}}. \end{aligned}$$

Por lo tanto se tiene que

$$\left|\sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}}{p}}\right| \leq \frac{1}{p}\sum_{b=0}^{p-1}\left|\sum_{x\in\mathcal{J}_1} e^{-2\pi i\frac{bx}{p}}\right|\left|\sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}+by}{p}}\right|.$$

Estimando la suma sobre $y\in\mathcal{J}_1$ mediante el Lema 2.1, y separando el término correspondiente a $b=0$ tenemos

$$\left|\sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}}{p}}\right| \leq \frac{2\,|\mathcal{J}_1|}{p^{1/2}}+\frac{2p^{1/2}}{p}\sum_{b=1}^{p-1}\left|\sum_{x\in\mathcal{J}_1} e^{-2\pi i\frac{bx}{p}}\right|.$$

Finalmente, ya que $|\mathcal{J}_1| < p$ y por el Lema 2.2 se obtiene

$$\begin{aligned}\left|\sum_{y\in\mathcal{J}_1} e^{2\pi i\frac{ay^{-1}}{p}}\right| &\leq 2p^{1/2}+2p^{1/2}\log p\\ &= p^{1/2}\log p\left(2+\frac{2}{\log p}\right)\\ &< 3p^{1/2}\log p.\end{aligned}$$

Ahora, separando un cuadrado de la potencia $4k$ en (2.25), y estimando la potencia $4k-2$ mediante (2.26) tenemos

$$\begin{aligned}\left|R-\frac{|\mathcal{J}_1|^{4k}}{p}\right| &\leq \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right|^2\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right|^{4k-2}\\ &\leq \left(3p^{1/2}\log p\right)^{4k-2}\frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right|^2\\ &\leq \left(3p^{1/2}\log p\right)^{4k-2}\frac{1}{p}\sum_{a=0}^{p-1}\left|\sum_{y\in\mathcal{J}_1} e_p\left(ay^{-1}\right)\right|^2\\ &= \left(3p^{1/2}\log p\right)^{4k-2}\frac{1}{p}\sum_{a=0}^{p-1}\sum_{y_1\in\mathcal{J}_1}\sum_{y_2\in\mathcal{J}_1} e_p\left(a\left(y_1^{-1}-y_2^{-1}\right)\right)\\ &= \left(3p^{1/2}\log p\right)^{4k-2}|\mathcal{J}_1|.\end{aligned}$$

Por lo tanto,

$$R > \frac{|\mathcal{J}_1|^{4k}}{p} - 3^{4k-2}|\mathcal{J}_1|p^{2k-1}(\log p)^{4k-2}.$$

Ya que $|\mathcal{J}_1| \geq |\mathcal{J}|-1 > \frac{1}{2}p^{(k+1)/2k}$, se sigue que $R>0$ y la afirmación se verifica para este caso.

Caso 2. $|\mathcal{J}| < p^{(k+1)/2k}$.
Recordemos que T_k es el número de soluciones a la congruencia

$$\begin{cases} y_1^{-1}+\ldots+y_k^{-1} \equiv y_{k+1}^{-1}+\ldots+y_{2k}^{-1} \pmod p,\\ y_1,\ldots,y_{2k}\in\mathcal{J}.\end{cases}$$

Del Lema 2.6 se sigue que para este caso se cumple

$$T_k < \left(|\mathcal{J}|^{2k^2/(k+1)} + \frac{|\mathcal{J}|^{2k}}{p} \right) |\mathcal{J}|^{o(1)} < |\mathcal{J}|^{2k^2/(k+1)+o(1)}.$$

Por otra parte, de la relación entre el número de soluciones de una ecuación simétrica y la cardinalidad del conjunto correspondiente, tenemos

$$|k\mathcal{J}^{-1}| > \frac{|\mathcal{J}|^{2k}}{|\mathcal{J}|^{2k^2/(k+1)+o(1)}} > |\mathcal{J}|^{2k/(k+1)} p^{-0.1\varepsilon}.$$

Sea $\mathcal{I}_0 \subset \mathbb{F}_p$ un intervalo tal que $|\mathcal{I}_0| > 0.3|\mathcal{I}|$ y $2\mathcal{I}_0 \subset \mathcal{I}$. La condición del Lema 2.3 se satisface con $\mathcal{A} = \mathcal{C} = \mathcal{I}_0$ y $\mathcal{B} = \mathcal{D} = k\mathcal{J}^{-1}$. Luego, obtenemos

$$\mathcal{I}\left(2k\mathcal{J}^{-1}\right) + \mathcal{I}\left(2k\mathcal{J}^{-1}\right) = \mathbb{F}_p$$

esto concluye la demostración del teorema. □

2.5 Demostración del Teorema 2.3

Sea R_1 el número de soluciones a la congruencia (2.4) con $x_i \in \mathcal{I}$, $y_j \in \mathcal{J}$. Hay tres casos a considerar.

Caso 1. $p^{5/199} < |\mathcal{J}| < p^{15/37}$.

En vista del Lema 2.8 (aplicado con $n = 12$) el número R_1 satisface

$$R_1 > \frac{|\mathcal{I}|^{12}|\mathcal{J}|^{12}}{p} - |\mathcal{I}|^{11}|\mathcal{J}|p^{0.1\varepsilon} - |\mathcal{I}||\mathcal{J}|^6 p^{5+0.1\varepsilon}.$$

De la condición del teorema se sigue que

$$|\mathcal{I}|^{11}|\mathcal{J}|p^{0.1\varepsilon} < \frac{0.1|\mathcal{I}|^{12}|\mathcal{J}|^{12}}{p}, \quad |\mathcal{I}||\mathcal{J}|^6 p^{5+0.1\varepsilon} < \frac{0.1|\mathcal{I}|^{12}|\mathcal{J}|^{12}}{p}.$$

Por lo tanto, $R_1 > 0$ y el resultado se sigue en este caso.

Caso 2. $|\mathcal{J}| > p^{5/8}$.

Consideremos un elemento $x_0 \in \mathcal{I} \setminus \{0\}$ fijo. Denotemos por R_2 al número de soluciones a la congruencia

$$y_1^{-1} + \ldots + y_{12}^{-1} \equiv \lambda x_0^{-1} \pmod{p}, \quad y_i \in \mathcal{J}.$$

Basta con mostrar que $R_2 > 0$. Denotando por $\mathcal{J}_1 = \mathcal{J} \setminus \{0\}$ y siguiendo exactamente el mismo argumento que en el **Caso 2** del Teorema 2.2, obtenemos

$$R_2 > \frac{|\mathcal{J}_1|^{12}}{p} - 2^{10}|\mathcal{J}_1|p^5 \left(\log p\right)^{10}.$$

Ya que $|\mathcal{J}_1| \geq |\mathcal{J}| - 1 > 0.5p^{5/8}$, se tiene que $R_2 > 0$.

Caso 3. $p^{15/37} < |\mathcal{J}| < p^{5/8}$.

Siguiendo la notación del Lema 2.6, denotamos por T_k al número de soluciones a la congruencia

$$\frac{1}{y_1} + \cdots + \frac{1}{y_k} \equiv \frac{1}{y_{k+1}} + \cdots + \frac{1}{y_{2k}} \pmod{p}, \quad y_i \in \mathcal{J}. \tag{2.27}$$

`Afirmación`. $T_3 \leq (T_2T_4)^{1/2}$. En efecto, expresando a T_3 mediante sumas trigonométricas tenemos

$$\begin{aligned} T_3 &= \sum_{y_1,\ldots,y_6 \in \mathcal{J}_1} \frac{1}{p} \sum_{a=0}^{p-1} e_p(a(y_1^{-1} + y_2^{-1} + y_3^{-1} - y_4^{-1} - y_5^{-1} - y_6^{-1})) \\ &= \frac{1}{p} \sum_{a=0}^{p-1} \left(\sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right)^3 \left(\overline{\sum_{y \in \mathcal{J}_1} e_p(ay^{-1})} \right)^3 \\ &= \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right|^6 \\ &= \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right|^2 \left| \sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right|^4. \end{aligned}$$

Ahora aplicando la desigualdad de Cauchy-Schwarz se obtiene

$$\begin{aligned} T_3 &\leq \left(\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right|^4 \right)^{1/2} \left(\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{y \in \mathcal{J}_1} e_p(ay^{-1}) \right|^8 \right)^{1/2} \\ &= (T_2T_4)^{1/2}. \end{aligned} \tag{2.28}$$

Observemos que cuando $k = 2$ el lado derecho de la congruencia (2.27) se puede fijar de a lo más $|\mathcal{J}|^2$ maneras distintas. De esta observación y del Corolario 2.1 fácilmente se obtiene que

$$T_2 \leq \left(\frac{|J|^{3/2+o(1)}}{p^{1/2}} + |\mathcal{J}|^{o(1)} \right) |\mathcal{J}|^2.$$

Ya que $|\mathcal{J}| > p^{15/37} > p^{1/3}$, se sigue que

$$T_2 \le \frac{|\mathcal{J}|^{7/2+o(1)}}{p^{1/2}}. \tag{2.29}$$

Más aún, por el Lema 2.6 y la condición $|\mathcal{J}| < p^{5/8}$, tenemos

$$T_4 < |\mathcal{J}|^{32/5+o(1)} + \frac{|\mathcal{J}|^{8+o(1)}}{p} < |\mathcal{J}|^{32/5+o(1)}.$$

Combinando esta estimación con (2.28) y (2.29), se colige que

$$T_3 < \frac{|J|^{99/20+o(1)}}{p^{1/4}}.$$

De la relación que entre el número de soluciones de una congruencia simétrica y la cardinalidad del conjunto correspondiente, se sigue que

$$\frac{|\mathcal{J}|^6}{T_3} \ll |3\mathcal{J}^{-1}| = |\mathcal{J}^{-1} + \mathcal{J}^{-1} + \mathcal{J}^{-1}|.$$

Esto implica que

$$|3\mathcal{J}^{-1}| \ge |\mathcal{J}|^{21/22} p^{1/4-0.1\varepsilon}.$$

Ahora, del mismo modo que en la demostración del Teorema 2.1, consideramos un intervalo $\mathcal{I}_0 \subset \mathbb{F}_p$ que satisface

$$|\mathcal{I}_0| > 0.3|\mathcal{I}|, \quad 2\mathcal{I}_0 \subset \mathcal{I}.$$

Denotando por

$$\mathcal{A} = \mathcal{D} = \mathcal{I}_0 \setminus \{0\}, \quad \mathcal{B} = \mathcal{C} = \left(3\mathcal{J}^{-1}\right) \setminus \{0\}.$$

De lo antes expuesto se infiere que

$$\begin{aligned} |\mathcal{A}||\mathcal{C}| &= |\mathcal{B}||\mathcal{D}| \ge 0.1|\mathcal{I}_0||3\mathcal{J}^{-1}| \\ &\ge |\mathcal{I}||\mathcal{J}|^{21/20} p^{1/4-0.2\varepsilon} \ge p^{1+0.1\varepsilon} \ge 4p. \end{aligned}$$

De esta manera, se satisface la condición del Lema 2.3. Por lo tanto,

$$(2\mathcal{I}_0)\left(6\mathcal{J}^{-1}\right) + (2\mathcal{I}_0)\left(6\mathcal{J}^{-1}\right) = \mathbb{F}_p.$$

Ya que $2\mathcal{I}_0 \subset \mathcal{I}$, la prueba concluye. □

Capítulo 3

Producto de subconjuntos de intervalos en $\mathbb{F}_p$

3.1 Planteamiento del problema y nuestros resultados

Sea p un número primo grande. Consideremos lo siguiente, un entero positivo h, un entero g de orden multiplicativo $T > h$, y enteros a, s con $\text{mcd}(a, p) = 1$. Denotemos por $J_{a,g}(s;h)$ al número de soluciones a la congruencia

$$\begin{cases} x \equiv ag^y \pmod{p}, \\ s+1 \leq x, y \leq s+h. \end{cases} \tag{3.1}$$

Queremos estimar superiormente a $J_{a,g}(s;h)$. Notemos que para un $s+1 \leq y \leq s+h$ fijo, esta congruencia tiene a lo más una solución $x \in [s+1, s+h]$. Así, la estimación $J_{a,g}(s;h) \leq h$ se cumple de manera trivial.

El problema de encontrar cotas superiores no triviales para $J_{a,g}(s;h)$ se remonta a un trabajo de Vinogradov [22] de 1926, en el cual se establece que

$$J_{a,g}(s;h) = \frac{h^2}{p} + O(p^{1/2}\log^2 p).$$

De esta fórmula asintótica se sigue que cuando $h \gg p^{3/4}\log p$ el comportamiento asintótico de $J_{a,g}(s;h)$ está dado por h^2/p. Por otro lado, si $h < p^{3/4}\log p$ se tiene la siguiente estimación

$$J_{a,g}(s;h) \ll p^{1/2}\log^2 p.$$

Posteriormente este problema y sus variantes han sido considerados en otros traba-

jos (ver por ejemplo [18, 11], y las referencias ahí mencionadas). Sin embargo hasta 2010 todas las cotas obtenidas eran triviales para $h < p^{1/2}$. El problema de encontrar cotas superiores no triviales a $J_{a,g}(s;h)$ para todos los rangos de h fue iniciado por Chan y Shparlinski en [6]. En este trabajo ellos aplican estimaciones explícitas de suma-producto de conjuntos en $\mathbb{F}_p$ para probar que

$$J_{a,g}(s;h) \leq h^{10/11+o(1)},$$

para $h < p^{11/19+o(1)}$. Este resultado fue refinado en los trabajos de Cilleruelo y Garaev [8], y de Bourgain, Garaev, Konyagin y Shparlinski [4, 5]. Concretamente, de [8] y [4] se sabe que para cualquier entero $n \geq 2$ fijo, se cumple

$$J_{a,g} \leq h^{1/n+o(1)} \quad \text{para} \quad h < p^{\frac{1}{n^2-1}}. \tag{3.2}$$

El caso $n \in \{2,3\}$ de este resultado fue establecido en [8], haciendo uso de herramientas de la teoría de aproximación de Dirichlet y propiedades de la ecuación generalizada de Pell. El caso $n \geq 4$ corresponde al trabajo [4], donde se aprovechan aspectos aritméticos de los números algebraicos y propiedades métricas de polinomios.

Las ideas de [4] fueron desarrolladas en [5], donde consideraciones clave acerca de la geometría de los números fueron agregadas. Esto les permitió obtener estimaciones finas para el número de soluciones a congruencias que involucran el producto de subconjuntos de intervalos en $\mathbb{F}_p$. Más precisamente, sea $L_n(p, \mathcal{X}; s)$ el número de soluciones a la congruencia

$$\begin{cases} x_1 x_2 \dots x_n \equiv y_1 y_2 \dots y_n \not\equiv 0 \pmod{p}, \\ x_i, y_i \in \mathcal{X}, \end{cases}$$

donde $\mathcal{X}$ es un subconjunto arbitrario de enteros del intervalo $[s+1, s+h]$. Bourgain et. al. demuestran que

$$L_2(p, \mathcal{X}; s) \leq |\mathcal{X}|^2 h^{o(1)} \quad \text{si} \quad \frac{h^3}{|\mathcal{X}|} < p,$$

y

$$L_3(p, \mathcal{X}; s) \leq |\mathcal{X}|^3 h^{o(1)} \quad \text{si} \quad \frac{h^8}{|\mathcal{X}|^4} < p.$$

Como una consecuencia de estos resultados ellos obtienen la siguiente mejora sobre la

estimación (3.2) para los casos $n = 2, 3$:

$$J_{a,g}(s;h) \leq \begin{cases} h^{1/2+o(1)} & \text{si} \quad h < p^{2/5}, \\ h^{1/3+o(1)} & \text{si} \quad h < p^{3/20}. \end{cases}$$

Basados en las ideas de [4, 5], en el trabajo [10] nosotros establecemos el siguiente resultado.

Teorema 3.1 (Díaz, Garaev, Hernández)**.** *Sea $\mathcal{X} \subseteq [s+1, s+h]$ un subconjunto de enteros tal que*

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} < p.$$

Entonces,

$$L_4(p, \mathcal{X}; s) \leq |\mathcal{X}|^4 e^{C\frac{\log h}{\log\log h}}$$

para alguna constante absoluta $C > 0$.

Este teorema lo aplicamos para obtener una estimación superior para el número de soluciones a (3.1). Específicamente, obtuvimos el siguiente teorema.

Teorema 3.2 (Díaz, Garaev, Hernández)**.** *Para $h < p^{4/51}$ se cumple que*

$$J_{a,g}(s;h) \leq h^{1/4+o(1)}.$$

Notemos que este resultado mejora el rango para h obtenido en [4], de $h < p^{1/15}$ a $h < p^{4/51}$.

3.2 Lemas

3.2.1 Resultante de polinomios

Sean $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ polinomios con coeficientes reales, tales que $a_n \neq 0, b_m \neq 0$. El resultante, $\text{Res}(f, g)$, de f y g se define

como el siguiente determinante

$$\mathrm{Res}(f,g) := \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{vmatrix} = a_n^m b_m^n \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (\lambda_i - \mu_j),$$

donde $\lambda_1, \dots, \lambda_n$ y $\mu_1, \dots, \mu_m$ son las raíces de $f(x)$ y $g(x)$ respectivamente, contadas con multiplicidad.

El siguiente es un resultado clásico de la teoría de polinomios, y será utilizado en la demostración del Teorema 3.1.

Teorema 3.3. *Sean $n, m \geq 0$ y sean f y g dos polinomios no nulos de grados n y m respectivamente. Se cumple que* $\mathrm{Res}(f,g) = 0$ *si y sólo si f y g tienen una raíz común.*

En seguida presentamos una cota para el resultante de polinomios obtenida por Bourgain, Garaev, Konyagin y Shparlinski [5]. Consideremos dos enteros $m, n \geq 2$ y $\sigma \in \mathbb{R}$. Se define la matriz circulante $A(m,n,\sigma)$ de tamaño $(n-1) \times (m+n-2)$ de la siguiente manera

$$A(m,n,\sigma) = \begin{pmatrix} \sigma & \sigma+1 & \dots & \sigma+m-1 & 0 & 0 & \dots & 0 \\ 0 & \sigma & \dots & \sigma+m-2 & \sigma+m-1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \sigma & \sigma+1 & \dots & \dots & \sigma+m-1 \end{pmatrix}.$$

Marquemos todos los elementos en la intersección del i-ésimo renglón y la j-ésima columna si $i \leq j \leq i+m-1$. Notemos que todos los elementos no marcados son cero y, recíprocamente, para $\sigma > 0$ todos los ceros no están marcados.

Lema 3.1 (B-G-K-Sh [5])**.** *Sean $m, n \geq 2$ enteros y $\sigma, \theta \in \mathbb{R}$. Si en la matriz*

$$X(m,n) = \begin{pmatrix} A(m,n,\sigma) \\ A(n,m,\theta) \end{pmatrix}$$

de tamaño $(m+n-2)\times(m+n-2)$*, seleccionamos* $m+n-2$ *elementos marcados de tal forma que cada columna y cada renglón contiene exactamente un elemento seleccionado, la suma de los elementos seleccionados es siempre igual a*

$$\Sigma(m,n,\sigma,\theta) = (m-1+\sigma)(n-1+\theta) - \sigma\theta.$$

Como una consecuencia a este lema se tiene el siguiente corolario.

Corolario 3.1 (B-G-K-Sh [5])**.** *Sean* $M \geq m, n \geq 2$ *enteros,* $\sigma + M - m \geq 0$ *y* $\theta + M - n \geq 0$*. Asuma que una de las siguientes condiciones se cumple*

1. $\sigma \geq 0$*;*
2. $\theta \geq 0$*;*
3. $\sigma + \theta \geq -1$*.*

Entonces $\Sigma(M,M,\sigma,\theta) \geq \Sigma(m,n,\sigma+M-m,\theta+M-n)$*.*

Demostración. Notemos que por el lema anterior

$$\Sigma(M,M,\sigma,\theta) - \Sigma(m,n,\sigma+M-m,\theta+M-n) = (\sigma+M-m)(\theta+M-n) - \sigma\theta.$$

Cualquiera de las condiciones $(1)-(3)$ implica que

$$(\sigma+M-m)(\theta+M-n) \geq \sigma\theta,$$

lo cual demuestra el corolario. □

Finalmente el siguiente lema es un caso particular de un resultado más general de B-G-K-Sh [5].

Lema 3.2. *Sean* $h > 1$ *y* $\sigma, \theta \in \mathbb{R}$ *tales que* $\theta \geq 0$*, y sea* $M \geq 1$ *un entero fijo. Sean* $P_1(Z)$ *y* $P_2(Z)$ *dos polinomios no constantes con coeficientes enteros,*

$$P_1(Z) = \sum_{i=0}^{M} a_i Z^{M-i} \quad y \quad P_2(Z) = \sum_{i=0}^{M} b_i Z^{M-i}$$

tales que

$$|a_i| < Ah^{i+\sigma}, \quad |b_i| < Ah^{i+\theta}, \quad i = 0,1,\ldots,M,$$

para algún A*. Entonces*

$$\mathrm{Res}(P_1,P_2) \ll h^{M^2+M(\sigma+\theta)},$$

donde la constante implicada en $\ll$ *depende únicamente de* A *y* M*.*

Demostración. Sin perdida de generalidad se puede asumir que $A \geq 1$. Definiendo

$$\sigma^* = \sigma + \frac{\log A}{\log h} \quad \text{y} \quad \theta^* = \theta + \frac{\log A}{\log h},$$

se tiene $\sigma^* \geq \sigma$ y $\theta^* \geq \theta \geq 0$. Luego se cumple la condición (2) del Corolario (3.1). De este modo se tiene

$$|a_i| < h^{i+\sigma^*}, \quad |b_i| < h^{i+\theta^*}, \quad i = 0, 1, \ldots, M.$$

Sea $\deg P_1 = m$ y $\deg P_2 = n$. Se tiene que $1 \leq m \leq M$ y $1 \leq n \leq M$.

Las desigualdades

$$|a_{M-m}| \geq 1, \quad |b_{M-n}| \geq 1,$$

implican que

$$\sigma^* + M - m \geq 0, \quad \theta^* + M - n \geq 0.$$

Recordamos que

$$\operatorname{Res}(P_1, P_2) = \det \begin{pmatrix} A_1 \\ A_2 \end{pmatrix},$$

donde

$$A_1 = \begin{pmatrix} a_{M-m} & \ldots & a_{M-1} & a_M & 0 & 0 & \ldots & 0 \\ 0 & a_{M-m} & \ldots & a_{M-1} & a_M & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_{M-m} & \ldots & \ldots & a_{M-1} & a_M \end{pmatrix}$$

y

$$A_2 = \begin{pmatrix} b_{M-n} & \ldots & b_{M-1} & b_M & 0 & 0 & \ldots & 0 \\ 0 & b_{M-n} & \ldots & b_{M-1} & b_M & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & b_{M-n} & \ldots & \ldots & b_{M-1} & b_M \end{pmatrix}.$$

De la representación del determinante mediante sumas y productos de sus elementos, del Lema 3.1 y del Corolario 3.1 se deriva que

$$\operatorname{Res}(P_1, P_2) \ll h^{\Sigma(M,M,\sigma^*,\theta^*)}.$$

Finalmente, la demostración concluye al observar

$$\Sigma(M, M, \sigma^*, \theta^*) = \Sigma(M, M, \sigma, \theta) + O\left(\frac{1}{h}\right). \qquad \square$$

3.2.2 Elementos acerca de los enteros algebraicos

Recordemos que dado un polinomio no nulo $P(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ su altura logarítmica $H(P)$ se define como

$$H(P) = \max_{0 \leq i \leq n} \{\log |a_i|\}.$$

Por extensión, la altura logarítmica de un número algebraico α se define como la altura logarítmica de su polinomio mínimo, esto es, del polinomio mónico de menor grado con coeficientes racionales que tiene a α como raíz.

Vamos a necesitar la cota de Chang [7, Proposición 2.5] para la función divisor en campos de números.

Lema 3.3 (Chang)**.** *Sea $\mathbb{K}$ una extensión finita de $\mathbb{Q}$ de grado $d = [\mathbb{K} : \mathbb{Q}]$, y sea $\mathbb{Z}_\mathbb{K}$ el anillo de enteros en $\mathbb{K}$. Sea también $\gamma \in \mathbb{Z}_\mathbb{K}$ un entero algebraico de altura logarítmica a lo más $H \geq 2$. Entonces el número de pares (γ_1, γ_2) de enteros algebraicos $\gamma_1, \gamma_2 \in \mathbb{Z}_\mathbb{K}$ de altura logarítmica a lo más H con $\gamma = \gamma_1 \gamma_2$ es a lo más $e^{O(H/\log H)}$, donde la constante implicada depende de d.*

También necesitaremos la siguiente consecuencia al Teorema 4.4 de [17].

Lema 3.4. *Sean $P(Z)$ y $Q(Z)$ dos polinomios con coeficientes en $\mathbb{Z}$ tales que $Q|P$. Si P es de altura logarítmica a lo más $H \geq 1$, entonces Q es de altura logarítmica a lo más $H + O(1)$, donde la constante implicada depende solo del grado de P.*

3.2.3 Elementos de la geometría de números

Recordemos que una retícula en $\mathbb{R}^n$ es cualquier subgrupo aditivo de $\mathbb{R}^n$ generado mediante combinaciones lineales enteras de n vectores linealmente independientes. Si $D \subset \mathbb{R}^n$ es compacto, convexo y con interior no vacío, decimos que D es un cuerpo convexo. Diremos que el cuerpo convexo D es centralmente simétrico si para cada $x \in D$ se tiene que $-x \in D$.

Consideremos una retícula $\Gamma \subset \mathbb{R}^n$ y un cuerpo convexo D centralmente simétrico. Para $i = 1, 2, \ldots, n$, el $i-$ésimo mínimo sucesivo $\lambda_i(D, \Gamma)$ de D con respecto a Γ se define como el mínimo número positivo λ tal que el conjunto λD contiene i vectores linealmente independientes de la retícula Γ. De la definición se sigue que $\lambda_1(D, \Gamma) \leq \lambda_2(D, \Gamma) \leq \cdots \leq \lambda_n(D, \Gamma)$. Vamos a necesitar el siguiente resultado de Betke, Henk y Wills [2].

Lema 3.5 (Betke-Henk-Wills)**.** *Para cualquier retícula Γ in $\mathbb{R}^n$ y cualquier cuerpo convexo*

centralmente simétrico D se cumple

$$|D \cap \Gamma| \leq \prod_{i=1}^{n} \left(\frac{2i}{\lambda_i(D,\Gamma)} + 1 \right).$$

Nosotros haremos uso de la siguiente consecuencia al lema anterior.

Corolario 3.2. *Para cualquier retícula Γ in $\mathbb{R}^n$ y cualquier cuerpo convexo centralmente simétrico D tenemos*

$$\prod_{i=1}^{n} \text{mín}\{\lambda_i(D,\Gamma), 1\} \leq \frac{(2n+1)!!}{|D \cap \Gamma|},$$

donde $(2n+1)!!$ denota el producto de los enteros positivos impares menores o iguales que $(2n+1)$.

Demostración (Corolario)**.** Sea $\lambda_i = \lambda_i(D,\Gamma)$. Por el Lema 3.5 se tiene que

$$\begin{aligned} |D \cap \Gamma| &\leq \prod_{i=1}^{n} \left(\frac{2i}{\lambda_i} + 1 \right) \\ &\leq \prod_{i=1}^{n} (2i+1) \, \text{máx} \left\{ \frac{1}{\lambda_i}, 1 \right\} \\ &= (2i+1)!! \prod_{i=1}^{n} \text{máx} \left\{ \frac{1}{\lambda_i}, 1 \right\}. \end{aligned}$$

Entonces

$$\prod_{i=1}^{n} \frac{1}{\text{máx} \left\{ \frac{1}{\lambda_i}, 1 \right\}} \leq (2i+1)!! |D \cap \Gamma|^{-1}.$$

La demostración concluye al notar que $\prod_{i=1}^{n} \frac{1}{\text{máx}\left\{ \frac{1}{\lambda_i}, 1 \right\}} = \prod_{i=1}^{n} \text{mín} \left\{ \lambda_i, 1 \right\}$. □

3.3 Demostración del Teorema 3.1

Recordemos que p denota a un número primo suficientemente grande. Sea $X = |\mathcal{X}|$ y ε una constante positiva pequeña. Observemos que basta con demostrar el teorema bajo las condiciones

$$\frac{h^{14}}{X^6} + \frac{h^{15}}{X^9} < \varepsilon p. \tag{3.3}$$

En efecto, si $X > \varepsilon h$, entonces el resultado se sigue de [5, Teorema 17]. Así, podemos asumir que $X < \varepsilon h$. En este caso podemos encontrar $\mathcal{X}'$ tal que $\mathcal{X} \subset \mathcal{X}' \subset [1,h] \cap \mathbb{Z}$ y

$|\mathcal{X}'| = \lfloor X/\varepsilon \rfloor$. Por lo tanto, para $\mathcal{X}'$ tenemos que

$$\frac{h^{14}}{|\mathcal{X}'|^6} + \frac{h^{15}}{|\mathcal{X}'|^9} < \varepsilon p.$$

y continuamos con $\mathcal{X}'$ en lugar de $|\mathcal{X}|$. Luego, podemos asumir que (3.3) se cumple.

Procediendo por contradicción, supongamos que $L_4(p, \mathcal{X}; s) > X^4 e^{C\frac{\log h}{\log\log h}}$, para alguna constante positiva suficientemente grande C (en otro caso no hay nada más que demostrar).

De (3.3) se sigue que $h^6 < h^8 < \varepsilon p$. En particular, si $s \equiv 0 \pmod p$, la congruencia se convierte en una igualdad con $s = 0$ y la contradicción se sigue para la cota del número de divisores. Entonces, vamos a suponer que $s \not\equiv 0 \pmod p$.

De [5, Teorema 22], vemos que la contribución a $L_4(p, \mathcal{X}; s)$ que proviene del conjunto de soluciones $x_i = y_j$ para algunos $1 \le i, j \le 4$ es a lo más $X^4 e^{O(\log h/\log\log h)}$. Por lo tanto, ya que C es suficientemente grande, podemos asumir que el número J de soluciones a la congruencia

$$\begin{cases} \prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod p, \\ x_i, y_j \in \mathcal{X}, \end{cases} \tag{3.4}$$

sujetas a la condición

$$\{x_1, x_2, x_3, x_4\} \cap \{y_1, y_2, y_3, y_4\} = \emptyset, \tag{3.5}$$

satisface

$$J > X^4 e^{0.6C\frac{\log h}{\log\log h}}. \tag{3.6}$$

Con cada solución $\mathbf{x} = (x_1, x_2, x_3, x_4)$ y $\mathbf{y} = (y_1, y_2, y_3, y_4)$ de (3.4) sujeta a (3.5), asociamos los polinomios

$$P_{\mathbf{x}}(Z) = \prod_{i=1}^{4}(Z + x_i) \quad \text{y} \quad P_{\mathbf{y}}(Z) = \prod_{i=1}^{4}(Z + y_i).$$

Ahora consideremos el polinomio

$$\begin{aligned} R_{\mathbf{x},\mathbf{y}}(Z) &= P_{\mathbf{y}}(Z) - P_{\mathbf{x}}(Z) \\ &= AZ^3 + BZ^2 + CZ + D, \end{aligned}$$

con $|A| \leq 4h$, $|B| \leq 6h^2$, $|C| \leq 4h^3$ y $|D| \leq h^4$.

Ya que $R_{\mathbf{x},\mathbf{y}}(s) \equiv 0 \pmod{p}$ y $h < p^{1/8}$, se sigue que $R_{\mathbf{x},\mathbf{y}}(Z)$ no es un polinomio constante, caso contrario sería idénticamente cero lo que contradice (3.5). Ahora, por el principio de las casillas de Dirichlet, existe x_1^* tal que tenemos al menos J/X soluciones de (3.4) sujetas a (3.5) con el mismo $x_1 = x_1^*$. Afirmamos que cualquier polinomio R inducido por estas soluciones ocurre a lo más $e^{O(\log h/\log\log h)}$ veces. En efecto, fijemos a R y asumamos que $R = R_{\mathbf{x},\mathbf{y}}$. Tenemos que

$$R(-x_1^*) = R_{\mathbf{x},\mathbf{y}}(-x_1^*) = (y_1 - x_1^*)(y_2 - x_1^*)(y_3 - x_1^*)(y_4 - x_1^*).$$

Ya que R está fijo, por el Lema 0.1 de la cota para la función divisor, se sigue que hay a lo más $e^{O(\log h/\log\log h)}$ posibilidades para y_1, y_2, y_3, y_4. Una vez que los y_i han sido fijados, tenemos a lo más $e^{O(\log h/\log\log h)}$ posibilidades para los x_i y la afirmación se sigue.

Por lo tanto, tenemos al menos $X^3 e^{0.5C\frac{\log h}{\log\log h}}$ polinomios diferentes $R_{\mathbf{x},\mathbf{y}}(Z)$. En otras palabras, la congruencia

$$us^3 + vs^2 + ws + t \equiv 0 \pmod{p},$$

tiene al menos $X^3 e^{0.5C\frac{\log h}{\log\log h}} > X^3 \log h$ soluciones en enteros u, v, w, t, sujetos a

$$|u| \leq 4h, \quad |v| \leq 6h^2, \quad |w| \leq 4h^3, \quad |t| \leq h^4.$$

Definimos ahora la retícula [1]

$$\Gamma = \{(u, v, w, t) \in \mathbb{Z}^4 : us^3 + vs^2 + ws + t \equiv 0 \pmod{p}\},$$

y el cuerpo convexo

$$D = \{(u, v, w, t) \in \mathbb{R}^4 : |u| \leq 4h, |v| \leq 6h^2, |w| \leq 4h^3, |t| \leq h^4\}.$$

Por lo visto anteriormente, tenemos que $|\Gamma \cap D| \geq X^3 \log h$. Por lo tanto, por el Corolario 3.2, los mínimos sucesivos $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, 2, 3, 4$, satisfacen la desigualdad

$$\prod_{i=1}^{4} \lambda_i \ll \frac{1}{X^3 \log h}. \tag{3.7}$$

[1] Ya que $\mathbb{Z}^n$ es un grupo abeliano libre finitamente generado, cualquier subgrupo de él también lo será. En particular, Γ es un grupo abeliano libre finitamente generado, y por lo tanto es una retícula.

Ya que h es suficientemente grande, tenemos que $\lambda_1 \leq 1$. Por la definición de los λ_i, tenemos que existen vectores linealmente independientes $(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma$ para $i = 1, 2, 3, 4$. Tenemos los siguientes cuatro casos.

Caso 1: $\lambda_4 \leq 1$. Por la desigualdad (3.7), tenemos $\lambda_1\lambda_2\lambda_3\lambda_4 \ll (X^3 \log h)^{-1}$. Consideremos el determinante

$$\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 & t_1 \\ u_2 & v_2 & w_2 & t_2 \\ u_3 & v_3 & w_3 & t_3 \\ u_4 & v_4 & w_4 & t_4 \end{pmatrix}. \tag{3.8}$$

Ya que $(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma$, tenemos que

$$|u_i| \leq 4h\lambda_i, \quad |v_i| \leq 6h^2\lambda_i, \quad |w_i| \leq 4h^3\lambda_i, \quad |t_i| \leq h^4\lambda_i.$$

Por lo tanto,

$$\Delta \ll \lambda_1\lambda_2\lambda_3\lambda_4 h^{10} \ll \frac{h^{10}}{X^3 \log h} = o(p)$$

cuando $p \to \infty$.

Como el sistema

$$\begin{pmatrix} u_1 & v_1 & w_1 & t_1 \\ u_2 & v_2 & w_2 & t_2 \\ u_3 & v_3 & w_3 & t_3 \\ u_4 & v_4 & w_4 & t_4 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \\ T \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \pmod{p},$$

tiene una solución no trivial, $(X, Y, Z, T) = (s^3, s^2, s, 1)$, se sigue que $\Delta \equiv 0 \pmod{p}$. Recordando que $\Delta = o(p)$ se tiene $\Delta = 0$, lo cual contradice el hecho de que (u_i, v_i, w_i, t_i), $i = 1, 2, 3, 4$, son vectores linealmente independientes. Luego, este caso es imposible.

Caso 2: $\lambda_3 \leq 1, \lambda_4 > 1$. De la desigualdad (3.7) tenemos que $\lambda_1\lambda_2\lambda_3 \ll (X^3 \log h)^{-1}$. Ya que $(u_i, v_i, w_i, t_i) \in \Gamma$ para $i = 1, 2, 3$, se sigue que

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix} \begin{pmatrix} s^3 \\ s^2 \\ s \end{pmatrix} \equiv \begin{pmatrix} -t_1 \\ -t_2 \\ -t_3 \end{pmatrix} \pmod{p}. \tag{3.9}$$

Sean

$$\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}, \quad \Delta_1 = \det \begin{pmatrix} -t_1 & v_1 & w_1 \\ -t_2 & v_2 & w_2 \\ -t_3 & v_3 & w_3 \end{pmatrix},$$

$$\Delta_2 = \det \begin{pmatrix} u_1 & -t_1 & w_1 \\ u_2 & -t_2 & w_2 \\ u_3 & -t_3 & w_3 \end{pmatrix}, \quad \Delta_3 = \det \begin{pmatrix} u_1 & v_1 & -t_1 \\ u_2 & v_2 & -t_2 \\ u_3 & v_3 & -t_3 \end{pmatrix}.$$

Entonces

$$\Delta \ll \frac{h^6}{X^3 \log h}, \quad \Delta_i \ll \frac{h^{10-i}}{X^3 \log h}, \quad i = 1, 2, 3. \tag{3.10}$$

Notemos que

$$\Delta \not\equiv 0 \pmod{p}. \tag{3.11}$$

Pues en otro caso, de la congruencia (3.9) tendríamos

$$\Delta \equiv \Delta_1 \equiv \Delta_2 \equiv \Delta_3 \equiv 0 \pmod{p}.$$

Entonces, por las estimaciones (3.10) se seguiría que

$$\Delta = \Delta_1 = \Delta_2 = \Delta_3 = 0.$$

Esto a su vez implica que el rango de la matriz

$$\begin{pmatrix} u_1 & v_1 & w_1 & t_1 \\ u_2 & v_2 & w_2 & t_2 \\ u_3 & v_3 & w_3 & t_3 \end{pmatrix}$$

es estrictamente menor que 3, lo cual es imposible ya que los vectores

$$(u_1, v_1, w_1, t_1), \quad (u_2, v_2, w_2, t_2), \quad (u_3, v_3, w_3, t_3),$$

son linealmente independientes. Por lo tanto, $\Delta \not\equiv 0 \pmod{p}$.

Entonces, al resolver el sistema (3.9) obtenemos

$$s^3 \equiv \frac{\Delta_1}{\Delta} \pmod{p}, \quad s^2 \equiv \frac{\Delta_2}{\Delta} \pmod{p}, \quad s \equiv \frac{\Delta_3}{\Delta} \pmod{p}. \tag{3.12}$$

De aquí se sigue que

$$\Delta_3^2 \equiv \Delta_2 \Delta \pmod{p}.$$

De las estimaciones (3.10) se sigue que el valor absoluto de ambos lados de esta congruencia es menor que $p/2$. Luego, esta congruencia es, de hecho, una igualdad. Entonces

$$\Delta_3^2 = \Delta_2 \Delta.$$

Por lo tanto, haciendo $d = \pm \mathrm{mcd}(\Delta_2, \Delta)$ para una elección apropiada del signo $\pm$, se sigue que

$$\Delta_2 = da^2, \quad \Delta = db^2, \quad \Delta_3 = dab \tag{3.13}$$

para algunos enteros a y b primos relativos. Sustituyendo esto en (3.12), llegamos a que

$$da^3 \equiv \Delta_1 b \pmod{p}.$$

Ahora, de (3.10) vemos que

$$|da^3| \ll \frac{h^{12}}{X^{4.5}} < \frac{p}{2} \quad \text{y} \quad |\Delta_1 b| \ll \frac{h^{12}}{4.5} < \frac{p}{2}.$$

Por lo tanto, obtenemos la igualdad

$$da^3 = \Delta_1 b.$$

Ya que $\mathrm{mcd}(a, b) = 1$, se sigue que $\Delta_1 = a^3 t$ y $d = bt$, para algún entero t. Entonces también tenemos que $\Delta = b^3 t$. Por lo tanto, de (3.10) tenemos que

$$a \ll \frac{h^3}{X} \quad \text{y} \quad b \ll \frac{h^2}{X}. \tag{3.14}$$

Entonces, de $s \equiv \frac{\Delta_3}{\Delta} \pmod{p}$ y de (3.13) se sigue que

$$s \equiv \frac{a}{b} \pmod{p}.$$

Sustituyendo esto en la congruencia (3.4), obtenemos

$$(bx_1 + a) \cdots (bx_4 + a) - (by_1 + a) \cdots (by_4 + a) \equiv 0 \pmod{p}.$$

De las estimaciones (3.10) y (3.14), así como de las condiciones del teorema se sigue que el valor absoluto del lado izquierdo es menor que p. Por lo tanto, tenemos la igualdad

$$(bx_1 + a)(bx_2 + a)(bx_3 + a)(bx_4 + a) = (by_1 + a)(by_2 + a)(by_3 + a)(by_4 + a).$$

Observemos que $bx_i + a \neq 0$ (en otro caso, $x_i + a/b \equiv 0 \pmod{p}$ lo cual contradice (3.4)). Ahora, hay X^4 maneras de fijar (y_1, y_2, y_3, y_4), y para cada una de ellas el lado izquierdo puede tener a lo más $e^{O(\log h/\log\log h)}$ soluciones en x_1, x_2, x_3, x_4. Esto nos conduce a una contradicción para C suficientemente grande.

Caso 3: $\lambda_2 \leq 1, \lambda_3 > 1$. En este caso tenemos que $\lambda_1\lambda_2 \ll (X^3 \log h)^{-1}$. Y tenemos dos vectores linealmente independientes $(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma$ con

$$|u_i| \leq 4\lambda_i h, \quad |v_i| \leq 6\lambda_i h^2, \quad |w_i| \leq 4\lambda_i h^3, \quad |t_i| \leq \lambda_i h^4,$$

para $i = 1, 2$. Consideremos los polinomios

$$R_1(Z) = u_1 Z^3 + v_1 Z^2 + w_1 Z + t_1 \quad \text{y} \quad R_2(Z) = u_2 Z^3 + v_2 Z^2 + w_2 Z + t_2.$$

Notemos que estos polinomios son no constantes, de otro modo $u_i = v_i = w_i = 0$, y entonces $R_i(s) = t_i \equiv 0 \pmod{p}$, lo que implica que $t_i = 0$ (pues $|t_i| \leq \lambda_i h^4 < p$). Así, $1 \leq deg(R_i) \leq 3$.

Ya que $R_1(s) \equiv R_2(s) \equiv 0 \pmod{p}$, entonces

$$\text{Res}(R_1(Z), R_2(Z)) \equiv \text{Res}(R_1(Z) - R_1(s), R_2(Z) - R_2(s)) \pmod{p}.$$

Como los polinomios $R_i(Z) - R_i(s)$, $i = 1, 2$, tienen a s como raíz común, por el Teorema 3.3 se sigue que $\text{Res}(R_1(Z) - R_1(s), R_2(Z) - R_2(s)) = 0$. Por lo tanto, $\text{Res}(R_1, R_2) \equiv 0 \pmod{p}$. Afirmamos ahora que $\text{Res}(R_1, R_2) = 0$. En efecto, si $\lambda_1 \leq \lambda_2 < 1/(4h)$, entonces $u_1 = u_2 = 0$. Aplicando el Lema 3.2 con $m = 2$ y $\sigma = \theta = 1$, obtenemos que $\text{Res}(R_1, R_2) \ll h^8$. Ya que, $h^8 \ll \varepsilon p$ para una constante positiva pequeña ε, se sigue que $|\text{Res}(\text{R}_1, \text{R}_2)| < p$. La afirmación se obtiene de este hecho y de que $\text{Res}(R_1, R_2) \equiv 0 \pmod{p}$.

Si $\lambda_2 \geq 1/(4h)$, entonces aplicamos el Lema 3.2 con $m = 3$ y

$$\sigma = 1 + \frac{\log 6\lambda_1}{\log h}, \quad \theta = 1 + \frac{\log 6\lambda_2}{\log h} > 0.$$

Recordando que $\lambda_1\lambda_2 \ll X^{-3}$ obtenemos

$$\text{Res}(R_1, R_2) \ll \frac{h^{15}}{X^9}.$$

Ya que $h^{15}/X^9 < \varepsilon p$, obtenemos que $|\text{Res}(R_1, R_2)| < p$ y otra vez la afirmación se sigue.

De este modo, $\mathrm{Res}(R_1, R_2) = 0$. Por lo tanto, los polinomios $R_1(Z)$ y $R_2(Z)$ tienen una raíz en común, digamos β_0. Ya que $R(\beta_0) = 0$, se sigue que uno de los números $u_1\beta_0, v_1\beta_0$ o $w_1\beta_0$ es un entero algebraico (dependiendo si $deg(R_1) = 3, 2$ o 1 respectivamente). Y por el Lema 3.4 este entero algebraico tiene altura logarítmica $O(\log h)$. De aquí se sigue que $\beta_0 = \alpha_0/q$, donde q es un entero positivo, $q < h^3$, y α_0 es un entero algebraico de altura logarítmica $O(\log h)$.

Ahora, dada una solución $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathcal{X}^8$ contada en J, formamos el polinomio

$$R(Z) = \prod_{i=1}^{4}(Z + x_i) - \prod_{j=1}^{4}(Z + y_j).$$

Ya que $R(s) \equiv 0 \pmod{p}$, $R(Z)$ no puede ser un polinomio constante, ya que de otro modo sería idénticamente cero, lo cual contradice (3.5). Así tenemos que

$$R(Z) = UZ^3 + VZ^2 + WZ + T,$$
$$|U| \leq 4h, \quad |V| \leq 6h^2, \quad |W| \leq 4h^3, \quad |T| \leq h^4.$$

Por lo tanto, de $R(s) \equiv 0 \pmod{p}$ se sigue que $(U, V, W, T) \in D \cap \Gamma$. Ya que $\lambda_3 > 1$, obtenemos que (U, V, W, T) es una combinación lineal de (u_1, v_1, w_1, t_1) y (u_2, v_2, w_2, t_2). Digamos

$$(U, V, W, T) = r_1(u_1, v_1, w_1, t_1) + r_2(u_2, v_2, w_2, t_2),$$

para algunos $r_1, r_2 \in \mathbb{R}$. Esto implica que

$$R(Z) = r_1R_1(Z) + r_2R_2(Z). \tag{3.15}$$

Se sigue entonces que $R(\beta_0) = R(\alpha_0/q) = 0$, esto es,

$$\prod_{i=1}^{4}(qx_i + \alpha_0) = \prod_{j=1}^{4}(qy_j + \alpha_0).$$

En particular, esta ecuación tiene al menos J soluciones con $x_i, y_j \in \mathcal{X}$ y $x_i \neq y_j$. Por lo tanto, recordando (3.6), vemos que existe una tupla fija $(y_1, y_2, y_3, y_4) = (b_1, b_2, b_3, b_4) \in \mathcal{X}^4$ tal que la ecuación

$$\prod_{i=1}^{4}(qx_i + \alpha_0) = \prod_{j=1}^{4}(qb_j + \alpha_0), \tag{3.16}$$

tiene al menos

$$\frac{J}{X^4} \geq e^{0.5C \log h / \log\log h} \tag{3.17}$$

soluciones $(x_1, x_2, x_3, x_4) \in \mathcal{X}^4$ con $\{x_1, x_2, x_3, x_4\} \cap \{b_1, b_2, b_3, b_4\} = \emptyset$. En particular,

$$(b_1 + \beta_0)(b_2 + \beta_0)(b_3 + \beta_0)(b_4 + \beta_0) \neq 0.$$

Recordando que $1 \leq x_i \leq h$, $1 \leq q < h^3$ y que α_0 es un entero algebraico de altura logarítmica $O(\log h)$. Ya que los enteros algebraicos son un subanillo de los números complejos, se tiene que los números

$$\prod_{i=1}^{4}(qx_i + \alpha_0) \quad \text{y} \quad \prod_{j=1}^{4}(qb_j + \alpha_0)$$

son enteros algebraicos; más aún son raíces de polinomios de $\mathbb{Z}[X]$ cuyos coeficientes están acotados (en valor absoluto) por $h^{O(1)}$. Por lo tanto, del Lema 3.4, estos números son de altura logarítmica a lo más $O(\log h)$.

Ahora, por el Lema 3.3 concluimos que para un h suficientemente grande la ecuación (3.16) tiene a lo más $e^{C_1 \log h / \log\log h}$ soluciones con $x_1, x_2, x_3, x_4 \in \mathcal{X}$. Esto contradice (3.17) para C suficientemente grande.

Caso 4: $\lambda_1 \leq 1, \lambda_2 > 1$. Sea $(u_1, v_1, w_1, t_1) \in \mathbb{Z}^4$ el vector no cero correspondiente a λ_1. Sabemos que

$$u_1 s^3 + v_1 s^2 + w_1 s + t_1 \equiv 0 \pmod{p}.$$

Consideremos el polinomio

$$R_1(Z) = u_1 Z^3 + v_1 Z^2 + w_1 Z + t_1.$$

Como en el **Caso 3**, tenemos que $R_1(Z)$ es un polinomio no constante. Dada una solución $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathcal{X}^8$ contada en J, consideremos el polinomio

$$R(Z) = \prod_{i=1}^{4}(Z + x_i) - \prod_{j=1}^{4}(Z + y_j).$$

Ya que $R(s) \equiv 0 \pmod{p}$, tenemos que $R(Z)$ también es un polinomio no constante (en otro caso sería idénticamente cero, contradiciendo (3.5)). Procediendo como en el caso anterior, escribimos $R(Z)$ como

$$R(Z) = UZ^3 + VZ^2 + WZ + T,$$
$$|U| \leq 4h, \quad |V| \leq 6h^2, \quad |W| \leq 4h^3, \quad |T| \leq h^4.$$

De $R(s) \equiv 0 \pmod{p}$ se sigue que $(U, V, W, T) \in D \cap \Gamma$. Ya que $\lambda_2 > 0$, los vectores (u_1, v_1, w_1, t_1) y (U, V, W, T) son linealmente dependientes. Luego $R_1(Z)|R(Z)$ en $\mathbb{Q}[Z]$.

Ya que $R_1(Z)$ es un polinomio no constante, tiene una raíz β_0. Entonces β_0 también es raíz de $R(Z)$. A partir de este punto la prueba procede como en el **Caso 3**. Esto concluye la demostración del Teorema 3.1. □

3.4 Demostración del Teorema 3.2

Sea $\mathcal{X}$ el conjunto de aquellos $x \in \{s+1, \ldots, s+h\}$ para los cuales

$$x \equiv ag^y \pmod{p}$$

para algún $y \in \{s+1, \ldots, s+h\}$. Observemos que $|\mathcal{X}| = J_{a,g}(s;h)$.

Para cada $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathcal{X}^8$ tenemos que

$$\frac{x_1x_2x_3x_4}{y_1y_2y_3y_4} \in \{g^t \pmod{p} : t \in [-4h+4, 4h-4]\}.$$

Por lo tanto, por el principio de las casillas de Dirichlet existe un $t_0 \in [-4h+4, 4h-4]$ tal que la congruencia

$$\begin{cases} x_1x_2x_3x_4 \equiv g^{t_0}y_1y_2y_3y_4 \pmod{p}, \\ x_i, y_i \in \mathcal{X} \end{cases} \tag{3.18}$$

tiene al menos $|\mathcal{X}|^8/8h$ soluciones.

Para un $\lambda \in \mathbb{F}_p^*$ fijo, denotemos mediante I_λ al número de soluciones a la congruencia

$$\begin{cases} x_1x_2x_3x_4 \equiv \lambda \pmod{p} \\ x_i \in \mathcal{X}; \end{cases}$$

y por T_λ al número de soluciones a

$$\begin{cases} g^{t_0}y_1y_2y_3y_4 \equiv \lambda \pmod{p} \\ y_i \in \mathcal{X}. \end{cases}$$

Observemos que $\sum_{\lambda=0}^{p-1} I_\lambda T_\lambda$ es el número de soluciones de (3.18). Además, como una

consecuencia de la desigualdad de Cauchy-Schwarz, tenemos que

$$\sum_{\lambda=0}^{p-1} I_\lambda T_\lambda \leq \left(\sum_{\lambda=0}^{p-1} I_\lambda^2\right)^{\frac{1}{2}} \left(\sum_{\lambda=0}^{p-1} T_\lambda^2\right)^{\frac{1}{2}}.$$

Notemos que la suma $\sum_{\lambda=0}^{p-1} I_\lambda^2$ es igual al número de soluciones a la congruencia

$$\begin{cases} x_1x_2x_3x_4 \equiv y_1y_2y_3y_4 \pmod{p}, \\ x_i, y_i \in \mathcal{X}. \end{cases} \tag{3.19}$$

Por otro lado, la suma $\sum_{\lambda=0}^{p-1} T_\lambda^2$ es igual al número de soluciones a la congruencia

$$\begin{cases} g^{t_0}x_1x_2x_3x_4 \equiv g^{t_0}y_1y_2y_3y_4 \pmod{p} \\ x_i, y_i \in \mathcal{X}. \end{cases} \tag{3.20}$$

Ya que g^{t_0} es un elemento invertible de $\mathbb{F}_p$, en esta congruencia podemos cancelar g^{t_0}. De este modo las congruencias (3.19) y (3.20) son equivalentes. Esto implica que

$$\sum_{\lambda=0}^{p-1} I_\lambda^2 = \sum_{\lambda=0}^{p-1} T_\lambda^2,$$

y así

$$\sum_{\lambda=0}^{p-1} I_\lambda T_\lambda \leq \sum_{\lambda=0}^{p-1} I_\lambda^2.$$

Por lo tanto, el número de soluciones de (3.19) es mayor o igual que $|\mathcal{X}|^8/8h$.

Hay dos casos a considerar.

Caso 1.

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} \geq p.$$

En este caso la condición $h < p^{4/51}$ implica que $|\mathcal{X}| < h^{1/4}$ y la afirmación del teorema se sigue.

Caso 2.

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} < p.$$

En este caso, del Teorema 3.1 tenemos

$$\frac{|\mathcal{X}|^8}{8h} \leq |\mathcal{X}|^{4+o(1)}.$$

Por lo tanto, $|\mathcal{X}| \leq h^{\frac{1}{4}+o(1)}$, y la demostración termina. □

Capítulo 4

Conclusión y trabajo a futuro

El objetivo de este trabajo de tesis fue presentar nuestros resultados respecto al estudio del número de soluciones a dos tipos especiales de congruencias módulo un número primo p. La primer congruencia que estudiamos es la siguiente

$$\sum_{i=1}^{n} \frac{x_i}{y_i} \equiv \lambda \pmod{p}, \tag{4.1}$$

donde $n \in \mathbb{Z}^+$ y $\lambda \in \mathbb{F}_p$ son fijos, y $(x_i, y_i) \in \mathcal{I} \times \mathcal{J}$ con intervalos de $\mathbb{F}_p$ tales que $\mathcal{I} \neq \{0\}$, $\mathcal{J} \neq \{0\}$. Esta congruencia fue estudiada en primera instancia por Shparlinski [20], donde obtiene una fórmula asintótica para el número de soluciones.

Respecto a esta congruencia nuestro interés fue obtener condiciones sobre los tamaños de los intervalos $\mathcal{I}, \mathcal{J}$ que garantizaran la existencia de soluciones. En esta dirección, los resultados obtenidos ampliaron el estado del arte cuando $n = 8$, $n = 12$ y $n = 4k$, $k \geq 3$; ver Teoremas 2.1, 2.2 y 2.3. Creemos que nuestros resultados son susceptibles de mejora, por ejemplo, debilitando más las condiciones impuestas a $|\mathcal{I}|$ y $|\mathcal{J}|$. Queda como trabajo a futuro obtener dichas mejoras.

La segunda congruencia que investigamos es

$$\prod_{i=1}^{n}(x_i + s) \equiv \prod_{j=1}^{n}(y_j + s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}, \tag{4.2}$$

donde n es un entero positivo fijo, $s \in \mathbb{Z}$ y $\mathcal{X} \subset [1, h]$ con h un entero positivo. Esta congruencia ha sido estudiada por Bourgain, Garaev, Konyagin y Shparlinski [5] para $n \in \{2, 3\}$.

Para esta congruencia se obtuvo una estimación superior para el número de solu-

ciones, $L_4(p, \mathcal{X}, s)$, a (4.2) cuando $n = 4$. Específicamente, se demostró que

$$L_4(p, \mathcal{X}, s) \leq |\mathcal{X}|^4 e^{C\frac{\log h}{\log\log h}}$$

para alguna constante absoluta $C > 0$ (ver Teorema 3.1). Posteriormente aplicamos esta estimación para obtener una cota superior no trivial para el número de soluciones, $J_{a,g}(s;h)$, a la congruencia

$$x \equiv ag^y \pmod{p}, \tag{4.3}$$

donde a y g son enteros fijos tales que a es primo relativo a p, g tiene orden multiplicativo mayor que un entero positivo h, y las variables x, y pertenecen a $\{s+1, \ldots, s+h\}$ donde $s \in \mathbb{Z}$.

El estudio de $J_{a,g}(s;h)$ se remonta a Vinogradov [22], y desde entonces han habido múltiples trabajos donde pueden encontrarse estimaciones para este número, por ejemplo, [4, 5, 6, 8, 11, 18]. La estimación que nosotros obtuvimos es (ver Teorema 3.2):

$$\text{Si } h < p^{4/51}, \text{ entonces } J_{a,g}(s;h) \leq h^{1/4+o(1)}.$$

Observando la información que se tiene al momento (los casos $n \in \{2, 3, 4\}$), creemos que la siguiente conjetura tiene lugar.

Conjetura 4.1. *Para un entero $n \geq 2$ fijo. Si $h < p^{\frac{n}{(n-1)(n^2+1)}}$, entonces*

$$J_{a,g}(s;h) \leq h^{1/n+o(1)}.$$

Bibliografía

[1] A. Ayyad, T. Cochrane, Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums', *J. Number Theory* **59** (1996), 398–413.

[2] U. Betke, M. Henk, J. M. Wills, 'Succesive-minima-type inequalities', *Discr. Coput. Geom.* **9** (1993), 165–175.

[3] J. Bourgain, M. Z. Garaev, 'Sumsets of reciprocals in prime fields and multilinear Kloosterman sums', (Russian) *Izv. Ross. Akad. Nauk Ser. Mat.* **78** (2004), 19–72, traducción al inglés en *Izv. Math.* **78** (2004), 656–707.

[4] J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comput.* **41** (2012), 1524–1557.

[5] J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Inst. Math.* **280** (2013), 61–90.

[6] T. H. Chan, I. E. Shparlinski,'On the concentration of points on modular hyperbolas and exponential curves', *Acta Arith.* **142** (2010), 59–66.

[7] M. C. Chang, 'Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems', *Geom. and Func. Anal.* **13** (2003), 720–736.

[8] J. Cilleruelo, M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. Func. Anal.* **21** (2011), 892–904.

[9] C. A. Díaz, M. Z. Garaev, 'Sums of fractions modulo p', *Arch. Math.* **106** (2016), 337–344.

[10] C. A. Díaz, M. Z. Garaev, J. Hernández, 'Products of subsets of small intervals and points on exponential curves modulo a prime', *Acta Arith.* **193** (2020), 309–319.

[11] M. Z. Garaev, 'On the logarithmic factor in error term estimates in certain additive congruence problems', *Acta Arith.* **124** (2006), 27–39.

[12] M. Z. Garaev, V. C. García, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications', *J. Number Theory* **128** (2008), 2520–2537.

[13] V. C. García, 'Distribution and additive properties of sequences with terms involving sumsets in prime fields', *Integers* **12** (2012), 8 pp.

[14] A. A. Glibichuk, 'Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem', *Mathematical Notes* **79** No. 3 (2006), 356–365.

[15] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, Rhode Island, 2004.

[16] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford Science Publications, Oxford, sixth edition, 1980.

[17] M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, Berlin, 1992.

[18] H. L. Montgomery, 'Distribution of small powers of a primitive root', *Advances in Number Theory* (Kingston, ON, 1991), Oxford Sci. Publ., Oxford University Press, New York, 1993, pp. 137–149.

[19] I. Schur, 'Über die Kongruenz $x^m + x^m \equiv z^m \bmod p$', *Jahresber. Deutsche Math.-Verein.* **25** (1916), 114–116.

[20] I. E. Shparlinski, 'Linear congruences with ratios', *Proc. Amer. Math. Soc.* Vol. **144** Num. 7 (2016).

[21] I. E. Shparlinski, 'On a question of Erdös and Graham', *Arch. Math.* **78** (2002), 445–448.

[22] I. M. Vinogradov, 'Distribution of index', (Russian) *Dokl. Akad. Nauk SSSR.* **4** (1926), 73–76.

[23] I. M. Vinogradov, *Fundamentos de la teoría de los números*, Ed. Mir, 2da. Edición, 1977.