UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIAS MATEMÁTICAS

FACULTAD DE CIENCIAS

Sobre Ciertos Problemas Aditivos y Multiplicativos en la Teoría Analítica de los Números

TESIS

QUE PARA OBTENER EL GRADO ACADÉMICO DE

DOCTOR EN CIENCIAS

PRESENTA

Victor Cuauhtemoc García Hernández

DIRECTOR DE TESIS: DR. MOUBARIZ GARAEV

MÉXICO, D.F. ENERO, 2009

Agradecimientos

A quienes en todo momento, con mis desatinos y casuales aciertos, insistieron en apoyarme de manera incondicional. Sin duda es a ustedes, familia querida, a quienes debo poquito más que todo.

Quiero expresar un profundo agradecimiento a mi director de tesis el profesor Moubariz Garaev por su infinita paciencia, dedicación y ser un gran ejemplo en muchos sentidos.

A los sinodales; profesores Moubariz Garaev, Luis Del Angel, Javier Cilleruelo, Florian Luca y Gabriel Villa. Gracias por su paciencia y tiempo en la revisión del trabajo y todo lo que implica haber aceptado este compromiso. A los profesores Antonio Zapata, Eugenio Balanzario, Pavel Naumkin, Daniel Juan, Fernando Barrera y Alejandro Casas por el interés y apoyo en este proyecto.

Agradezco también a todo el personal de la UNAM, Morelia y Cuidad de México. En el transcurso de estos estudios fuí becario del Consejo Nacional de Ciencia y Tecnología. También recibí apoyos por parte de la Unidad Morelia (IM-UNAM) y del proyecto PAPIIT IN 100307 de la UNAM.

A los amigos de siempre y a los "nuevos". A ustedes, complices que se volvieron familia, gracias por atravezarse sin cuidado.

Índice general

Introducción

La teoría aditiva de los números tiene un lugar importante en las matemáticas, de manera particular en la teoría de los números.

Dado un conjunto de números enteros $\mathcal{X}$, muchos problemas aditivos pueden enunciarse en la manera siguiente: saber si para algún entero $k \geq 2$ y cierta clase de enteros N la ecuación

$$x_1 + \cdots + x_k = N$$

admite solución para

$$x_1, \ldots, x_k \in \mathcal{X}.$$

Algunos ejemplos clásicos son:

- La *Conjetura de Goldbach.* El ejemplo afirma que todo entero par mayor o igual a cuatro es la suma de dos números primos. En nuestra formulación debe tomarse $\mathcal{X} = \{2, 3, 5, 7, 11, \ldots\}$, el conjunto de los números primos, y para cualquier entero par $N \geq 4$ se debe probar que la ecuación

  $$p + q = N,$$

  tiene solución en los primos p, q. Este problema aún continúa abierto.

- El *Problema de Waring.* La pregunta consiste en saber si dado un entero $n \geq 2$ existe $k = k(n)$ tal que todo entero positivo se escribe como suma de k potencias enésimas. Aquí debemos tomar

  $$\mathcal{X} = \{0^n, 1^n, 2^n, 3^n, \ldots\}$$

y demostrar que para todo entero positivo N la ecuación

$$x_1^n + \cdots + x_k^n = N$$

tiene solución en enteros no negativos $x_1, \ldots, x_k$. El problema de Waring fué resuelto por Hilbert en 1909.

- El problema de Waring planteado en potencias de primos, inicialmente estudiado por Hua y Vinogradov, es conocido como el problema de *Waring-Goldbach.* La pregunta es saber si dado n, existe $k = k(n)$ tal que para ciertos enteros N la ecuación

$$p_1^n + \cdots + p_k^n = N$$

es soluble en números primos $p_1, \ldots, p_k$.

Un panorama amplio acerca del estudio y avance de estos y otros problemas aditivos se puede consultar en [34], [36], [40], [53] y las referencias citadas.

Diremos que $\mathcal{X}$ es una *base aditiva de orden* $k = k(\mathcal{X})$ si todo entero se puede escribir como suma de k elementos del conjunto $\mathcal{X}$ y además existe un entero que no se representa como suma de $k-1$ términos de $\mathcal{X}$. También diremos que $\mathcal{X}$ es una *base aditiva finita* si es base aditiva de orden k, para algún k.

De manera natural también se plantean problemas aditivos en el conjunto de clases de equivalencia módulo un entero m. Dado un subconjunto de los enteros $\mathcal{X}$, la pregunta es saber si para algún entero positivo k y ciertas clases residuales $\lambda \pmod m$ la congruencia

$$x_1 + \cdots + x_k \equiv \lambda \pmod m,$$

tiene solución para

$$x_1, \ldots, x_k \in \mathcal{X}.$$

Se dice que $\mathcal{X}$ es una *base aditiva* de orden $k = k(\mathcal{X})$ del sistema completo de residuos módulo m si toda clase residual se puede representar como suma de k elementos del conjunto dado y existe alguna clase residual que no se representa como la suma de $k-1$ términos de $\mathcal{X}$ (puede consultarse [37] para una definición). También se dice que $\mathcal{X}$ es una *base aditiva finita* del sistema de residuos módulo m si es base aditiva de orden k, para algún k.

Dado un conjunto de números enteros, en el proceso de decidir si se trata de una base aditiva finita es fundamental la información sobre la naturaleza y propiedades de sus elementos; por ejemplo, propiedades distribucionales, propiedades de tipo aritméticas e incluso si el mismo problema aditivo se puede abordar desde el punto de vista de otras disciplinas tales como la combinatoria o el análisis.

El presente trabajo reune nuevos avances[1] sobre problemas aditivos planteados en distintas funciones aritméticas. En algunos casos los resultados son acerca de propiedades distribucionales o aritméticas. La tesis se divide en tres capítulos de los cuales se presenta un resumen a continuación.

A lo largo del trabajo, las proposiciones presentadas como teoremas se refieren a los resultados originales. Adoptamos la notación de Landau $f(x) = O(g(x))$ o, de manera equivalente, la notación de Vinogradov $f(x) \ll g(x)$ para indicar que existe una constante $C > 0$ tal que $|f(x)| \leq Cg(x)$, para x suficientemente grande. Cuando ocurre de manera simultanea $f(x) \ll g(x)$ y $g(x) \ll f(x)$ se denota $f(x) \approx g(x)$. La notación $f(x) = o(g(x))$, para $g(x) \geq 0$, indica que $\lim_{x\to\infty} f(x)/g(x) = 0$. Se dice que $f(x)$ es asintóticamente igual a $g(x)$ si tiene lugar la igualdad $f(x) = g(x)(1 + o(1))$ y en este caso se denota $f(x) \sim g(x)$. Como es usual, denotaremos por $\mathbb{F}_p$ al sistema completo de residuos módulo un número primo p.

Capítulo 1

Este capítulo unifica los resultados de los tres trabajos conjuntos con Garaev y Konyagin [18],[19] y [20] sobre problemas aditivos, propiedades multiplicativas y distribucionales relacionados con la función τ de Ramanujan.

Los métodos expuestos en general explotan propiedades conocidas de la función τ tales como la multiplicatividad de la función, la conexión entre características aditivas y multiplicativas y la estimación $|\tau(n)| \leq d(n)n^{11/2}$ (Delinge [11]), donde $d(n)$ denota al número de divisores de n. En casos particulares también se emplean un resultado de Bourgain referente al problema llamado "sum-product estimate" [4] y un resultado de combinatoria de Glibichuk [30], entre otros.

[1] Algunos de estos resultados son trabajos en conjunto.

Sección 1.1

En esta sección se presentan resultados sobre problemas aditivos que involucran valores de la función τ de Ramanujan.

Después del trabajo de Serre [48] se sabe que, para cualquier primo p distinto de $2, 3, 5, 7, 23$ y 691, toda clase residual módulo p se puede escribir como $\tau(n) \pmod p$ para algún entero positivo n. Usando el profundo resultado de Bourgain, Katz y Tao [6], Shparlinski [51] demostró que los valores $\tau(n)$, para $n \leq p^4$, forman una base aditiva finita del sistema de residuos módulo un número primo p. Aquí se presentan tres resultados nuevos que en particular mejoran en muchos sentidos al obtenido por Shparlinski. El Teorema 1 establece que los valores $\tau(n)$ forman una base aditiva finita de los números enteros y más aún, todo entero $|N| \geq 2$ admite una representación como la suma de 148000 términos $\tau(n)$ con el argumento $n \leq |N|^{2/11} e^{-c \log |N| / \log\log |N|}$, para alguna constante $c > 0$. En vista del resultado mencionado de Deligne, notamos que el orden de las variables es óptimo, aparte del valor de la constante c. En particular, del Teorema 1 se sigue que para todo primo $p > p_0$ los valores $\tau(n)$ con $n \ll p^{2/11}$ forman una base aditiva finita de $\mathbb{F}_p$, hecho que reduce en un factor 22 la potencia de p obtenida por Shparlinski. En la demostración del Teorema 1 resulta fundamental el vínculo establecido entre las propiedades mencionadas de la función τ y el problema de Waring–Goldbach.

En general, se espera que todo entero $|N| \geq 2$ se escriba como suma de seis o siete sumandos de la forma $\tau(n)$ con $n \leq |N|^{2/11} e^{-c_1 \log |N| / \log\log |N|}$. El Teorema 1 es en cierta forma inmejorable si hablamos del orden de las variables, por lo que surge la pregunta de saber en qué casos se podría reducir incondicionalmente el número de sumandos. Utilizando resultados y avances que conciernen al problema de Waring-Goldbach (ver por ejemplo, [40]), el número de sumandos 148000 podría ser reducido aunque no de manera considerable frente a los seis o siete sumandos esperados. De manera natural se puede anticipar que el problema planteado en el conjunto de clases residuales permita establecer avances en esta dirección. Efectivamente, como consecuencia del Teorema 2 se tiene que para todo primo $p \geq p_0$ los valores $\tau(n)$, con $n \ll p^2 \log^4 p$, forman una base aditiva finita del sistema de residuos módulo p de orden a lo más 96. También se demostró que para cualquier $\varepsilon > 0$ la sucesión de enteros $\tau(n)$, con $n \leq p^{3+\varepsilon}$, es una base aditiva finita del sistema de residuos módulo p de orden a lo más 16.

Sección 1.2

Esta sección se enfoca en presentar nuevos resultados sobre propiedades distribucionales y multiplicativas de la función τ. El primer resultado se refiere al problema de la proporción de los valores $\tau(n)$ respecto del argumento $n \leq x$. Se cree que tiene lugar el siguiente comportamiento asintótico:

$$\#\{\tau(n) \ : \ n \leq x\} \sim x.$$

En [51] Shparlinski demostró la desigualdad

$$\#\{\tau(n) \ : \ n \leq x\} \geq x^{1/3+o(1)}.$$

En el mismo trabajo también observó que si el número de soluciones de la ecuación diofántica $u^2 = v^{11} + h$ tuviese una cota superior de la forma $h^{o(1)}$, entonces

$$\#\{\tau(n) \ : \ n \leq x\} \geq x^{1/2+o(1)}.$$

Aquí se presenta un segundo método que establece de manera incondicional este hecho. El Teorema 4 afirma la estimación

$$\#\{\tau(n) \ : \ n \leq x\} \gg x^{1/2} e^{-c \log x/ \log\log x},$$

para alguna constante absoluta $c > 0$.

Luca y Shparlinski demostraron en [41] propiedades aritméticas de la función τ. Por ejemplo, en uno de sus resultados probaron que existe una infinidad de enteros positivos n tales que $\tau(n) \neq 0$ y $P(\tau(n)) \geq (\log n)^{33/31+o(1)}$, donde $P(m)$ denota al factor primo más grande de m. También demostraron que

$$\omega\left(\prod_{\substack{p \leq x^{1/3} \\ \tau(p) \neq 0}} \tau(p)\tau(p^2)\tau(p^3)\right) \geq \left(\frac{1}{6\log 7} + o(1)\right) \log x,$$

aquí $\omega(m)$ denota al número de los distintos factores primos de m. En el trabajo [20], conjunto con Garaev y Konyagin, se obtuvieron resultados más fuertes utilizando diferentes métodos. El Lema 1, resultado de interés independiente, establece para

$$\mathcal{N} \subset \{1, 2, 3, \ldots, x\}, \quad \text{con} \quad |\mathcal{N}| > x^{\delta} e^{-c \log x/ \log\log x} + 1,$$

la estimación

$$\omega\left(\prod_{n\in\mathcal{N}} n\right) \gg \frac{(\log x)^{1/(1-\delta)}}{\log\log x},$$

donde la constante implícita puede depender de δ y c. Se asume que $0 < \delta < 1$ y c es una constante positiva.

La combinación del Teorema 4, el Lema 1 y el resultado de Deligne tiene por consecuencia la estimación

$$\omega\left(\prod_{\substack{p\leq x\\ \tau(p)\neq 0}} \tau(p)\tau(p^2)\right) \gg \frac{(\log x)^{11/10}}{\log\log x},$$

mejorando el resultado de [41]. No obstante el Teorema 5 proporciona aún una mejor estimación. El Teorema 5 brinda la estimación

$$\omega\left(\prod_{\substack{p\leq x\\ \tau(p)\neq 0}} \tau(p)\tau(p^2)\right) \gg \frac{(\log x)^{13/11}}{\log\log x}.$$

En particular, establece la existencia de una infinidad de enteros n tales que $\tau(n) \neq 0$ y $P(\tau(n)) \gg (\log n)^{13/11}$.

Capítulo 2

Este capítulo, basado en el trabajo conjunto con Garaev [17], se enfoca en el estudio y aplicaciones del problema de la solubilidad de la congruencia

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod{p}, \tag{1}$$

para λ un entero dado y las variables x_i en subconjuntos establecidos.

En el capítulo presente se exponen nuevos avances acerca de la solubilidad de la congruencia (1) desde varias perspectivas; las sumas trigonométricas, el punto de vista de la combinatoria y la conjugación de ambas.

Se sabe que el estudio de la congruencia (1) tiene vínculos con varios problemas de la teoría de números. Por ejemplo el problema de la representabilidad de clases residuales como producto de enteros pequeños y la

estimación del momento cuarto de las sumas de caracteres, se pueden consultar las referencias [2], [10], [13], [21], [47], [49] y [50]. En este capítulo también se presentan aportaciones en estos dos problemas.

Sean L_i, N_i, $1 \leq i \leq 4$, enteros tales que $0 \leq L_i < L_i + N_i < p$. Denotemos por J al número de soluciones de la congruencia (1), para $\lambda \equiv 0 \pmod{p}$, en el conjunto

$$L_i + 1 \leq x_i \leq L_i + N_i, \quad (1 \leq i \leq 4). \tag{2}$$

Se sabe que el valor J puede expresarse en términos de sumas de caracteres

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x_1,x_2,x_3,x_4} \chi(x_1 x_2 x_3^* x_4^*),$$

donde χ recorre el conjunto de los caracteres módulo p, x^* denota el inverso multiplicativo de $x \not\equiv 0 \pmod{p}$ y el rango que recorren las variables x_1, x_2, x_3 y x_4 en las sumatorias está definido por (2). Ayyad, Cochrane y Zheng [2] establecieron la fórmula asintótica

$$J = \frac{N_1 N_2 N_3 N_4}{p} + O\left(\sqrt{N_1 N_2 N_3 N_4}\log^2 p\right), \tag{3}$$

además de la estimación

$$J \approx \frac{N_1 N_2 N_3 N_4}{p} + O\left(\sqrt{N_1 N_2 N_3 N_4}\log p\right),$$

cuando $N_1 = N_2$, $N_3 = N_4$ o bien $N_1 = N_3$, $N_2 = N_4$. Resultados de los cuales se derivan, respectivamente, la siguientes estimaciones para el momento cuarto de las sumas de caracteres, siendo L y $N > 0$ enteros arbitrarios:

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log^2 p. \tag{4}$$

Si además $N \ll \sqrt{p \log p}$, entonces

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log p. \tag{5}$$

En esta dirección se destaca el resultado de Montgomery y Vaughan [43] que establece

$$\frac{1}{p-1}\sum_{\chi\neq\chi_0}\max_{N}\left|\sum_{x=1}^{N}\chi(x)\right|^4 \ll p^2;$$

en particular, cuando N es de orden p, en (4) es posible remover el factor $\log^2 p$. El trabajo de Burgess [7] tiene por consecuencia la estimación

$$\frac{1}{p}\sum_{L=1}^{p}\left\{\frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x=L+1}^{L+N}\chi(x)\right|^4\right\} \ll N^2,$$

la cual muestra que en promedio sobre L se puede remover el factor $\log^2 p$.

Sección 2.1

El Teorema 6 presenta una nueva fórmula asintótica para J,

$$J=\frac{N_1N_2N_3N_4}{p}+O\left(\sqrt{N_1N_2N_3N_4}\Big(\sqrt{\log p}+\delta(N_1N_2)\Big)\Big(\sqrt{\log p}+\delta(N_3N_4)\Big)\right), \tag{6}$$

donde

$$\delta(X)=\begin{cases}0, & \text{si} \quad X\leq p,\\ \log\frac{X}{p}, & \text{si} \quad X\geq p.\end{cases}$$

Teorema del cual se siguen nuevos resultados. Sobre el momento cuarto de las sumas de caracteres el Teorema 6 tiene por consecuencia la estimación

$$\frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x=L+1}^{L+N}\chi(x)\right|^4 \ll N^2\Big(\log p+\log^2\frac{N^2}{p}\Big).$$

En particular, la estimación (5) es efectiva en el rango $N\ll p^{1/2}e^{c\sqrt{\log p}}$ para alguna constante positiva fija c. Además, el Teorema 6 implica el comportamiento asintótico $J\sim N_1N_2N_3N_4/p$ en un rango mas amplio de los parámetros que aquel sugerido por (3). Por ejemplo, si $N_1=N_2=N_3=N_4=N$ y si

$$\frac{N}{p^{1/2}(\log p)^{1/2}}\to\infty, \quad p\to\infty,$$

entonces

$$J=\frac{N^4}{p}(1+o(1)),$$

mientras (3) implica esta fórmula asintótica cuando

$$\frac{N}{p^{1/2}\log p} \to \infty, \quad p \to \infty.$$

El problema de la solubilidad de la congruencia (1) se puede conectar con el problema de la representabilidad de clases residuales $h \pmod p$ en la forma

$$xy \equiv h \pmod p, \quad 1 \le x \le N_1,\ 1 \le y \le N_2.$$

Se conjetura que toda clase residual distinta de cero es representable si $N_1 = N_2 = N$ para $N \le p^{1/2+\varepsilon}$. De manera incondicional, del trabajo de Garaev [14] se sigue que, para alguna constante absoluta $c > 0$,

$$\mathbb{F}_p^* = \{xy \pmod p \ :\ 1 \le x, y \le cp^{3/4}\},$$

aquí $\mathbb{F}_p^*$ denota al conjunto $\mathbb{F}_p \setminus \{0\}$. Por otra parte, el trabajo de Tenenbaum [52] implica que si

$$N_1 = N_2 = N \le p^{1/2}(\log p)^{0,5\kappa-\varepsilon},$$

donde $\kappa = 1 - (\log(e\log 2))/\log 2$ es como 0,08607..., entonces el conjunto

$$\{xy \pmod p \ :\ 1 \le x, y \le N\}$$

contiene sólo $o(p)$ clases residuales módulo p.

Otra consecuencia del Teorema 6 se tiene en este tema. El Teorema 7 afirma que si $N_1N_2 = \Delta p\log p$, donde $\Delta = \Delta(p) \to \infty$ si $p \to \infty$, entonces el conjunto

$$\{xy \pmod p : \quad L_1 + 1 \le x \le L_1 + N_1, \quad L_2 + 1 \le y \le L_2 + N_2\}$$

contiene $\left(1 + O(\frac{1}{\Delta} + \frac{\log^2\Delta}{\Delta\log p})\right)p$ clases residuales módulo p. En particular, este conjunto contiene casi todas las clases residuales módulo p.

Sección 2.2

En lo que respecta a la solubilidad de la congruencia (1), de la fórmula asintótica (3) obtenida por Ayyad, Cocharane y Zheng se sigue que si $N_1N_2N_3N_4 > cp^2\log^4 p$ entonces la congruencia es soluble en el conjunto (2).

Los autores preguntaron en qué casos el factor $\log^4 p$ podría ser removido totalmente, en vista de la existencia de conjuntos del tipo (2) de tamaño $O(p^2)$ sin soluciones para (1). Mediante la combinación de técnicas de sumas trigonométricas con argumentos de combinatoria se obtiene el Teorema 8, el cual muestra que el factor $\log^4 p$ puede ser disminuido a $\log p$. De manera más precisa; el Teorema 8 establece que existe una constante c tal que si $N_1N_2N_3N_4 > cp^2 \log p$, entonces el conjunto (2) contiene una solución de la congruencia (1).

Se sabe que, dado un entero λ, el problema de resolver la congruencia

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod{p} \tag{7}$$

difiere esencialmente en los casos $\lambda \equiv 0 \pmod{p}$ y $\lambda \not\equiv 0 \pmod{p}$. El Teorema 8 corresponde al caso $\lambda \equiv 0 \pmod{p}$. Para λ arbitrario, es posible demostrar que si $N_1N_2N_3N_4 > cp^2 \log^3 p$, entonces el conjunto (2) admite soluciones para la congruencia (7). La pregunta natural es saber en qué casos el factor $\log^3 p$ puede ser removido totalmente (notemos que si N_1N_2 tiene la misma magnitud que N_3N_4, entonces es posible cambiar $\log^3 p$ por $\log^2 p$). Un posible enfoque de esta pregunta es el estudio de la congruencia (7) desde el punto de vista de la combinatoria. Por ejemplo, se sigue de un resultado de Glibichuk [30, Teorema 1], que si $\mathcal{A}$ y $\mathcal{B}$ son subconjuntos de $\mathbb{F}_p$ tales que $|\mathcal{A}||\mathcal{B}| \geq 2p$, entonces

$$2(2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p\,, \quad (2\mathcal{A})(2\mathcal{B}) - (2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p,$$

donde se definen los conjuntos

$$\mathcal{A}+\mathcal{B} = \{a+b:\ a\in\mathcal{A},\, b\in\mathcal{B}\}, \quad \mathcal{A}-\mathcal{B} = \{a-b:\ a\in\mathcal{A},\, b\in\mathcal{B}\},$$

$$k\,\mathcal{A} = \{a_1+\cdots+a_k:\ a_i\in\mathcal{A},\, 1\leq i\leq k\}, \quad \mathcal{A}\,\mathcal{B} = \{ab: \quad a\in\mathcal{A},\, b\in\mathcal{B}\}.$$

En particular, si $N_1N_2 > 10p$ entonces para cualquier entero λ la congruencia (7) es soluble en las variables

$$L_1+1 \leq x_1, x_3 \leq L_1+N_1, \quad L_2+1 \leq x_2, x_4 \leq L_2+N_2.$$

De esta observación se establece de manera natural la conjetura siguiente.

Conjetura 1. Existe una constante positiva c tal que si $\mathcal{A},\mathcal{B},\mathcal{C},\mathcal{D}$ son subconjuntos de $\mathbb{F}_p^*$ con $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > cp^2$, entonces

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

La validez de esta conjetura permite remover los factores logarítmicos en la resultado antes mencionado, en particular responde a la pregunta de Ayyad, Cochrane y Zheng. El empleo de técnicas de sumas trigonométricas junto con argumentos de combinatoria utilizados en [5], [6] y [30] permiten responder de manera afirmativa a la Conjetura 1 en casos importantes. El Teorema 9 establece que dados $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ conjuntos de $\mathbb{F}_p^*$ tales que $|\mathcal{A}||\mathcal{C}|, |\mathcal{B}||\mathcal{D}| > (2+\sqrt{2})p$, entonces

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

En particular, si $N_1 N_3 > 15p$, $N_2 N_4 > 15p$, entonces para cualquier entero λ la congruencia

$$x_1 x_2 \equiv x_3 x_4 + \lambda \pmod{p},$$

es soluble en el conjunto (2).

Capítulo 3

El presente capítulo se compone de los resultados del trabajo conjunto con Garaev [16] y los trabajos [28], [29] acerca de propiedades aritméticas y distribucionales de sucesiones con términos relacionados con factoriales módulo un número primo.

El problema de la distribución de sucesiones con términos relacionados con factoriales ha sido investigado en diversos trabajos tales como [8], [9], [22]–[25] y [42]. Se espera que la sucesión (ver [31, **F11**])

$$1!\,, 2!\,, 3!\,, \ldots\,, (p-1)!\,,$$

posea aproximadamente $(1-1/e)p$ clases residuales distintas módulo p. Este hecho implicaría la representabilidad de toda clase residual módulo p como suma o producto de dos factoriales. De manera incondicional, del Teorema de Wilson se sigue que para cualquier entero $1 \leq x \leq (p-1)/2$ se tiene

$$(2x-1)! \cdot (p-2x)! \equiv 1 \pmod{p}. \tag{8}$$

Identidad que ha sido un punto de partida en los trabajos [8] y [23, Teorema 13] para estimar el tamaño del conjunto

$$\{m!n! \pmod{p} \ : \ 1 \leq m, n \leq p\}.$$

En el trabajo [23] de Garaev, Luca y Shparlinski se obtuvo la estimación

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{5}{8}p + O(p^{1/2}\log^2 p).$$

Posteriormente, esta desigualdad fué mejorada por Chen y Dai en [8] al obtener

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{3}{4}p + O(p^{1/2}\log^2 p).$$

Ambos resultados son mejorados por el Teorema 10. El Teorema 10, del trabajo [29], establece

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{41}{48}p + O(p^{1/2}\log^3 p).$$

El ingrediente principal en la demostración consiste en la manipulación de la identidad (8) para elegir conjuntos ajenos de clases residuales de la forma $m!n! \pmod p$ de tal forma que cada conjunto pueda ser estimado por el número de soluciones de un sistema de congruencias. Esta última tarea es resuelta vía la estimación de sumas híbridas de caracteres.

En los trabajos de Garaev, Luca y Shparlinski [23], [24] se han estimado sumas exponenciales y de caracteres que involucran factoriales de enteros en intervalos de pequeña longitud. Estos resultados han sido fundamentales para establecer la representabilidad de clases residuales en términos de factoriales de tamaño restringido y en varios casos también fórmulas asintóticas para el número de tales representaciones.

Sección 3.1

Mediante el Teorema de Wilson (ver la identidad 8) y el principio de las casillas de Dirichlet se puede demostrar que toda clase residual módulo p se representa en la forma

$$m_1!n_1! + m_2!n_2! \pmod p,$$

para irrestrictos enteros m_1, m_2, n_1, n_2. Del trabajo [24] de Garaev, Luca y Shparlinski, se obtiene la siguiente estimación para la doble suma exponencial con argumento de la forma $m!n!$,

$$\max_{(a,p)=1} \left| \sum_{m=1}^{N} \sum_{n=1}^{N} e^{2\pi i a m!n!/p} \right| \ll N^{11/6} p^{1/8}.$$

Con tal resultado establecieron la representabilidad de clases residuales como suma de términos de la forma $m!n!$, con las variables en intervalos de pequeña longitud. En particular, establecieron que toda clase residual $\lambda \pmod p$ puede escribirse como

$$\sum_{i=1}^{7} m_i!n_i! \equiv \lambda \pmod p,$$

para ciertos enteros positivos $m_1, n_1, \ldots, m_7, n_7$ no mayores que $cp^{33/34}$, con alguna constante absoluta $c > 0$. En esta sección se presenta el Teorema 11, del trabajo conjunto con Garaev [16], resultado que mejora al anterior en dos direcciones, el número de sumandos y el tamaño de las variables. El Teorema 11 demuestra que cualquier clase residual λ módulo p puede escribirse como

$$\sum_{i=1}^{5} m_i!n_i! \equiv \lambda \pmod p,$$

para ciertos enteros positivos $m_1, n_1, \ldots, m_5, n_5$ con

$$\max_{1\leq i\leq 5}\{m_i, n_i\} \leq cp^{27/28},$$

donde $c > 0$ es una constante absoluta.

Sección 3.2

En esta sección se retoman los resultados de Garaev, Luca y Shparlinki obtenidos en [23], [26] y [27] referentes a la representabilidad de clases residuales como producto de factoriales, suma de sumas armónicas y coeficientes binomiales.

En [23] Garaev, Luca y Shparlinski demostraron que para cualquier carácter χ módulo p distinto del carácter principal se tiene la estimación

$$\sum_{n=L+1}^{L+N} \chi(n!) \ll N^{3/4}p^{1/8}\log^{3/4} p,$$

donde L, N denotan enteros no negativos. Combinando este resultado con la estimación superior del número de soluciones de cierta congruencia se tiene que para $\lambda \not\equiv 0 \pmod p$ dado, el número de soluciones de la congruencia

$$\prod_{i=1}^{7} n_i! \equiv \lambda \pmod p; \quad L+1 \leq n_1, \ldots, n_7 \leq L+N, \tag{9}$$

asintóticamente se comporta como N^7/p, para $0 < L+1 \leq L+N \leq p$ y

$$Np^{-11/12}\log^{-1/2} p \to 0 \quad \text{cuando} \quad p \to \infty.$$

Como consecuencia inmediata, sucede que para todo $\lambda \not\equiv 0 \pmod p$, la congruencia (9) admite solución en los enteros positivos $n_i \ll N^{11/12}\log^{1/2} p$, $i = 1, \ldots, 7$.

Los métodos empleados en la demostración de los resultados anteriores fueron aplicados en otras funciones aritméticas para obtener resultados similares. En [26], Garaev, Luca y Shparlinski obtuvieron resultados, análogos al anterior, para sumas armónicas

$$H_s(n) = \sum_{i=1}^{n} \frac{1}{i^s},$$

donde s es una entero positivo fijo y $H_s(n)$ es calculado módulo p. En particular, se obtuvo una estimación no trivial para una suma exponencial con argumento $H_s(n)$, resultado con el cual, en el mismo trabajo, demostraron que para cualquier entero λ el número de soluciones de la congruencia

$$\sum_{i=1}^{7} H_s(n_i) \equiv \lambda \pmod p; \quad L+1 \leq n_1, \ldots, n_7 \leq L+N,$$

tiene un comportamiento asintótico como N^7/p, para $0 \leq L < L+N < p$ y

$$Np^{-11/12}\log^{-1/2} p \to 0 \quad \text{cuando} \quad p \to \infty.$$

En el trabajo de Garaev, Luca y Shparlinski [27] propiedades distribucionales de los semi-coeficientes binomiales y números de Catalán

$$b_n = \binom{2n}{n}, \qquad c_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 0, 1, \ldots,$$

también han sido investigados. Demostraron que para primos suficientemente grandes p y todo entero λ existen enteros positivos $r, s \ll p^{13/2}\log^6 p$ tales que

$$b_r \equiv \lambda \pmod p \quad \text{y} \quad c_s \equiv \lambda \pmod p.$$

Aunque las potencias de p que aparecen en los resultados mencionados hasta ahora no han sido disminuidas, los factores logarítmicos en ciertos casos

pueden ser removidos. Uno de los propósitos de este trabajo es abordar esta cuestión, para dicha tarea se retomaron los argumentos descritos en [23], [26], [27] y se combinaron con el método expuesto por Garaev en [14].

En esta sección se presentan los resultados obtenidos en [28]. El Teorema 12 extiende a uno de los resultados de [23]. El Teorema 12 establece dos estimaciones para cualquier carácter χ distinto del carácter principal, una de ellas es:

$$\sum_{x=1}^{N}\sum_{y=1}^{M}\chi((x+y+L)!) \ll MN^{3/4}p^{1/8}\log^{1/4}(NM^{-1}+2),$$

siendo L, M, M enteros tales que

$$N \geq 1, \quad M \geq 1, \quad 0 \leq L < L+N+M \leq p.$$

La otra estimación es de la misma naturaleza. Combinando este resultado con la estimación superior del número de soluciones de cierta congruencia especial se obtiene el Teorema 13, el cual establece una fórmula asintótica para el número de soluciones de la congruencia

$$n_1! \cdots n_7! \equiv \lambda \pmod{p}; \quad 1 \leq n_1, \ldots, n_7 \leq N, \tag{10}$$

siendo λ cualquier clase residual distinta de cero. Del Teorema 13 se sigue que para cualquier $\lambda \not\equiv 0 \pmod{p}$ la congruencia (10) tiene solución en enteros positivos $n_1, \ldots, n_7$ satisfaciendo

$$\max_{1\leq i\leq 7} n_i \ll p^{11/12}.$$

También se demuestran resultados similares para las sumas armónicas. El Teorema 15 establece para todo entero λ una fórmula asintótica para el número de soluciones de la congruencia

$$H_s(n_1) + \cdots + H_s(n_7) \equiv \lambda \pmod{p}; \quad 1 \leq n_1, \ldots, n_7 \leq N.$$

En particular, del Teorema 15 se sigue que la congruencia anterior es soluble en enteros positivos $n_1, \ldots, n_7$ que satisfacen

$$\max_{1\leq i\leq 7} n_i \ll p^{11/12}.$$

Respecto a los semi-coeficientes binomiales y los números de Catalán, el Teorema 16 establece que para todos los primos suficientemente grandes p

y todo entero λ existen enteros positivos $r, s \ll p^{13/2}$ tales que $b_r \equiv c_s \equiv \lambda$ (mód p).

De esta forma, en cada uno de los resultados se garantiza la solubilidad de la respectiva congruencia con variables en el rango conocido sin el correspondiente factor logarítmico.

Capítulo 1

Problemas aritméticos que involucran a la función τ de Ramanujan

La función τ de Ramanujan se puede definir mediante los coeficientes $\tau(n)$ de la expansión

$$X\prod_{n=1}^{\infty}(1-X^n)^{24}=\sum_{n=1}^{\infty}\tau(n)X^n. \tag{1.1}$$

La función $\tau(n)$ posee propiedades aritméticas importantes. Algunos ejemplos son las siguientes propiedades conjeturadas por Ramanujan (1887-1920) que no fueron demostradas hasta años despues.

(i) La función $\tau(n)$ es una función multiplicativa;

$$\tau(mn)=\tau(m)\tau(n), \quad \text{si} \quad (m,n)=1.$$

(ii) Para cualquier entero $\alpha \geq 0$ y cualquier primo p se tiene

$$\tau(p^{\alpha+2})=\tau(p^{\alpha+1})\tau(p)-p^{11}\tau(p^{\alpha}).$$

En particular

$$\tau(p^2) = \tau^2(p) - p^{11}.$$

(iii) Para todo entero $n \geq 1$ se cumple

$$\begin{aligned} \tau(n) &\equiv \sum_{d|n} d^{11} \pmod{691}, \\ \tau(n) &\equiv \sum_{d|n} d^{11} \pmod{2^8}. \end{aligned}$$

(iv) Tiene lugar la desiguldad $|\tau(p)| \leq 2p^{11/2}$ para cualquier primo p. En general para todo entero $n \geq 1$ se cumple la desigualdad

$$|\tau(n)| \leq d(n)\, n^{11/2},$$

donde $d(n)$ es el número de divisores n.

Las demostraciones pueden verificarse en [1], [11], [35] y [38]. Mordell demostró (i) y (ii), (iv) es consecuencia de la demostración de una conjetura de Weil obtenida por Deligne en [11].

Del resultado de Deligne y las propiedades de la función divisor se tiene que existe una constante $c_0 > 0$ tal que

$$|\tau(n)| \leq n^{11/2} e^{c_0 \log n / \log\log n},$$

para cualquier $n \geq 3$. Notamos que los N^6 números

$$\sum_{i=1}^{6} \tau(a_1), \qquad 1 \leq a_1, \ldots, a_6 \leq N$$

son enteros de magnitud $O(N^{11/2+\varepsilon})$. Por lo que, en promedio, todo entero se puede escribir en distintas formas como la suma de seis valores $\tau(n)$ y de forma particular se espera una representación de cero como la suma de seis valores $\tau(n)$. Con tal observación en mente se buscaron seis enteros positivos fijos $a_1, \ldots, a_6$ tales que

$$\sum_{i=1}^{6} \tau(a_i) = 0.$$

Existen varias fórmulas que conectan $\tau(n)$ con la función

$$\sigma_s(n) = \sum_{d|n} d^s.$$

Por ejemplo, se sabe que

$$\tau(n) = \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sum_{k=1}^{n-1}\sigma_5(k)\sigma_5(n-k).$$

Otra fórmula (ver [46]) establece

$$\tau(n) = n^4\sigma_0(n) - 24\sum_{k=1}^{n-1}(35k^4 - 52k^3n + 18k^2n^2)\sigma_0(k)\sigma_0(n-k).$$

Fórmulas de este tipo son útiles en el cálculo numérico de $\tau(n)$. En particular se puede deducir que

$$\begin{array}{lll} \tau(12) = -370944, & \tau(27) = -73279080, & \tau(55) = 2582175960, \\ \tau(69) = 4698104544, & \tau(90) = 13173496560, & \tau(105) = -20380127040. \end{array}$$

De esta forma, tenemos la siguiente identidad que será útil más adelante

$$\tau(12) + \tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105) = 0.$$

1.1. Problemas aditivos del tipo Waring

El trabajo de Serre [48] implica que toda clase residual módulo un primo $p \neq 2, 3, 5, 7, 23, 691$ se puede escribir como $\tau(n) \pmod p$ para algún entero positivo n. Varias propiedades de $\tau(n)$ módulo p se pueden encontrar en este trabajo.

Basado en el profundo resultado de Bourgain, Katz y Tao [6] y usando la estimación de Vinogradov para la doble suma exponencial, Shparlinski en [51] demostró que los valores $\tau(n)$, $n \leq p^4$, forman una base aditiva finita módulo p, es decir, existe una constante s tal que toda clase residual módulo p se puede escribir como $\tau(n_1) + \cdots + \tau(n_s) \pmod p$, para enteros $1 \leq n_1, \ldots, n_s \leq p^4$. En conjunto con Garaev y Konyagin en [18] y [19] establecimos resultados que mejoran en varias direcciones al obtenido por Shparlinski.

Teorema 1. *El conjunto de los valores $\tau(n)$ es una base aditiva finita de los enteros. Más aún, para cualquier entero $|N| \geq 2$ la ecuación*

$$\sum_{i=1}^{148000} \tau(n_i) = N$$

es soluble en enteros positivos $n_1, \ldots, n_{148000}$ con la propiedad

$$\max_{1 \leq i \leq 148000} n_i \ll |N|^{2/11} e^{-c \log |N| / \log\log |N|},$$

para alguna constante absoluta $c > 0$.

De manera particular, del Teorema 1 se sigue que para todo primo $p > p_0$ los valores $\tau(n)$ con $n \ll p^{2/11}$ forman una base aditiva finita de $\mathbb{F}_p$, hecho que disminuye en un factor 22 la potencia de p obtenida por Shparlinski, y de hecho es la potencia fija de p más pequeña posible. En general observamos que, en vista del resultado de Deligne, el orden de las variables en el Teorema 1 es óptimo, aparte del valor de la constante c.

Utilizando resultados y avances que conciernen al problema de Waring–Goldbach (ver por ejemplo, [40]), el número de sumandos 148000 podría ser reducido aunque no de manera considerable frente a los seis o siete sumandos que se esperan. En esta dirección, junto con Garaev y Konyagin, en [18] obtuvimos los siguientes dos teoremas, donde p se asume como un número primo suficientemente grande.

Teorema 2. *Para todo entero λ la congruencia*

$$\sum_{i=1}^{16} \tau(n_i) - \sum_{i=17}^{32} \tau(n_i) \equiv \lambda \pmod{p}$$

admite solución en los enteros positivos $n_1, \ldots, n_{32}$ tales que

$$\max_{1 \leq i \leq 32} n_i \ll p^2 \log^4 p, \qquad (23!, n_i) = 1.$$

Se sigue del Teorema 2 que

$$\mathbb{F}_p = \left\{ \sum_{i=1}^{16} \tau(n_i) - \sum_{i=17}^{32} \tau(n_i) \pmod{p} \ : \ \max_{1 \leq i \leq 32} n_i \ll p^2 \log^4 p, \ (23!, n_i) = 1 \right\}$$

y al multiplicar el conjunto anterior por $\tau(12)$, donde

$$\tau(12) = -\tau(27) - \tau(55) - \tau(69) - \tau(90) - \tau(105),$$

en virtud de la multiplicatividad de la función $\tau(n)$, se tiene que la sucesión de los valores $\tau(n)$, $n \ll p^2 \log^4 p$, es una base aditiva finita de $\mathbb{F}_p$ de orden a lo más 96. De esta manera, toda clase residual módulo p se puede representar como

$$\sum_{i=1}^{96} \tau(n_i) \pmod{p},$$

para enteros positivos $n_1, \ldots, n_{96}$ bajo las condiciones

$$\max_{1 \le i \le 96} n_i \ll p^2 \log^4 p.$$

Es posible reducir el número de sumandos a costa de aumentar el orden en el rango de las variables.

Teorema 3. *Para todo entero λ y para todo $\varepsilon > 0$, la congruencia*

$$\sum_{i=1}^{16} \tau(n_i) \equiv \lambda \pmod{p}$$

es soluble en los enteros positivos $n_1, \ldots, n_{16}$ tales que

$$\max_{1 \le i \le 16} n_i \ll p^{3+\varepsilon}.$$

1.2. Propiedades distribucionales y aritméticas de la función $\tau(n)$

Sobre el problema de la proporción del número de valores $\tau(n)$, respecto del argumento $n \le x$, se espera que

$$\#\{\tau(n) : n \le x\} \gg x.$$

De hecho, parece que tiene lugar el comportamiento asintótico

$$\#\{\tau(n) : n \le x\} \sim x.$$

Shparlinski demostró en [51] de manera incondicional que

$$\#\{\tau(n) \,:\, n \leq x\} \geq x^{1/3+o(1)}.$$

En el mismo trabajo también observó que si el número de soluciones de la ecuación diofántica $u^2 = v^{11} + h$ tuviese una cota superior de la forma $h^{o(1)}$, entonces

$$\#\{\tau(n) \,:\, n \leq x\} \geq x^{1/2+o(1)}.$$

En [20], junto con Garaev y Konyagin establecimos de manera incondicional este hecho.

Teorema 4. *Para cualquier entero $x \geq 10$,*

$$\#\{\tau(n) \,:\, n \leq x\} \gg x^{1/2} e^{-4\log x/\log\log x}.$$

Estimaciones de esta naturaleza se pueden aplicar para obtener propiedades aritméticas de τ.

Luca y Shparlinski demostraron en [41] otras propiedades aritméticas de la función τ. Por ejemplo, en uno de sus resultados probaron que existe una infinidad de enteros positivos n tales que $\tau(n) \neq 0$ y $P(\tau(n)) \geq (\log n)^{33/31+o(1)}$, donde $P(m)$ denota al factor primo más grande de m. También demostraron que

$$\omega\left(\prod_{\substack{p\leq x^{1/3}\\ \tau(p)\neq 0}} \tau(p)\tau(p^2)\tau(p^3)\right) \geq \left(\frac{1}{6\log 7} + o(1)\right)\log x,$$

donde aquí $\omega(m)$ denota al número de los distintos factores primos de m. En el trabajo [20], conjunto con Garaev y Konyagin, obtuvimos resultados más fuertes utilizando diferentes métodos.

En el siguiente lema, que puede ser de interés independiente, x se asume como un número suficientemente grande.

Lema 1. *Sean δ y c constantes positivas, $\delta < 1$. Sea*

$$\mathcal{N} \subset \{1, 2, 3, \ldots, x\}, \qquad |\mathcal{N}| > x^{\delta} e^{-c\log x/\log\log x} + 1.$$

Entonces

$$\omega\left(\prod_{n\in\mathcal{N}} n\right) \gg \frac{(\log x)^{1/(1-\delta)}}{\log\log x},$$

donde la constante implícita puede depender de δ y c.

La combinación del Lema 1, el Teorema 4 y el resultado de Deligne implica la desigualdad

$$\omega\left(\prod_{\substack{p\le x\\ \tau(p)\neq 0}}\tau(p)\tau(p^2)\right)\gg\frac{(\log x)^{11/10}}{\log\log x},$$

mejorando el resultado de [41]. Sin embargo, el siguiente teorema proporciona aún una mejor estimación.

Teorema 5. *Para cualquier $x\ge 10$,*

$$\omega\left(\prod_{\substack{p\le x\\ \tau(p)\neq 0}}\tau(p)\tau(p^2)\right)\gg\frac{(\log x)^{13/11}}{\log\log x}.$$

En particular, existe una infinidad de enteros n tales que $\tau(n)\neq 0$ y $P(\tau(n))\gg(\log n)^{13/11}$.

1.3. Lemas

Lema 1. *Sean δ y c constantes positivas, $\delta<1$. Sea*

$$\mathcal{N}\subset\{1,2,3,\dots,x\},\qquad |\mathcal{N}|>x^{\delta}e^{-c\log x/\log\log x}+1.$$

Entonces

$$\omega\left(\prod_{n\in\mathcal{N}}n\right)\gg\frac{(\log x)^{1/(1-\delta)}}{\log\log x},$$

donde la constante implícita puede depender de δ y c.

Demostración. Sean $x\ge y\ge 3$ y denotemos por $\Psi(x,y)$ al número de enteros positivos menores que x que no tienen divisores primos mayores o iguales que y. Conforme a la estimación obtenida por de Bruijn en la forma dada por Hildebrand y Tenenbaum en [33, Teorema 1.4] se sabe que

$$\log\Psi(x,y)\le Z\left(1+\frac{c_1}{\log y}+\frac{c_2}{\log\log x}\right),\tag{1.2}$$

donde

$$Z = Z(x,y) = \frac{\log x}{\log y}\log\left(1+\frac{y}{\log x}\right) + \frac{y}{\log y}\log\left(1+\frac{\log x}{y}\right) \tag{1.3}$$

y c_1, c_2 son constantes absolutas positivas. Sea

$$M = \frac{4+2c+2c_1+2c_2}{(1-\delta)^2}.$$

Podemos asumir que $x > e^{e^{10M/\delta}}$. Tomemos $y = e^{-M}(\log x)^{1/(1-\delta)}$. Bajo esta elección de los parámetros obtenemos

$$\begin{aligned} Z &\leq \frac{\log x}{\log y}\log\left(\frac{ey}{\log x}\right) + \frac{\log x}{\log y} \\ &= \log x - \frac{\log x \log\log x}{\log y} + 2\frac{\log x}{\log y} \\ &= \delta\log x - \frac{\log x(\log\log x - (1-\delta)\log y)}{\log y} + 2\frac{\log x}{\log y} \\ &= \delta\log x - \frac{((1-\delta)M-2)\log x}{\log y} \\ &\leq \delta\log x - \frac{(1-\delta)^2 M\log x}{2\log\log x}. \end{aligned}$$

Sustituyendo esta estimación en (1.2), tenemos

$$\begin{aligned} \log\Psi(x,y) &\leq \left(\delta\log x - \frac{(1-\delta)^2 M\log x}{2\log\log x}\right)\left(1+\frac{c_1+c_2}{\log\log x}\right) \\ &\leq \delta\log x - \frac{((1-\delta)^2 M - 2c_1 - 2c_2)\log x}{2\log\log x} \\ &< \delta\log x - c\frac{\log x}{\log\log x}. \end{aligned}$$

Por lo tanto

$$\Psi(x, e^{-M}(\log x)^{1/(1-\delta)}) < |\mathcal{N}|. \tag{1.4}$$

Sean $k = \omega\left(\prod_{n\in\mathcal{N}} n\right)$ y $q_1 < \cdots < q_k$ los divisores primos de $\prod_{n\in\mathcal{N}} n$ dispuestos en orden ascendente. Entonces cada $n \in \mathcal{N}$ puede ser escrito de manera única en la forma $n = q_1^{\alpha_1(n)}\cdots q_k^{\alpha_k(n)}$, con $\alpha_i(n) \geq 0$. Llamemos

$$\mathcal{N}' = \left\{p_1^{\alpha_1(n)}\cdots p_k^{\alpha_k(n)} \ : \ n \in \mathcal{N}\right\},$$

donde $2 = p_1 < p_2 < \cdots < p_k$ denotan a los primeros k números primos. En virtud del teorema fundamental de la aritmética sucede $|\mathcal{N}| = |\mathcal{N}'|$. Usando la desigualdad (1.4) y este hecho se tiene

$$\Psi(x, e^{-M}(\log x)^{1/(1-\delta)}) < |\mathcal{N}'|. \tag{1.5}$$

Por definición, para cada $n' \in \mathcal{N}'$ existe $n \in \mathcal{N}$ tal que

$$n' = p_1^{\alpha_1(n)} \cdots p_k^{\alpha_k(n)} \leq q_1^{\alpha_1(n)} \cdots q_k^{\alpha_k(n)} = n \leq x.$$

Así, $\mathcal{N}' \subset \{1, 2, \ldots, x\}$. Por lo tanto, de (1.5) se sigue que existe un elemento $n' \in \mathcal{N}'$ tal que $P(n') > e^{-M}(\log x)^{1/(1-\delta)}$. En otras palabras

$$p_k > e^{-M}(\log x)^{1/(1-\delta)}.$$

Finalmente el resultado se sigue del teorema de los números primos. □

El siguiente lema es una versión del resultado clásico de Hua [34].

Lema 2. *Sea s_0 un entero fijo $s_0 \geq 2049$. Denotemos por J al número de soluciones de la ecuación*

$$q_1^{11} + \cdots + q_{s_0}^{11} = N,$$

en los primos $q_1, \ldots, q_{s_0}$ con la condición $q_i \geq \log^3 N$, para todo $1 \leq i \leq s_0$. Entonces existen constantes positivas $c_1 = c_1(s_0)$ y $c_2 = c_2(s_0)$ tales que para todo entero N suficientemente grande, $N \equiv s_0 \pmod 2$, tiene lugar la desigualdad

$$c_1 \frac{N^{s_0/11-1}}{(\log N)^{s_o}} \leq J \leq c_2 \frac{N^{s_0/11-1}}{(\log N)^{s_0}}.$$

El siguiente resultado esta basado en el lema anterior.

Lema 3. *Todo entero L de valor absoluto suficientemente grande puede ser representado en la forma*

$$L = \tau(n_1) + \cdots + \tau(n_{74000}),$$

con enteros positivos $n_1, \ldots, n_{74000}$ libres de divisores primos en el intervalo $(\log\log|L|, \log^2|L|)$ y tales que

$$\max_{1 \leq i \leq 74000} n_i \ll |L|^{2/11}.$$

Demostración. Sea M un entero positivo par suficientemente grande. Definamos

$$\mathcal{Q} = \{q \,:\, q \text{ es primo, } \log^2 M < q \leq M^{1/11}\}.$$

Diremos que un subconjunto $\mathcal{Q}'$ de $\mathcal{Q}$ es admisible si la ecuación

$$\sum_{i=1}^{6} \tau(q_i') = \sum_{i=7}^{12} \tau(q_i')$$

no tiene solucion en los primos $q_1', \ldots, q_{12}' \in \mathcal{Q}'$ bajo la condición

$$q_1' < \cdots < q_6', \quad q_7' < \cdots < q_{12}', \qquad (q_1', \ldots, q_6') \neq (q_7', \ldots, q_{12}').$$

Existen conjuntos admisibles con al menos 12 elementos. Efectivamente, recordemos que para todo primo impar q tienen lugar las identidades

$$\tau(q) \equiv q^{11} + 1 \pmod{691}, \qquad \tau(q) \equiv q^{11} + 1 \pmod{2^8}. \tag{1.6}$$

El Teorema chino del residuo garantiza que para cada $1 \leq i \leq 12$ existe a_i tal que

$$a_i \equiv 2^i - 1 \pmod{691}, \quad a_i \equiv 2^i - 1 \pmod{2^8}.$$

Sea g una raíz primitiva módulo 691 y recordemos que 5 es un elemento que pertenece al orden 2^6 según el módulo 2^8. Dado que $(11, 690) = (11, 2^7) = 1$ se tiene que g^{11} es raíz primitiva módulo 691 y 5^{11} pertenece al orden 2^6 módulo 2^8. De esta forma, para cada $1 \leq i \leq 12$, existen enteros $\alpha_i, \beta_i, \gamma_i$, (donde $\gamma_i = 0$ o $\gamma_i = 1$) tales que

$$(g^{11})^{\alpha_i} \equiv a_i \pmod{691} \quad \text{y} \quad (-1)^{\gamma_i}(5^{11})^{\beta_i} \equiv \left((-1)^{\gamma_i} 5^{\beta_i}\right)^{11} \equiv a_i \pmod{2^8}. \tag{1.7}$$

De esta forma, en virtud del Teorema de los números primos en progresiones aritméticas y dado que M es suficientemente grande, es posible encontrar y fijar números primos $l_i \in \mathcal{Q}$, $1 \leq i \leq 12$, tales que

$$l_i \equiv g^{\alpha_i} \pmod{691} \quad \text{y} \quad l_i \equiv (-1)^{\gamma_i} 5^{\beta_i} \pmod{2^8}.$$

Combinando las congruencias anteriores con (1.7) y (1.6) obtenemos

$$\tau(l_i) \equiv 2^i \pmod{691 \times 2^8}.$$

Por lo tanto $\{l_1, \ldots, l_{12}\}$ es un subconjunto admisible de $\mathcal{Q}$.

Sea $\mathcal{Q}'$ un conjunto admisible de $\mathcal{Q}$ de tamaño máximo. Si existen distintos conjuntos admisibles de orden máximo fijemos a alguno de ellos. En particular $|\mathcal{Q}'| \geq 12$ y dado que las sumatorias del tipo

$$\sum_{i=1}^{6} \tau(q_i'); \quad q_1', \ldots, q_6' \in \mathcal{Q}', \quad q_1' < \cdots < q_6',$$

son distintas se tiene

$$\begin{aligned} |\mathcal{Q}'|^6 \ll & \#\{(q_1', \ldots, q_6') \ : \ q_1', \ldots, q_6' \in \mathcal{Q}', \quad q_1' < \cdots < q_6'\} = \\ & \# \left\{ \sum_{i=1}^{6} \tau(q_i') \ : \ q_1', \ldots, q_6' \in \mathcal{Q}', \quad q_1' < \cdots < q_6' \right\}. \end{aligned}$$

Utilizando la estimación de Deligne para $\tau(q)$ tenemos

$$|\mathcal{Q}'|^6 \ll (M^{1/11})^{11/2}, \quad \text{por lo que} \quad |\mathcal{Q}'| \ll M^{1/11-1/132}.$$

Dado $q \in \mathcal{Q} \setminus \mathcal{Q}'$ considere al conjunto $\mathcal{Q}' \cup \{q\}$. La maximalidad del tamaño de $\mathcal{Q}'$ garantiza que existen $q_1', \ldots, q_{12}'$ en $\mathcal{Q}' \cup \{q\}$ tales que

$$\sum_{i=1}^{6} \tau(q_i') = \sum_{i=7}^{12} \tau(q_i'), \tag{1.8}$$

donde

$$q_1' < \cdots < q_6', \quad q_7' < \cdots < q_{12}', \qquad (q_1', \ldots, q_6') \neq (q_7', \ldots, q_{12}'). \tag{1.9}$$

La elección de $\mathcal{Q}'$ garantiza

$$q \in \{q_1', \ldots, q_{12}'\}.$$

De hecho, las condiciones (1.9) obligan a que q aparezca en la sucesión $q_1', \ldots, q_{12}'$ a lo más dos veces. Si incide en dicha sucesión dos ocasiones entonces podemos cancelar $\tau(q)$ en (1.8) y renombrando las variables tenemos

$$\sum_{i=1}^{5} \tau(q_i') = \sum_{i=6}^{10} \tau(q_i')$$

para ciertos $q_1', \ldots, q_{10}' \in \mathcal{Q}'$ con

$$q_1' < \cdots < q_5', \quad q_6' < \cdots < q_{10}', \quad (q_1', \ldots, q_5') \neq (q_6', \ldots, q_{10}').$$

Dado que $|\mathcal{Q}'| \geq 12$ podemos tomar $q' \in \mathcal{Q}'\backslash\{q'_1, \ldots, q'_{10}\}$ de tal forma que

$$\tau(q') + \sum_{i=1}^{5} \tau(q'_i) = \tau(q') + \sum_{i=6}^{10} \tau(q'_i)$$

con las variables $q', q'_1, \ldots, q'_{10}$ satisfaciendo (1.8) y (1.9). Hecho que contradice la definición de $\mathcal{Q}'$. Por lo tanto sólo es posible que q aparezca una vez en la sucesión $q'_1, \ldots, q'_{12}$. Concluimos que para todo $q \in \mathcal{Q}\backslash\mathcal{Q}'$ existen $q'_1, \ldots, q'_{11} \in \mathcal{Q}'$ tales que

$$\tau(q) = \sum_{i=1}^{6} \tau(q'_i) - \sum_{i=7}^{11} \tau(q'_i).$$

En particular, tenemos que para todo $q \in \mathcal{Q}\backslash\mathcal{Q}'$ existen $q'_1, \ldots, q'_{11} \in \mathcal{Q}'$ tales que

$$q^{11} = \tau^2(q) - \tau(q^2) = \sum_{i=1}^{6} \tau(qq'_i) - \sum_{i=7}^{11} \tau(qq'_i) - \tau(q^2). \tag{1.10}$$

El siguiente objetivo es probar la solubilidad de la ecuación de Waring-Goldbach

$$q_1^{11} + \cdots + q_{2050}^{11} = M \tag{1.11}$$

en primos $q_1, \ldots, q_{2050} \in \mathcal{Q}\backslash\mathcal{Q}'$. El Lema 2, tomando $s_0 = 2050$, garantiza que existe una constante $c_1 > 0$ tal que para I, el número de soluciones de (1.11), tiene lugar la estimación

$$c_1 \frac{M^{2050/11-1}}{(\log M)^{2050}} \leq I.$$

Aplicando el Lema 2 con $s_0 = 2049$ y la estimación $|\mathcal{Q}'| \ll M^{1/11-1/132}$ tenemos para I', el número de soluciones de (1.11) con al menos una variable perteneciendo a $\mathcal{Q}'$, la estimación

$$I' \ll |\mathcal{Q}'| \frac{M^{2049/11-1}}{(\log M)^{2049}} \ll \frac{M^{2050/11-1-1/132}}{(\log M)^{2049}}.$$

En consecuencia $I' < I$ y se sigue que la ecuación (1.11) es soluble en las variables $q_1, \ldots, q_{2050}$ en $\mathcal{Q}\backslash\mathcal{Q}'$. Fijemos alguna de estas soluciones $(q_1, \ldots, q_{2050})$. A cada q_i, $1 \leq i \leq 2050$ aplicamos (1.10) con $q = q_i$, reordenamos los sumandos y notando que $qq'_j \leq M^{2/11}$ a la vez que qq'_j carece de divisores primos

menores que $\log^2 M$ tenemos que todo entero par M suficientemente grande se puede representar como

$$M = \sum_{i=1}^{6\times 2050} \tau(n_i) - \sum_{i=1}^{6\times 2050} \tau(m_i)$$

donde $m_i n_i$ carece de divisores primos menores que $\log^2 M$ para todo $1 \leq i \leq 6 \times 2050$ y además

$$\max_{1\leq i\leq 6\times 2050} \{n_i, m_i\} \leq M^{2/11}.$$

Es claro que multiplicando la ecuación anterior por -1 obtenemos una representación de la misma naturaleza para $-M$. También es posible remover la condición de paridad; según la paridad de M, basta considerar $M+1 = M+\tau(1)$ o $M+\tau(n)$ para algún n conveniente tal que $\tau(n) \equiv 0 \pmod 2$. De esta forma, cualquier entero M con valor absoluto suficientemente grande se puede escribir como

$$M = \sum_{i=1}^{6\times 2050} \tau(n_i) - \sum_{i=1}^{6\times 2050+1} \tau(m_i) \tag{1.12}$$

donde $m_i n_i$ no tiene divisores primos menores que $\log^2 |M|$ para todo $1 \leq i \leq 6 \times 2050$ y además

$$\max_{1\leq i\leq 6\times 2050+1} \{n_i, m_i\} \leq |M|^{2/11}.$$

Sucede además que

$$-\tau(12) = 370944 = \tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105).$$

De esta forma, multiplicando (1.12) por $-\tau(12)$ tenemos

$$370944M = \sum_{i=1}^{6\times 6\times 2050+1} \tau(n_i), \tag{1.13}$$

donde n_i no tiene factores primos en el intervalo $(23!, \log^2 |M|)$ y además

$$\max_{1\leq i\leq 6\times 6\times 2050+1} \{n_i, m_i\} \leq 106|M|^{2/11}.$$

Ahora demostraremos que todo entero $0 \leq r < 370944$ puede ser escrito como suma de exactamente 199 números $\tau(n)$, $n \leq 105$. Remarcamos que

$$\tau(1) = 1, \quad \tau(2) = -24, \quad \tau(3) = 252, \quad \tau(5) = 4830, \quad \tau(8) = 84480.$$

Si $0 \leq r < 370944$, entonces existen enteros r_4 y r_4' tales que

$$r = \tau(8)r_4 + r_4', \quad 0 \leq r_4 \leq 4,\ 0 \leq r_4' < \tau(8).$$

Para cada r_4' existen enteros r_3 y r_3' tales que

$$r_4' = \tau(5)r_3 + r_3', \quad 0 \leq r_3 \leq 17,\ 0 \leq r_3' < \tau(5).$$

Para cada r_3' existen enteros r_2 y r_2' tales que

$$r_3' = \tau(3)r_2 - r_2', \quad 0 \leq r_2 \leq 20,\ 0 \leq r_2' < \tau(3).$$

Para cada r_2' existen enteros r_1 y r_0 tales que

$$r_2' = -\tau(2)r_1 - r_1', \quad 0 \leq r_1 \leq 11,\ 0 \leq r_0 < -\tau(2).$$

De esta forma, r se puede escribir como

$$r = \tau(8)r_4 + \tau(5)r_3 + \tau(3)r_2 + \tau(2)r_1 + \tau(1)r_0,$$

donde

$$r_4 + r_3 + r_2 + r_1 + r_0 \leq 75.$$

Por lo tanto, todo entero $0 \leq r < 370944$ se puede escribir como la suma de a lo más 75 números $\tau(n)$, $n \leq 8$. Por otra parte, todo entero mayor que 29 se puede escribir como $6x + 7y$, para ciertos enteros positivos x, y. Conforme a este hecho y junto con las identidades

$$\begin{aligned} \tau(12) + \tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105) &= 0, \\ \tau(6) + \tau(14) + \tau(29) + \tau(41) + \tau(42) + \tau(44) + \tau(48) &= 0, \end{aligned}$$

tenemos que todo entero $0 \leq r < 370944$ puede ser representado como

$$\sum_{i=1}^{199} \tau(n_i), \qquad \max_{1 \leq i \leq 199} n_i \leq 105.$$

Sea L un entero arbitrario con valor absoluto $|L|$ suficientemente grande. En del argumento anterior, existen enteros $n_1, \ldots, n_{199}$ menores que 105 tales que

$$L \equiv \sum_{i=1}^{198} \tau(n_i) \pmod{370944},$$

por lo que existe un entero M de valor absoluto suficientemente grande tal que es posible aplicar (1.13) para obtener

$$L = \sum_{i=1}^{199} \tau(n_i) + 370944M = \sum_{i=1}^{74000} \tau(n_i),$$

con ciertos enteros positivos $n_1, \ldots, n_{74000}$ los cuales carecen de divisores primos en el intervalo $(\log\log|L|, \log^2|L|)$ y además

$$\max_{1\leq i\leq 74000} n_i \ll |L|^{2/11}.$$

□

Notamos que se pueden aplicar los mismos argumentos para demostrar que todo entero L de valor absoluto suficientemente grande se puede escribir como suma de 73999 sumandos de la forma $\tau(n)$, $1 \leq n \ll |L|^{2/11}$. Este hecho será utilizado en la demostración del Teorema 1.

El siguiente lema es consecuencia de un resultado más general obtenido por Murty [45].

Lema 4. *Para una densidad positiva de números primos se tiene*

$$|\tau(p)| > 1{,}4p^{11/2}.$$

Dados $\mathcal{X}$, $\mathcal{Y}$ subconjuntos de $\mathbb{F}_p$ y k un entero positivo se denota

$$\mathcal{X}+\mathcal{Y} = \{x+y \ : \ x\in\mathcal{X},\ y\in\mathcal{Y}\}, \quad \mathcal{X}\mathcal{Y} = \{xy \ : \ x\in\mathcal{X}, y\in\mathcal{Y}\},$$

$$k\mathcal{X} = \{x_1+\cdots+x_k \ : \ x_1,\ldots,x_k\in\mathcal{X}\}.$$

El siguiente resultado de combinatoria [30] se debe a Glibichuk.

Lema 5. *Si $\mathcal{X}$ y $\mathcal{Y}$ son subconjuntos de $\mathbb{F}_p$ tales que $|\mathcal{X}||\mathcal{Y}| \geq 2p$, entonces*

$$8\mathcal{X}\mathcal{Y} = \mathbb{F}_p.$$

1.4. Demostración del Teorema 1

Sea N un entero, $|N| \geq N_0$, donde N_0 es alguna constante positiva. Conforme a lo establecido en el Lema 4, existe una constante $C > 100$ tal que el intervalo

$$\left[\frac{\log|N|}{C^2}, \frac{\log|N|}{C}\right]$$

contiene $\gg \log|N|/\log\log|N|$ números primos cumpliendo $|\tau(q)| > 1{,}4q^{11/2}$. Sea T el producto de todos estos números primos, salvo quizás un término a fin de tener $\tau(T) > 0$. En virtud de la multiplicatividad de la función $\tau(n)$, existe una constante $c_1 > 0$ tal que

$$\tau(T)/T^{11/2} > e^{c_1 \log|N|/\log\log|N|}. \tag{1.14}$$

Por otra parte, para alguna constante grande C_1, tenemos

$$\left(\log|N|/C^2\right)^{\log|N|/C_1 \log\log|N|} < T < e^{2\log|N|/C}.$$

De este hecho se tiene

$$|N|^{c_2} < T < |N|^{0{,}02}, \tag{1.15}$$

donde $c_2 > 0$ es alguna constante absoluta, y además cada divisor primo q de T satisface

$$\log|N|/C^2 < q < \log|N|.$$

Para T definido en esta forma, existen enteros L y u tales que

$$N = \tau(T)L + u, \qquad \tau(T) \leq u \leq 2\tau(T). \tag{1.16}$$

Combinando la estimación de Deligne con las desigualdades (1.14) y (1.15) se tiene $|N|^{11c_2/2} < \tau(T) < |N|^{1/5}$. Claramente, si $|N|$ es un número grande, también lo serán u y $|L|$. De acuerdo al Lema 3, u se puede escribir en la forma

$$u = \sum_{i=1}^{74000} \tau(k_i), \qquad \max_i k_i \ll u^{2/11}. \tag{1.17}$$

En vista de que $|L|$ también es un entero grande, al aplicar nuevamente el Lema 3 tenemos

$$L = \sum_{i=1}^{74000} \tau(n_i), \qquad \max_i n_i \ll |L|^{2/11}, \tag{1.18}$$

donde los enteros $n_1, \ldots, n_{74000}$ carecen de divisores primos en el intervalo $(\log\log|L|, \log^2|L|)$. En particular, dado que $|N|^{4/5} \ll |L| \leq |N|$, los enteros $n_1, \ldots, n_{74000}$ no tienen divisores primos en el intervalo $(\log\log|N|, \log|N|)$ y conforme a la elección de T tenemos $(n_i, T) = 1$. Por lo tanto, usando la multiplicatividad de la función $\tau(n)$ y la representación (1.18) resulta

$$\tau(T)L = \sum_{i=1}^{74000} \tau(Tn_i). \tag{1.19}$$

De (1.14) y (1.16) tenemos

$$T \leq \tau(T)^{2/11} e^{-(2c_1/11)\log|N|/\log\log|N|} \ll \left(\frac{|N|}{|L|}\right)^{2/11} e^{-(2c_1/11)\log|N|/\log\log|N|}.$$

Por lo tanto

$$Tn_i \ll T|L|^{2/11} \leq |N|^{2/11} e^{-c\log|N|/\log\log|N|}$$

para alguna constante $c > 0$. Combinando este hecho con (1.16), (1.17) y (1.19), concluimos la demostración para enteros $|N| \geq N_0$. Si N es tal que $2 \leq |N| < N_0$ entonces tomemos algún entero fijo n_0 tal que $2|\tau(n_0)| > N_0$. De esta forma

$$|N - \tau(n_0)| > N_0.$$

Por lo tanto $N - \tau(n_0)$ puede ser escrito como la suma de 147999 valores $\tau(n)$, $n \ll 1$. Concluyendo la demostración del Teorema 1. □

1.5. Demostración del Teorema 2

Sea C una constante positiva grande. Definamos a los conjuntos

$$\begin{aligned} \mathcal{Q} &= \{q : 23 < q \leq Cp^{1/2}\log p,\ q \text{ es número primo}\}, \\ \mathcal{T} &= \{\tau(q) : q \in \mathcal{Q}\}. \end{aligned}$$

Si $|\mathcal{T}| > 3p^{1/2}$, entonces podemos dividir a $\mathcal{T}$ en dos subconjuntos ajenos $\mathcal{X}, \mathcal{Y}$ tales que $|\mathcal{X}||\mathcal{Y}| > 2p$ y de esta forma el resultado se tiene aplicando el Lema 5.

Supongamos que $|\mathcal{T}| \leq 3p^{1/2}$. Sucede que

$$\mathcal{Q} = \bigcup_{i=1}^{|\mathcal{T}|} \mathcal{A}_i$$

donde los conjuntos $\mathcal{A}_i$ estan definidos de tal forma que $\tau(q) \equiv \tau(q') \pmod p$ si, y sólo si $q, q' \in \mathcal{A}_i$.

Es claro que cada conjunto $\mathcal{A}_i$ admite un subconjunto $\mathcal{A}_i'$ tal que

$$0 \leq |\mathcal{A}_i| - |\mathcal{A}_i'| \leq 3, \quad |\mathcal{A}_i'| \equiv 0 \pmod 4.$$

Llamemos

$$\mathcal{Q}' = \bigcup_{i=1}^{|\mathcal{T}|} \mathcal{A}_i'.$$

El teorema de los números primos garantiza que $|\mathcal{Q}| \geq Cp^{1/2}$ si p es suficientemente grande. De esta forma

$$|\mathcal{Q}'| \geq |\mathcal{Q}| - 3|\mathcal{T}| \geq |\mathcal{Q}| - 9p^{1/2} \geq (C-9)p^{1/2}. \tag{1.20}$$

Dado que cada conjunto $|\mathcal{A}_i'|$ tiene cardinalidad par, podemos encontrar $|\mathcal{A}_i'|/2$ parejas distintas que pertenecen a $\mathcal{A}_i'$. En total tenemos

$$\sum_{i=1}^{|\mathcal{T}|} |\mathcal{A}_i'|/2 = |\mathcal{Q}'|/2$$

parejas (q, q'). Dividimos este conjunto de parejas en dos conjuntos ajenos J_1 y J_2 con $|J_1| = |J_2| = |\mathcal{Q}'|/4$. Consideremos a los conjuntos

$$\begin{aligned} \mathcal{X} &= \{\tau(qq') - \tau(q^2) \pmod p : (q, q') \in J_1\}, \\ \mathcal{Y} &= \{\tau(qq') - \tau(q^2) \pmod p : (q, q') \in J_2\}. \end{aligned}$$

Dado que

$$\tau(qq') - \tau(q^2) = \tau(q)\tau(q') - \tau(q^2) \equiv \tau^2(q) - \tau(q^2) \equiv q^{11} \pmod p$$

y el valor $q^{11} \pmod p$ se toma a lo más 11 veces tenemos

$$|\mathcal{X}| \geq |J_1|/11 \geq |\mathcal{Q}'|/44, \quad |\mathcal{Y}| \geq |J_2|/11 \geq |\mathcal{Q}'|/44.$$

Por lo tanto, al tomar $C = 100$ (por ejemplo), notamos que de (1.20) se tiene $|\mathcal{X}||\mathcal{Y}| \geq 2p$. La demostración se concluye al aplicando el Lema 5. $\square$

1.6. Demostración del Teorema 3

Considere el conjunto de las clases residuales

$$\mathcal{A}' = \{\tau(q) \,:\, p/2 < q < p\}.$$

Dado $a' \in \mathcal{A}'$, denotaremos por $I(a')$ al número de soluciones de la congruencia

$$\tau(q) \equiv a' \pmod{p}, \quad p/2 < q < p.$$

Del teorema de los números primos tenemos

$$\sum_{a' \in \mathcal{A}'} I(a') = \sum_{p/2<q<p} 1 \gg p/\log p.$$

En consecuencia, existe un elemento a'_0 de $\mathcal{A}'$ tal que

$$I(a'_0) \gg p|\mathcal{A}'|^{-1} \log^{-1} p. \tag{1.21}$$

Elegimos $\mathcal{A} = \mathcal{A}' \backslash \{a'_0\}$ si $|\mathcal{A}'| \geq 2$ y $\mathcal{A} = \{\tau(1)\}$ si $|\mathcal{A}'| = 1$. Entonces

$$|\mathcal{A}'|/2 \leq |\mathcal{A}| \leq |\mathcal{A}'|. \tag{1.22}$$

Definimos el conjunto

$$\mathcal{B} = \{\tau(q^2) \pmod{p} \,:\, p/2 < q < p,\ \tau(q) \equiv a'_0 \pmod{p}\}.$$

Los elementos de $\mathcal{B}$ estan caracterizados por

$$\tau(q^2) = \tau^2(q) - q^{11} \equiv (a'_0)^2 - q^{11} \pmod{p},$$

donde $p/2 < q < p$ y $\tau(q) \equiv a'_0 \pmod{p}$. Por lo tanto, conforme a (1.21) y (1.22) q puede tomar cualquier valor en un conjunto que contiene

$$\gg p|\mathcal{A}'|^{-1} \log^{-1} p \gg p|\mathcal{A}|^{-1} \log^{-1} p$$

distintas clases residuales módulo p. Dado que $q^{11} \pmod{p}$ toma cada uno de sus valores a lo más 11 veces, tenemos

$$|\mathcal{B}| \gg p|\mathcal{A}|^{-1} \log^{-1} p. \tag{1.23}$$

Escojamos un valor arbitrario ε con $0 < \varepsilon < 0{,}1$. Sea $\mathcal{C}$ el conjunto que consiste de los distintos valores de la sucesión

$$\tau(q) \pmod p,\ \tau(q^2) \pmod p,$$

donde $q \leq p^{0,5\varepsilon}$. Aplicando el argumento anterior a los conjuntos

$$\{\tau(q) \pmod p\ :\ q \leq p^{0,5\varepsilon}\},$$

$$\{\tau(q^2) \pmod p\ :\ q \leq p^{0,5\varepsilon}\},$$

observamos que $|\mathcal{C}| \gg p^{\varepsilon/6}$. Observe que los conjuntos $\mathcal{A}, \mathcal{B}$ y $\mathcal{C}$ consisten de elementos de la forma $\tau(n_1), \tau(n_2)$ y $\tau(n_3)$ respectivamente, en tal forma que n_1, n_2 y n_3 son primos relativos a pares y $n_1 \leq p$, $n_2 \leq p^2$ y $n_3 \leq p^{\varepsilon}$.

Si $|\mathcal{A}| < p^{0,1\varepsilon}$, entonces por (1.23) se tiene $|\mathcal{B}| \gg p^{1-\varepsilon/9}$. Por lo tanto $|\mathcal{B}||\mathcal{C}| \gg p^{1+0,01\varepsilon}$ y es posible aplicar el Lema 5 tomando $\mathcal{X} = \mathcal{B}$, $\mathcal{Y} = \mathcal{C}$ y usemos la propiedad multiplicativa de la función $\tau(n)$. Los elementos del conjunto

$$\mathcal{X}\mathcal{Y} = \{xy\ :\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$$

serán en este caso de la forma $\tau(n) \pmod p$, con $n \leq p^{2+\varepsilon}$.

Si $|\mathcal{A}| > p^{2/3}$, entonces dividamos al conjunto $\mathcal{A}$ en dos conjuntos ajenos $\mathcal{A}_1, \mathcal{A}_2$ ambos con más de $p^{2/3}/3$ elementos. Apliquemos el Lema 5 con $\mathcal{X} = \mathcal{A}_1$ y $\mathcal{Y} = \mathcal{A}_2$. En este caso los elementos de $\mathcal{X}\mathcal{Y}$ son de la forma $\tau(n)$ (mód p) con $n \leq p^2$.

Si $p^{\varepsilon/10} < |\mathcal{A}| < p^{2/3}$, entonces llamemos $\mathcal{D}$ al conjunto de mayor tamaño de entre $\mathcal{A} + \mathcal{C}$ y $\mathcal{A}\mathcal{C}$. Dado que $|\mathcal{C}| \gg p^{\varepsilon/6}$ la estimación de Bourgain [4, Teorema 1.1] implica que existe una constante $\gamma = \gamma(\varepsilon) > 0$ tal que

$$|\mathcal{D}| \gg p^{\gamma}|\mathcal{A}|.$$

Entonces $|\mathcal{B}||\mathcal{D}| \gg p^{1+\gamma/2}$ y aplicamos el Lema 5 con $\mathcal{X} = \mathcal{B}$ y $\mathcal{Y} = \mathcal{D}$. En este caso los elementos del conjunto $\mathcal{X}\mathcal{Y}$ serán de la forma $\tau(n_1)+\tau(n_2) \pmod p$, donde $1 \leq n_1, n_2 \leq p^3$ o bien de la forma $\tau(n) \pmod p$ con $n \leq p^{3+\varepsilon}$. Con esto concluimos la demostración del Teorema 3. □

1.7. Demostración del Teorema 4

Sea x un número positivo suficientemente grande. Usaremos el hecho de que el número de divisores de un entero $n \geq 3$ cumple con la desigualdad

$$d(n) \ll e^{0,7 \log n / \log\log n},$$

se puede consultar por ejemplo [44, Capítulo 1], para una mejor estimación. Denotemos

$$\mathcal{N}_1 = \{\tau(p^2) \ : \ p \leq x^{1/2}\}, \qquad \mathcal{N}_2 = \{\tau(pq) \ : \ p < q \leq x^{1/2}\}.$$

Es suficiente demostrar que

$$\text{máx}\{|\mathcal{N}_1|, |\mathcal{N}_2|\} > x^{1/2} e^{-4 \log x / \log\log x}.$$

Denotemos por J al número de soluciones de la ecuación

$$\tau(p^2) = \tau(q^2)$$

en los números primos $p \leq x^{1/2}$, $q \leq x^{1/2}$, y llamemos $I(\lambda)$ al número de soluciones de la ecuación

$$\tau(p^2) = \lambda$$

en los primos $p \leq x^{1/2}$.

Si $J \leq x^{1/2} e^{3{,}9 \log x / \log\log x}$, entonces, usando la desigualdad de Cauchy-Schwartz y el teorema de los números primos tenemos

$$x^{1/2} e^{3{,}9 \log x / \log\log x} \geq J = \sum_{\lambda \in \mathcal{N}_1} I^2(\lambda) \geq \frac{1}{|\mathcal{N}_1|} \left(\sum_{\lambda \in \mathcal{N}_1} I(\lambda) \right)^2 > \frac{x}{|\mathcal{N}_1| \log^2 x}.$$

Por lo tanto

$$|\mathcal{N}_1| > x^{1/2} e^{-4 \log x / \log\log x}$$

y el resultado queda demostrado en este caso.

Supongamos ahora que $J > x^{1/2} e^{3{,}9 \log x / \log\log x}$. Denotemos

$$\mathcal{L} = \{(p, q) \ : \ p < q \leq x^{1/2}, \, \tau(p^2) = \tau(q^2)\}.$$

La hipótesis en J garantiza que $|\mathcal{L}| > 0{,}4\, x^{1/2} e^{3{,}9 \log x / \log\log x}$. Por otra parte, si (p, q) pertenece a $\mathcal{L}$, entonces

$$\tau^2(q) - \tau^2(p) = \tau(q^2) - \tau(p^2) + q^{11} - p^{11} = q^{11} - p^{11}.$$

Para un entero positivo $\lambda \leq x^{11/2}$, la ecuación $q^{11} - p^{11} = \lambda$ tiene a lo más

$$10 d(\lambda) < e^{3{,}9 \log x / \log\log x}$$

soluciones. De esta forma, cuando las parejas (p, q) recorren el conjunto $\mathcal{L}$, el número $q^{11} - p^{11}$ recorre un conjunto con al menos

$$|\mathcal{L}|e^{-3,9 \log x/ \log\log x} > 0{,}4x^{1/2}$$

enteros distintos. En consecuencia

$$\#\{\tau(q^2) - \tau(p^2) \ : \ p \leq x^{1/2},\ p^{1/2}\} > 0{,}4x^{1/2}.$$

Por lo tanto, definiendo

$$\mathcal{A} = \{\tau(p) \ : \ p \leq x^{1/2}\},$$

obtenemos

$$|\mathcal{A}| \geq \#\{\tau^2(p) \ : \ p \leq x^{1/2}\} > 0{,}5p^{1/4}.$$

Separando al conjunto $\mathcal{A}$ en dos conjuntos ajenos $\mathcal{A}_1, \mathcal{A}_2$ tales que $|\mathcal{A}_1| \geq |\mathcal{A}_2| \geq 0{,}1p^{1/4}$, consideremos la sucesión

$$a_1 a_2 \ : \qquad a_1 \in \mathcal{A}_1,\ a_2 \in \mathcal{A}_2$$

Usando el hecho de que cada entero λ puede ser escrito $O(d(\lambda))$ veces en la forma $a_1 a_2$, tenemos

$$|\mathcal{N}_2| > x^{1/2} e^{-4 \log x/ \log\log x}.$$

Con lo cual concluimos la demostración del Teorema 4. □

1.8. Demostración del Teorema 5

Sea $\mathcal{Q}$ el conjunto de los primos divisores del número

$$\prod_{\substack{p \leq x \\ \tau(p) \neq 0}} \tau(p)\tau(p^2).$$

Sea ε una constante positiva pequeña que será elegida más adelante. Podemos suponer que $|\mathcal{Q}| \leq \varepsilon \frac{(\log x)^{13/11}}{\log\log x}$, en el otro caso el resultado se tiene. Sea $\mathcal{Y}$ el conjunto de los números $\mathcal{Q}$–suaves (es decir, con divisores primos en $\mathcal{Q}$) de cualquier signo y con valor absoluto no superior a x. Denotemos por $\mathcal{Z}$ al conjunto de los enteros positivos de la forma yq donde $y \in \mathcal{Y}$ y $q \in \mathcal{Q}$.

En virtud del Lema 1, es posible fijar a un ε suficientemente pequeño de tal forma que

$$|\mathcal{Y}| \leq x^{2/13}, \quad |\mathcal{Z}| \leq x^{2/13} \tag{1.24}$$

Si para cualquier entero $\lambda \neq 0$ el número de soluciones de la ecuación $\tau(q) = \lambda$ en primos $p \leq x$ con $p \notin \mathcal{Q}$, es menor que $x^{2/13}e^{40\log x/\log\log x}$, entonces, utilzando el Lema 4, obtenemos

$$\#\{\tau(p) \,:\, p \leq x,\, \tau(p) \neq 0,\, p \notin \mathcal{Q}\} \gg x^{11/13}e^{-41\log x/\log\log x}$$

y el teorema se sigue del resultado de Deligne y del Lema 1.

Sea ahora $\lambda \neq 0$ tal que el número de soluciones de la ecuación $\tau(p) = \lambda$ en primos $p \leq x$ con $p \notin \mathcal{Q}$ es $\geq x^{2/13}e^{40\log x/\log\log x}$. Denotemos por $\mathcal{P}$ a este conjunto de soluciones. Por lo tanto

$$|\mathcal{P}| \geq x^{2/13}e^{40\log x/\log\log x}. \tag{1.25}$$

Para cualquier $p \in \mathcal{P}$ el número $\lambda^2 - p^{11} = \tau(p^2)$ es $\mathcal{Q}$–suave. Esto implica que $\lambda^2 - p^{11}$ pertenece a $\mathcal{Y}$ o bien es divisible por algún elemento del conjunto $\mathcal{Z} \setminus \mathcal{Y}$. Notemos que para cualquier z en $\mathcal{Z} \setminus \mathcal{Y}$ tenemos $x < z \leq 2x^{12}$.

Los primos p para los cuales $\lambda^2 - p^{11}$ pertenece a $\mathcal{Y}$ contribuyen al conjunto $\mathcal{P}$ con a lo más $|\mathcal{Y}|$ elementos. Considere aquellos primos $p \leq x$, $p \notin \mathcal{Q}$, para los cuales $\lambda^2 - p^{11}$ es divisible por algún z de $\mathcal{Z} \setminus \mathcal{Y}$. Para z dado, el número de soluciones de la congruencia

$$\lambda^2 - p^{11} \equiv 0 \pmod{z}$$

en primos $p \leq z$, $(p, z) = 1$, es $\ll 11^{\omega(z)} \ll e^{3\log z/\log\log z} \ll e^{36\log x/\log\log x}$. Entonces, el número total de primos $p \leq x$, $p \notin \mathcal{Q}$, para los cuales $\lambda^2 - p^{11}$ es divisible por algún z en $\mathcal{Z} \setminus \mathcal{Y}$ es

$$\ll |\mathcal{Z}|e^{36\log x/\log\log x}.$$

De esta forma, al considerar (1.24), obtenemos

$$|\mathcal{P}| \ll |\mathcal{Y}| + |\mathcal{Z}|e^{36\log x/\log\log x} \ll x^{2/13}e^{36\log x/\log\log x}.$$

Afirmación que contradice (1.25) y de esta forma concluimos la demostración. □

Capítulo 2

La congruencia $x_1x_2 \equiv x_3x_4 + \lambda \pmod{p}$ y aplicaciones

La congruencia

$$x_1x_2 \equiv x_3x_4 \pmod{p}, \tag{2.1}$$

donde p es un primo suficientemente grande, aparece en muchos problemas de la teoría de números. Las propiedades distribucionales de sus soluciones han resultado ser muy importantes en varias aplicaciones, por ejemplo en el problema de la representabilidad de clases residuales como producto de enteros pequeños y en la estimación del momento cuarto de la suma de caracteres. Se pueden consultar las referencias [2], [10], [13], [21], [47], [49] y [50]. Sean L_i, N_i, $1 \leq i \leq 4$, enteros tales que $0 \leq L_i < L_i + N_i < p$. Denotemos por J al número de soluciones de la congruencia (2.1) en el conjunto

$$L_i + 1 \leq x_i \leq L_i + N_i, \quad (1 \leq i \leq 4). \tag{2.2}$$

En vista de la identidad

$$\sum_{\chi} \chi(u) = \begin{cases} p-1, & \text{si } u \equiv 1 \pmod{p}, \\ 0, & \text{si } u \not\equiv 1 \pmod{p}, \end{cases}$$

donde χ recorre el conjunto de los caracteres multiplicativos módulo p, el valor J puede expresarse en términos de sumas de caracteres

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x_1,x_2,x_3,x_4} \chi(x_1x_2x_3^*x_4^*),$$

donde x^* denota el inverso multiplicativo de $x \not\equiv 0 \pmod p$ y el rango que recorren las variables x_1, x_2, x_3 y x_4 en las sumatorias está definido por (2.2). El carácter principal $\chi = \chi_0$ contribuye a la sumatoria la cantidad $N_1N_2N_3N_4/(p-1)$, que en muchas ocasiones indica el comportamiento asintótico de J. Ayyad, Cochrane y Zheng [2] demostraron que

$$J = \frac{N_1N_2N_3N_4}{p} + O\left(\sqrt{N_1N_2N_3N_4}\log^2 p\right). \tag{2.3}$$

Los autores manifestaron la esperanza de poder sustituir el factor $\log^2 p$ por $\log p$ el cual sería, en términos generales, el mejor término de error posible, (puede consultarse la discusión [2, p. 339]). En el caso particular $N_1 = N_2$, $N_3 = N_4$ o $N_1 = N_3$, $N_2 = N_4$, ellos probaron

$$J \approx \frac{N_1N_2N_3N_4}{p} + O\left(\sqrt{N_1N_2N_3N_4}\log p\right), \tag{2.4}$$

reduciendo un factor $\log p$ a costa de la fórmula asintótica.

Como consecuencias de (2.3) y (2.4) los autores de [2] obtuvieron las siguientes estimaciones para el momento cuarto de la suma de caracteres: para cualesquiera enteros L y $N > 0$ tenemos

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log^2 p; \tag{2.5}$$

si además $N \ll \sqrt{p \log p}$, entonces

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log p. \tag{2.6}$$

Estos resultados mejoran aquel de Friedlander e Iwaniec [12, Lema 3] donde obtuvieron $N^2 \log^6 p$ en lugar de $N^2 \log^2 p$ en la parte derecha de (2.5); remarcamos que en la demostración de [12, Lema 3] parece que existe una

pequeña omisión en la potencia del factor logarítmico cuando es aplicada la desigualdad de Hölder, aparentemente debe de ser $N^2 \log^8 p$ en lugar de $N^2 \log^6 p$. Estimaciones similares pueden encontrarse en Vaughan [54, p. 184], ver también Harman [32, Lemma 2]. El método de [12], [32] y [54] se aplica para módulos en general pero restringidos a $L = 0$.

Tal como se mencionó en [2], el trabajo de Montgomery y Vaughan [43] tiene por consecuencia la estimación

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \max_N \left| \sum_{x=1}^{N} \chi(x) \right|^4 \ll p^2;$$

en particular, cuando N es de orden p, en (2.5) es posible remover el factor $\log^2 p$. El trabajo de Burgess [7] implica la estimación

$$\frac{1}{p} \sum_{L=1}^{p} \left\{ \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \right\} \ll N^2,$$

la cual muestra que en promedio sobre L se puede remover el factor $\log^2 p$.

2.1. Nuevo término de error para J

Teorema 6. *Tiene lugar la siguiente fórmula asintótica:*

$$J = \frac{N_1 N_2 N_3 N_4}{p} + O\left(\sqrt{N_1 N_2 N_3 N_4} \Big(\sqrt{\log p} + \delta(N_1 N_2) \Big) \Big(\sqrt{\log p} + \delta(N_3 N_4) \Big) \right), \tag{2.7}$$

donde

$$\delta(X) = \begin{cases} 0, & si \quad X \leq p, \\ \log \frac{X}{p}, & si \quad X \geq p. \end{cases}$$

La igualdad en (2.7) *también se tiene si los productos $N_1 N_2$ y $N_3 N_4$ son reemplazados por cualquier otra combinación de las parejas N_i.*

El Teorema 6 tiene como consecuencia la siguiente estimación para el momento cuarto de la suma de caracteres:

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \Big(\log p + \log^2 \frac{N^2}{p} \Big).$$

En particular, la estimación (2.6) es efectiva en el rango $N \ll p^{1/2}e^{c\sqrt{\log p}}$ para alguna constante positiva fija c. Además, el Teorema 6 implica el comportamiento asintótico $J \sim N_1N_2N_3N_4/p$ en un rango mas amplio de los parámetros que aquel sugerido por (2.3). Por ejemplo, si $N_1 = N_2 = N_3 = N_4 = N$ y si

$$\frac{N}{p^{1/2}(\log p)^{1/2}} \to \infty, \quad p \to \infty,$$

entonces

$$J = \frac{N^4}{p}(1 + o(1)),$$

mientras (2.3) implica esta fórmula asintótica cuando

$$\frac{N}{p^{1/2}\log p} \to \infty, \quad p \to \infty.$$

El problema de la solubilidad de la congruencia (2.1) se puede conectar con el problema de la representabilidad de clases residuales $h \pmod p$ en la forma

$$xy \equiv h \pmod p, \quad 1 \le x \le N_1,\ 1 \le y \le N_2.$$

Se conjetura que toda clase residual distinta de cero es representable si $N_1 = N_2 = N$ para $N \le p^{1/2+\varepsilon}$. De manera incondicional, del trabajo de Garaev [14] se sigue que, para alguna constante absoluta $c > 0$,

$$\mathbb{F}_p^* = \{xy \pmod p \ :\ 1 \le x, y \le cp^{3/4}\},$$

donde $\mathbb{F}_p^*$ denota al conjunto $\mathbb{F}_p \setminus \{0\}$. Por otra parte, el trabajo de Tenenbaum [52] implica que si

$$N_1 = N_2 = N \le p^{1/2}(\log p)^{0{,}5\kappa - \varepsilon},$$

donde $\kappa = 1 - (\log(e\log 2))/\log 2 \approx 0{,}08607...$, entonces el conjunto

$$\{xy \pmod p \ :\ 1 \le x, y \le N\}$$

contiene sólo $o(p)$ clases residuales módulo p.

Usando el Teorema 6 es posible obtener el siguiente resultado sobre la representabilidad de clases residuales como producto de enteros pequeños.

Teorema 7. *Sean* $N_1N_2 = \Delta p \log p$, *donde* $\Delta = \Delta(p) \to \infty$ *si* $p \to \infty$. *Entonces el conjunto*

$$\{xy \pmod p : \quad L_1 + 1 \le x \le L_1 + N_1, \quad L_2 + 1 \le y \le L_2 + N_2\}$$

contiene $\left(1 + O(\frac{1}{\Delta} + \frac{\log^2 \Delta}{\Delta \log p})\right)p$ *clases residuales módulo* p. *En particular, este conjunto contiene casi todas las clases residuales módulo* p.

Un corolario del trabajo de Garaev y Karatsuba [21, Teorema 1.1] implica que el conjunto

$$\{qy \pmod p : \quad q \le p^{1/2}, \quad 1 \le y \le \Delta p^{1/2} \log p\},$$

donde q denota números primos, contiene $(1 + O(\Delta^{-1}))p$ clases residuales módulo p. Este resultado puede ser establecido en una manera más general y hay una versión para módulos compuestos. Información más extensa en estos temas se puede consultar en [15] y [21]. También pueden consultarse los trabajos [49], [50] y las referencias allí citadas.

2.2. Propiedades de Combinatoria y Solubilidad

En vista de (2.3) se sigue de inmediato que si $N_1N_2N_3N_4 > cp^2 \log^4 p$, donde $c > 0$ es una constante absoluta, entonces el conjunto (2.2) contiene una solución de la congruencia (2.1). Ayyad, Cochrane y Zheng [2] preguntaron en qué casos el factor $\log^4 p$ puede ser removido totalmente. El siguiente resultado, del trabajo conjunto con Garaev [17], muestra que en general el factor $\log^4 p$ puede ser disminuido a $\log p$. Si además se tiene que N_1N_3 y N_2N_4 son de la misma magnitud, demostraremos que de hecho el factor $\log^4 p$ puede ser removido totalmente.

Teorema 8. *Existe una constante* c *tal que si* $N_1N_2N_3N_4 > cp^2 \log p$, *entonces el conjunto* (2.2) *contiene una solución de la congruencia* (2.1).

La demostración de este Teorema emplea una de las ideas del trabajo de Garaev y Karatsuba [21, Teorema 1.7] y depende de las sumas trigonométricas.

Debemos remarcar que en una serie de artículos el problema de la representabilidad de cero por una forma cuadrática no singular $Q(x_1, x_2, x_3, x_4)$

(mód p) en intervalos de pequeña longitud ha sido investigado. Se sabe que el problema de la solubilidad de la congruencia

$$Q(x_1, x_2, x_3, x_4) \equiv \lambda \pmod p$$

difiere esencialmente en los casos $\lambda \equiv 0 \pmod p$ y $\lambda \not\equiv 0 \pmod p$. Se puede ver la pregunta que surge en [10, p.176]. Una situación similar ocurre en nuestro problema. Considere la congruencia

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod p. \tag{2.8}$$

El Teorema 8 corresponde al caso $\lambda \equiv 0 \pmod p$. Para λ arbitrario, los Teoremas 6 y 7 junto con los Lemas 8 y 9 tienen como consecuencia que existe una constante $c > 0$, tal que si $N_1N_2N_3N_4 > cp^2 \log^3 p$, entonces el conjunto (2.2) admite soluciones para (2.8). La pregunta es saber en qué casos el factor $\log^3 p$ puede ser removido totalmente (notemos que si N_1N_2 tiene la misma magnitud que N_3N_4, entonces es posible cambiar $\log^3 p$ por $\log^2 p$). Un posible enfoque de esta pregunta es el estudio de la congruencia (2.8) desde el punto de vista de la combinatoria. Para $\mathcal{A}$ y $\mathcal{B}$ subconjuntos dados del sistema completo de residuos $\mathbb{F}_p$ se definen los conjuntos

$$\mathcal{A} + \mathcal{B} = \{a + b : \ a \in \mathcal{A},\, b \in \mathcal{B}\}, \quad \mathcal{A} - \mathcal{B} = \{a - b : \ a \in \mathcal{A},\, b \in \mathcal{B}\},$$

$$k\,\mathcal{A} = \{a_1 + \cdots + a_k : \ a_i \in \mathcal{A},\, 1 \le i \le k\}, \quad \mathcal{A}\,\mathcal{B} = \{ab : \quad a \in \mathcal{A},\, b \in \mathcal{B}\}.$$

La cardinalidad de $\mathcal{A}$ se denota por $|\mathcal{A}|$. En [30] Glibichuk demostró que si $\mathcal{A}$ y $\mathcal{B}$ son subconjuntos de $\mathbb{F}_p$ tales que $|\mathcal{A}||\mathcal{B}| \ge 2p$, entonces

$$8\mathcal{A}\mathcal{B} = \mathbb{F}_p.$$

Más aún, el resultado de Glibichuk (ver la desigualdad al término de la demostración de [30, Teorema 1]) también tiene como consecuencia

$$2(2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p\,, \quad (2\mathcal{A})(2\mathcal{B}) - (2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p\,.$$

En particular, si $N_1N_2 > 10p$ entonces para cualquier entero λ la congruencia (2.8) es soluble en las variables

$$L_1 + 1 \le x_1, x_3 \le L_1 + N_1, \quad L_2 + 1 \le x_2, x_4 \le L_2 + N_2.$$

Esta observación conduce de manera natural a la siguiente conjetura.

Conjetura 1. *Existe una constante positiva c tal que si $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ son subconjuntos de $\mathbb{F}_p^*$ con $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > cp^2$, entonces*

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

La validez de esta conjetura permitiría remover los factores logarítmicos en la resultado antes mencionado, en particular contestaría a la pregunta de Ayyad, Cochrane y Zheng [2]. El empleo de técnicas de sumas trigonométricas junto con argumentos de combinatoria utilizados en [5], [6] y [30] nos permiten responder de manera afirmativa a la Conjetura 1 en casos importantes.

Teorema 9. *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

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

En particular, si $N_1N_3 > 15p$, $N_2N_4 > 15p$, entonces para cualquier entero λ la congruencia

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod{p}.$$

es soluble en el conjunto (2.2).

En fechas recientes Bourgain demostró que existe una constante $c > 0$ tal que para todo entero λ la congruencia

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod{p}$$

tiene solución en el conjunto (2.2) si $N_1N_2N_3N_4 > cp^2$, respondiendo en particular a la pregunta planteada por Ayyad, Cochrane y Zheng.

2.3. Notación y Lemas

A través de este capítulo usaremos la abreviación

$$\mathbf{e}_p(z) = e^{2\pi iz/p}.$$

Recordamos la identidad

$$\sum_{a=0}^{p-1} \mathbf{e}_p(au) = \begin{cases} p, & \text{si } u \equiv 0 \pmod p, \\ 0, & \text{si } u \not\equiv 0 \pmod p, \end{cases}$$

la cual es muy útil para calcular el número de soluciones de varias congruencias.

La idea principal para la demostración del Teorema 6 esta basada en la combinación de los métodos de [2] y [14]. En particular, necesitamos el siguiente Lema de [2].

Lema 6. *La siguiente estimación tiene lugar:*

$$J \ll \frac{N_1N_2N_3N_4}{p} + (p + N_1N_2 \log p)^{1/2}(p + N_3N_4 \log p)^{1/2}.$$

Más aún, la desigualdad tiene lugar si los productos N_1N_2 y N_3N_4 son reemplazados por cualquier otra combinación a pares de N_i.

Lema 7. *Para demostrar el Teorema 6 es suficiente establecer* (2.7) *en el caso $L_1 = L_3$, $L_2 = L_4$, $N_1 = N_3$, $N_2 = N_4$.*

Demostración. La demostración es similar al argumento descrito en [2, p. 408]. Tenemos

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x_1=L_1+1}^{L_1+N_1} \sum_{x_2=L_2+1}^{L_2+N_2} \sum_{x_3=L_3+1}^{L_3+N_3} \sum_{x_4=L_4+1}^{L_4+N_4} \chi(x_1x_2x_3^*x_4^*).$$

Tomando el término que corresponde al carácter principal $\chi = \chi_0$ y posteriormente aplicando la desigualdad de Cauchy-Schwartz, tenemos

$$J - \frac{N_1N_2N_3N_4}{p-1} \ll \sqrt{S_1S_2},$$

donde

$$S_1 = \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x_1=L_1+1}^{L_1+N_1} \sum_{x_2=L_2+1}^{L_2+N_2} \chi(x_1x_2) \right|^2,$$

$$S_2 = \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x_3=L_3+1}^{L_3+N_3} \sum_{x_4=L_4+1}^{L_4+N_4} \chi(x_3^*x_4^*) \right|^2.$$

Claramente,

$$S_1 = J' - \frac{N_1^2 N_3^2}{p-1}, \qquad S_2 = J'' - \frac{N_2^2 N_4^2}{p-1},$$

donde J' es el número de soluciones de la congruencia

$$x_1 x_2 \equiv y_1 y_2 \pmod{p}, \quad L_1{+}1 \le x_1, y_1 \le L_1{+}N_1, \quad L_2{+}1 \le x_2, y_2 \le L_2{+}N_2$$

y J'' es el número de soluciones de la congruencia

$$x_3 x_4 \equiv y_3 y_4 \pmod{p}, \quad L_3{+}1 \le x_3, y_3 \le L_3{+}N_3, \quad L_4{+}1 \le x_4, y_4 \le L_4{+}N_4.$$

Por lo tanto, asumiendo que (2.7) tiene lugar en el caso $L_1 = L_3$, $L_2 = L_4$, $N_1 = N_3$, $N_2 = N_4$, obtenemos

$$S_1 \ll N_1 N_2 \Big(\sqrt{\log p} + \delta(N_1 N_2)\Big)^2, \quad S_2 \ll N_3 N_4 \Big(\sqrt{\log p} + \delta(N_3 N_4)\Big)^2.$$

El caso del apareamiento $\delta(N_1 N_3)$ y $\delta(N_2 N_4)$ se trabaja de manera análoga; con la diferencia de que en este caso definimos S_1, S_2 como

$$S_1 = \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x_1 = L_1+1}^{L_1+N_1} \sum_{x_3 = L_3+1}^{L_3+N_3} \chi(x_1 x_3^*) \right|^2,$$

$$S_2 = \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x_2 = L_2+1}^{L_2+N_2} \sum_{x_4 = L_4+1}^{L_4+N_4} \chi(x_2 x_4^*) \right|^2.$$

□

El siguiente resultado es muy conocido y además bastante útil para la estimación de cardinalidades de conjuntos mediante el número de soluciones de una ecuación asociada.

Lema 8. *Sea s_n cualquier sucesión de elementos (no necesariamente distintos) del sistema completo de residuos $\mathbb{F}_p$. Sea $M \ge 1$ un entero. Si I denota el número de soluciones de la ecuación*

$$s_n = s_m, \quad 1 \le n, m \le M,$$

entonces

$$\#\{s_n : 1 \le n \le M\} \ge \frac{M^2}{I}.$$

Demostración. Sea $\lambda \in \{s_n : 1 \leq n \leq M\}$, denotemos por $I(\lambda)$ al número de soluciones de la ecuación $s_n = \lambda$. Entonces,

$$\sum_{\lambda} I(\lambda) = M, \quad \sum_{\lambda} I^2(\lambda) = I,$$

donde λ en las sumatorias corre a través del conjunto $\{s_n : 1 \leq n \leq M\}$. La estimación requerida se sigue ahora de la desigualdad de Cauchy-Schwartz. □

El siguiente lema es una versión débil del lema mencionado en [2, Sección 1].

Lema 9. *Si* $N_1 = N_2$, $N_3 = N_4$ *y* $N_2N_4 \ll p$, *entonces*

$$J \ll N_2N_4 \log p.$$

Notemos que el Lema 9 también puede ser visto como un caso particular del Teorema 6.

2.4. Demostración del Teorema 6

Conforme a lo establecido en el Lema 7, es suficiente considerar

$$L_1 = L_3, \ L_2 = L_4, \ N_1 = N_3, \ N_2 = N_4.$$

Por lo que, en este caso J denota al número de soluciones de la congruencia

$$x_1x_2x_3^* \equiv x_4 \pmod{p}$$

con las variables sujetas a las condiciones

$$L_1 + 1 \leq x_1, x_3 \leq L_1 + N_1, \quad L_2 + 1 \leq x_2, x_4 \leq L_2 + N_2.$$

Nuestro objetivo es demostrar

$$J - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + (\delta(N_1N_2))^2\Big).$$

Podemos suponer que $N_1 \geq 10, N_2 \geq 10$. Siguiendo la idea de [14], primero tomaremos dos parametros positivos $M_1 \leq N_1/2$, $M_2 \leq N_2/2$, los cuales

serán definidos explícitamente más adelante. Definamos por J_1 al número de soluciones de la congruencia

$$(x_1 + y_1)x_2x_3^* \equiv x_4 + y_4 \pmod{p}$$

sujeta a las condiciones

$$\begin{aligned} L_1 + 1 \leq x_1 \leq L_1 + N_1 - M_1, \quad 1 \leq y_1 \leq M_1, \\ L_2 + 1 \leq x_2 \leq L_2 + N_2, \quad L_1 + 1 \leq x_3 \leq L_1 + N_1, \\ L_2 + 1 \leq x_4 \leq L_2 + N_2 - M_2, \quad 1 \leq y_4 \leq M_2. \end{aligned} \tag{2.9}$$

Por J_2 denotamos al número de soluciones de la congruencia

$$(x_1 - y_1)x_2x_3^* \equiv x_4 - y_4 \pmod{p}$$

sujeta a las condiciones

$$\begin{aligned} L_1 + 1 \leq x_1 \leq L_1 + N_1 + M_1, \quad 1 \leq y_1 \leq M_1, \\ L_2 + 1 \leq x_2 \leq L_2 + N_2, \quad L_1 + 1 \leq x_3 \leq L_1 + N_1, \\ L_2 + 1 \leq x_4 \leq L_2 + N_2 + M_2, \quad 1 \leq y_4 \leq M_2. \end{aligned} \tag{2.10}$$

Entonces,

$$\frac{J_1}{M_1M_2} \leq J \leq \frac{J_2}{M_1M_2}. \tag{2.11}$$

Demostraremos que para M_1 y M_2, elegidos adecuadamente, se tiene la siguiente estimación

$$\frac{J_1}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + (\delta(N_1N_2))^2\Big),$$

$$\frac{J_2}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + (\delta(N_1N_2))^2\Big).$$

Este hecho terminará la demostración del Teorema 6.

Expresamos a J_1 en términos de sumas trigonométricas, esto es

$$J_1 = \frac{1}{p} \sum_{-(p-1)/2 \leq a \leq (p-1)/2} \sum_{x_1,x_2,x_3,x_4,y_1,y_4} \mathbf{e}_p(a((x_1 + y_1)x_2x_3^* - x_4 - y_4)),$$

donde las variables estas sujetas a las condiciones (2.9). Separando el término correspondiente a $a = 0$, obtenemos

$$J_1 - \frac{N_1N_2(N_1 - M_1)(N_2 - M_2)M_1M_2}{p} \ll \frac{1}{p} \sum_{1 \le a \le (p-1)/2} f(a) \left| \sum_{x_1,x_2,x_3,y_1} \mathbf{e}_p(a(x_1 + y_1)x_2x_3^*) \right|,$$

donde

$$f(a) = \min(N_2, p/|a|) \min(M_2, p/|a|).$$

Para $1 \le |b| \le (p-1)/2$ sea $I(a, b)$ el número de soluciones de la congruencia

$$ax_2x_3^* \equiv b \pmod p, \quad L_2 + 1 \le x_2 \le L_2 + N_2, \quad L_1 + 1 \le x_3 \le L_1 + N_1.$$

Entonces,

$$J_1 - \frac{N_1N_2(N_1 - M_1)(N_2 - M_2)M_1M_2}{p} \ll \frac{1}{p} \sum_{1 \le a \le (p-1)/2} \sum_{1 \le |b| \le (p-1)/2} f(a)g(b)I(a, b),$$

donde

$$g(b) = \min(N_1, p/|b|) \min(M_1, p/|b|).$$

Sin perder la generalidad, podemos remover el signo del módulo de $|b|$ (mediante la reflección del intervalo del rango de x_3 con respecto al punto $p/2$). Definamos los siguientes intervalos:

$$\mathcal{A}_1 = [1, p/N_2] \cap \mathbb{Z}, \quad \mathcal{A}_2 = [p/N_2, p/M_2] \cap \mathbb{Z}, \quad \mathcal{A}_3 = [p/M_2, (p-1)/2] \cap \mathbb{Z},$$

$$\mathcal{B}_1 = [1, p/N_1] \cap \mathbb{Z}, \quad \mathcal{B}_2 = [p/N_1, p/M_1] \cap \mathbb{Z}, \quad \mathcal{B}_3 = [p/M_1, (p-1)/2] \cap \mathbb{Z}.$$

Entonces, tenemos

$$J_1 - \frac{N_1N_2(N_1 - M_1)(N_2 - M_2)M_1M_2}{p} \ll \sum_{\nu=1}^{3} \sum_{\mu=1}^{3} T_{\nu\mu}, \tag{2.12}$$

donde

$$T_{\nu\mu} = \frac{1}{p} \sum_{a \in \mathcal{A}_\nu} \sum_{b \in \mathcal{B}_\mu} f(a)g(b) \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \le x_2 \le L_2+N_2 \\ L_1+1 \le x_3 \le L_1+N_1}} 1.$$

A fin de estimar $T_{\nu\mu}$ usamos el Lema 6. Para T_{11} se tiene inmediatamente

$$T_{11} \ll N_1N_2M_1M_2\log p. \tag{2.13}$$

Para estimar T_{12}, descomponemos al intervalo donde se suma b en subintervalos de la forma $e^{j-1}p/N_1 \le b \le e^jp/N_1$, donde $1 \le j \ll \log\frac{N_1}{M_1}$. Por lo tanto, al aplicar el Lema 6 se tiene

$$\begin{aligned} T_{12} &\ll N_2M_1M_2 \sum_{j\ll\log\frac{N_1}{M_1}} \frac{1}{e^j(p/N_1)} \sum_{a\le p/N_2} \sum_{b\le e^jp/N_1} \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\le x_2\le L_2+N_2\\ L_1+1\le x_3\le L_1+N_1}} 1 \\ &\ll \frac{N_1N_2M_1M_2}{p} \sum_{j\ll\log\frac{N_1}{M_1}} \frac{1}{e^j}\Big(e^jp + e^{j/2}p\log p\Big) \ll N_1N_2M_1M_2\log p. \end{aligned}$$

La misma estimación se tiene para T_{21}, por lo tanto

$$T_{12} + T_{21} \ll N_1N_2M_1M_2\log p. \tag{2.14}$$

Para T_{13} se tiene

$$\begin{aligned} T_{13} &\ll pN_2M_2 \sum_j \frac{1}{e^{2j}(p^2/M_1^2)} \sum_{a\le p/N_2} \sum_{b\le e^jp/M_1} \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\le x_2\le L_2+N_2\\ L_1+1\le x_3\le L_1+N_1}} 1 \\ &\ll \frac{M_1^2N_2M_2}{p} \sum_j \frac{1}{e^{2j}}\Big(\frac{e^jN_1p}{M_1} + e^{j/2}(N_1/M_1)^{1/2}p\log p\Big) \\ &\ll N_1N_2M_1M_2\log p. \end{aligned}$$

La misma estimación se garantiza para T_{31}, en consecuencia

$$T_{13} + T_{31} \ll N_1N_2M_1M_2\log p. \tag{2.15}$$

Más adelante, estimamos T_{22} quien aportará el término $\delta(N_1N_2)$ que aparece en el enunciado del Teorema 6. Tenemos

$$\begin{aligned} T_{22} &\ll pM_1M_2 \sum_{\substack{i\ll\log(N_2/M_2)\\ j\ll\log(N_1/M_1)}} \frac{N_1N_2}{e^{i+j}p^2} \sum_{a\le e^ip/N_2} \sum_{b\le e^jp/N_1} \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\le x_2\le L_2+N_2\\ L_1+1\le x_3\le L_1+N_1}} 1 \\ &\ll \frac{N_1N_2M_1M_2}{p} \sum_{\substack{i\ll\log(N_2/M_2)\\ j\ll\log(N_1/M_1)}} \frac{1}{e^{i+j}}\Big(e^{i+j}p + e^{(i+j)/2}p\log p\Big), \end{aligned}$$

de aquí se obtiene

$$T_{22} \ll N_1N_2M_1M_2\Big(\log p + \log\frac{N_1}{M_1}\log\frac{N_2}{M_2}\Big). \tag{2.16}$$

De manera análoga se trabaja con T_{23} y T_{32} :

$$\begin{aligned} T_{23} &\ll M_2p^2 \sum_{\substack{i\ll\log(N_2/M_2)\\ j}} \frac{N_2M_1^2}{e^{i+2j}p^3} \sum_{a\le e^ip/N_2} \sum_{b\le e^jp/M_1} \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\le x_2\le L_2+N_2\\ L_1+1\le x_3\le L_1+N_1}} 1 \\ &\ll \frac{N_2M_2M_1^2}{p} \sum_{\substack{i\ll\log(N_2/M_2)\\ j}} \frac{1}{e^{i+2j}}\Big(\frac{e^{i+j}N_1p}{M_1} + e^{(i+j)/2}p\log p(N_1/M_1)^{1/2}\Big) \\ &\ll N_1N_2M_1M_2\log p. \end{aligned}$$

La misma estimación se tiene para T_{32}, por lo que tenemos

$$T_{23} + T_{32} \ll N_1N_2M_1M_2\log p. \tag{2.17}$$

Finalmente, para T_{33} resulta

$$\begin{aligned} T_{33} &= p^3\sum_{i,j}\frac{M_2^2M_1^2}{e^{2i+2j}p^4} \sum_{a\le e^ip/M_2} \sum_{b\le e^jp/M_1} \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\le x_2\le L_2+N_2\\ L_1+1\le x_3\le L_1+N_1}} 1 \\ &\ll \frac{M_1^2M_2^2}{p}\sum_{i,j}\frac{1}{e^{2i+2j}}\Big(\frac{(e^ip/M_2)N_2(p/M_1)e^jN_1}{p} + e^{(i+j)/2}\sqrt{\frac{N_1N_2}{N_2M_2}}p\log p\Big). \end{aligned}$$

Así,

$$T_{33} \ll N_1N_2M_1M_2\log p. \tag{2.18}$$

Insertando (2.13)–(2.18) en (2.12), deducimos

$$\frac{J_1}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + \log\frac{N_1}{M_1}\log\frac{N_2}{M_2} + \frac{N_1M_2}{p} + \frac{N_2M_1}{p}\Big),$$

siempre que $M_1 \le N_1/2$, $M_2 \le N_2/2$.

Si $N_1N_2 \le 10p$, definimos $M_1 = [N_1/2]$, $M_2 = [N_2/2]$ y se obtiene

$$\frac{J_1}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\log p.$$

Si $N_1N_2 \geq 10p$, entonces definimos $M_1 = [p/N_2] < N_1/2$, $M_2 = [p/N_1] < N_2/2$ y sucede

$$\frac{J_1}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + \log^2 \frac{N_1N_2}{p}\Big). \tag{2.19}$$

Así, la estimación (2.19) se garantiza en ambos casos.

De manera análoga,

$$\frac{J_2}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\Big(\log p + \log^2 \frac{N_1N_2}{p}\Big). \tag{2.20}$$

Sustituyendo (2.19) y (2.20) en (2.11) concluimos la demostración del Teorema 6. □

2.5. Demostración del Teorema 7

Podemos suponer que $\Delta < p$. Sea J el número de soluciones de la congruencia (2.1) bajo las condiciones

$$L_1 + 1 \leq x_1, x_3 \leq L_1 + N_1, \quad L_2 + 1 \leq x_2, x_4 \leq L_2 + N_2,$$

y sea $I(\lambda)$ el número de soluciones de la congruencia

$$x_1x_2 \equiv \lambda \pmod p, \quad L_1 + 1 \leq x_1 \leq L_1 + N_1, \quad L_2 + 1 \leq x_2 \leq L_2 + N_2.$$

Entonces

$$\sum_{\lambda=0}^{p-1}\Big(I(\lambda) - \frac{N_1N_2}{p}\Big)^2 = \sum_{\lambda=0}^{p-1} I^2(\lambda) - \frac{N_1^2N_2^2}{p}.$$

Dado que $\sum_{\lambda=0}^{p-1} I^2(\lambda) = J$, del Teorema 6 obtenemos

$$\sum_{\lambda=0}^{p-1}\Big(I(\lambda) - \Delta\, \log p\Big)^2 \ll N_1N_2(\log p + \log^2 \Delta) = \Delta\, p(\log p + \log^2 \Delta)\log p.$$

Sea $\mathcal{E} \subset \{0, 1, 2, \ldots, p-1\}$ tal que $I(\lambda) = 0$ para $\lambda \in \mathcal{E}$. Entonces

$$|\mathcal{E}|\Delta^2 \log^2 p \ll \Delta\, p(\log p + \log^2 \Delta)\log p$$

y el resultado se sigue. □

2.6. Demostración del Teorema 8

Podemos suponer que $N_1N_3 \geq N_2N_4$. Denotemos

$$\mathcal{H}_1 = \{x_1x_3^* \pmod p : \quad L_1 \leq x_1 \leq L_1 + N_1, \quad L_3 + 1 \leq x_3 \leq L_3 + N_3\},$$

$$\mathcal{H}_2 = \{x_4x_2^* \pmod p : \quad L_2 \leq x_2 \leq L_2 + N_2, \quad L_4 + 1 \leq x_4 \leq L_4 + N_4\}.$$

Por el principio de las casillas de Dirichlet es suficiente probar que $|\mathcal{H}_1| + |\mathcal{H}_2| > p$. Sea

$$\mathcal{R}_1 = \{h \pmod p : \quad h \notin \mathcal{H}_1\}.$$

Entonces la congruencia

$$x + t - (y + z)h \equiv 0 \pmod p$$

no tiene soluciones en las variables h, x, t, y, z con $h \in \mathcal{R}_1$ y

$$\begin{aligned} [0{,}5L_1] + 1 \leq x, t \leq [0{,}5L_1] + [0{,}5N_1], \\ [0{,}5L_3] + 1 \leq y, z \leq [0{,}5L_3] + [0{,}5N_3]. \end{aligned} \tag{2.21}$$

Por lo tanto,

$$\sum_{a=0}^{p-1} \sum_{h \in \mathcal{R}_1} \sum_{x,t} \sum_{y,z} \mathbf{e}_p(a(x + t - h(y + z))) = 0,$$

donde el rango sumatoria de las variables x, t, y, z esta dado por (2.21). Separando el término correspondiente a $a = 0$, tenemos

$$|\mathcal{R}_1| X_1^2 X_3^2 \leq \sum_{a=1}^{p-1} \left| \sum_{x,t} \mathbf{e}_p(a(x + t)) \right| \left| \sum_{y,z} \sum_{h \in \mathcal{R}_1} \mathbf{e}_p(ah(y + z)) \right|,$$

donde $X_i = [0{,}5N_i]$. Por otra parte, para $(a, p) = 1$, tenemos

$$\begin{aligned} \left| \sum_{y,z} \sum_{h \in \mathcal{R}_1} \mathbf{e}_p(ah(y + z)) \right| &\leq \sum_{h=0}^{p-1} \left| \sum_{y,z} \mathbf{e}_p(ah(y + z)) \right| = \\ &\leq \sum_{n=0}^{p-1} \left| \sum_{y,z} \mathbf{e}_p(n(y + z)) \right| = pX_3. \end{aligned}$$

También,

$$\sum_{a=1}^{p-1}\left|\sum_{x,t}\mathbf{e}_p(a(x+t))\right| \leq pX_1.$$

En consecuencia,

$$|\mathcal{R}_1|X_1^2X_3^2 \leq p^2X_1X_3.$$

Dado que p es un primo suficientemente grande, deducimos

$$|\mathcal{H}_1| = p - |\mathcal{R}_1| \geq p - \frac{p^2}{X_1X_3} \geq p - \frac{4{,}5p^2}{N_1N_3}. \tag{2.22}$$

Si $N_2N_4 > 10p$, entonces definiendo

$$\mathcal{R}_2 = \{h \pmod p : \quad h \notin \mathcal{H}_2\},$$

y siguiendo las mismas lineas de la demostración de la desigualdad (2.22), obtenemos

$$|\mathcal{H}_2| = p - |\mathcal{R}_2| \geq p - \frac{4{,}5p^2}{N_2N_4}.$$

Por lo tanto,

$$|\mathcal{H}_1| + |\mathcal{H}_2| \geq 2p - \frac{4{,}5p^2}{N_2N_4} - \frac{4{,}5p^2}{N_1N_3} > p,$$

y el resultado se tiene en el caso $N_2N_4 > 10p$.

Supongamos ahora que $N_2N_4 \leq 10p$. Denotemos por I al número de soluciones de la congruencia

$$x_4x_2^* \equiv y_4y_2^* \pmod p, \quad L_2{+}1 \leq x_2, y_2 \leq L_2{+}N_2, \quad L_4{+}1 \leq x_4, y_4 \leq L_4{+}N_4.$$

En virtud del Lema 9 se tiene,

$$I \ll N_2N_4 \log p.$$

Por lo tanto, en vista del Lema 8,

$$|\mathcal{H}_2| \geq \frac{N_2^2N_4^2}{I} \geq \frac{c_0N_2N_4}{\log p},$$

donde c_0 es una constante absoluta. Combinando este hecho con (2.22), obtenemos

$$|\mathcal{H}_1| + |\mathcal{H}_2| \geq p - \frac{4{,}5p^2}{N_1N_3} + \frac{c_0N_2N_4}{\log p} \geq p + \frac{c_0N_2N_4}{\log p} - \frac{4{,}5N_2N_4}{c\log p}.$$

Tomando $c = 5c_0$, concluimos

$$|\mathcal{H}_1| + |\mathcal{H}_2| > p.$$

□

2.7. Demostración del Teorema 9

Sea $\mathcal{H}$ el conjunto de los diferentes elementos de la forma $(d_1+d_2)(b_1+b_2)^*$, donde

$$d_1 \in \mathcal{D}, \quad d_2 \in \mathcal{D}, \quad b_1 \in \mathcal{B}, \quad b_2 \in \mathcal{B}, \quad b_1 + b_2 \neq 0. \tag{2.23}$$

Lema 10. *Tiene lugar la siguiente estimación:*

$$|\mathcal{H}| \geq p - \frac{p^2}{|\mathcal{B}||\mathcal{D}| - p}.$$

Demostración. La demostración del Lema 10 sigue las mismas lineas que la prueba del Teorema 8. Sea

$$\mathcal{R} = \mathbb{F}_p \setminus \mathcal{H}.$$

Entonces la ecuación

$$d_1 + d_2 - (b_1 + b_2)h = 0 \tag{2.24}$$

no admite soluciones con $h \in \mathcal{R}$ y d_1, d_2, b_1, b_2 bajo las condiciones dadas en (2.23). Por lo tanto, dado que $b_1 + b_2 = 0$ implica $d_1 + d_2 = 0$, la ecuación (2.24) tiene a lo más $|\mathcal{B}||\mathcal{D}||\mathcal{R}|$ soluciones sujetas a

$$d_1 \in \mathcal{D}, \quad d_2 \in \mathcal{D}, \quad b_1 \in \mathcal{B}, \quad b_2 \in \mathcal{B}, \quad h \in \mathcal{R}.$$

De esta forma,

$$\frac{1}{p} \sum_{a=0}^{p-1} \sum_{h \in \mathcal{R}} \sum_{\substack{d_1 \in \mathcal{D} \\ d_2 \in \mathcal{D}}} \sum_{\substack{b_1 \in \mathcal{B} \\ b_2 \in \mathcal{B}}} \mathbf{e}_p(a(d_1 + d_2 - (b_1 + b_2)h)) \leq |\mathcal{B}||\mathcal{D}||\mathcal{R}|.$$

Separando el término correspondiente a $a = 0$, tenemos

$$\frac{1}{p}|\mathcal{R}||\mathcal{D}|^2|\mathcal{B}|^2 \leq |\mathcal{B}||\mathcal{D}||\mathcal{R}| + \frac{1}{p} \sum_{a=1}^{p-1} \sum_{h=0}^{p-1} \left| \sum_{d \in \mathcal{D}} \mathbf{e}_p(ad) \right|^2 \left| \sum_{b \in \mathcal{B}} \mathbf{e}_p(ahb) \right|^2.$$

Así,

$$|\mathcal{R}||\mathcal{D}|^2|\mathcal{B}|^2 \leq |\mathcal{B}||\mathcal{D}||\mathcal{R}|p + |\mathcal{D}||\mathcal{B}|p^2,$$

lo cual implica

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

□

Para demostrar el Teorema 9, denotemos por T al número de soluciones de la ecuación

$$a_1 + \lambda c_1 = a_2 + \lambda c_2, \quad a_1 \in \mathcal{A},\, a_2 \in \mathcal{A}, \quad c_1 \in \mathcal{C},\, c_2 \in \mathcal{C}, \quad \lambda \in \mathcal{H}.$$

Si $c_1 = c_2$, entonces $a_1 = a_2$ y λ puede ser un elemento arbitraro de $\mathcal{H}$. De lo contrario, para a_1, a_2, c_1, c_2 dados con $c_1 \neq c_2$ tenemos a lo más un posible valor para λ. Por lo tanto

$$T \leq |\mathcal{A}||\mathcal{C}||\mathcal{H}| + |\mathcal{A}|^2|\mathcal{C}|^2.$$

Así, existe un elemento $\lambda \in \mathcal{H}$ tal que

$$I \leq |\mathcal{A}||\mathcal{C}| + \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{H}|},$$

donde I denota al número de soluciones de la ecuación

$$a_1 + \lambda c_1 = a_2 + \lambda c_2, \quad a_1 \in \mathcal{A},\, a_2 \in \mathcal{A}, \quad c_1 \in \mathcal{A},\, c_2 \in \mathcal{C}.$$

De esto y en virtud del Lema 8, tenemos

$$\#\{a + \lambda c :\, a \in \mathcal{A},\, c \in \mathcal{C}\} \geq \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{I} \geq \frac{|\mathcal{A}||\mathcal{C}||\mathcal{H}|}{|\mathcal{A}||\mathcal{C}| + |\mathcal{H}|}. \tag{2.25}$$

Dado que λ es un elemento fijo de $\mathcal{H}$, existen elementos fijos d_0', d_0'' en $\mathcal{D}$ y elementos fijos b_0', b_0'' de $\mathcal{B}$ tales que

$$\lambda = (d_0' + d_0'')(b_0' + b_0'')^*.$$

Por lo tanto, de (2.25) obtenemos

$$\#\{a(b_0' + b_0'') + c(d_0' + d_0'') :\, a \in \mathcal{A},\, c \in \mathcal{C}\} \geq \frac{|\mathcal{A}||\mathcal{C}||\mathcal{H}|}{|\mathcal{A}||\mathcal{C}| + |\mathcal{H}|}.$$

Recordando las desigualdades $|\mathcal{A}||\mathcal{C}| > (2+\sqrt{2})p$, $|\mathcal{B}||\mathcal{D}| > (2+\sqrt{2})p$ y usando el Lema 10, tenemos

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

Finalmente, del principio de las casillas de Dirichlet concluimos que

$$\{(a_1+a_2)(b_0'+b_0'')+(c_1+c_2)(d_0'+d_0'') : a_1 \in \mathcal{A},\, a_2 \in \mathcal{A},\, c_1 \in \mathcal{C},\, c_2 \in \mathcal{C}\} = \mathbb{F}_p.$$

□

Capítulo 3

Distribución y propiedades aritméticas de $n!\pmod p$

El problema de la distribución de sucesiones con términos relacionados con factoriales módulo un número primo ha sido un tema bastante investigado, por ejemplo en los trabajos recientes [8], [9], [22]–[25], [42] y las referencias citadas. En [31, **F11**] se conjeturó que la sucesión $n!$ no incide en alrededor p/e clases residuales módulo p. De ser cierta esta conjetura la sucesión $n!$ debería tener aproximadamente $(1-1/e)p$ valores distintos módulo p, se puede consultar [9] para más resultados de esta naturaleza. Esto a su vez implicaría la representabilidad de toda clase residual módulo p como suma o producto de dos factoriales. De manera incondicional, del Teorema de Wilson se sigue que cualquier entero $1 \leq x \leq (p-1)/2$ satisface la congruencia

$$(2x-1)! \cdot (p-2x)! \equiv 1 \pmod p, \tag{3.1}$$

identidad que fue punto de partida en los trabajos [8] y [23, Teorema 13] para estimar el tamaño del conjunto

$$\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\}.$$

En el trabajo [23], Garaev, Luca y Shparlinski demostraron que

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{5}{8}p + O(p^{1/2}\log^2 p).$$

Posteriomente este resultado fué mejorado por Chen y Dai [8] al obtener

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{3}{4}p + O(p^{1/2}\log^2 p).$$

Ambos resultados fueron mejorados en [29] donde, al igual que en los metodos de [8] y [23, Teorema 13], se partió de la identidad (3.1). Mediante la manipulación de la congruencia (3.1) es posible elegir conjuntos ajenos de clases residuales representables como $m!n! \pmod p$ de tal forma que el tamaño de cada uno de ellos puede estimarse contando el número de soluciones de sistemas de congruencias. Para los sistemas de congruencias se encontraron fórmulas asintóticas, en los casos más elaborados empleando estimaciones de sumas híbridas de caracteres. El resultado es el siguiente.

Teorema 10. *La siguiente estimación tiene lugar*

$$\#\{m!n! \pmod p \ : \ 1 \leq m, n \leq p\} \geq \frac{41}{48}p + O(p^{1/2}\log^3 p).$$

Sin embargo, los resultados discutidos hasta ahora no se pueden aplicar para probar representaciones en términos de factoriales de enteros de tamaño restringido, tampoco se derivan fórmulas asintóticas para el número de soluciones de estas representaciones. En esta dirección se han hecho avances en los trabajos [22]–[25]. En particular, se han estimado sumas exponenciales y de caracteres que involucran factoriales de enteros en intervalos de pequeña longitud. Estos resultados han sido fundamentales para establecer la representabilidad de clases residuales en términos de factoriales de tamaño restringido y en varios casos también fórmulas asintóticas para el número de tales representaciones.

3.1. Congruencias del tipo Waring

Mediante el Teorema de Wilson (ver la identidad (3.1)) y el principio de las casillas de Dirichlet se puede demostrar que toda clase residual módulo p se representa en la forma

$$m_1!n_1! + m_2!n_2! \pmod p,$$

para irrestrictos enteros m_1, m_2, n_1, n_2. Del trabajo [24] de Garaev, Luca y Shparlinski, se obtiene la siguiente estimación para la doble suma exponencial con argumento de la forma $m!n!$,

$$\max_{(a,p)=1} \left| \sum_{m=1}^{N} \sum_{n=1}^{N} e^{2\pi i a m!n!/p} \right| \ll N^{11/6} p^{1/8}.$$

Con tal resultado establecieron la representabilidad de clases residuales como suma de términos de la forma $m!n!$, con las variables en intervalos de pequeña longitud. En particular, establecieron que toda clase residual $\lambda \pmod p$ puede escribirse como

$$\sum_{i=1}^{7} m_i!n_i! \equiv \lambda \pmod p,$$

para ciertos enteros positivos $m_1, n_1, \ldots, m_7, n_7$ no mayores que $cp^{33/34}$, con alguna constante absoluta $c > 0$. El siguiente resultado, del trabajo conjunto con Garaev [16], mejora al anterior en dos direcciones, el número de sumandos y el tamaño de las variables.

Teorema 11. *Cualquier clase residual λ módulo p puede escribirse como*

$$\sum_{i=1}^{5} m_i!n_i! \equiv \lambda \pmod p,$$

para ciertos enteros positivos $m_1, n_1, \ldots, m_5, n_5$ con $\max_{1\le i\le 5}\{m_i, n_i\} \le cp^{27/28}$, donde c es una constante absoluta.

En [25] se definió a $l = l(p)$ como el entero $l \ge 1$ más pequeño tal que para cualquier entero λ la congruencia

$$n_1! + \cdots + n_l! \equiv \lambda \pmod p,$$

tiene solución en los enteros positivos $n_1, \ldots, n_l$. Un problema abierto es demostrar que $l(p) = O(1)$, la conjetura presentada en [31, **F11**] implicaría $l(p) = 2$. Una estimación del tipo

$$\max_{(a,p)=1} \left| \sum_{x=1}^{p} e^{2\pi i a x!/p} \right| \ll p^{1-c},$$

para alguna constante $c > 0$, resuelve completamente este problema. De manera incondicional es posible demostrar que $l(p) \ll \log^2 p$ y por otra parte, aplicando un argumento de combinatoria (ver por ejemplo [30, Lemma 1]) y el hecho de que

$$\#\{n! \pmod p \ : \quad 1 \leq n \leq p\} > p^{1/2},$$

se demuestra que existe un entero c_p tal que la congruencia

$$x! + y! + c_p z! + c_p w! \equiv \lambda \pmod p, \quad 1 \leq x, y, z, w, \leq p,$$

es soluble para todo entero λ módulo p.

3.2. Representabilidad de clases residuales como producto de factoriales, suma de sumas armónicas y coeficientes binomiales

En [23] Garaev, Luca y Shparlinski demostraron que para cualquier carácter $\chi \not\equiv \chi_0 \pmod p$ se tiene

$$\sum_{n=L+1}^{L+N} \chi(n!) \ll N^{3/4} p^{1/8} \log^{3/4} p,$$

donde L, N denotan enteros no negativos. Combinando este resultado con estimaciones superiores para el número de soluciones de congruencias especiales (Lema 12) demostraron que para $\lambda \not\equiv 0 \pmod p$ dado, el número de soluciones de la congruencia

$$\prod_{i=1}^{7} n_i! \equiv \lambda \pmod p; \quad L+1 \leq n_1, \ldots, n_7 \leq L+N, \tag{3.2}$$

asintóticamente se comporta como N^7/p, para $0 < L+1 \leq L+N \leq p$ y

$$Np^{-11/12} \log^{-1/2} p \to 0 \quad \text{cuando} \quad p \to \infty.$$

Más aún, el Teorema 8 de [23] proporciona una fórmula asintótica para el número de soluciones de la congruencia

$$\prod_{i=1}^{k} n_i! \equiv \lambda \pmod p; \quad L+1 \leq n_1, \ldots, n_k \leq L+N.$$

El número 7 de factores en (3.2) es el entero más pequeño k para el cual esta fórmula asintótica es efectiva con $N = o(p)$.

En [26], Garaev, Luca y Shparlinski obtuvieron resultados análogos al anterior para sumas armónicas

$$H_s(n) = \sum_{i=1}^{n} \frac{1}{i^s},$$

donde s es una entero positivo fijo y $H_s(n)$ es calculado módulo p. En particular, obtuvieron una estimación no trivial para una suma exponencial con argumento $H_s(n)$ y probaron que para cualquier entero λ el número de soluciones de la congruencia

$$\sum_{i=1}^{7} H_s(n_i) \equiv \lambda \pmod{p}; \quad L+1 \le n_1, \dots, n_7 \le L+N,$$

tiene un comportamiento asintótico como N^7/p, para $0 \le L < L+N < p$ y

$$Np^{-11/12} \log^{-1/2} p \to 0 \quad \text{cuando} \quad p \to \infty.$$

En [27] propiedades distribucionales de los semi-coeficientes binomiales

$$b_n = \binom{2n}{n}, \qquad n = 0, 1, \dots,$$

y números de Catalán

$$c_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 0, 1, \dots,$$

también han sido investigados. Se demostró en [27] que para primos suficientemente grandes p y todo entero λ existen enteros positivos $r, s \ll p^{13/2} \log^6 p$ tales que

$$b_r \equiv \lambda \pmod{p} \quad \text{y} \quad c_s \equiv \lambda \pmod{p}.$$

Este hecho mejoró de manera sustancial el resultado previamente establecido en [3] donde se requere que los enteros r, s sean de la magnitud $p^{O(p)}$.

Aunque las potencias de p que aparecen en los resultados mencionados hasta ahora no han sido disminuidas, los factores logaritmicos en ciertos casos pueden ser removidos. Uno de los propósitos de este capítulo es abordar esta cuestión. Para dicha tarea se retomaron los argumentos descritos en [23], [26] y [27], y se combinaron con el método expuesto por Garaev en [14]. Los siguientes teoremas se establecieron en [28].

Teorema 12. *Sean*

$$N \geq 1, \quad M \geq 1, \quad 0 \leq L < L + N + M \leq p.$$

Si $\chi \pmod p$ *es un carácter no principal módulo* p*, entonces la siguiente estimación tiene lugar*

$$\sum_{x=1}^{N} \sum_{y=1}^{M} \chi((x+y+L)!) \ll MN^{3/4} p^{1/8} \log^{1/4}(NM^{-1}+2).$$

Además, si $L - M \geq 0$*, entonces también tenemos*

$$\sum_{x=1}^{N} \sum_{y=1}^{M} \chi((x-y+L)!) \ll MN^{3/4} p^{1/8} \log^{1/4}(NM^{-1}+2).$$

Combinando el Teorema 12 con el Lema 12 bajo el método de [14], se obtiene el siguiente resultado.

Teorema 13. *Sea* $1 \leq N \leq p$*. Sea* λ *un entero,* $\lambda \not\equiv 0 \pmod p$*. Si* J *denota al número de soluciones de la congruencia*

$$n_1! \cdots n_7! \equiv \lambda \pmod p; \quad 1 \leq n_1, \ldots, n_7 \leq N,$$

entonces

$$J = \frac{N^7}{p-1} + O\left(N^{11/2} p^{3/8} \log^{3/4}(Np^{-11/12}+2)\right).$$

Corolario 1. *Para cualquier clase residual* $\lambda \not\equiv 0 \pmod p$ *la congruencia*

$$n_1! \cdots n_7! \equiv \lambda \pmod p$$

tiene solución en enteros positivos $n_1, \ldots, n_7$ *satisfaciendo*

$$\max_{1 \leq i \leq 7} n_i \ll p^{11/12}.$$

También se presentan resultados similares para sumas armónicas.

Teorema 14. *Sea*

$$N \geq 1, \quad M \geq 1, \quad 0 \leq L < L + N + M < p.$$

Entonces las siguiente desigualdad tiene lugar:

$$\max_{(a,p)=1} \left| \sum_{x=1}^{N} \sum_{y=1}^{M} e^{2\pi i a H_s(x+y+L)/p} \right| \ll MN^{3/4} p^{1/8} \log^{1/4}(NM^{-1}+2).$$

Además, si $L - M \geq 0$, *entonces también tenemos*

$$\max_{(a,p)=1} \left| \sum_{x=1}^{N} \sum_{y=1}^{M} e^{2\pi i a H_s(x-y+L)/p} \right| \ll MN^{3/4} p^{1/8} \log^{1/4}(NM^{-1}+2).$$

Teorema 15. *Sea* $1 \leq N \leq p$. *Sea* λ *un entero arbitrario, si* J_1 *denota al número de soluciones de la congruencia*

$$H_s(n_1) + \cdots + H_s(n_7) \equiv \lambda \pmod{p}; \quad 1 \leq n_1, \ldots, n_7 \leq N,$$

entonces

$$J_1 = \frac{N^7}{p} + O\left(N^{11/2} p^{3/8} \log^{3/4}(Np^{-11/12}+2)\right).$$

Del Teorema 15 obtenemos el siguiente resultado:

Corolario 2. *Para cualquier clase residual* $\lambda \pmod{p}$ *la congruencia*

$$H_s(n_1) + \cdots + H_s(n_7) \equiv \lambda \pmod{p}$$

es soluble en enteros positivos $n_1, \ldots, n_7$ *que satisfacen*

$$\max_{1 \leq i \leq 7} n_i \ll p^{11/12}.$$

Considere ahora los semi-coeficientes binomiales

$$b_n = \binom{2n}{n}, \qquad n = 0, 1, \ldots,$$

y los números de Catalán

$$c_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 0, 1, \ldots,$$

donde, en la forma usual, definimos $0! = 1$.

Teorema 16. *Para todos los primos suficientemente grandes* p *y todo entero* λ *existen enteros positivos* $r, s \ll p^{13/2}$ *tales que* $b_r \equiv c_s \equiv \lambda \pmod{p}$.

En las secciones 3.6 y 3.7 demostraremos los Teoremas 12 y 13 respectivamente. Las demostraciones de los Teoremas 14, 15 y 16 serán omitidas ya que se pueden obtener siguiendo los mismos argumentos de las demostraciones de los Teoremas 12 y 13.

3.3. Lemas

A lo largo del capítulo emplearemos la abreviación

$$\mathbf{e}_p(z) = e^{2\pi iz/p}.$$

El siguiente lema está tomado del trabajo de Garaev [14] y presenta una estimación superior para el valor promedio del producto de módulos de dos sumas racionales lineales.

Lema 11. *Sean L_1, L_2, A, B enteros tales que, $1 \leq A, B \leq p$. Entonces, la siguiente estimación tiene lugar:*

$$\sum_{a=0}^{p-1} \left| \sum_{x=L_1+1}^{L_1+A} \mathbf{e}_p(ax) \right| \left| \sum_{y=L_2+1}^{L_2+B} \mathbf{e}_p(ay) \right| \ll pA \log(BA^{-1} + 2).$$

El siguiente resultado fue obtenido en [23].

Lema 12. *Sean $0 \leq L < L + N \leq p$ y k un entero positivo fijo. Entonces el número de soluciones de la congruencia*

$$n_1! \cdots n_k! \equiv n_{k+1}! \cdots n_{2k}! \pmod{p}; \quad L < n_1, \ldots, n_{2k} \leq L + N$$

es $\ll N^{2k-1+2^{-k}}$, donde la constante implicíta sólo depende de k.

Un resultado de naturaleza aditiva, análogo al Lema 12 también fué establecido para sumas armónicas

$$H_s(n) = \sum_{i=1}^{n} \frac{1}{i^s},$$

donde s es un entero positivo fijo y $H_s(n)$ esta calculado módulo p.

Lema 13. *Sean $0 \leq L < L + N \leq p$ y s, k enteros positivos fijos. El número de soluciones de la congruencia*

$$\sum_{i=1}^{k} H_s(n_i) \equiv \sum_{i=k+1}^{2k} H_s(n_i) \pmod{p}; \quad L < n_1, \ldots, n_{2k} \leq L + N$$

es $\ll N^{2k-1+2^{-k}}$, donde la constante implicíta puede depender sólo de k y s.

La demostración puede consultarse en [26]. El siguiente Lema es un caso especial de [24, Teorema 1]

Lema 14. *Sea N un entero positivo, $N < p$. Entonces tiene lugar la estimación*

$$\max_{(a,p)=1} \left| \sum_{x=1}^{N} \sum_{y=1}^{N} \mathbf{e}_p(ax!y!) \right| \ll N^{11/6} p^{1/8}.$$

3.4. Demostración del Teorema 10

Sea

$$\mathcal{E} = \{n!m! \pmod p \ : \ 1 \leq n, m \leq p\}.$$

El punto de partida, como en [8, 9] y [23], es utilizar la congruencia

$$(2x-1)! \cdot (p-2x)! \equiv 1 \pmod p, \tag{3.3}$$

la cual tiene lugar para cualquier entero positivo $x \leq p_1$, donde $p_1 = (p-1)/2$. Sea

$$\mathcal{E}_1 = \{2, 4, \ldots, 2p_1\}.$$

Denotemos por $\mathcal{E}_2$ al conjunto de los enteros positivos impares menores que p y de la forma

$$(2x-1)^* \pmod p, \quad 1 \leq x \leq p_1.$$

Aquí a^* se define por $aa^* \equiv 1 \pmod p$, con $a \not\equiv 0 \pmod p$.

Sea $\mathcal{E}_3$ el conjunto de los enteros positivos impares menores que p que se representan como $(2z)^* \pmod p$, para algún $1 \leq z \leq p_1$, y al mismo tiempo en la forma

$$(2x)^*(2x+1)^* \pmod p, \quad 1 \leq x \leq p_1 - 1.$$

Ahora, definimos $\mathcal{E}_4$ al conjunto de los enteros positivos impares menores que p que se pueden escribir como $(2z)^* \pmod p$ para algún $1 \leq z \leq p_1$ y a la vez en la forma

$$(2x-1)^*(2x)^*(2x+1)^* \pmod p$$

para algún $1 \leq x \leq p_1 - 1$ que cumple con la condición

$$\left(\frac{4(2x-1)(2x)(2x+1)+1}{p}\right) = -1, \qquad \left(\frac{1-3x^2}{p}\right) = -1.$$

Aquí y a lo largo de la sección $\left(\frac{\cdot}{p}\right)$ es el símbolo de Legendre. Finalmente, denotamos por $\mathcal{E}_5$ al conjunto de los enteros positivos impares menores que p los cuales se escriben como $(2z)^*$ (mód p) para algún $1 \leq z \leq p_1$ y a la vez en la forma

$$(2x-1)^*(2x)^*(2x+1)^* \pmod{p}$$

para algún $1 \leq x \leq p_1 - 1$ bajo las condiciones

$$\left(\frac{4(2x-1)(2x)(2x+1)+1}{p}\right) = -1, \qquad \left(\frac{1-3x^2}{p}\right) = 1.$$

Para cada numero del conjunto $\mathcal{E}_i$ le asociamos la clase residual a la cual este numero pertence. Con esta convención, dado que $(2x)!(p-2x)! \equiv 2x$ (mód p), tenemos $\mathcal{E}_1 \subset \mathcal{E}$.

Si $u \in \mathcal{E}_4$ o $u \in \mathcal{E}_5$, entonces $u \equiv (2x-1)^*(2x)^*(2x+1)^* \pmod{p}$ para algún $x \leq p_1 - 1$. Combinando con (3.3) obtenemos

$$u \equiv (2x-2)! \cdot (p-2x-2)! \pmod{p},$$

de allí $u \in \mathcal{E}$. Por lo que, $\mathcal{E}_4 \subset \mathcal{E}$, $\mathcal{E}_5 \subset \mathcal{E}$. El mismo argumento verifica que $\mathcal{E}_2 \subset \mathcal{E}$, $\mathcal{E}_3 \subset \mathcal{E}$.

No es complicado verificar que $\mathcal{E}_i \cap \mathcal{E}_j = \emptyset$ para $1 \leq i \neq j \leq 5$. De hecho, si, por ejemplo, $u \in \mathcal{E}_3$, entonces $\left(\frac{4u^*+1}{p}\right) = 1$, mientras si $u \in \mathcal{E}_4 \cup \mathcal{E}_5$, tenemos $\left(\frac{4u^*+1}{p}\right) = -1$. Por lo tanto $\mathcal{E}_3 \cap \mathcal{E}_4 = \emptyset$, $\mathcal{E}_3 \cap \mathcal{E}_5 = \emptyset$. Los otros casos se verifican de manera similar. En consecuencia

$$|\mathcal{E}| \geq |\mathcal{E}_1| + |\mathcal{E}_2| + |\mathcal{E}_3| + |\mathcal{E}_4| + |\mathcal{E}_5| = \frac{p-1}{2} + |\mathcal{E}_2| + |\mathcal{E}_3| + |\mathcal{E}_4| + |\mathcal{E}_5|.$$

Afirmamos que las siguientes estimaciones tienen lugar:

$$|\mathcal{E}_2| \geq (\tfrac{1}{4} + o(1))p, \qquad |\mathcal{E}_3| \geq (\tfrac{1}{16} + o(1))p, \tag{3.4}$$

$$|\mathcal{E}_4| \geq (\tfrac{1}{32} + o(1))p, \qquad |\mathcal{E}_5| \geq (\tfrac{1}{96} + o(1))p. \tag{3.5}$$

Con el fin de estimar $|\mathcal{E}_4|$, denotamos por I al numero de soluciones del sistema de congruencias

$$\begin{cases} 2r - 1 \equiv (2x-1)^*(2x)^*(2x+1)^* \pmod{p} \\ 2z \equiv (2x-1)(2x)(2x+1) \pmod{p} \\ \left(\frac{4(2x-1)(2x)(2x+1)+1}{p}\right) = -1 \\ \left(\frac{1-3x^2}{p}\right) = -1 \end{cases}$$

bajo las condiciones

$$1 \leq x \leq p_1 - 1, \quad 1 \leq z \leq p_1, \quad 1 \leq r \leq p_1.$$

Observe que para $z \not\equiv 0 \pmod{p}$ dado, si la congruencia

$$(2x-1)2x(2x+1) \equiv 2z \pmod{p} \tag{3.6}$$

tiene dos soluciones distintas de cero $x \not\equiv y \pmod{p}$, entonces tenemos

$$(2y+x)^2 \equiv 1 - 3x^2 \pmod{p}.$$

Esto significa que para dado r, el sistema de congruencias anterior tiene a lo más una solución. Esto implica que $|\mathcal{E}_4| \geq I$.

Corresponde ahora analizar la cardinalidad de $\mathcal{E}_5$. Denotemos por J al número de soluciones del sistema de congruencias

$$\begin{cases} 2r - 1 \equiv (2x-1)^*(2x)^*(2x+1)^* \pmod{p} \\ 2z \equiv (2x-1)(2x)(2x+1) \pmod{p} \\ \left(\frac{4(2x-1)(2x)(2x+1)+1}{p}\right) = -1 \\ \left(\frac{1-3x^2}{p}\right) = 1 \end{cases}$$

con las condiciones

$$1 \leq x \leq p_1 - 1, \quad 1 \leq z \leq p_1, \quad 1 \leq r \leq p_1.$$

Dado r, tenemos a lo más tres soluciones de este sistema. En consecuencia, $|\mathcal{E}_5| \geq J/3$, y resulta

$$|\mathcal{E}_4| \geq I, \quad |\mathcal{E}_5| \geq \frac{J}{3}. \tag{3.7}$$

Para I y J obtendremos las fórmulas asintóticas

$$I = \frac{p}{32} + O(p^{1/2}\log^3 p), \quad J = \frac{p}{32} + O(p^{1/2}\log^3 p).$$

Llamamos $g(x) = (2x-1)2x(2x+1)$. Usando identidades trigonométricas básicas obtenemos

$$\begin{aligned} I &= \frac{1}{p^2}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\sum_{x=1}^{p_1-1}\delta(x)\gamma(x)\sum_{r=1}^{p_1}\sum_{z=1}^{p_1}\mathbf{e}_p(a(2r-1-(g(x))^*))\mathbf{e}_p(b(2z-g(x))) \\ &- \frac{1}{p^2}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\sum_{x\in\mathcal{A}}\delta(x)\gamma(x)\sum_{r=1}^{p_1}\sum_{z=1}^{p_1}\mathbf{e}_p(a(2r-1-(g(x))^*))\mathbf{e}_p(b(2z-g(x))), \end{aligned}$$

donde

$$2\delta(x) = 1 - \left(\frac{4g(x)+1}{p}\right), \qquad 2\gamma(x) = 1 - \left(\frac{1-3x^2}{p}\right)$$

y

$$\mathcal{A} = \{x : 1 \le x \le p_1 - 1,\ (4g(x)+1)(1-3x^2) \equiv 0 \pmod{p}\}.$$

Claramente, $|\mathcal{A}| \le 5$. Por lo que, empleando la bien conocida estimación

$$\sum_{a=1}^{p-1} \left| \sum_{n=X+1}^{X+Y} \mathbf{e}_p(an) \right| < p \log p,$$

luego

$$\begin{aligned} &\left| \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{x \in \mathcal{A}} \delta(x)\gamma(x) \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} \mathbf{e}_p(a(2r-1-(g(x))^*)) \mathbf{e}_p(b(2z-g(x))) \right| \\ &\ll \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \left| \sum_{r=1}^{p_1} \mathbf{e}_p(2ar) \right| \left| \sum_{z=1}^{p_1} \mathbf{e}_p(2bz) \right| \ll \log^2 p. \end{aligned}$$

Por lo tanto

$$\begin{aligned} I \;=\; & \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{x=1}^{p_1-1} \delta(x)\gamma(x) \sum_{r=1}^{p_1} \sum_{z=1}^{p_1} \mathbf{e}_p(a(2r-1-(g(x))^*)) \mathbf{e}_p(b(2z-g(x))) \\ & + O(\log^2 p). \end{aligned}$$

Separando el término que corresponde a $a = b = 0$, obtenemos

$$I = \frac{p_1^2}{p^2} \sum_{x=1}^{p_1-1} \delta(x)\gamma(x) + R_1 + O(\log^2 p) = \frac{p}{32} + R_1 + R_2 + O(\log^2 p), \quad (3.8)$$

donde

$$R_1 \ll \frac{1}{p^2} \sum_{\substack{0 \le a,b \le p-1 \\ (a,b) \ne (0,0)}} \left| \sum_{r=1}^{p_1} \mathbf{e}_p(a(2r-1)) \sum_{z=1}^{p_1} \mathbf{e}_p(b2z) \right| S(a,b), \quad (3.9)$$

$$S(a,b) = \left| \sum_{x=1}^{p_1-1} \delta(x)\gamma(x) \mathbf{e}_p(a(g(x))^* + bg(x)) \right|,$$

$$R_2 \ll \left| \sum_{x=1}^{p_1-1} - \left(\frac{4g(x)+1}{p}\right) - \left(\frac{1-3x^2}{p}\right) + \left(\frac{(4g(x)+1)(1-3x^2)}{p}\right) \right|.$$

Lo siguiente será demostrar que para $0 \leq a, b \leq p-1$ con $(a,b) \neq (0,0)$, sucede

$$R_1 + R_2 \ll p^{1/2} \log^3 p.$$

Aplicando la técnica de extender el rango de sumatoria de un intervalo corto al sistema completo de residuos tenemos

$$\begin{aligned} S(a,b) &= \left| \sum_{x=1}^{p_1-1} {\sum_{y=0}^{p-1}}' \delta(y)\gamma(y)\mathbf{e}_p(a(g(y))^* + bg(y)) \frac{1}{p} \sum_{\nu=0}^{p-1} \mathbf{e}_p(\nu(y-x)) \right| \\ &\leq \frac{1}{p} \sum_{\nu=0}^{p-1} \left| \sum_{x=1}^{p_1-1} \mathbf{e}_p(\nu x) \right| \left| {\sum_{y=0}^{p-1}}' \delta(y)\gamma(y)\mathbf{e}_p(a(g(y))^* + bg(y) + \nu y) \right|, \end{aligned}$$

donde $\sum'$ indica que el rango de la sumatoria sobre y excluye a los puntos $0, p_1$ and p_1+1 (que son polos de $g(y)^*$). Dado que

$$4\delta(y)\gamma(y) = 1 - \left(\frac{4g(y)+1}{p}\right) - \left(\frac{1-3y^2}{p}\right) + \left(\frac{(4g(y)+1)(1-3y^2)}{p}\right),$$

en virtud de las estimaciones de Weil para sumas híbridas de caracteres con argumentos racionales (se puede consultar, por ejemplo, [39]), tenemos

$$\left| {\sum_{y=0}^{p-1}}' \delta(y)\gamma(y)\mathbf{e}_p(a(g(y))^* + bg(y) + \nu y) \right| \ll p^{1/2}.$$

Por lo tanto,

$$S(a,b) \ll \frac{p^{1/2}}{p} \sum_{\nu=0}^{p-1} \left| \sum_{x=1}^{p_1-1} \mathbf{e}_p(\nu x) \right| \ll p^{1/2} \log p.$$

Combinando este hecho con (3.9), obtenemos

$$R_1 \ll \frac{p^{1/2} \log p}{p^2} \left(\sum_{a=0}^{p-1} \left| \sum_{r=1}^{p_1} \mathbf{e}_p(2ar) \right| \right)^2 \ll p^{1/2} \log^3 p.$$

De manera similar, se verifica $R_2 \ll p^{1/2} \log p$. Luego, por (3.8), se obtiene

$$I = \frac{p}{32} + O(p^{1/2} \log^3 p).$$

Análogamente,

$$J = \frac{p}{32} + O(p^{1/2}\log^3 p).$$

De esta forma, en virtud de (3.7), sucede

$$|\mathcal{E}_4| \geq \frac{p}{32} + O(p^{1/2}\log^3 p), \quad |\mathcal{E}_5| \geq \frac{p}{96} + O(p^{1/2}\log^3 p),$$

lo cual comprueba la estimación requerida (3.4).

Aplicando esencialmente el mismo argumento a $\mathcal{E}_2, \mathcal{E}_3$ se verifica (3.5). En consecuencia, concluimos

$$|\mathcal{E}| \geq \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{16} + \frac{1}{32} + \frac{1}{96}\right) p + O(p^{1/2}\log^3 p) = \frac{41}{48}p + O(p^{1/2}\log^3 p).$$

□

3.5. Demostración del Teorema 11

El nuevo enfoque para esta demostración es considerar a la congruencia planteada en el Teorema 11 con las restricciones adicionales

$$m_1 = m_2 = m_3 - 1 = m_4 - 1.$$

De esta manera, demostraremos la representabilidad de cualquier entero λ en la forma

$$(m-1)!(n_1! + n_2!) + m!(n_3! + n_4!) + m_5!n_5! \equiv \lambda \pmod{p}$$

con $1 \leq m, m_5, n_1, \ldots, n_5 \leq N$, $N = O(p^{27/28})$ y encontraremos una fórmula asintótica para el número de dichas representaciones.

Sea N un entero $N < p$. Denotemos por $J = J(\lambda, N)$ al número de soluciones de la congruencia

$$(m-1)!(n_1! + n_2!) + m!(n_3! + n_4!) + m_5!n_5! \equiv \lambda \pmod{p}$$

en enteros $m, m_5, n_1, \ldots, n_5$ tales que

$$1 \leq m, m_5, n_1, \ldots, n_5 \leq N.$$

Expresamos a J en términos de sumas exponenciales y dado que

$$\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\sum_{n_3=1}^{N}\sum_{n_4=1}^{N}\mathbf{e}_p(a((m-1)!(n_1!+n_2!)+m!(n_3!+n_4!)+m_5!n_5!-\lambda))=$$
$$\left(\sum_{n_1=1}^{N}\sum_{n_3=1}^{N}\mathbf{e}_p(a((m-1)!n_1!+m!n_3!))\right)^2\mathbf{e}_p(am_5!n_5!)\mathbf{e}_p(-a\lambda),$$

tenemos

$$J=\frac{1}{p}\sum_{a=0}^{p-1}\left\{\sum_{m=1}^{N}\left(\sum_{n_1=1}^{N}\sum_{n_3=1}^{N}\mathbf{e}_p(a((m-1)!n_1!+m!n_3!))\right)^2 S(a)\mathbf{e}_p(-a\lambda)\right\},$$

donde

$$S(a)=\sum_{m_5=1}^{N}\sum_{n_5}^{N}\mathbf{e}_p(am_5!n_5!).$$

Separando el término que corresponde a $a=0$ y estimando el resto de los sumandos por sus módulos obtenemos

$$\left|J-\frac{N^7}{p}\right|\leq\frac{1}{p}\sum_{a=1}^{p-1}\left\{\sum_{m=1}^{N}\left|\sum_{n_1=1}^{N}\sum_{n_3=1}^{N}\mathbf{e}_p(a((m-1)!n_1!+m!n_3!))\right|^2|S(a)|\right\}.$$

El término $|S(a)|$ se estima de manera uniforme sobre $1\leq a\leq p-1$, conforme al Lema 14. De esta forma

$$J-\frac{n^7}{p}\ll N^{11/6}p^{1/8}T(N), \tag{3.10}$$

donde

$$T(N)=\frac{1}{p}\sum_{a=0}^{p-1}\sum_{m=1}^{N}\left|\sum_{n_1=1}^{N}\sum_{n_3=1}^{N}\mathbf{e}_p(a((m-1)!n_1!+m!n_3!))\right|^2.$$

Ahora observe que $T(N)$ representa al número de soluciones de la congruencia

$$(m-1)!n_1!+m!n_3!\equiv(m-1)!n_2!+m!n_4!\pmod p,\quad 1\leq m,n_1,\ldots,n_4.$$

Dado que $p > N \geq m$ es posible cancelar $(m-1)!$ en ambos lados de la congruencia y obtener la congruencia equivalente

$$n_1! - n_2! \equiv m(n_4! - n_3!) \pmod{p}, \quad 1 \leq m, n_1, \ldots, n_4. \tag{3.11}$$

Dados n_1, n_2, n_3, n_4 con $n_4! \not\equiv n_3! \pmod{p}$, existe a lo más un valor para m que satisface la congruencia (3.11). Por lo tanto, la congruencia (3.11) tiene a lo más N^4 soluciones con la condición $n_4! \not\equiv n_3! \pmod{p}$. De esta forma

$$T(N) \ll N^4 + T_1(N),$$

donde $T_1(N)$ es el número de soluciones de (3.11) bajo la condición

$$n_4! \equiv n_3! \pmod{p}.$$

Esta condición y la naturaleza de la congruencia (3.11) implican $n_1! \equiv n_2! \pmod{p}$. Conforme a lo establecido en el Lema 12, tomado $k = 1$, el número de tales (n_1, n_2, n_3, n_4) es menor o igual que

$$(\#\{(x, y) \ : \quad x! \equiv y! \pmod{p},\ 1 \leq x, y \leq N\})^2 \ll N^3.$$

Por lo tanto, ya que $m \leq N$, tenemos $T_1(N) \ll N^4$. En consecuencia

$$T(N) \ll N^4.$$

Complementamos la estimación (3.10) con este hecho para obtener

$$J = \frac{N^7}{p} + O(N^{35/6}p^{1/8}) = \frac{N^7}{p}(1 + O(N^{-7/6}p^{9/8})).$$

En particular, para algún $N = O(p^{27/28})$, obtenemos $J > 0$. □

3.6. Demostración del Teorema 12

Denotemos

$$F_1 = \sum_{x=1}^{N}\sum_{y=1}^{M} \chi((x + y + L)!)$$

y

$$F_2 = \sum_{x=1}^{N}\sum_{y=1}^{M} \chi((x - y + L)!).$$

Las demostraciones de las estimaciones requeridas para F_1 y F_2 son similares, por lo que sólo trataremos con F_1.

Si

$$\frac{N^{1/2}}{p^{1/4}\log^{1/2}(NM^{-1}+2)} < 10,$$

entonces la estimación es trivial. Por lo tanto, podemos asumir que

$$K := \left[\frac{N^{1/2}}{p^{1/4}\log^{1/2}(NM^{-1}+2)}\right] > 9.$$

Al aplicar defasamiento en los argumentos se tiene

$$F_1 = \frac{1}{K}\sum_{k=1}^{K}\sum_{x=1}^{N}\sum_{y=1}^{M}\chi((x+y+k+L)!) + O(KM). \tag{3.12}$$

Elevando al cuadrado los módulos y usando la desigualdad de Cauchy-Schwrtz, se tiene

$$F_1^2 \ll \frac{NM}{K^2}\sum_{x=1}^{N}\sum_{y=1}^{M}\left|\sum_{k=1}^{K}\chi\left((x+y+k+L)!\right)\right|^2 + K^2M^2. \tag{3.13}$$

Así

$$F_1^2 \ll \frac{NM}{K^2}\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}W(k_1,k_2) + K^2M^2, \tag{3.14}$$

donde

$$W(k_1,k_2) = \sum_{x=1}^{N}\sum_{y=1}^{M}\chi\left((x+y+k_1+L)!\right)\overline{\chi\left((x+y+k_2+L)!\right)}.$$

Sustituyendo $z = x+y+L$, obtenemos

$$|W(k_1,k_2)| = \frac{1}{p}\left|\sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\sum_{a=0}^{p-1}\sum_{x=1}^{N}\sum_{y=1}^{M}\mathbf{e}_p(a(z-(x+y+L)))\right|$$

$$\leq \frac{1}{p}\sum_{a=0}^{p-1}\left|\sum_{x=1}^{N}\mathbf{e}_p(ax)\right|\left|\sum_{y=1}^{M}\mathbf{e}_p(ay)\right|\left|\sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\,\mathbf{e}_p(az)\right|.$$

Por la definición de $W(k_1, k_2)$ tenemos

$$|W(k,k)| \le NM.$$

Si $k_1 \ne k_2$, entonces, acorde a las estimaciones clásicas de Weil,

$$\left|\sum_{z=0}^{p-1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, \mathbf{e}_p(az)\right| \le Kp^{1/2}.$$

De hecho, si $k_1 > k_2$, entonces tenemos

$$\begin{aligned}
&\left|\sum_{z=0}^{p-1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, \mathbf{e}_p(az)\right| \le \\
&\left|\sum_{z=0}^{p-k_1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, \mathbf{e}_p(az)\right| \le \\
&\left|\sum_{z=0}^{p-k_1} \chi((z+k_2+1)\cdots(z+k_1))\, \mathbf{e}_p(az)\right| \le \\
&\left|\sum_{z=0}^{p-1} \chi((z+k_2+1)\cdots(z+k_1))\, \mathbf{e}_p(az)\right| + K \le Kp^{1/2}.
\end{aligned}$$

De esta forma, cuando $k_1 \ne k_2$ obtenemos

$$|W(k_1,k_2)| \le Kp^{-1/2} \sum_{a=0}^{p-1} \left|\sum_{x=1}^{N} \mathbf{e}_p(ax)\right| \left|\sum_{y=1}^{M} \mathbf{e}_p(ay)\right| \ll Kp^{1/2} M \log(NM^{-1}+2).$$

Sustituyendo las estimaciones obtenidas para $W(k_1, k_2)$ en (3.14), deducimos

$$F_1^2 \ll \frac{NM}{K^2}\left(\sum_{k=1}^{K} NM + \sum_{k_1=1}^{K}\sum_{k_2=1}^{K} Kp^{1/2} M \log(NM^{-1}+2)\right) + K^2M^2 \ll$$
$$\frac{N^2M^2}{K} + Kp^{1/2}NM^2 \log(NM^{-1}+2) + K^2M^2.$$

Recordamos la defínción de K y observamos que los dos primeros términos son del mismo orden, igual al requerido y además el tercer sumando nunca domina a los dos primeros. Por lo tanto, la demostración queda concluida. □

3.7. Demostración del Teorema 13

Podemos suponer que $N \leq p/2$ dado que para $N > p/2$ el correspondiente resultado de [23] proporciona una fórmula mejor que la del Teorema 13.

Sea $\lambda \not\equiv 0 \pmod p$ y sea $J = J(\lambda, N)$ el número de soluciones de la congruencia

$$n_1! \cdots n_7! \equiv \lambda \pmod p; \quad 1 \leq n_1, \ldots, n_7 \leq N.$$

Denote $r = \left[\frac{\log N}{\log 2}\right]$. Dividimos al intervalo $[1, N]$ en intervalos ajenos

$$[1, N] = [1, N/2^r] \cup \left(N/2^r, N/2^{r-1}\right] \cup \cdots \cup (N/4, N/2] \cup (N/2, N].$$

Dado $1 \leq j_1, j_2, j_3 \leq r-2$, denote por $J(j_1, j_2, j_3)$ al número de soluciones de la congruencia

$$n_1! \cdots n_7! \equiv \lambda \pmod p$$

sujeta a las condiciones

$$\frac{N}{2^{j_i}} < n_i \leq \frac{N}{2^{j_i - 1}}, \quad i = 1, 2, 3; \qquad 1 \leq n_4, n_5, n_6, n_7 \leq N.$$

Entonces

$$J = J_1 + O(J_2),$$

donde

$$J_1 = \sum_{j_1=1}^{r-2} \sum_{j_2=1}^{r-2} \sum_{j_3=1}^{r-2} J(j_1, j_2, j_3) \tag{3.15}$$

y J_2 es el número de soluciones de la congruencia

$$n_1! \cdots n_7! \equiv \lambda \pmod p; \quad 1 \leq n_1 \leq 8, \qquad 1 \leq n_2, \ldots, n_7 \leq N.$$

Note que

$$\begin{aligned} J_2 &= \frac{1}{p-1} \sum_{\chi} \left(\sum_{n_1 \leq 8} \chi(n_1!) \right) \left(\sum_{n \leq N} \chi(n!) \right)^6 \overline{\chi(\lambda)} \\ &\ll \frac{1}{p-1} \sum_{\chi} \left| \sum_{n \leq N} \chi(n!) \right|^6. \end{aligned}$$

El último término es igual al número de soluciones de la congruencia

$$n_1!n_2!n_3! \equiv n_4!n_5!n_6! \pmod{p}; \qquad 1 \leq n_1, \ldots, n_6 \leq N.$$

Por lo tanto, de el Lema 12 (tomando $k = 3$), tenemos

$$J_2 \ll N^{5+1/8}.$$

De esta forma,

$$J = J_1 + O\left(N^{5+1/8}\right). \tag{3.16}$$

Siguiendo los argumentos de [14], estableceremos una fórmula asintótica efectiva para J_1. Sean $1 \leq j_1, j_2, j_3 \leq r-2$ enteros fijos y sean

$$M_1 = M_1(j_1, j_2, j_3), \quad M_2 = M_2(j_1, j_2, j_3), \quad M_3 = M_3(j_1, j_2, j_3)$$

enteros positivos fijos a escogerse más adelante tales que

$$2 \leq M_1 < N2^{-j_1} - 1, \quad 2 \leq M_2 < N2^{-j_2} - 1, \quad 2 \leq M_3 < N2^{-j_3} - 1.$$

Denote por $J'(j_1, j_2, j_3)$ al número de soluciones de la congruencia

$$(n_1 + m_1)!(n_2 + m_2)!(n_3 + m_3)!n_4!n_5!n_6!n_7! \equiv \lambda \pmod{p}$$

sujeto a las condiciones

$$1 \leq m_i \leq M_i, \quad \frac{N}{2^{j_i}} - M_i < n_i \leq \frac{N}{2^{j_i - 1}}, \quad i = 1, 2, 3; \quad 1 \leq n_4, n_5, n_6, n_7 \leq N.$$

Para m_1, m_2, m_3 fijos, el número de soluciones de la congruencia anterior es $\geq J(j_1, j_2, j_3)$. Por lo tanto,

$$J(j_1, j_2, j_3) \leq \frac{J'(j_1, j_2, j_3)}{M_1 M_2 M_3}.$$

Análogamente, definimos $J''(j_1, j_2, j_3)$ al número de soluciones de la congruencia

$$(n_1 - m_1)!(n_2 - m_2)!(n_3 - m_3)!n_4!n_5!n_6!n_7! \equiv \lambda \pmod{p}$$

sujeta a las condiciones

$$1 \leq m_i \leq M, \quad \frac{N}{2^{j_i}} + M_i < n_i \leq \frac{N}{2^{j_i - 1}}, \quad i = 1, 2, 3, \quad 1 \leq n_4, n_5, n_6, n_7 \leq N.$$

Para fijos m_1, m_2, m_3 el número de soluciones de la congruencia anterior es $\leq J(j_1, j_2, j_3)$. Así,

$$\frac{J''(j_1, j_2, j_3)}{M_1 M_2 M_3} \leq J(j_1, j_2, j_3).$$

De esta forma

$$\frac{J''(j_1, j_2, j_3)}{M_1 M_2 M_3} \leq J(j_1, j_2, j_3) \leq \frac{J'(j_1, j_2, j_3)}{M_1 M_2 M_3}. \tag{3.17}$$

Nuestro objetivo es usar esta desigualdad para demostrar que

$$J(j_1, j_2, j_3) = \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + O\Big(\frac{p^{3/8} N^{11/2}}{2^{3(j_1+j_2+j_3)/4}} \big(\log (N p^{-11/12} + 2) \big)^{3/4} \Big).$$

Sea

$$L_i = [N 2^{-j_i}] - M_i, \quad N_i = [N 2^{-j_i+1}] - L_i, \quad i = 1, 2, 3.$$

Escribimos $J'(j_1, j_2, j_3)$ en términos de sumas de caracteres y obtenemos

$$J'(j_1, j_2, j_3) = \frac{1}{p-1} \sum_{\chi} \left(\prod_{i=1}^{3} \mathcal{F}(\chi; M_i, N_i, L_i) \right) \left(\sum_{n=1}^{N} \chi(n!) \right)^4 \overline{\chi(\lambda)},$$

donde χ corre a través del conjunto de los caracteres multiplicativos módulo p y

$$\mathcal{F}(\chi; M_i, N_i, L_i) = \sum_{m_i=1}^{M_i} \sum_{L_i < n_i \leq L_i + N_i} \chi((n_i + m_i)!).$$

Separando el término correspondiente al carácter principal $\chi = \chi_0$, obtenemos

$$J'(j_1, j_2, j_3) = \frac{N^4}{p-1} \prod_{i=1}^{3} \left(\frac{N}{2^{j_i}} + M_i + 2\,\theta_i \right) M_i +$$

$$+ O\left(\left(\prod_{i=1}^{3} \max_{\chi \neq \chi_0} |\mathcal{F}(\chi; M_i, N_i, L_i)| \right) \frac{1}{p-1} \sum_{\chi} \left| \sum_{n=1}^{N} \chi(n!) \right|^4 \right),$$

donde $|\theta_i| \leq 1$, $i = 1, 2, 3$. Observamos que

$$\frac{1}{p-1} \sum_{\chi} \left| \sum_{n=1}^{N} \chi(n!) \right|^4$$

es igual al número de soluciones de la congruencia

$$n_1!n_2! \equiv n_3!n_4! \pmod{p}; \qquad 1 \le n_1, n_2, n_3, n_4 \le N.$$

Por lo que, en virtud del Lema 12 tomando $k = 2$, tenemos

$$\frac{1}{p-1}\sum_{\chi}\left|\sum_{n=1}^{N}\chi(n!)\right|^4 \ll N^{3+1/4}.$$

Por lo tanto, usando esta estimación, el Teorema 12 para estimar $\mathcal{F}(\chi; M_i, N_i, L_i)$ y también tomando en cuenta que $2^{j_i}M_i/N \ll 1$ y $N_i \ll N2^{-j_i} + M_i$, deducimos:

$$\begin{aligned}
\frac{J'(j_1,j_2,j_3)}{M_1M_2M_3} &= \frac{N^4}{p-1}\prod_{i=1}^{3}\left(\frac{N}{2^{j_i}} + M_i + 2\,\theta_i\right) + \\
&+O\left(p^{3/8}N^{13/4}\prod_{i=1}^{3}N_i^{3/4}\big(\log\left(N_iM_i^{-1}+2\right)\big)^{1/4}\right) \\
&= \frac{N^7}{p-1}2^{-(j_1+j_2+j_3)} + O\left(\frac{N^7}{p}2^{-(j_1+j_2+j_3)}\left(\frac{2^{j_1}}{N}M_1 + \frac{2^{j_2}}{N}M_2 + \frac{2^{j_3}}{N}M_3\right) + \right. \\
&\left. +\frac{p^{3/8}N^{11/2}}{2^{3(j_1+j_2+j_3)/4}}\prod_{i=1}^{3}\big(\log\left(N2^{-j_i}M_i^{-1}+2\right)\big)^{1/4}\right).
\end{aligned}$$

Ahora, demostraremos que para una elección conveniente de los parámetros M_1, M_2, M_3 tenemos la siguiente fórmula asintótica

$$\frac{J'(j_1,j_2,j_3)}{M_1M_2M_3} = \frac{N^7}{p-1}2^{-(j_1+j_2+j_3)} + O\left(\frac{p^{3/8}N^{11/2}}{2^{3(j_1+j_2+j_3)/4}}\log^{3/4}(Np^{-11/12}+2)\right). \tag{3.18}$$

Si j_1, j_2, j_3 son tales que $N2^{-(j_1+j_2+j_3)/6} < 100p^{11/12}$, entonces escogemos

$$M_i = [N2^{-j_i-1}], \quad i = 1, 2, 3$$

para obtener

$$\frac{J'(j_1,j_2,j_3)}{M_1M_2M_3} = O(Np^{9/2}\log^{3/4}(Np^{-11/12}+2)),$$

y la estimación (3.18) esta demostrada en este caso, puesto que el término de error en (3.18) es el término que domina.

Si j_1, j_2, j_3 son tales que $N2^{-(j_1+j_2+j_3)/6} \geq 100p^{11/12}$, entonces definimos

$$V = \left[\left(\frac{N^2 2^{-(j_1+j_2+j_3)/3} p^{-11/6}}{\log(N2^{-(j_1+j_2+j_3)/6} p^{-11/12})} \right)^{3/4} \right].$$

Claramente, $V \geq 2$. Dado que $\max\{2^{j_1}, 2^{j_2}, 2^{j_3}\} < N < p$, también se verifica que

$$V < 0{,}5N^{3/2} 2^{-(j_1+j_2+j_3)/4} p^{-11/8} < 0{,}5 \min\{N2^{-j_1}, N2^{-j_2}, N2^{-j_3}\}.$$

De esta forma, en esta situación podemos elegir

$$M_i = \left[\frac{N2^{-j_i}}{V} \right], \quad i = 1, 2, 3,$$

y obtener

$$\begin{aligned} \frac{J'(j_1, j_2, j_3)}{M_1 M_2 M_3} &= \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + \\ &+ O\left(\frac{p^{3/8} N^{11/2}}{2^{3(j_1+j_2+j_3)/4}} \log^{3/4}(N2^{-(j_1+j_2+j_3)/6} p^{-11/12} + 2) \right) \\ &= \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + O\left(\frac{p^{3/8} N^{11/2} \log^{3/4}(Np^{-11/12} + 2)}{2^{3(j_1+j_2+j_3)/4}} \right). \end{aligned}$$

En consecuencia, la estimación requerida (3.18) se afirma en ambos casos. Ahora combinando esto con (3.17), tenemos

$$J(j_1, j_2, j_3) \leq \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + O\left(\frac{p^{3/8} N^{11/2} \log^{3/4}(Np^{-11/12} + 2)}{2^{3(j_1+j_2+j_3)/4}} \right).$$

Análogamente, obtenemos la misma fórmula asintótica para $J''(j_1, j_2, j_3)$ y usando (3.17) deducimos que

$$J(j_1, j_2, j_3) \geq \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + O\left(\frac{p^{3/8} N^{11/2} \log^{3/4}(Np^{-11/12} + 2)}{2^{3(j_1+j_2+j_3)/4}} \right).$$

Por lo tanto,

$$J(j_1, j_2, j_3) = \frac{N^7}{p-1} 2^{-(j_1+j_2+j_3)} + O\left(\frac{p^{3/8} N^{11/2} \log^{3/4}(Np^{-11/12} + 2)}{2^{3(j_1+j_2+j_3)/4}} \right).$$

En virtud de (3.15) y (3.16), obtenemos

$$\begin{aligned} J &= \sum_{j_1=1}^{r-2}\sum_{j_2=1}^{r-2}\sum_{j_3=1}^{r-2} J(j_1,j_2,j_3) + O(N^{5+1/8}) \\ &= \frac{N^7}{p-1}\left(\sum_{j=1}^{\infty}\frac{1}{2^j} - \sum_{j>r-2}\frac{1}{2^j}\right)^3 + R(N) + O(N^{5+1/8}) \\ &= \frac{N^7}{p-1} + R(N) + O\left(\frac{1}{p}N^6 + N^{5+1/8}\right) \end{aligned}$$

donde

$$\begin{aligned} R(N) &\ll p^{3/8}N^{11/2}\log^{3/4}(Np^{-11/12}+2)\sum_{j_1=1}^{r-2}\sum_{j_2=1}^{r-2}\sum_{j_3=1}^{r-2}\frac{1}{2^{3(j_1+j_2+j_3)/4}} \\ &\ll p^{3/8}N^{11/2}\log^{3/4}(Np^{-11/12}+2). \end{aligned}$$

Dado que

$$\frac{1}{p}N^6 + N^{5+1/8} \ll p^{3/8}N^{11/2}\log^{3/4}(Np^{-11/12}+2),$$

concluimos

$$J = \frac{N^7}{p-1} + O\left(p^{3/8}N^{11/2}\log^{3/4}(Np^{-11/12}+2)\right).$$

□

Bibliografía

[1] T. M. Apostol, 'Modular functions and Dirichlet series in number theory', Second ed., Graduate Texts in Mathematics 41, Springer-Verlag, New York, 1990.

[2] A. Ayyad, T. Cochrane and Zh. Zheng, *The congruence* $x_1x_2 \equiv x_3x_4$ (mód p), *the equation* $x_1x_2 = x_3x_4$, *and mean values of character sums,* J. Number Theory **59** (1996), 398–413.

[3] D. Berend and J. E. Harmse, *On some arithmetical properties of middle binomial coefficients,* Acta Arith. **84** (1998), 31–41.

[4] J. Bourgain, *More on the sum-product phenomenom in prime fields and applications,* Int. J. Number Theory **1** (2005), no. 1, 1–32.

[5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order,* J. London Math. Soc. (2) **73** (2006), 380–398.

[6] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields and their applications,* Geom. Func. Anal. **14** (2004), 27–57.

[7] D. A. Burgess, *Mean values of character sums,* Mathematika **33** (1986), 1–5.

[8] Y. G. Chen and L. X. Dai, *Congruences with factorials modulo p,* Integers **6** (2006), A21, 3 pp.

[9] C. Cobeli, M. Vâjâitu and A. Zaharescu, *The sequence* $n!$ (mód p), J. Ramanujan Math. Soc. **15** (2000), 135–154.

[10] T. Cochrane and Zh. Zheng, *Small solutions of the congruence* $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv c \pmod{p}$, Acta Math. Sinica (N.S.) **14** (1998), 175–182.

[11] P. Deligne, *La conjecture de Weil* I, (French), Inst. Hautes Études Sci. Publ. Math., **43** (1974), 273–307.

[12] J. B. Friedlander and H. Iwaniec, *The divisor problem for arithmetic progressions,* Acta Arith. **45** (1985), 273–277.

[13] J. B. Friedlander and H. Iwaniec, *Estimates for character sums,* Proc. Amer. Math. Soc. **119** (1993), 365–372.

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

[15] M. Z. Garaev, *Character sums in shorts intervals and the multiplication table modulo a large prime,* Monatsh. Math. **148** (2006), 127–138.

[16] M. Z. Garaev, V. C. Garcia *Waring type congruences involving factorials modulo a prime,* Arch. Math. (Basel) **88** (2007), no. 1, 35–41.

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

[18] M. Z. Garaev, V. C. Garcia and S. V. Konyagin, *Waring problem with the Ramanujan* τ*-function,* Izvestiya Mathematics (Russian Academy of Sciences) translated from Izv. Ross. Akad. Nauk Ser. Mat. **72** (2008), no. 1, 39–50.

[19] M. Z. Garaev, V. C. Garcia and S. V. Konyagin, *Waring problem with the Ramanujan* τ*-function II,* Can. Math. Bull, (to appear).

[20] M. Z. Garaev, V. C. Garcia, S. V. Konyagin, *A note on the Ramanujan* τ*-function.* Arch. Math. (Basel) **89** (2007), no. 5, 411–418.

[21] M. Z. Garaev and A. A. Karatsuba, *The representation of residue classes by products of small integers,* Proc. Edin. Math. Soc. (2), **50** (2007), 363–375.

[22] M. Z. Garaev and F. Luca, *Character sums and product of factorials modulo p,* J. Théor. Nombres Bordeaux **17** (2005), 161–170.

[23] M. Z. Garaev, F. Luca and I. E. Shparlinski, *Character sums and congruences with n!,* Trans. Amer. Math Soc. **356** (2004), 5089–5102.

[24] M. Z. Garaev, F. Luca and I. E. Shparlinski, *Exponential sums and congruences with factorials,* J. Reine Angew. Math. **584** (2005), 29–44.

[25] M. Z. Garaev, F. Luca and I. E. Shparlinski, *Waring problems with factorials,* Bull. Aust. Math. Soc. **71** (2005), 259-264.

[26] M. Z. Garaev, F. Luca and I. E. Shparlinski, *Distribution of harmonic sums and Bernoulli polynomials modulo a prime*, Math. Zeitschr. **253** (2006), 855–865.

[27] M. Z. Garaev, F. Luca and I. E. Shparlinski, *Catalan and Apéry numbers in residue classes*, J. Combin. Theory (Ser. A) **113** (2006), 851–865.

[28] V. C. Garcia, *Representations of residue classes by factorials, binomial coefficients and harmonic sums modulo a prime,* Bol. Soc. Mat. Mexicana, (to appear).

[29] V. C. Garcia, *On the value set of n!m! modulo a large prime ,* Bol. Soc. Mat. Mexicana **13** (2007), 1–6 .

[30] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem,* Mat. Zametki, **79** (2006), 384–395; translation in: Math. Notes **79** (2006), 356–365.

[31] R. K. Guy, 'Unsolved Problems in number theory', Springer-Verlag, New York, 1994.

[32] G. Harman, *Diophantine approximation with square-free integers,* Math. Proc. Cambridge Philos. Soc. **95** (1984), 381–388.

[33] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors,* J. Théor. Nombres Bordeaux **5** (1993), 411–484.

[34] L. K. Hua, 'Additive theory of prime numbers', AMS, Providence, Rhode Island, 1965.

[35] H. Iwaniec, 'Topics in Clasical Automorphic Forms', AMS, Providence, Rhode Island, 1997.

[36] A. A. Karatsuba, 'Basic Analytic Number Theory', Springer-Verlag, New York, 1993.

[37] A. A. Karatsuba, *Additive Congruences,* Izv. Math. **61** (1997), no. 2, 317–329.

[38] N. Koblitz, 'Introduction to elliptic curves and modular forms', Springer-Verlag, New York, 1993.

[39] E. Kowalski, *Exponential sums over definable subsets of finite fields*, Israel J. Math. **160** (2007), 219–251.

[40] A.V. Kumchev and D.I. Tolev, *An Invitation to Additive Number Theory,* Serdica Math. J. **31** (2005), 1–74.

[41] F. Luca and I. E. Shparlinski, *Arithmetic properties of the Ramanujan function,* Proc. Indian Acad. Sci. Math. Sci. **116** (2006), 1–8.

[42] F. Luca and P. Stănică, *Products of factorials modulo p*, Colloq. Math. **96** (2003), 191–205.

[43] H. L. Montgomery and R. C. Vaughan, *Mean values of character sums,* Canad. J. Math. **31** (1979), no. 3, 476–487.

[44] M. R. Murty, 'Problems in analytic number theory', Springer-Verlag, New York, 2001.

[45] M. R. Murty, *Oscillations of Fourier coefficients of modular forms,* Math. Ann. **262** (1983), no. 4, 431–446.

[46] D. Niebur, *A formula for Ramanujan's $\tau-$function,* Illinois J. Math. **19** (1975), 448–449.

[47] S. Shi, *On the equation $n_1n_2 = n_3n_4$ and mean value of character sums,* J. Number Theory **128** (2008), no. 2, 313–321.

[48] J. P. Serre, *Congruences et formes modulaires* [dáprès H. P. F. Swinnerton-Dyer] (French), Lecture Notes in Math, **317**, 319–338, Springer, Berlin, 1973.

[49] I. E. Shparlinski, *Distribution of points on modular hyperbolas,* in: Sailing on the Sea of Number Theory: Proc. 4th China-Japan Seminar on Number Theory, Weihai, 2006, World Scientific, 2007, pp. 155–189.

[50] I. E. Shparlinski, *Distribution of modular inverses and multiples of small integers and the Sato-Tate conjecture on average,* Michigan Math. J. **56** (2008), no. 1, 99–111.

[51] I. E. Shparlinski, *On the value set of the Ramanujan function,* Arch. Math. **85** (2005), 508–513.

[52] G. Tenenbaum, *Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné*, Compositio Math. **51** (1984), no. 2, 243–263 (in French).

[53] R. C. Vaughan, 'The Hardy–Littlewood method', second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[54] R. C. Vaughan, *Diophantine approximation by prime numbers, III,* Proc. London Math. Soc. **33** (1976), 177–192.