Universidad Michoacana de San Nicolás de Hidalgo
Universidad Nacional Autónoma de México

Posgrado Conjunto en Ciencias Matemáticas

La distribución de factoriales módulo un número primo y puntos sobre curvas en pequeñas cajas

T E S I S

---

que para obtener el grado de Doctor en Ciencias Matemáticas presenta:

José Hernández Santiago

Asesor: Dr. Moubariz Garaev

Morelia, Mich., México. — Enero de 2019.

Resumen

RESUMEN. Son dos los tópicos que se abordan en esta tesis: por un lado se encuentra el estudio de la distribución de los factoriales módulo un número primo y, por el otro, el estudio del número de soluciones (dentro de cuadrados del plano) de las congruencias $y^2 \equiv f(x) \pmod{p}$ y $y \equiv f(x) \pmod{p}$ donde p es un número primo y $f(x)$ es un polinomio de coeficientes enteros de grado mayor o igual que 3 y cuyo coeficiente principal no es múltiplo de p.

En la tesis se expondrán nuestras contribuciones a estos dos temas y se discutirá como es que nuestros resultados permitieron avanzar el estado del arte en cada caso.

ABSTRACT. In this thesis we deal with two themes: the distribution of the sequence of factorials modulo a prime number and the study of the number of solutions to the congruences $y^2 \equiv f(x) \pmod{p}$ and $y \equiv f(x) \pmod{p}$ where (x, y) belongs to an arbitrary square of the plane, p is a prime number, and $f(x)$ is a polynomial with integer coefficients whose degree is at least 3 and whose leading coefficient is not a multiple of p.

We present our contributions to these two topics and we discuss how it is that our results advanced the state of the art in each case.

Palabras clave: congruencias, cuerpos convexos, ecuaciones sobre campos finitos, retículas, sumas de caracteres, sumas exponenciales.

Agradecimientos

Al CONACYT, por la beca que me otorgó para llevar a cabo mis estudios de doctorado en el Posgrado Conjunto en Ciencias Matemáticas de la Universidad Nacional Autónoma de México y la Universidad Michoacana de San Nicolás de Hidalgo.

A la gente del Centro de Ciencias Matemáticas UNAM por todo el apoyo y facilidades que me han brindado durante tantos años y, en particular, durante mi época como estudiante de doctorado.

Al Dr. Moubariz Garaev, por haber fungido como mi asesor durante mis estudios de maestría y de doctorado y por toda la teoría de números que tuvo a bien compartirme en sus cursos y seminarios en Morelia.

A los doctores Eugenio Balanzario, Raymundo Bautista, Abel Castorena y Víctor C. García por haber aceptado participar en el proceso de revisión de esta tesis. A los doctores Eugenio y Víctor les agradezco también el haber formado parte de mi comité tutor en el doctorado.

Finalmente, no quiero dejar pasar esta ocasión sin externar mi profunda gratitud hacia mi madre y mi familia en Cacahuatepec por todo el apoyo y por todo el aliento que de ellos recibí para llevar mis estudios hasta este punto. De manera muy especial le agradezco a Isabel, el centro de mi familia, por todo su cariño, por su respaldo y por ser, junto con mis pequeños Gus y Alek, la luz de mi vida.

Índice general

Introducción

Son dos los temas que se abordan en esta tesis: por un lado se encuentra el estudio de la distribución de los factoriales módulo un número primo y, por el otro, el estudio del número de soluciones (dentro de cuadrados del plano) de las congruencias $y^2 \equiv f(x) \pmod{p}$ y $y \equiv f(x) \pmod{p}$ donde p es un número primo y $f(x)$ es un polinomio de coeficientes enteros de grado mayor o igual que 3 y cuyo coeficiente principal no es múltiplo de p. Aunque es posible que ambas cuestiones parezcan totalmente desconectadas a simple vista, un hecho que quedará de manifiesto en este trabajo es que hay un estadio en el análisis de cada uno de estos problemas en el que es posible recurrir al método de sumas exponenciales para obtener avances en torno a ellos.

Los resultados que expondremos en esta tesis fueron publicados en los siguientes artículos conjuntos (ver ítemes [6] y [11] de la Bibliografía):

a) Con M. Z. Garaev: *A note on n! modulo p*. Monatshefte für Mathematik, **182** (2017), pp. 23-31.

b) Con M.-C. Chang, J. Cilleruelo†, M. Z. Garaev, I. E. Shparlinski y A. Zumalacárregui: *Points on curves in small boxes and applications*. Michigan Mathematical Journal, **63** (2014), pp. 503-534.

La tesis consta de dos capítulos: el capítulo uno es el que destinamos a la discusión de nuestras contribuciones al tema de la distribución de factoriales

módulo un número primo y el capítulo dos es el que se destinó a la presentación de los resultados sobre la estimación de los números de soluciones de las congruencias arriba mencionadas. La intención básica en los párrafos que siguen es describir con mayor detalle los problemas estudiados y los resultados obtenidos e indicar cómo nuestros teoremas avanzan *el estado del arte* en cada caso. La lectura de los sumarios que a continuación se presentan se puede acompañar y/o complementar con la lectura de las secciones 1.1 y 2.1-2.2 de la tesis.

Idea general del capítulo 1

Esencialmente son dos las cuestiones que se estudiarán en este capítulo[1]:

a) la estimación del cardinal de $\mathcal{A}(N) := \{n! \pmod p \colon 1 \leq n \leq N\}$ y

b) la representación de los elementos de $\mathbb{F}_p^*$ como productos de factoriales.

Ambas cuestiones habían sido tratadas previamente en la literatura y en este apartado de la tesis expondremos los resultados que en torno a ellas publicamos en [11].

El interés en el problema listado en a) se remonta a una pregunta de P. Erdős de alrededor de 1960 (ver, por ejemplo, [21]). De acuerdo con Rokowska y Schinzel (*ibid.*, [21, pág. 84]), Erdős fue quien planteó el problema de determinar la existencia de un número primo $p > 5$ tal que los números

$$2!, 3!, 4!, \ldots, (p-1)!$$

fuesen todos incongruentes entre sí módulo p. Aunque hasta el momento no se cuenta con una respuesta definitiva a esta pregunta, con base en evidencia computacional y en ciertas consideraciones heurísticas, se ha llegado a

[1] Para disipar dudas relacionadas con la notación, consultar el apartado intitulado Notación que inicia en la pág. 9.

conjeturar que el conjunto de número primos $p > 5$ tales que $|\mathcal{A}(p-1) \setminus \{1 \pmod p\}| = p-2$ es vacío. Trudgian denominó en [26] a un número primo $p > 5$ como *socialista* cuando la respuesta a la anterior pregunta de Erdős es afirmativa, esto es, cuando los factoriales $2!, \ldots, (p-1)!$ resultan ser todos incongruentes entre sí módulo p; refinando la caracterización para dichos primos que Rokowska y Schinzel establecieron en [21], Trudgian probó en [26] que no existe ningún primo socialista en el intervalo $(5, 10^9)$.

Aunque, como puede inferirse de lo relatado endenantes, no se cuenta por el momento con un resultado sobre el cardinal exacto del conjunto

$$\mathcal{A}(p-1) = \{1! \pmod p, 2! \pmod p, \ldots, (p-2)! \pmod p, (p-1)! \pmod p\}$$

para un primo arbitrario p, la evidencia experimental permite conjeturar que

$$|\mathcal{A}(p-1)| \sim \left(1 - \frac{1}{e}\right)p.$$

Las gráficas que se muestran a continuación permiten efectuar un primer cotejo de la admisibilidad de la hipótesis anterior:

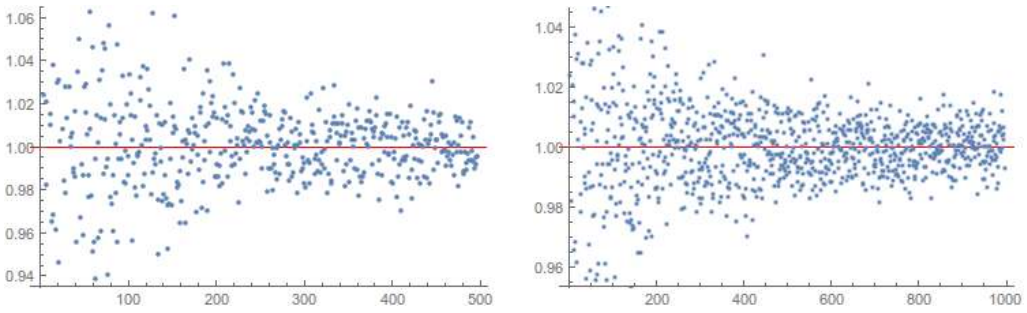


Fig. Los cocientes $\mathcal{A}(p-1)/(1-1/e)p$ para los primeros quinientos (izq.) y mil (der.) núm. primos.

El primer problema que trataremos en el capítulo es el estudio de la cardinalidad de $\mathcal{A}(N) = \{n! \pmod p : 1 \leq n \leq N\}$ cuando p es un número primo y

$N \in \mathbb{N} \cap (1, p)$. Una primera observación que puede hacerse sobre dicho cardinal es que

$$|\mathcal{A}(N)| \geq N^{1/2}. \tag{1}$$

En lo sucesivo nos referiremos a esta desigualdad como *la estimación trivial inferior para* $|\mathcal{A}(N)|$. De acuerdo con el teorema principal del artículo [14] de V. García, para todo primo p suficientemente grande se cumple que

$$|\{m!n! \pmod p \colon 1 \leq m, n \leq p\}| \geq \left(\frac{41}{48} + o(1)\right)p. \tag{2}$$

A la vez que este resultado superó uno establecido previamente en [12] también redundó en una mejora a la estimación trivial (1) cuando $N = p - 1$: más específicamente, de (2) se colige que

$$|\mathcal{A}(p-1)| > cp^{1/2}$$

para cualquier constante $c < \sqrt{\frac{41}{24}}$ y cualquier número primo p suficientemente grande. Varios años después, O. Klurman y M. Munsch demostrarían en [19] que si ε es un número real positivo suficientemente pequeño y $N \in (p^{1/4+\varepsilon}, p)$ entonces

$$|\mathcal{A}(N)| \geq \sqrt{\frac{3}{2}} N^{1/2}.$$

En el primer teorema de este capítulo se establecerá una estimación inferior para el cardinal del conjunto

$$\frac{\mathcal{A}(N)}{\mathcal{A}(N)} := \left\{\frac{a}{b} \colon a, b \in \mathcal{A}(N)\right\}$$

de la cual se deriva fácilmente **la mejor** acotación inferior para $|\mathcal{A}(N)|$ que se conoce hasta el momento (al menos cuando N es un número natural que pertenece a un intervalo de la forma $(p^{1/2+\varepsilon}, p^{1-\varepsilon})$).

Teorema. *Si* $\varepsilon \in (0, \frac{1}{4})$ *y* $N \in (p^{\frac{1}{2}+\varepsilon}, p^{1-\varepsilon}) \cap \mathbb{N}$*, entonces existe una constante* $c_0 := c_0(\varepsilon) > 0$ *tal que*

$$\left|\frac{\mathcal{A}(N)}{\mathcal{A}(N)}\right| > c_0 N \log N.$$

Este resultado nos permitió obtener nuevos avances en el problema mencionado en b).

Asumiendo la validez de la conjetura de que $|\mathcal{A}(p-1)| \sim \left(1 - \frac{1}{e}\right) p$ se deduce fácilmente que para cada $\lambda \in \mathbb{F}_p \setminus \{0\}$ existen $n_1, n_2 \in \{1, \ldots, p-1\}$ de tal modo que

$$\lambda \equiv n_1! n_2! \pmod{p}.$$

Por otro lado, sin apelar al (potencial) cumplimiento de la conjetura es posible demostrar que para todo $\lambda \in \mathbb{F}_p \setminus \{0\}$ existen $n_1, n_2, n_3 \in \mathbb{N}$ tales que

$$\lambda \equiv n_1! n_2! n_3! \pmod{p}.$$

En efecto, del teorema de Wilson se desprende que para cada $b \in \{1, 2, \ldots, p-1\}$ se tiene que

$$b!(p-1-b)! \equiv (-1)^{b+1} \pmod{p}. \tag{3}$$

(Ver [10, pág. 515] o también la entrada 67 en [17, pág. 57].) En particular, si $b \equiv \lambda^{-1} \pmod{p}$ entonces

$$\begin{aligned} \lambda &\equiv (-1)^{b+1}(b-1)!(p-1-b)! \pmod{p} \\ &\equiv ((p-1)!)^{r_b}(b-1)!(p-1-b)! \pmod{p} \end{aligned}$$

donde r_b es igual a 0 cuando $b+1$ es par e igual a 1 cuando $b+1$ es impar. El argumento anterior ya no aplica igual de bien cuando se introducen restricciones sobre el tamaño de los n_i que pueden figurar en la representación

de los elementos invertibles de $\mathbb{F}_p$ como productos de factoriales. No obstante, M. Garaev, F. Luca e I. Shparlinski en [12], mediante estimaciones de sumas de caracteres con argumentos en la sucesión de factoriales, lograron establecer que si $\varepsilon > 0$ entonces para cada $\lambda \in \mathbb{F}_p \setminus \{0\}$ existen $n_1, \ldots, n_7$ tales que

$$\lambda \equiv n_1! \cdots n_7! \pmod{p} \qquad \text{y} \qquad \max\{n_1, \ldots, n_7\} = O(p^{11/12+\varepsilon}).$$

En [15], V. García debilitaría la condición sobre el valor absoluto de los n_i a $n_i \ll p^{11/12}$. En el segundo teorema del capítulo estableceremos la siguiente mejora a los dos resultados previamente mencionados que presentamos a la comunidad en [11]:

Teorema. *Todo número entero λ que no es divisible por p puede representarse en la forma*

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

para algunos números naturales $n_1, \ldots, n_7$ que satisfacen

$$\max\{n_1, \ldots, n_7\} \ll \frac{p^{11/12}}{(\log p)^{1/2}}.$$

Idea general del capítulo 2

Sean p un número primo y f un polinomio de coeficientes enteros cuyo coeficiente principal no es divisible por p. Supongamos que $m = \deg(f) \geq 3$ y que $M \in [1, p) \cap \mathbb{N}$. En este capítulo nos concentramos en el estudio del número de soluciones de las congruencias

$$y^2 \equiv f(x) \pmod{p}, \qquad (x, y) \in [R+1, R+M] \times [S+1, S+M] \tag{4}$$

y

$$y \equiv f(x) \pmod{p}, \qquad (x, y) \in [R+1, R+M] \times [S+1, S+M]. \tag{5}$$

Cuando $m = 3$, el estudio de la congruencia (4) puede considerarse como *el análogo módulo p* del conteo de puntos de coordenadas enteras y/o racionales sobre una curva elíptica en algún rectángulo del plano. Cuando $m \geq 4$, a las ecuaciones del tipo $y^2 = f(x)$ se les conoce como *hiperelípticas* y, por esa razón, cabe decir en tal caso que (4) es una ec. hiperelíptica en el campo de p elementos.

Denotemos con $I_f(M; R, S)$ al número de soluciones de (4) y con $J_f(M; R, S)$ al número de soluciones de (5). Cuando el polinomio $F(x, y) = y^2 - f(x) \in \mathbb{Z}[x, y]$ es absolutamente irreducible, al expresar $I_f(M; R, S)$ mediante sumas exponenciales y apelar—entre otras cosas— a la notabilísima estimación de A. Weil del cardinal de $\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \colon F(x, y) \equiv 0 \pmod{p}\}$, se obtiene la siguiente fórmula asintótica

$$I_f(M; R, S) = \frac{M^2}{p} + O(p^{\frac{1}{2}} (\log p)^2). \tag{6}$$

Aun cuando la fórmula representa un primer avance hacia una mejor comprensión de $I_f(M; R, S)$ es relativamente fácil identificar algunas de sus limitaciones: por un lado, es claro que el término de error en ella domina al término principal cuando $M \leq p^{\frac{3}{4}} \log p$; por otro lado, si $M \leq p^{\frac{1}{2}} (\log p)^2$, entonces la fórmula resulta ser incluso más débil que la estimación superior trivial $I_f(M; R, S) \leq 2M$.

En los teoremas de este capítulo se establecen estimaciones superiores para $I_f(M; R, S)$ y $J_f(M; R, S)$ que resultan ser no triviales cuando M está en ciertos intervalos de longitud $o(p)$. He aquí el primer teorema que demostraremos:

Teorema. *La estimación*

$$I_f(M; R, S) \leq M^{1/3+o(1)} + \frac{M^{5/3+o(1)}}{p^{1/6}} \qquad (M \to \infty)$$

se cumple uniformemente para todo polinomio f de grado 3, de coeficientes enteros y cuyo coeficiente principal no es múltiplo de p.

De este resultado se desprende que si $M \ll p^{\frac{1}{8}}$ entonces

$$I_f(M;R,S) \leq M^{\frac{1}{3}+o(1)}. \tag{7}$$

Contraponiendo esto con lo que se tenía en [9], notamos que lo anterior representa un avance en el conocimiento del rango para M en el que vale la estimación esencialmente óptima (7). De este teorema se infiere también que si $M < p^{\frac{1}{4}-\varepsilon}$ para algún $\varepsilon > 0$ entonces existe $\delta := \delta(\varepsilon) > 0$ tal que se verifica la estimación no trivial

$$I_f(M;R,S) \ll M^{1-\delta}.$$

Cabe mencionar que, en los trabajos previamente publicados sobre este asunto, la conclusión anterior se podía garantizar sólo cuando $M < p^{\frac{1}{5}-\varepsilon}$. Por otra parte, en el segundo teorema que presentaremos en el capítulo se establece, combinando principalmente (pero no exclusivamente) resultados de geometría de números, el teorema del valor medio de Vinogradov y el teorema de Bombieri-Pila sobre puntos de coordenadas enteras sobre curvas algebraicas planas, la siguiente estimación superior para $I_f(M;R,S)$ que resulta no trivial siempre que $M < p^{\frac{1}{3}-\varepsilon}$.

Teorema. *La estimación*

$$I_f(M;R,S) \leq M^{1/3+o(1)} + \left(\frac{M^3}{p}\right)^{1/16} M^{1+o(1)} \qquad (M \to \infty)$$

se cumple uniformemente para todo polinomio f de grado 3, de coeficientes enteros y cuyo coeficiente principal no es múltiplo de p.

La acotación de $I_f(M;R,S)$ cuando f es de grado mayor o igual a 4 es el tema del tercer teorema del capítulo; al demostrarla se echará mano de ideas introducidas en [8]. El teorema implicará, en particular, una estimación no trivial para $I_f(M;R,S)$ cuando $M < p^{\frac{1}{3}-\varepsilon}$ (y $\deg(f) \geq 4$). La demostración e incluso la

formulación exacta del mismo requiere de familiaridad con el teorema del valor medio de Vinogradov; es por ello que optamos por enunciarlo en forma hasta la sección 2.2 de la tesis.

Finalmente, nuestra contribución al problema (5) se aborda en el cuarto teorema fuerte del capítulo y es como se enuncia a continuación.

Teorema. *Sea f un polinomio de grado $m \geq 2$, de coeficientes enteros y cuyo coeficiente principal no es múltiplo de p. Se cumple entonces que*

$$J_f(M;R,S) \ll \frac{M^2}{p} + M^{1-1/2^{m-1}} p^{o(1)} \qquad (p \to \infty).$$

Es menester mencionar que en [8] hay estimaciones que, para valores grandes de m, superan la garantizada por este resultado; no obstante, nuestra estimación resulta ser más fina que la de [8] cuando m es pequeño.

Notación

Si $n \in \mathbb{Z}$, entonces con n (mód p) denotamos a la clase de congruencia módulo p a la que pertenece n; p denota a un número primo fijo (pero arbitrario) y $\mathbb{F}_p$ es el campo conformado por las clases de congruencia módulo p (los elementos de $\mathbb{F}_p$ los identificamos con los elementos del conjunto $\{0, 1, \ldots, p-1\}$).

Si $x \in \mathbb{R}$, entonces $\lfloor x \rfloor$ representa al mayor número entero que es menor o igual a x, $\lceil x \rceil$ al menor número entero que es mayor o igual a x y $\|x\|$ a la distancia de x al número entero más cercano. A $\lfloor x \rfloor$ se le denomina típicamente la *parte entera* del número real x y a la diferencia $x - \lfloor x \rfloor =: \{x\}$ la *parte fraccionaria* de x; evidentemente para todo $x \in \mathbb{R}$ se tiene que $\|x\| = \min\{\{x\}, 1 - \{x\}\}$.

En varios puntos del segundo capítulo mediante $f \in \mathbb{F}_p[X]$ indicaremos que f es un polinomio de coeficientes enteros cuyo coeficiente principal no es múltiplo del número primo p.

Usamos el símbolo de Vinogradov $\ll$ con su denotación usual: si $a \geq 0$, $f\colon [a,\infty) \to \mathbb{C}$ y $g\colon [a,\infty) \to (0,\infty)$, escribimos

$$f(x) \ll g(x) \quad (x \to \infty) \tag{8}$$

para indicar que existen constantes $C > 0$ y $x_0 \geq a$ de tal modo que $|f(x)| \leq C\, g(x)$ para cada $x \in [x_0,\infty)$. Aunque la *constante implicada* C es independiente de x, en ocasiones depende de otros parámetros los cuales especificaremos cuando consideremos necesario hacerlo (por lo general son fáciles de inferir del contexto); cuando C no depende de ningún parámetro adicional se suele decir que C es una *constante absoluta*. En nuestro trabajo, estaremos considerando la notación en (8) y la notación $f(x) = O(g(x)) \quad (x \to \infty)$ como equivalentes. Para definir $f(x) \gg g(x) \quad (x \to \infty)$ sólo hay que calcar, *mutatis mutandis*, la definición de (8). Por otro lado, con $f \asymp g$ indicamos que las funciones f y g son del *mismo orden de magnitud*, i.e., que existen constantes $C_1, C_2 > 0$ tales que $C_1\, g(x) \leq |f(x)| \leq C_2\, g(x)$ para todo x suficientemente grande.

La notación $f(x) = o(g(x)) \quad (x \to \infty)$ significa que el cociente $f(x)/g(x)$ tiende a 0 cuando $x \to +\infty$. En particular, si $a_1, a_2, \ldots$ es una sucesión de números complejos, entonces la "igualdad" $a_n = 1 + o(1)$ indica que $a_n \to 1$ cuando $n \to \infty$ (del término $o(1)$ sólo puede decirse que tiene a 0; sobre su signo, por ejemplo, no puede decirse mucho en términos generales).

Finalmente, la notación $T = N^{o(1)}$ indica que para todo $\varepsilon > 0$ existe una constante $c_\varepsilon > 0$ (que sólo depende de $\varepsilon > 0$) tal que $T \leq c_\varepsilon\, N^{\varepsilon}$.

Capítulo 1

La distribución de factoriales módulo un primo

1.1. Preludio

Sean $\varepsilon \in (0,1)$, p un número primo y L y N números enteros tales que $0 < L+1 < L+N < p$. Consideremos el conjunto

$$\mathcal{A}(L,N) := \{n! \pmod p \colon L+1 \leq n \leq L+N\}.$$

Puesto que

$$\{1\} \cup \{L+2, \ldots, L+N\} \pmod p \subseteq \left\{\frac{a_1}{a_2} \colon a_1, a_2 \in \mathcal{A}(L,N)\right\}$$

se sigue que

$$|\mathcal{A}(L,N)| \geq N^{\frac{1}{2}}. \tag{1.1}$$

En particular, de esto se desprende que $|\mathcal{A}(0,p-1)| \geq (p-1)^{\frac{1}{2}}$. Por otro lado, del resultado de V. García en [14] sobre la cardinalidad del conjunto $\{n!m! \pmod p \colon 1 \leq n,m \leq p\}$ se sabe que $|\mathcal{A}(0,p-1)| > cp^{\frac{1}{2}}$ para cualquier constante $c < \sqrt{\frac{41}{24}}$ y cualquier número primo p suficientemente grande.

O. Klurman y M. Munsch demostraron en [19] la siguiente mejora a la estimación trivial en (1.1):

$$|\mathcal{A}(L,N)| \geq \sqrt{\frac{3}{2}} N^{\frac{1}{2}} \tag{1.2}$$

para $N \in (p^{\frac{1}{4}+\varepsilon}, p)$.

Utilizando una consecuencia de una célebre estimación de E. Bombieri para sumas exponenciales sobre curvas algebraicas, demostraremos en este capítulo que si $p^{\frac{1}{2}+\varepsilon} < N < p^{1-\varepsilon}$, entonces la constante en (1.2) puede hacerse arbitrariamente grande; este resultado lo aplicaremos a su tiempo al problema de la representación de clases de restos módulo p como productos de factoriales de números naturales de tamaño restringido. Enunciamos a continuación el primer teorema que estableceremos en este capítulo.

Teorema 1.1. *Si $\varepsilon \in (0, \frac{1}{4})$ y $N \in (p^{\frac{1}{2}+\varepsilon}, p^{1-\varepsilon})$, entonces existe una constante $c_0 := c_0(\varepsilon) > 0$ tal que*

$$\left|\frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}\right| > c_0 N \log N.$$

Nótese que de este teorema se desprende inmediatamente que si $\varepsilon \in (0, \frac{1}{4})$ y $p^{\frac{1}{2}+\varepsilon} < N < p^{1-\varepsilon}$, entonces

$$|\mathcal{A}(L,N)| > (c_0 N \log N)^{\frac{1}{2}} = (c_0^{\frac{1}{2}} \log^{\frac{1}{2}} N) N^{\frac{1}{2}} \tag{1.3}$$

para alguna constante $c_0 := c_0(\varepsilon) > 0$.

La estimación (1.3) ha permitido avanzar *el estado del arte* en el problema de la representación de elementos de $\mathbb{F}_p \setminus \{0\}$ como productos de factoriales de números naturales de tamaño restringido.

M. Garaev, F. Luca e I. Shparlinski habían demostrado en [12] que si $\lambda \not\equiv 0 \pmod{p}$ entonces λ puede representarse en la forma

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

para algunos números naturales $n_1, \dots, n_7 \leq c_1 p^{\frac{11}{12}+\varepsilon}$ donde $c_1 := c_1(\varepsilon)$ es una constante positiva. V. García debilitaría después la condición sobre el valor absoluto de los n_i a $n_i \ll p^{\frac{11}{12}}$ en [15]. Apelando al Teorema 1.1 es posible superar estas contribuciones.

Teorema 1.2. *Cualquier número entero λ que no es divisible por p puede representarse en la forma*

$$\lambda \equiv n_1! \cdots n_7! \pmod{p},$$

para algunos números naturales $n_1, \dots, n_7$ que satisfacen

$$\max\{n_1, \dots, n_7\} \ll \frac{p^{11/12}}{(\log p)^{1/2}}.$$

Este es el segundo resultado fuerte que demostraremos en este capítulo.

1.2. Lemas preliminares

Lema 1.1 (Bombieri, 1966; cf. [2, Teorema 6] o [4, Teorema 2])**.** *Sean $(b_1, b_2) \in \mathbb{F}_p \times \mathbb{F}_p \setminus \{(0,0)\}$ y $f(x,y) \in \mathbb{F}_p[x,y]$ un polinomio de grado $d \geq 1$ con esta propiedad: no existe $c \in \mathbb{F}_p$ para el cual se verifique que $b_1 x + b_2 y + c \mid f(x,y)$. Se cumple entonces la estimación*

$$\left| \sum_{f(x,y)=0} e^{2\pi i \frac{b_1 x + b_2 y}{p}} \right| \leq 2d^2 p^{\frac{1}{2}}.$$

El siguiente lema se debe a I. Z. Ruzsa (ver [22, pág. 287]) y será instrumental en la demostración del Teorema 1.2.

Lema 1.2 (Desigualdad triangular de Ruzsa)**.** *Si X, Y, Z son subconjuntos finitos y no vacíos de un grupo abeliano G, entonces se tiene que*

$$\left|\frac{X}{Y}\right| \leq \frac{|XZ||ZY|}{|Z|}.$$

Otro resultado al que se recurrirá en la demostración del Teorema 1.2 es la estimación para sumas de caracteres con factoriales establecida por V. García en el teorema 3.1 de [15].

Lema 1.3 (García, 2008)**.** *Si χ es un caracter no principal módulo p y N un número natural menor que p, entonces*

$$\left|\sum_{m\leq N}\sum_{m\leq N}\chi((m+n)!)\right| \ll N^{\frac{7}{4}}p^{\frac{1}{8}}.$$

Demostración. Notemos en primera instancia que si $N^2 \leq p$ entonces la estimación es incluso más débil que la estimación trivial. Consecuentemente, podemos suponer en lo sucesivo que $N^2 > p$.

Sea K un número natural menor que N que especificaremos más adelante. Si $k \in [1, K] \cap \mathbb{N}$, entonces al considerar el *shift* $m+n \mapsto m+n+k$ se tiene que

$$\sum_{n\leq N}\chi((m+n)!) = \sum_{n\leq N}\chi((m+n+k)!) + \sum_{1\leq n\leq K}\chi((m+n)!) - \sum_{N<n\leq N+K}\chi((m+n)!).$$

De esta identidad se sigue que

$$\sum_{m\leq N}\sum_{N\leq N}\chi((m+n)!) = \sum_{m\leq N}\sum_{n\leq N}\chi((m+n+k)!) + O(KN),$$

lo cual implica a su vez que

$$\sum_{m\leq N}\sum_{n\leq N}\chi((m+n)!) = \frac{1}{K}\sum_{k=1}^{K}\sum_{m\leq N}\sum_{n\leq N}\chi((m+n+k)!) + O(KN). \tag{1.4}$$

Denotemos con $\mathcal{S}$ al módulo de $\sum_{m\leq N}\sum_{n\leq N}\chi((m+n)!)$. Aplicando la desigualdad de Cauchy-Schwarz en (1.4) se llega a que

$$\begin{aligned}
\mathcal{S}^2 &\ll \frac{1}{K^2}\left|\sum_{k=1}^{K}\sum_{m\leq N}\sum_{n\leq N}\chi((m+n+k)!)\right|^2 + K^2N^2 \\
&\leq \frac{N^2}{K^2}\sum_{m\leq N}\sum_{n\leq N}\left|\sum_{k=1}^{K}\chi((m+n+k)!)\right|^2 + K^2N^2 \\
&= \frac{N^2}{K^2}\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\sum_{m\leq N}\sum_{n\leq N}\chi((m+n+k_1)!)\overline{\chi((m+n+k_2)!)} + K^2N^2. \qquad (1.5)
\end{aligned}$$

Así pues, todo se ha reducido a estimar

$$\sum_{m\le N}\sum_{n\le N}\chi((m+n+k_1)!)\overline{\chi((m+n+k_2)!)} =: \mathfrak{S}(k_1,k_2)$$

para $(k_1,k_2)\in\{1,\dots,K\}\times\{1,\dots,K\}$. Si con $J(z)$ denotamos al número de soluciones de la congruencia

$$m+n\equiv z \pmod p, \quad 1\le m,n\le N$$

entonces resulta que

$$\begin{aligned}
\mathfrak{S}(k_1,k_2) &= \sum_{m\le N}\sum_{n\le N}\chi((m+n+k_1)!)\overline{\chi((m+n+k_2)!)}\\
&= \sum_{z=0}^{p-1} J(z)\,\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\\
&= \sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\sum_{m=1}^{N}\sum_{n=1}^{N}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(z-(m+n))}{p}}\\
&= \frac{1}{p}\sum_{a=0}^{p-1}\sum_{m=1}^{N}\sum_{n=1}^{N}\sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\,e^{2\pi i\frac{az}{p}}\,e^{-2\pi i\frac{am}{p}}\,e^{-2\pi i\frac{an}{p}}
\end{aligned}$$

y por lo tanto

$$|\mathfrak{S}(k_1,k_2)|\le\frac{1}{p}\sum_{a=0}^{p-1}\left|\sum_{m=1}^{N}e^{2\pi i\frac{am}{p}}\right|\left|\sum_{n=1}^{N}e^{2\pi i\frac{an}{p}}\right|\left|\sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\,e^{2\pi i\frac{az}{p}}\right|.$$

Cuando $k_1=k_2=k$, la desigualdad anterior deviene en

$$|\mathfrak{S}(k_1,k_2)|\le\frac{N^2}{p}\sum_{a=0}^{p-1}\left|\sum_{z=0}^{p-1}\chi((z+k_1)!)\overline{\chi((z+k_2)!)}\,e^{2\pi i\frac{az}{p}}\right| = \frac{N^2}{p}\left|\sum_{z=0}^{p-1}e^{2\pi i\frac{az}{p}}-e^{2\pi i\frac{az_{k_1}}{p}}\right|$$

donde z_{k_1} es el elemento en $\{0,1,\dots,p-1\}$ tal que $z_{k_1}+k_1\equiv 0 \pmod p$. En vista de que

$$\begin{aligned}
\sum_{a=0}^{p-1}\left|\sum_{z=0}^{p-1}e^{2\pi i\frac{az}{p}}-e^{2\pi i\frac{az_{k_1}}{p}}\right| &= (p-1)+\sum_{a=1}^{p-1}\left|\sum_{z=0}^{p-1}e^{2\pi i\frac{az}{p}}-e^{2\pi i\frac{az_{k_1}}{p}}\right|\\
&= (p-1)+\sum_{a=1}^{p-1}\left|-e^{2\pi i\frac{az_{k_1}}{p}}\right|\\
&= 2(p-1),
\end{aligned}$$

se concluye que

$$|\mathfrak{S}(k,k)| < 2N^2 \tag{1.6}$$

para cada $k \in \{1,\dots,K\}$.

Consideremos ahora el caso en que $k_1 > k_2$. Apelando a propiedades básicas de los caracteres de Dirichlet módulo p tiene cabida aseverar que

$$\begin{aligned}\sum_{z=0}^{p-1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, e^{2\pi i\frac{az}{p}} &= \sum_{0\le z<p-k_1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, e^{2\pi i\frac{az}{p}} \\ &+ \sum_{p-k_1\le z\le p-1} \chi((z+k_1)\cdots 1)\overline{\chi((z+k_2)\cdots 1)}\, e^{2\pi i\frac{az}{p}} \\ &= \sum_{0\le z<p-k_1} \chi((z+k_2+1)\cdots(z+k_1))\, e^{2\pi i\frac{az}{p}},\end{aligned}$$

de lo cual se desprende que

$$\left|\sum_{z=0}^{p-1} \chi((z+k_1)!)\overline{\chi((z+k_2)!)}\, e^{2\pi i\frac{az}{p}}\right| \le \left|\sum_{z=0}^{p-1} \chi((z+k_2+1)\cdots(z+k_1))\, e^{2\pi i\frac{az}{p}}\right| + K.$$

De lo anterior y de la cota de A. Weil para sumas híbridas de caracteres (cf. [23, Teorema 2G]) se colige que si $k_1 > k_2$ entonces

$$\begin{aligned}|\mathfrak{S}(k_1,k_2)| &\le Kp^{-1/2}\sum_{a=0}^{p-1}\left|\sum_{m=1}^{N} e^{2\pi i\frac{am}{p}}\right|\left|\sum_{n=1}^{N} e^{2\pi i\frac{an}{p}}\right| \\ &= Kp^{-1/2}\sum_{a=0}^{p-1}\sum_{m=1}^{N}\sum_{n=1}^{N} e^{2\pi i\frac{a(m-n)}{p}} \\ &= Kp^{1/2}N. \end{aligned} \tag{1.7}$$

Combinando lo obtenido en (1.5), (1.6) y (1.7) se tiene que

$$\begin{aligned}\mathcal{S}^2 &\ll \frac{N^2}{K^2}\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}|\mathfrak{S}(k_1,k_2)| + K^2N^2\\ &\ll \frac{N^2}{K^2}\left(KN^2 + K^3p^{1/2}N\right) + K^2N^2\\ &= \frac{N^4}{K} + N^3p^{1/2}K + K^2N^2\\ &\ll \frac{N^4}{K} + N^3p^{1/2}K.\end{aligned}$$

Al hacer $K := \lfloor N^{1/2}/p^{1/4}\rfloor$ la estimación previa deviene en

$$\mathcal{S}^2 \ll N^{7/2}p^{1/4}$$

y la prueba termina. ∎

1.3. Demostración del Teorema 1.1

Para $j \in \{1,2,\ldots,M\}$, definamos

$$X_j := \left\{\prod_{i=1}^{j}(x+L+i) \pmod p\colon 1 \le x < 0.6N\right\}.$$

Claramente, para cada $j \in \{1,2,\ldots,M\}$ se cumple que

$$X_j \subseteq \frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)};$$

a fin de obtener la estimación en cuestión para el cardinal de $\frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}$, lo que haremos es estimar inferiormente el cardinal de $X_1 \cup \cdots \cup X_M$ de una manera *conveniente*.

Como $p(x) := \prod_{i=1}^{j}(x+L+i)$ es un polinomio mónico de coeficientes enteros y grado j, entonces

$$|X_j| \ge \frac{N}{2j}. \tag{1.8}$$

Afirmamos que para cada $j \geq 2$ es válida la estimación:

$$|X_j \setminus (X_1 \cup \cdots \cup X_{j-1})| \geq \frac{N}{3j}. \tag{1.9}$$

En efecto, en vista de que

$$\begin{aligned} |X_j \setminus (X_1 \cup \cdots \cup X_{j-1})| &= |X_j \setminus ((X_j \cap X_1) \cup \cdots \cup (X_j \cap X_{j-1}))| \\ &= |X_j| - |(X_j \cap X_1) \cup \cdots \cup (X_j \cap X_{j-1})| \\ &\geq |X_j| - |X_j \cap X_1| - \cdots - |X_j \cap X_{j-1}|, \end{aligned} \tag{1.10}$$

al invocar la desigualdad (1.8) se llega a que

$$\begin{aligned} |X_j \setminus (X_1 \cup \cdots \cup X_{j-1})| &\geq |X_j| - |X_j \cap X_1| - \cdots - |X_j \cap X_{j-1}| \\ &\geq \frac{N}{2j} - |X_j \cap X_1| - \cdots - |X_j \cap X_{j-1}|. \end{aligned}$$

Así pues, para establecer (1.9) basta con demostrar que

$$|X_j \cap X_k| \leq \frac{N}{6j^2}$$

para cada $k \in \{1, \ldots, j-1\}$; esto es de lo que nos ocuparemos continuación. Denotemos con $J(j,k)$ al número de soluciones de la congruencia

$$\prod_{i=1}^{j}(x+L+i) \equiv \prod_{i=1}^{k}(y+L+i) \pmod{p}, \quad 1 \leq x, y < 0.6N.$$

Por un lado resulta claro que

$$|X_j \cap X_k| \leq J(j,k). \tag{1.11}$$

Por otro lado, haciendo $f(x,y) = \prod_{i=1}^{j}(x+L+i) - \prod_{i=1}^{k}(y+L+i) \in \mathbb{F}_p[x,y]$, podemos expresar el número $J(j,k)$ mediante sumas exponenciales de la siguiente manera

$$\begin{aligned} J(j,k) = \sum_{\substack{1 \leq x,y < 0.6N \\ f(x,y)=0}} 1 &= \frac{1}{p^2} \sum_{f(x,y)=0} \left(\sum_{1 \leq u < 0.6N} \sum_{b_1=0}^{p-1} e^{2\pi i \frac{b_1(x-u)}{p}} \right) \left(\sum_{1 \leq v < 0.6N} \sum_{b_2=0}^{p-1} e^{2\pi i \frac{b_2(y-v)}{p}} \right) \\ &= \frac{1}{p^2} \sum_{b_1=0}^{p-1} \sum_{b_2=0}^{p-1} \sum_{1 \leq u < 0.6N} \sum_{1 \leq v < 0.6N} \sum_{f(x,y)=0} e^{2\pi i \frac{(b_1(x-u)+b_2(y-v))}{p}}. \end{aligned}$$

La cota superior trivial para el número de soluciones de la ecuación

$$f(x,y)=0, \quad (x,y)\in \mathbb{F}_p\times\mathbb{F}_p$$

es jp; de esto y de la estimación elemental

$$\sum_{b=1}^{p-1}\left|\sum_{1\le z<0.6N} e^{2\pi i\frac{bz}{p}}\right| < p\log p$$

(ver, por ejemplo, [13, pág. 134]) se obtiene que

$$\begin{aligned} J(j,k) &= \frac{1}{p^2}\sum_{1\le u<0.6N}\sum_{1\le v<0.6N}\sum_{f(x,y)=0} 1 \\ &+ \frac{1}{p^2}\sum_{\substack{0\le b_1,b_2\le p-1\\(b_1,b_2)\neq(0,0)}}\sum_{1\le u<0.6N} e^{2\pi i\frac{b_1(-u)}{p}}\sum_{1\le v<0.6N} e^{2\pi i\frac{b_2(-v)}{p}}\sum_{f(x,y)=0} e^{2\pi i\frac{b_1x+b_2y}{p}} \\ &< \frac{(0.6N)^2 jp}{p^2} + 2.2\,(\log p)^2 \max_{\substack{0\le b_1,b_2\le p-1\\(b_1,b_2)\neq(0,0)}}\left|\sum_{f(x,y)=0} e^{2\pi i\frac{b_1x+b_2y}{p}}\right| \\ &< \frac{jN^2}{p} + 2.2\,(\log p)^2 \max_{\substack{0\le b_1,b_2\le p-1\\(b_1,b_2)\neq(0,0)}}\left|\sum_{f(x,y)=0} e^{2\pi i\frac{b_1x+b_2y}{p}}\right|. \end{aligned}$$

Para estimar la suma en la línea previa recurrimos al Lema 1.1. Notemos que si $(A,B,C)\in\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p$ y $(A,B)\in\mathbb{F}_p\times\mathbb{F}_p\setminus\{(0,0)\}$ entonces $Ax+By+C\nmid f(x,y)$ pues, en caso contrario, se tendría que

$$(x+L+1)\cdots(x+L+j)-(y+L+1)\cdots(y+L+k)=(Ax+By+C)g(x,y) \tag{1.12}$$

para algún $g(x,y)\in\mathbb{F}_p[x,y]$. Si $B\neq 0$ y B^* es su inverso multiplicativo en $\mathbb{F}_p$, al hacer $y=(-Ax-C)B^*$ y sustituir en (1.12) se llega a que

$$(x+L+1)\cdots(x+L+j)-((-Ax-C)B^*+L+1)\cdots((-Ax-C)B^*+L+k)=0,$$

lo que es decididamente absurdo (¡recuérdese que $j>k\ge 1$!). Si $B=0$ entonces $A\neq 0$; al hacer $x=-CA^*$ y sustituir después en (1.12) se tiene que

$$(-CA^*+L+1)\cdots(-CA^*+L+j)-(y+L+1)\cdots(y+L+k)=0$$

lo cual es un absurdo también. Así pues, en vista de que $f(x,y)$ satisface las condiciones del Lema 1.1, se colige que

$$J(j,k) \;<\; \frac{jN^2}{p} + 4.4\,(\log p)^2 j^2 p^{\frac{1}{2}}.$$

Luego, eligiendo $M := \left\lfloor \text{mín}\left\{ \left(\frac{1}{12}\cdot\frac{p}{N}\right)^{\frac{1}{3}}, \left(\frac{p^{0.5\varepsilon}}{12}\right)^{\frac{1}{4}} \right\} \right\rfloor$, se llega a que

$$J(j,k) < \frac{N}{6j^2}.$$

Aplicando esta desigualdad en (1.11) se desprende que $|X_j \cap X_k| < \frac{N}{6j^2}$; al poner esto en (1.10) se obtiene que

$$|X_j \setminus (X_1 \cup \cdots \cup X_{j-1})| > \frac{N}{2j} - \frac{(j-1)N}{6j^2} > \frac{N}{2j} - \frac{N}{6j} = \frac{N}{3j}$$

que es justo lo que se había anunciado en (1.9). En conclusión:

$$\begin{aligned}
\left|\frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}\right| &\geq |X_1 \cup \cdots \cup X_M| \\
&= |X_1| + \sum_{j=2}^{M} |X_j \setminus (X_1 \cup \cdots \cup X_{j-1})| \\
&> \sum_{j=1}^{M} \frac{N}{3j} \\
&\geq \frac{N}{3}\int_1^{M+1} \frac{1}{t}\,dt \\
&= \frac{N}{3}\log(M+1) \\
&\geq c_0\, N \log N
\end{aligned}$$

para alguna constante $c_0 := c_0(\varepsilon) > 0$. ∎

1.4. Demostración del Teorema 1.2

Sean $\lambda \not\equiv 0 \pmod{p}$, $N \in (p^{0.51}, p^{0.99}) \cap \mathbb{N}$ y $A := \mathcal{A}(0,N)$. Por el Teorema 1.1,

$$\left|\frac{A}{A}\right| > c_0\, N \log N$$

para alguna constante $c_0 > 0$. De esto y la desigualdad triangular de Ruzsa se desprende que

$$|AA|^2 \geq |A| \left|\frac{A}{A}\right| > (c_0 N \log N)^{\frac{3}{2}}.$$

En consecuencia:

$$|AA| > c_1 (N \log p)^{\frac{3}{4}} \tag{1.13}$$

para alguna constante $c_1 := c_1(\varepsilon) > 0$.

Hagamos $\mathcal{I} := \{1, \ldots, N\}$ y denotemos con J al número de soluciones de la congruencia

$$(n_1 + m_1)!(n_2 + m_2)!(n_3 + m_3)!\, xy \equiv \lambda \pmod{p}$$

sujeta a las restricciones

$$n_1, n_2, n_3, m_1, m_2, m_3 \in \mathcal{I}, \quad x, y \in AA.$$

Se trata de demostrar que si N se elige de manera *conveniente* entonces $J > 0$. Por propiedades básicas de los caracteres, el número J puede ser expresado del siguiente modo:

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{\substack{n_1,n_2,n_3,\\ m_1,m_2,m_3}} \sum_{x,y \in AA} \chi((n_1 + m_1)!(n_2 + m_2)!(n_3 + m_3)!\, xy) \chi(\lambda^{-1}).$$

Separando el término que corresponde al caracter principal se obtiene que

$$J \geq \frac{N^6 |AA|^2}{p-1} - \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{n,m \in \mathcal{I}} \chi((n+m)!) \right|^3 \left| \sum_{x \in AA} \chi(x) \right|^2. \tag{1.14}$$

Al aplicar el Lema 1.3 para estimar inferiormente el lado derecho de (1.14) se llega a que

$$\begin{aligned} J &\geq \frac{N^6 |AA|^2}{p-1} - c_2 N^{\frac{21}{4}} p^{\frac{3}{8}} |AA| \\ &\geq \frac{N^{\frac{21}{4}} |AA|}{p-1} \left(|AA| N^{\frac{3}{4}} - c_2 p^{\frac{11}{8}} \right). \end{aligned}$$

De esto y (1.13) se sigue que

$$J \geq \frac{N^{\frac{21}{4}}|AA|}{p-1}\left(c_1 N^{\frac{3}{2}}(\log p)^{\frac{3}{4}} - c_2 p^{\frac{11}{8}}\right).$$

La conclusión deseada se obtiene al hacer (por ejemplo)

$$N = \left\lceil \left(\frac{c_2}{c_1}\right)^{\frac{2}{3}} p^{\frac{11}{12}}(\log p)^{-\frac{1}{2}} \right\rceil.$$

■

1.5. Observaciones ulteriores

Como hemos mencionado previamente, O. Klurman y M. Munsch demostraron en [19] que la estimación

$$|\mathcal{A}(L,N)| \geq cN^{\frac{1}{2}}$$

vale siempre que $N \in (p^{\frac{1}{4}+\varepsilon}, p)$ y que $c \leq \sqrt{\frac{3}{2}}$. Esbozaremos a continuación cómo es que, apelando a resultados de los trabajos [5, 7], es posible relajar la condición $N > p^{\frac{1}{4}+\varepsilon}$ de Klurman y Munsch. Supongamos que $N < p^{\frac{2}{3}}$ es suficientemente grande. Denotemos con $\mathcal{I}$ al conjunto $\{L+2, \ldots, L+N\} \pmod p$. En vista de que $\{1\} \cup \{L+2, \ldots, L+N\} \pmod p \subseteq \{\frac{a_1}{a_2} : a_1, a_2 \in \mathcal{A}(L,N)\}$, por un lado tenemos que

$$\mathcal{I} \subseteq \frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}, \quad \mathcal{I}^{-1} \subseteq \frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}.$$

Por otra parte, del teorema 3 de [5] o del teorema 1 de [7] se sigue que $|\mathcal{I} \cap \mathcal{I}^{-1}| < N^{1-\delta}$ para alguna constante absoluta $\delta > 0$. Así entonces,

$$\left|\frac{\mathcal{A}(L,N)}{\mathcal{A}(L,N)}\right| \geq |\mathcal{I} \cup \mathcal{I}^{-1}| = |\mathcal{I}| + |\mathcal{I}^{-1}| - |\mathcal{I} \cap \mathcal{I}^{-1}| > 2N - 2 - N^{1-\delta}$$

y, en consecuencia, $|\mathcal{A}(L,N)| > (\sqrt{2} + o(1))N^{\frac{1}{2}}$ cuando $N \to \infty$.

Finalmente, en la demostración del Teorema 1.2 utilizamos el hecho de que si $N < p^{1-\varepsilon}$ entonces

$$|\mathcal{A}(0,N)\mathcal{A}(0,N)| \gg (N\log N)^{\frac{3}{4}}.$$

Esta estimación puede mejorarse considerablemente para valores *pequeños* de N. Supongamos por ejemplo que $N < p^{\frac{1}{2}}$. Para cualesquiera $m, n \in [1,N] \cap \mathbb{N}$ se tiene que

$$\frac{n}{m} \pmod p \in \frac{\mathcal{A}(0,N)\mathcal{A}(0,N)}{\mathcal{A}(0,N)\mathcal{A}(0,N)}.$$

Luego, notando que a distintos números racionales n/m, donde $1 \leq n, m < p^{\frac{1}{2}}$, les corresponden distintas clases $n/m \pmod p$ (bajo la aplicación natural), se desprende que

$$\begin{aligned}\left|\frac{\mathcal{A}(0,N)\mathcal{A}(0,N)}{\mathcal{A}(0,N)\mathcal{A}(0,N)}\right| &\geq \left|\left\{\frac{n}{m} : m,n \in [1,N]\cap\mathbb{N},\ \mathrm{mcd}(m,n)=1\right\}\right| \\ &= \left(\frac{6}{\pi^2}+o(1)\right)N^2\end{aligned}$$

cuando $N \to \infty$. Así pues, para $N < p^{\frac{1}{2}}$ se verifica que $|\mathcal{A}(0,N)\mathcal{A}(0,N)| \gg N$.

Capítulo 2

Puntos sobre curvas en pequeñas cajas

2.1. Planteamiento básico del problema

Sean p un número primo y f un polinomio de coeficientes enteros cuyo coeficiente principal no es divisible por p. Supongamos que $\deg(f) = m \geq 3$ y que M es un número natural del intervalo $[1, p)$. El tema principal en este capítulo será la estimación del número de soluciones $I_f(M; R, S)$ de la congruencia

$$y^2 \equiv f(x) \pmod{p} \tag{2.1}$$

que pertenecen a

$$[R+1, R+M] \times [S+1, S+M]. \tag{2.2}$$

Cuando el polinomio $F(x, y) = y^2 - f(x)$ es absolutamente irreducible es posible obtener una fórmula asintótica para $I_f(M; R, S)$ expresando esta cantidad mediante sumas exponenciales y apelando después a la célebre estimación de A. Weil para el cardinal del conjunto $\mathcal{Z}_F := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \colon F(x, y) \equiv 0 \pmod{p}\}$.

Más específicamente, se tiene que[1]

$$\begin{aligned} I_f(M;R,S) &= \sum_{\substack{R+1\le x\le R+M,\, S+1\le y\le S+M\\ (x,y)\in\mathcal{Z}_F}} 1 \\ &= \frac{1}{p^2}\sum_{(x,y)\in\mathcal{Z}_F}\left(\sum_{R+1\le a\le R+M}\sum_{r=1}^{p} e^{2\pi i\frac{r(x-a)}{p}}\right)\left(\sum_{S+1\le b\le S+M}\sum_{t=1}^{p} e^{2\pi i\frac{t(y-b)}{p}}\right) \\ &= \frac{1}{p^2}\sum_{r=1}^{p}\sum_{t=1}^{p}\left(\sum_{(x,y)\in\mathcal{Z}_F} e^{2\pi i\frac{(rx+ty)}{p}}\right)\left(\sum_{R+1\le a\le R+M} e^{-2\pi i\frac{ra}{p}}\sum_{S+1\le b\le S+M} e^{-2\pi i\frac{tb}{p}}\right) \\ &= \frac{M^2}{p^2}|\mathcal{Z}_F| \\ &+ O\left(\frac{1}{p^2}\sum_{(r,t)\in\mathbb{F}_p^2\setminus\{(0,0)\}}\sum_{(x,y)\in\mathcal{Z}_F} e^{2\pi i\frac{(rx+ty)}{p}}\sum_{R+1\le a\le R+M} e^{-2\pi i\frac{ra}{p}}\sum_{S+1\le b\le S+M} e^{-2\pi i\frac{tb}{p}}\right). \end{aligned}$$

Luego, de la fórmula de Weil

$$|\mathcal{Z}_F| = p + O(p^{\frac{1}{2}}),$$

de la estimación de E. Bombieri (ver [2, Teorema 6] o [4, Teorema 2])

$$\max_{(r,t)\in\mathbb{F}_p^2\setminus\{(0,0)\}}\left|\sum_{(x,y)\in\mathcal{Z}_F} e^{2\pi i\frac{(rx+ty)}{p}}\right| \ll_m p^{1/2}$$

y de la estimación elemental (ver, por ejemplo, [13, pág. 134])

$$\sum_{r=1}^{p-1}\left|\sum_{R+1\le a\le R+M} e^{-2\pi i\frac{ra}{p}}\right| \ll p\log p$$

se desprende que

$$I_f(M;R,S) = \frac{M^2}{p} + O(p^{\frac{1}{2}}(\log p)^2) \tag{2.3}$$

donde la constante implicada depende únicamente de m. Es fácil ver que en esta fórmula el término de error domina al término principal cuando $M \le p^{\frac{3}{4}}\log p$;

[1] Compárese con lo hecho con $J(j,k)$ en la demostración del Teorema 1.1.

por otro lado, si $M \leq p^{\frac{1}{2}}(\log p)^2$, entonces la fórmula es más débil que la acotación superior trivial $I_f(M; R, S) \leq 2M$.

En este capítulo demostraremos una estimación no trivial para $I_f(M; R, S)$ cuando $M < p^{\frac{1}{3}-\varepsilon}$. En particular, en el caso $m = 3$, el rango para M sobre el que podremos garantizar esta estimación será más extenso que aquel que se conocía de trabajos anteriores.

Un segundo problema que abordaremos en este capítulo será el estudio del número de soluciones $J_f(M; R, S)$ del problema

$$y \equiv f(x) \pmod{p}, \quad (x, y) \in [R+1, R+M] \times [S+1, S+M]$$

donde f es un polinomio de coeficientes enteros de grado $m \geq 2$ cuyo coeficiente principal no es múltiplo del número primo p. Presentaremos una nueva estimación superior para $J_f(M; R, S)$ que para ciertos grados mejora la publicada en [8].

2.2. Resultados obtenidos

Teorema 2.1. *La estimación*

$$I_f(M; R, S) \leq M^{\frac{1}{3}+o(1)} + \frac{M^{\frac{5}{3}+o(1)}}{p^{\frac{1}{6}}} \qquad (M \to \infty)$$

se cumple uniformemente para todo $f \in \mathbb{F}_p[X]$ *de grado* 3.

Como una consecuencia inmediata de este teorema se tiene que si $M \ll p^{\frac{1}{8}}$ entonces

$$I_f(M; R, S) \leq M^{\frac{1}{3}+o(1)};$$

cabe mencionar que el teorema 5.1 de [9] garantiza esta conclusión sólo cuando $M \ll p^{\frac{1}{9}}$. Se hace énfasis en tener información sobre el rango en el cual se cumple que $I_f(M; R, S) \leq M^{\frac{1}{3}+o(1)}$ pues esa estimación es esencialmente la mejor posible.

De hecho, es claro que para cualquier $M \in [1, p) \cap \mathbb{N}$, al tomar $f(X) = X^m$, se obtiene que

$$I_f(M; 0, 0) \geq \left|\left\{(t^2, t^m) \colon 1 \leq t \leq M^{\frac{1}{m}}\right\}\right| = \left\lfloor M^{\frac{1}{m}} \right\rfloor \gg M^{\frac{1}{m}}.$$

Por otro lado, si $M < p^{\frac{1}{4}-\varepsilon_0}$ para algún $\varepsilon_0 > 0$, el Teorema 2.1 implica la estimación no trivial $I_f(M; R, S) \ll M^{1-\delta}$ para alguna $\delta > 0$ que depende únicamente de ε_0. Aunque no resulta difícil convencerse de la validez de esta aseveración esbozamos a continuación una demostración de ella. El Teorema 2.1 implica que para cada $\varepsilon \in (0, \frac{2}{3})$ existe una constante positiva c_ε tal que

$$I_f(M; R, S) \leq c_\varepsilon \left(M^{1/3+\varepsilon} + \frac{M^{5/3+\varepsilon}}{p^{1/6}} \right).$$

Si para algún ε en el intervalo en cuestión se observa que el primer término de la expresión en paréntesis es mayor o igual que el segundo entonces $I_f(M; R, S) \ll M^{1/3+\varepsilon}$. Así pues, en este caso se verifica que $I_f(M; R, S) \ll M^{1-\delta}$ para cada $\delta \in (0, \frac{2}{3} - \varepsilon)$. Ahora bien, si para cada $\varepsilon \in (0, \frac{2}{3})$ resulta que el segundo término de la expresión en paréntesis es mayor o igual que el primero entonces, eligiendo $\varepsilon \in (0, \frac{2}{3})$ de tal modo que tenga lugar la desigualdad $\varepsilon < \frac{2}{3}\varepsilon_0$, se obtiene que

$$\begin{aligned} I_f(M; R, S) &\ll \frac{M^{5/3+\varepsilon}}{p^{1/6}} \\ &= \frac{M^{1+\varepsilon} M^{2/3}}{p^{1/6}} \\ &< \frac{M^{1+\varepsilon} p^{(2/3)(1/4-\varepsilon_0)}}{p^{1/6}} \\ &< M^{1+\varepsilon} M^{-(2/3)\varepsilon_0} \\ &= M^{1-((2/3)\varepsilon_0 - \varepsilon)}. \end{aligned}$$

Luego, al hacer $\delta := \frac{2}{3}\varepsilon_0 - \varepsilon$ se llega a la conclusión deseada.

Las consideraciones anteriores redundan en una mejora de la condición $M < p^{\frac{1}{5}-\varepsilon}$ que ya podía inferirse de [9, Teorema 5.1]. Por otra parte, la cota en el teorema que sigue es no trivial para $M < p^{\frac{1}{3}-\varepsilon}$.

Teorema 2.2. *La estimación*

$$I_f(M;R,S) \leq M^{\frac{1}{3}+o(1)} + \left(\frac{M^3}{p}\right)^{\frac{1}{16}} M^{1+o(1)} \qquad (M \to \infty)$$

se cumple uniformemente para todo $f \in \mathbb{F}_p[X]$ *de grado* 3.

La prueba de este teorema depende de resultados de geometría de números, de las contribuciones recientes de T. Wooley en torno al teorema del valor medio de Vinogradov (ver, por ejemplo, [27]) y de algunos teoremas de aproximación diofantina. La manera en que aplicamos la geometría de números es similar a la aplicación que de ella se hace en [3].

De los dos teoremas anteriores se desprende el corolario:

Corolario 2.1. *La estimación*

$$I_f(M;R,S) \leq M^{1+o(1)} \begin{cases} M^{-2/3} & si \;\; M < p^{1/8} \\ (M^4/p)^{1/6} & si \;\; p^{1/8} \leq M < p^{5/23} \\ (M^3/p)^{1/16} & si \;\; p^{5/23} \leq M < p^{1/3} \end{cases}$$

se cumple uniformemente para todo $f \in \mathbb{F}_p[X]$ *de grado* 3.

El resultado que se enuncia a continuación indica que cuando $\deg(f) \geq 4$ también tenemos una acotación no trivial para $I_f(M;R,S)$ en el rango $M < p^{\frac{1}{3}-\varepsilon}$. A fin de formularlo definimos primero $J_{k,m}(H)$ como el número de soluciones del siguiente sistema de m ecuaciones diofánticas en $2k$ variables

$$\begin{cases} x_1^m + \cdots + x_k^m = x_{k+1}^m + \cdots + x_{2k}^m \\ \vdots \\ x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k} \end{cases}$$

donde $1 \leq x_1, \ldots, x_{2k} \leq H$. Además, definimos $\kappa(m)$ como el menor número natural κ tal que, para todo $k \geq \kappa$, existe una constante $C(k,m)$ tal que

$$J_{k,m}(H) \leq C(k,m) H^{2k-\frac{m(m+1)}{2}+o(1)} \qquad (H \to \infty). \tag{2.4}$$

Es de mencionarse que, de acuerdo con el teorema 1.1 de [27], ahora se sabe que

$$\kappa(m) \leq m^2 - 1$$

para cada $m \geq 3$.

Teorema 2.3. *La estimación*

$$I_f(M;R,S) \leq M\left(\frac{M^3}{p}\right)^{\frac{1}{2\kappa(m)}+o(1)} + M^{1-\frac{m-3}{2\kappa(m)}+o(1)} \qquad (M \to \infty)$$

se cumple uniformemente para cada $f \in \mathbb{F}_p[X]$ *de grado mayor o igual que* 4.

En particular, para todo $\varepsilon > 0$ existe $\delta > 0$ que depende únicamente de ε y $\deg(f)$ tal que

$$I_f(M;R,S) \ll M^{1-\delta}$$

siempre que $M < p^{\frac{1}{3}-\varepsilon}$ y $\deg(f) \geq 4$.

Finalmente, estableceremos una nueva estimación para $J_f(M;R,S)$.

Teorema 2.4. *Sea* $f \in \mathbb{F}_p[X]$ *con* $\deg(f) = m \geq 2$. *Vale entonces la estimación:*

$$J_f(M;R,S) \ll \frac{M^2}{p} + M^{1-\frac{1}{2^{m-1}}}p^{o(1)} \qquad (p \to \infty).$$

Cabe mencionar que en [8] se estableció la cota

$$J_f(M;R,S) \ll M\left(\frac{M}{p}\right)^{\frac{1}{2\kappa(m)}+o(1)} + M^{1-\frac{m-1}{2\kappa(m)}+o(1)} \tag{2.5}$$

la cual es mejor que la garantizada por el Teorema 2.4 para valores grandes de m; sin embargo, para valores pequeños de m, el Teorema 2.4 proporciona estimaciones más finas que las implicadas por (2.5).

2.3. Lemas preliminares

2.3.1. Distribución uniforme y sumas exponenciales

El resultado que se enuncia a continuación es conocido y puede encontrarse por ejemplo en el capítulo 1 de [20].

Lema 2.1. *Sean $\gamma_1, \dots, \gamma_M$ elementos distintos del intervalo $[0,1]$. Para cada $K \in \mathbb{N}$ y $[\alpha, \beta] \subseteq [0,1]$ se tiene que*

$$\Big|\{n \in \{1,\dots,M\} \colon \gamma_n \in [\alpha,\beta]\}\Big| - M(\beta-\alpha) \ll \frac{M}{K} + \sum_{k=1}^{K} \left(\frac{1}{K} + \min\{\beta-\alpha, 1/k\}\right) \left|\sum_{n=1}^{M} e^{2\pi i k \gamma_n}\right|$$

Para aplicar el Lema 2.1 necesitamos la siguiente estimación para sumas de Weyl la cual puede encontrarse en [18, pág. 201].

Lema 2.2. *Sea $f \in \mathbb{R}[X]$ con $\deg(f) = m \geq 2$. Supóngase que el coeficiente principal de f es igual a ϑ. Se cumple entonces que*

$$\left|\sum_{n=1}^{M} e^{2\pi i f(n)}\right| \ll M^{1-\frac{m}{2^{m-1}}} \left(\sum_{-M<\ell_1,\dots,\ell_{m-1}<M} \min\{M, \|\vartheta m! \ell_1 \cdots \ell_{m-1}\|^{-1}\}\right)^{2^{1-m}}.$$

2.3.2. Puntos de coordenadas enteras sobre curvas planas

Eventualmente apelaremos a la estimación de Bombieri y Pila sobre el número de puntos de coordenadas enteras sobre curvas algebraicas planas:

Lema 2.3. *Supongamos que C es una curva plana absolutamente irreducible de grado $d \geq 2$ y que $H \geq e^{d^6}$. Se tiene que el número de puntos de coordenadas enteras sobre C y dentro del cuadrado $[0,H] \times [0,H]$ no excede a*

$$H^{\frac{1}{d}} e^{12\sqrt{d \log H \log\log H}}.$$

El lema que se presenta enseguida es un caso particular de un resultado más general de T. Wooley en [27].

Lema 2.4. *Sea $M \in \mathbb{N}$. El número de soluciones del sistema de ecuaciones*

$$\begin{aligned} x_1^3 + \cdots + x_8^3 &= x_9^3 + \cdots + x_{16}^3 \\ x_1^2 + \cdots + x_8^2 &= x_9^2 + \cdots + x_{16}^2 \\ x_1 + \cdots + x_8 &= x_9 + \cdots + x_{16} \end{aligned}$$

en números enteros x_i, con $|x_i| \leq M$, es a lo más $M^{10+o(1)}$.

Demostración. Si para $i \in \{1, \ldots, 16\}$ hacemos $x_i = X_i - M - 1$, donde cada X_i es un número entero en el intervalo $[1, 2M+1]$, entonces es claro que el número de soluciones del sistema de ecuaciones dado es igual al número de soluciones del sistema

$$\begin{aligned} X_1^3 + \cdots + X_8^3 &= X_9^3 + \cdots + X_{16}^3 \\ X_1^2 + \cdots + X_8^2 &= X_9^2 + \cdots + X_{16}^2 \\ X_1 + \cdots + X_8 &= X_9 + \cdots + X_{16} \end{aligned}$$

en números enteros X_i con $1 \leq X_i \leq 2M+1$. Este número se denota usualmente como $J_{8,3}(2M+1)$; como $\kappa(3) \leq 8$, de (2.4) se desprende que

$$J_{8,3}(2M+1) \leq C(8,3)(2M+1)^{16-\frac{3\cdot 4}{2}+o(1)} \ll M^{10+o(1)}.$$

∎

Cabe señalar que el Lema 2.4 puede ser formulado de manera más general pero para nuestros propósitos inmediatos basta contar con la versión recién demostrada.

2.3.3. Congruencias con abundantes soluciones

En la demostración del Teorema 2.1 se echará mano del siguiente resultado:

Lema 2.5. *Sean $f, g \in \mathbb{F}_p[X]$. Supongamos que* $\deg(f) = n$, $\deg(g) = m$ *y que $m \nmid n$. Si $x_1, \ldots, x_n$ son números enteros distintos entre sí módulo p y $y_1, \ldots, y_n$ son enteros arbitrarios, entonces la congruencia*

$$f(x) \equiv g(y) \pmod{p}, \qquad 0 \leq x, y < p \tag{2.6}$$

tiene a lo más $(m+1)n$ soluciones que satisfacen

$$\det \begin{pmatrix} x^n & x^{n-1} & \ldots & x & y \\ x_1^n & x_1^{n-1} & \ldots & x_1 & y_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_n^n & x_n^{n-1} & \ldots & x_n & y_n \end{pmatrix} \equiv 0 \pmod{p} \tag{2.7}$$

Demostración. Supongamos que (x, y) es una solución de (2.6) con $y \neq 0$ y que satisface (2.7). De la hipótesis de que $x_i \not\equiv x_j \pmod{p}$ siempre que i y j son elementos de $\{1, \ldots, n\}$, distintos, se desprende que

$$\det \begin{pmatrix} x_1^n & x_1^{n-1} & \ldots & x_1 \\ x_2^n & x_2^{n-1} & \ldots & x_2 \\ \vdots & \vdots & \ddots & \vdots \\ x_n^n & x_n^{n-1} & \ldots & x_n \end{pmatrix} = x_1 x_2 \cdots x_n \prod_{1 \leq i < j \leq n} (x_j - x_i) \not\equiv 0 \pmod{p};$$

en consecuencia, $y \equiv h(x) \pmod{p}$ para algún $h(X) \in \mathbb{F}_p[X] \setminus \{0\}$ de grado a lo más n y que no depende de x o de y. De esto y de (2.6) se obtiene que x es solución de la congruencia

$$f(X) \equiv g(h(X)) \pmod{p}.$$

Puesto que el número de soluciones de esta congruencia es menor o igual a máx$\{n, m\deg(h)\}$ se concluye que la ecuación (2.6) tiene a lo más $(m+1)n$ soluciones que satisfacen (2.7). ∎

2.3.4. Elementos de la geometría de números

Recordemos que una *retícula* en $\mathbb{R}^n$ es cualquier subgrupo aditivo de $\mathbb{R}^n$ generado por n vectores linealmente independientes. Si $D \subseteq \mathbb{R}^n$ es compacto, convexo, con interior no vacío decimos que D es un *cuerpo convexo* y si D es un cuerpo convexo que satisface la propiedad de que $-x \in D$ para todo $x \in D$ decimos que D es *centralmente simétrico*.

Dada una retícula $\Gamma \subseteq \mathbb{R}^n$ y un cuerpo convexo D, definimos el *i-ésimo mínimo sucesivo* $\lambda_i(D,\Gamma)$ *de* D *con respecto a* Γ como el mínimo $\lambda > 0$ tal que el conjunto λD contiene i vectores de Γ linealmente independientes. Es evidente de la definición que $\lambda_1(D,\Gamma) \leq \lambda_2(D,\Gamma) \leq \ldots \leq \lambda_n(D,\Gamma)$. El siguiente lema puede encontrarse en [1] (el ejercicio 3.5.6 de [25] pide establecer una variante un tanto más simple del mismo pero que es suficiente para nuestros fines).

Lema 2.6. *Si* Γ *es una retícula en* $\mathbb{R}^n$ *y* $D \subseteq \mathbb{R}^n$ *es un cuerpo convexo centralmente simétrico, entonces se cumple que*

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

Si denotamos mediante $(2n+1)!!$ al producto de los primeros $n+1$ números impares positivos y notamos que

$$\frac{2i}{\lambda_i(D,\Gamma)} + 1 \leq (2i+1)\,\text{máx}\left\{ \frac{1}{\lambda_i(D,\Gamma)}, 1 \right\},$$

obtenemos la siguiente desigualdad a la cual recurriremos eventualmente.

Corolario 2.2. *Se cumple que*

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

2.4. Demostración del Teorema 2.1

Durante esta demostración denotaremos a $I_f(M;R,S)$ simplemente mediante $\mathcal{I}$ y supondremos que $\mathcal{I}$ es grande.

Sea L un número entero del intervalo $[1, 0.01\mathcal{I}]$ fijo, pero a especificar más adelante. Al considerar la partición del rectángulo $[R+1, R+M]\times[S+1, S+M]$ en los L subrectángulos determinados por la división del segmento de extremos $(R+1,0)$ y $(R+M,0)$ en L partes iguales es posible inferir la existencia de un número Q tal que la ecuación

$$y^2 \equiv f(x) \pmod{p}, \qquad Q \leq x \leq Q+(M-1)/L, \quad S+1 \leq y \leq S+M \tag{2.8}$$

tiene al menos $\mathcal{I}/L$ soluciones:

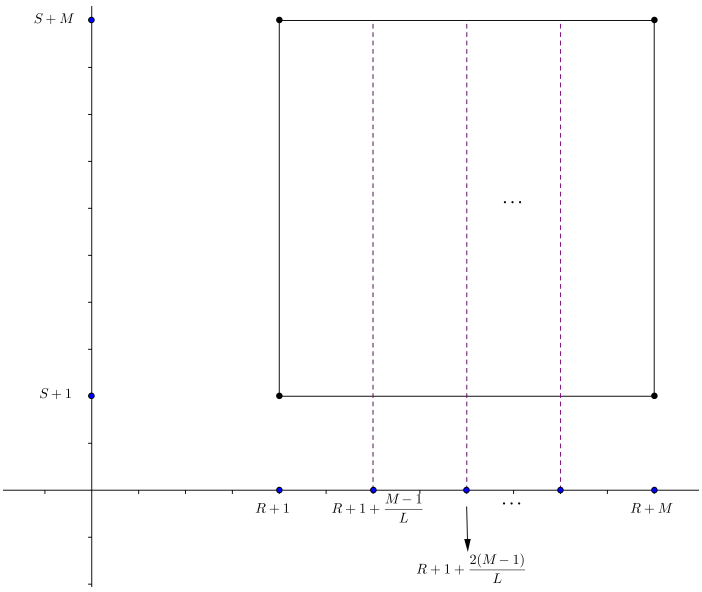


Fig. 2.1

Luego, al dividir el intervalo $[Q, Q + (M-1)/L]$ en $k_0 = \lceil \mathcal{I}/(30L) \rceil$ partes iguales se obtienen k_0 subintervalos cuya longitud no excede a $\frac{\frac{M}{L}}{k_0} = \frac{M}{L} \cdot \frac{1}{k_0} \leq \frac{M}{L} \cdot \frac{30L}{\mathcal{I}} = \frac{30M}{\mathcal{I}}$ (veáse la figura 2.2); como la congruencia en (2.8) admite a lo más dos soluciones con una abscisa dada y en el rectángulo $[Q, Q+(M-1)/L] \times [S+1, S+M]$ hay al menos $\mathcal{I}/L > 20k_0$ soluciones de la misma, entonces se afirma la existencia de un subrectángulo de $[Q, Q + (M-1)/L] \times [S+1, S+M]$, con base no mayor a $30M/\mathcal{I}$, que contiene al menos 10 soluciones de (2.8) cuyas abscisas son distintas entre sí. Dentro de estas 10 soluciones denotemos con (x_0, y_0) a aquella con menor abscisa.

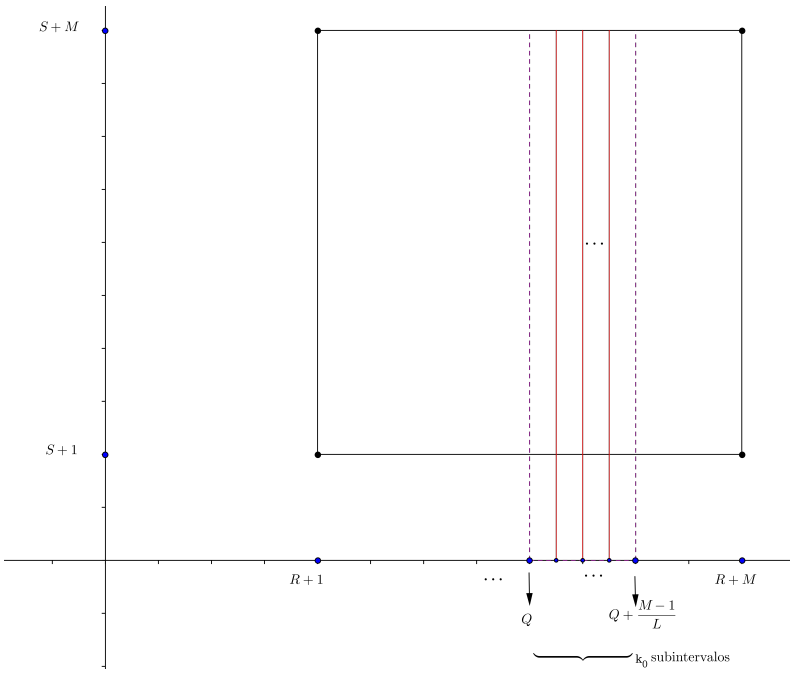


Fig. 2.2

Ahora bien, puesto que es posible definir una aplicación inyectiva entre las soluciones de (2.8) y las soluciones de

$$(y_0 + y)^2 \equiv f(x_0 + x) \pmod{p}, \qquad -M/L \leq x \leq M/L, \quad -M \leq y \leq M$$

y como ésta congruencia es equivalente a una de la forma

$$y^2 \equiv c_3x^3 + c_2x^2 + c_1x + c_0y \pmod{p}, \qquad -M/L \leq x \leq M/L, \quad -M \leq y \leq M \tag{2.9}$$

para algún $(c_3, c_2, c_1, c_0) \in \mathbb{Z}^4$ y donde $(c_3, p) = 1$, se sigue que $\mathcal{I}/L$ está acotado superiormente por el número de soluciones de (2.9). Por lo hecho en el párrafo anterior sabemos que (2.9) cuenta con al menos 10 soluciones (x, y) cuyas abscisas son distintas entre sí y que satisfacen $0 \leq x \leq 30M/\mathcal{I}$. Si $(x_1, y_1), (x_2, y_2)$ y (x_3, y_3) son tres de tales soluciones, entonces (2.9) da lugar a la siguiente ecuación matricial:

$$\begin{pmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod{p} \tag{2.10}$$

Del Lema (2.5) sabemos que a lo más 9 pares $(x, y) \in [0, p) \times [0, p)$ satisfacen simultáneamente (2.10) y la congruencia

$$\det \begin{pmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \equiv 0 \pmod{p}.$$

De esto se desprende que al menos una de las 10 soluciones de (2.9) que se distinguieron anteriormente, llamémosle (x_4, y_4), es tal que

$$\Delta := \det \begin{pmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \not\equiv 0 \pmod{p}.$$

Con este dato y apelando a la regla de Cramer procedemos a resolver el sistema de congruencias

$$\begin{pmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_4^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod{p}. \tag{2.11}$$

Para $j \in \{0,1,2,3\}$, denotemos por Δ_j al determinante de la matriz de tamaño 4×4 que se obtiene al reemplazar la $(j+1)$-ésima columna de la matriz de tamaño 4×4 que aparece en el lado izquierdo de (2.11) por el vector $(y_4^2, y_3^2, y_2^2, y_1^2)^t$. De estas consideraciones y la regla de Cramer se obtiene que

$$c_j \equiv \Delta_{4-j}\Delta^* \pmod{p}$$

para $j \in \{0,1,2,3\}$ y donde Δ^* es uno de los representantes del inverso multiplicativo de la clase módulo p a la que pertenece Δ. En vista de todo esto se tiene que la congruencia (2.9) puede reescribirse como

$$\Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x + \Delta_4 y - \Delta y^2 \equiv 0 \pmod{p}.$$

Nótese que, como $p \nmid c_3$, entonces $\Delta_1 \not\equiv 0 \pmod{p}$; por otro lado, la congruencia anterior da lugar a la siguiente ecuación diofántica auxiliar:

$$\Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x + \Delta_4 y - \Delta y^2 = pz, \qquad (x,y,z) \in \mathbb{Z}^3. \tag{2.12}$$

Considerando las estimaciones

$$\begin{aligned} 1 \leq |\Delta| &\ll (M/\mathcal{I})^6 M, \\ |\Delta_4| &\ll (M/\mathcal{I})^6 M^2, \\ |\Delta_3| &\ll (M/\mathcal{I})^5 M^3, \\ |\Delta_2| &\ll (M/\mathcal{I})^4 M^3, \\ |\Delta_1| &\ll (M/\mathcal{I})^3 M^3 \end{aligned}$$

y que $L \ll \mathcal{I}$ se deduce que

$$\begin{aligned} |z| &\ll \frac{1}{p}(|\Delta_1|(M/L)^3 + |\Delta_2|(M/L)^2 + |\Delta_3|(M/L) + |\Delta_4|M + |\Delta|M^2) \\ &\ll \frac{M^3}{p}\left(\frac{M^6}{\mathcal{I}^3L^3} + \frac{M^6}{\mathcal{I}^4L^2} + \frac{M^6}{\mathcal{I}^5L} + \frac{M^6}{\mathcal{I}^6}\right) \\ &\ll \frac{M^9}{p\mathcal{I}^3L^3}. \end{aligned}$$

Así pues, al ser $\Delta \neq 0$ y $\Delta_1 \neq 0$, se cumple que para cada z *admisible* la curva algebraica C_z determinada por (2.12) es absolutamente irreducible; al invocar el teorema de Bombieri y Pila sobre puntos de coordenadas enteras en curvas algebraicas planas se colige que cada C_z contiene a lo más $M^{1/3+o(1)}$ elementos de $\{(x, y) \in \mathbb{Z}^2 : |x|, |y| \leq M\}$. De todo esto se desprende que

$$\frac{\mathcal{I}}{L} \leq M^{1/3+o(1)}\left(1 + \frac{M^9}{p\mathcal{I}^3L^3}\right)$$

para cada $L \in \mathbb{Z} \cap [1, 0.01\mathcal{I}]$. Esta desigualdad puede reescribirse como $\mathcal{I}^4 \leq LM^{1/3+o(1)}\left(\mathcal{I}^3 + \frac{M^9}{pL^3}\right)$: cuando $\frac{M^9}{pL^3} \leq \mathcal{I}^3$, la desigualdad deviene en $\mathcal{I} \leq LM^{1/3+o(1)}$; cuando $\mathcal{I}^3 < \frac{M^9}{pL^3}$, de ella se desprende que $\mathcal{I} \leq \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}}$. De estas dos estimaciones se sigue que

$$\mathcal{I} \leq LM^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}} \tag{2.13}$$

para cada $L \in \mathbb{Z} \cap [1, 0.01\mathcal{I}]$.

Si $M \leq 10p^{1/8}$, entonces haciendo $L = 1$ de la estimación (2.13) se obtiene que

$$\mathcal{I} \leq M^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}} \leq M^{1/3+o(1)}.$$

Supongamos ahora que $M > 10p^{1/8}$. Puede asumirse además que $\mathcal{I} > M^{5/3}p^{-1/6}$ pues, en caso contrario, habría nada más que hacer. Así las cosas, al elegir $L = \lfloor M^{4/3}p^{-1/6} \rfloor$ se tiene que $L \in \mathbb{Z} \cap [1, 0.01\mathcal{I}]$ y, más aún, que

$$\mathcal{I} \leq LM^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}} \leq \frac{M^{5/3+o(1)}}{p^{1/6}}.$$

De todo lo anterior se concluye que

$$\mathcal{I} \leq M^{1/3+o(1)} + \frac{M^{5/3+o(1)}}{p^{1/6}}.$$

∎

2.5. Demostración del Teorema 2.2

Se trata de demostrar que la estimación

$$I_f(M; R, S) \leq M^{1/3+o(1)} + \left(\frac{M^3}{p}\right)^{1/16} M^{1+o(1)}$$

se cumple uniformemente sobre todos los polinomios $f \in \mathbb{F}_p[X]$ de grado 3. Puesto que para $M \leq p^{5/23}$ se observa que

$$\frac{M^{5/3}}{p^{1/6}} \leq \left(\frac{M^3}{p}\right)^{1/16} M,$$

la estimación deseada se seguiría en este caso de la garantizada por el Teorema 2.1. Así pues, en lo sucesivo estaremos suponiendo que

$$M > p^{5/23}. \tag{2.14}$$

Fijemos una solución (x_0, y_0) de

$$y^2 \equiv f(x) \pmod{p}, \qquad R+1 \leq x \leq R+M, \quad S+1 \leq y \leq S+M.$$

Considerando que hay una aplicación inyectiva entre el conjunto de soluciones de esta congruencia y el conjunto de soluciones de

$$y^2 - c_0 y \equiv c_3 x^3 + c_2 x^2 + c_1 x \pmod{p}, \qquad |x|, |y| \leq M \tag{2.15}$$

—donde c_3, c_2, c_1, c_0 son números enteros determinados por x_0, y_0 y los coeficientes de f y, además, $p \nmid c_3$—se tiene que a fin de estimar $I_f(M; R, S)$ *basta* con

estudiar el cardinal del conjunto de soluciones de (2.15). Denotemos con $\mathcal{W}$ al conjunto de pares (x, y) que satisfacen (2.15), con $\mathcal{X}$ al conjunto conformado por aquellas x's tales que $(x, y) \in \mathcal{W}$ para alguna y y con ρ al cociente $|\mathcal{X}|/M$.

Sea $\epsilon > 0$. Si $\rho \leq (M^3/p)^{1/16}$, entonces se cumple que el número de soluciones de (2.15) es menor o igual que

$$2|\mathcal{X}| = 2M\rho \leq 2\left(\frac{M^3}{p}\right)^{1/16} M \leq \left(\frac{M^3}{p}\right)^{1/16} M^{1+o(1)}$$

tal como se desea establecer. Así entonces, tiene cabida suponer de aquí en adelante que

$$\rho \geq \left(\frac{M^3}{p}\right)^{\frac{1}{16}} M^{\epsilon}. \tag{2.16}$$

De hecho, en lo que sigue estaremos suponiendo también que $M < \left(\frac{p}{16}\right)^{1/3}$. Nótese que de (2.14) y (2.16) se sigue que

$$\rho > M^{-1/10}. \tag{2.17}$$

Ahora bien, dado $v \in \{1, 2, 3\}$, denotemos mediante $I_{v,8}$ al intervalo $[-8M^v, 8M^v]$. Consideremos el subconjunto $\mathcal{S}$ de $I_{1,8}\times I_{2,8}\times I_{3,8}$ conformado por aquellas triadas $\mathbf{s} = (s_1, s_2, s_3)$ en las que

$$\begin{cases} s_1 \equiv x_1 + \cdots + x_8 \pmod{p} \\ s_2 \equiv x_1^2 + \cdots + x_8^2 \pmod{p} \\ s_3 \equiv x_1^3 + \cdots + x_8^3 \pmod{p} \end{cases} \tag{2.18}$$

para algún $(x_1, x_2, \ldots, x_8) \in \mathcal{X}^8$. Vamos a estimar inferiormente el cardinal de este conjunto. Para $s \in \mathcal{S}$, hagamos

$$N(\mathbf{s}) := \{(x_1, \ldots, x_8) \in \mathcal{X}^8 \colon s_i \equiv x_1^i + \cdots + x_8^i \,(\mathrm{mód}\, p),\ i = 1, 2, 3, \}$$

En vista de que $\bigcup_{\mathbf{s}\in\mathcal{S}} N(\mathbf{s}) = \mathcal{X}^8$ y que $N(\mathbf{s}) \cap N(\mathbf{s}') = \emptyset$ (siempre que $\mathbf{s}, \mathbf{s}' \in \mathcal{S}$ y $\mathbf{s} \neq \mathbf{s}'$) se obtiene que

$$|\mathcal{X}|^8 = \sum_{\mathbf{s}\in\mathcal{S}} |N(\mathbf{s})| \leq \left(|\mathcal{S}| \sum_{\mathbf{s}\in\mathcal{S}} |N(\mathbf{s})|^2 \right)^{1/2}. \tag{2.19}$$

La suma que aparece más a la derecha se puede estimar mediante el argumento estándar: dado que $\sum_{\mathbf{s}\in\mathcal{S}} |N(\mathbf{s})|^2 = \sum_{\mathbf{s}\in\mathcal{S}} |N(\mathbf{s}) \times N(\mathbf{s})|$ es igual a

$$\sum_{\mathbf{s}\in\mathcal{S}} \left| \left\{ (x_{1,\mathbf{s}}, \ldots, x_{16,\mathbf{s}}) \in \mathcal{X}^{16} \colon \forall i \in \{1,2,3\}, \left\langle \begin{array}{rcll} s_i & \equiv & x_{1,\mathbf{s}}^i + \cdots + x_{8,\mathbf{s}}^i & (\text{mód } p) \\ s_i & \equiv & x_{9,\mathbf{s}}^i + \cdots + x_{16,\mathbf{s}}^i & (\text{mód } p) \end{array} \right\rangle \right\} \right|,$$

se deduce que $\sum_{\mathbf{s}\in\mathcal{S}} |N(\mathbf{s})|^2$ es igual al cardinal del conjunto de soluciones del sistema de congruencias

$$\left\{ \begin{array}{rcccccccccl} x_1 & + & \cdots & + & x_8 & \equiv & x_9 & + & \cdots & + & x_{16} \quad (\text{mód } p) \\ x_1^2 & + & \cdots & + & x_8^2 & \equiv & x_9^2 & + & \cdots & + & x_{16}^2 \quad (\text{mód } p) \\ x_1^3 & + & \cdots & + & x_8^3 & \equiv & x_9^3 & + & \cdots & + & x_{16}^3 \quad (\text{mód } p) \end{array} \right. \tag{2.20}$$

en el cual todas las incógnitas son números enteros del intervalo $[-M, M]$. Apelando al supuesto de que $M < (\frac{p}{16})^{1/3}$ vemos que este sistema de congruencias conlleva al sistema de ecuaciones diofánticas

$$\left\{ \begin{array}{rcccccccccl} x_1 & + & \cdots & + & x_8 & = & x_9 & + & \cdots & + & x_{16} \\ x_1^2 & + & \cdots & + & x_8^2 & = & x_9^2 & + & \cdots & + & x_{16}^2 \\ x_1^3 & + & \cdots & + & x_8^3 & = & x_9^3 & + & \cdots & + & x_{16}^3 \end{array} \right.$$

el cual tiene, de acuerdo con el Lema 2.4, a lo más $M^{10+o(1)}$ soluciones $(x_1, \ldots, x_{16}) \in [-M, M]^{16}$. De esto y (2.19) se desprende que $|\mathcal{X}|^8 \leq (|\mathcal{S}|M^{10+o(1)})^{1/2}$ lo cual, a su vez, indica que

$$|\mathcal{S}| \geq \frac{|\mathcal{X}|^{16}}{M^{10+o(1)}} = \rho^{16} M^{6+o(1)}.$$

Esto permite garantizar la existencia de al menos $\rho^{16}M^{6+o(1)}$ triadas $(z_1, z_2, z_3) \in I_{1,8} \times I_{2,8} \times I_{3,8}$ tales que

$$c_3 z_3 + c_2 z_2 + c_1 z_1 \equiv \tilde{z}_2 - c_0 \tilde{z}_1 \pmod{p}$$

para algunos $\tilde{z}_1 \in I_{1,8}$ y $\tilde{z}_2 \in I_{2,8}$. En particular, de esto se sigue que el conjunto de soluciones de la congruencia

$$c_3z_3+c_2z_2+\tilde{z}_2+c_1z_1+c_0\tilde{z}_1 \equiv 0 \pmod{p}, \qquad (z_1,\tilde{z}_1,z_2,\tilde{z}_2,z_3) \in I_{1,8}\times I_{1,8}\times I_{2,8}\times I_{2,8}\times I_{3,8}$$

tiene un subconjunto $\mathcal{S}$ de cuya cardinalidad se sabe que

$$|\mathcal{S}| \geq \rho^{16}M^{6+o(1)}. \tag{2.21}$$

En el resto de la demostración se emula el argumento en [3, págs. 82-84]. Consideremos la retícula

$$\Gamma = \{(X_2, X_3, \tilde{X}_2, X_1, \tilde{X}_1) \in \mathbb{Z}^5 \colon X_2 + c_3X_3 + c_2\tilde{X}_2 + c_1X_1 + c_0\tilde{X}_1 \equiv 0 \pmod{p}\}$$

y el cuerpo convexo

$$D = \{(x_2, x_3, \tilde{x}_2, x_1, \tilde{x}_1) \in \mathbb{R}^5 \colon |x_1|, |\tilde{x}_1| \leq 8M;\ |x_2|, |\tilde{x}_2| \leq 8M^2;\ |x_3| \leq 8M^3\}.$$

En la luz de (2.21) se obtiene que

$$|D \cap \Gamma| \geq \rho^{16}M^{6+o(1)}.$$

De esta desigualdad y el Corolario 2.2 se infiere que, si $\lambda_i := \lambda_i(D, \Gamma)$ es el i-ésimo mínimo sucesivo del cuerpo convexo D (con respecto a Γ), entonces

$$\prod_{i=1}^{5} \min\{1, \lambda_i\} \leq \rho^{-16}M^{-6+o(1)}. \tag{2.22}$$

Afirmamos ahora que para cada $i \in \{1, 2, 3, 4, 5\}$ existe

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \tilde{v}_{2,i}, v_{1,i}, \tilde{v}_{1,i}) \in \lambda_i D \cap \Gamma \tag{2.23}$$

de tal suerte que $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$ es linealmente independiente: en efecto, $\mathbf{v}_1$ puede ser cualquier elemento de $(\lambda_1 D \cap \Gamma) \setminus \{(0, 0, 0, 0, 0)\}$; luego, asumiendo que

$i \in \{2,3,4,5\}$ y que los vectores $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$ han sido especificados, $\mathbf{v}_i$ puede ser cualquier elemento de $(\lambda_i D \cap \Gamma) \setminus \langle \mathbf{v}_1, \ldots, \mathbf{v}_{i-1} \rangle$.

Notemos también que $\lambda_3 < 1$ pues, en caso contrario, de (2.22) se obtendría que

$$\text{mín}\{1, \lambda_1^2\} \leq \text{mín}\{1, \lambda_1\}\,\text{mín}\{1, \lambda_2\} \leq \rho^{-16} M^{-6+o(1)}.$$

A su vez, de estas desigualdades y (2.17) se tendría que

$$\lambda_1 \leq \frac{1}{10M^2}.$$

Consecuentemente, en el vector $\mathbf{v}_1$ sería $v_{2,1} = \tilde{v}_{2,1} = v_{1,1} = \tilde{v}_{1,1} = 0$; de esto y la definición de Γ se llegaría a que $v_{3,1} \equiv 0 \pmod{p}$. Como se ha supuesto que $M < \left(\frac{p}{16}\right)^{1/3}$, la congruencia anterior sería equivalente a la igualdad $v_{3,1} = 0$; por lo consiguiente, $\mathbf{v}_1 = (0,0,0,0,0)$. ¡Contradicción!

Consideramos a continuación un análisis de las distintas posibilidades que pueden tenerse sobre los mínimos sucesivos.

Caso 1: $\lambda_5 \leq 1$. La estimación (2.22) deviene en este caso en

$$\prod_{i=1}^{5} \lambda_i \leq \rho^{-16} M^{-6+o(1)}.$$

Luego, si Δ es el determinante de la matriz de tamaño 5×5 conformada por los vectores $\mathbf{v}_1, \ldots, \mathbf{v}_5$ se observa que

$$\Delta \ll M^{2+3+2+1+1} \prod_{i=1}^{5} \lambda_i \leq \rho^{-16} M^{3+o(1)}.$$

De (2.16) y esta estimación se deduce que $|\Delta| < p$. Por otro lado, al ser $\mathbf{v}_1, \ldots, \mathbf{v}_5$ elementos de Γ, se cumple que $\Delta \equiv 0 \pmod{p}$; así entonces, $\Delta = 0$ lo cual entra en contradicción con el hecho de que $\{\mathbf{v}_1, \ldots, \mathbf{v}_5\}$ es un subconjunto de $\mathbb{R}^5$ linealmente independiente.

Caso 2: $\lambda_4 \leq 1$, $\lambda_5 > 1$. En este caso, hagamos

$$V := \begin{pmatrix} v_{3,1} & \tilde{v}_{2,1} & v_{1,1} & \tilde{v}_{1,1} \\ v_{3,2} & \tilde{v}_{2,2} & v_{1,2} & \tilde{v}_{1,2} \\ v_{3,3} & \tilde{v}_{2,3} & v_{1,3} & \tilde{v}_{1,3} \\ v_{3,4} & \tilde{v}_{2,4} & v_{1,4} & \tilde{v}_{1,4} \end{pmatrix}, \qquad \mathbf{w} := \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \\ -v_{2,3} \\ -v_{2,4} \end{pmatrix}, \qquad \mathbf{c} := \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix}$$

Se verifica entonces que

$$V\mathbf{c} \equiv \mathbf{w} \pmod{p}.$$

Como en la prueba del Teorema 2.1 analizaremos a continuación este sistema de congruencias recurriendo a la regla de Cramer. Denotemos con Δ al determinante de V y, para $j \in \{1, 2, 3, 4\}$, denotemos con Δ_j el determinante de la matriz de tamaño 4×4 que se obtiene al reemplazar la j-ésima columna de V por $\mathbf{w}$. La estimación (2.22) implica en este caso que

$$|\Delta| \ll \lambda_1\lambda_2\lambda_3\lambda_4 M^{3+2+1+1} \leq \rho^{-16} M^{1+o(1)} \tag{2.24}$$

y que

$$|\Delta_1| \leq \rho^{-16} M^{o(1)}, \quad |\Delta_2| \leq \rho^{-16} M^{1+o(1)}, \quad |\Delta_3| \leq \rho^{-16} M^{2+o(1)}, \quad |\Delta_4| \leq \rho^{-16} M^{2+o(1)}. \tag{2.25}$$

Nótese que de (2.16), (2.24) y (2.25) es posible establecer que

$$|\Delta|, |\Delta_1|, |\Delta_2|, |\Delta_3|, |\Delta_4| < p. \tag{2.26}$$

Si $|\Delta| \equiv 0 \pmod{p}$, entonces de la regla de Cramer se obtiene que $\begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \Delta_3 \\ \Delta_4 \end{pmatrix} = \Delta\mathbf{c} \equiv 0 \pmod{p}$; de esto y (2.26) se arriba a que $\Delta = \Delta_1 = \Delta_2 = \Delta_3 = \Delta_4 = 0$. Sin

embargo, dado que lo anterior implica que, al desarrollar el determinante de la matriz

$$\begin{pmatrix} v_{2,1} & v_{3,1} & \tilde{v}_{2,1} & v_{1,1} & \tilde{v}_{1,1} \\ v_{2,2} & v_{3,2} & \tilde{v}_{2,2} & v_{1,2} & \tilde{v}_{1,2} \\ v_{2,3} & v_{3,3} & \tilde{v}_{2,3} & v_{1,3} & \tilde{v}_{1,3} \\ v_{2,4} & v_{3,4} & \tilde{v}_{2,4} & v_{1,4} & \tilde{v}_{1,4} \\ v_{2,5} & v_{3,5} & \tilde{v}_{2,5} & v_{1,5} & \tilde{v}_{1,5} \end{pmatrix}$$

con respecto al quinto renglón se obtendría (claramente) un 0 como resultado, entonces el supuesto de que $p \mid \Delta$ no se sostiene (recuérdese que $\{\mathbf{v}_1, \ldots, \mathbf{v}_5\}$ es un subconjunto de $\mathbb{R}^5$ linealmente independiente). En consecuencia, $p \nmid 0$ y consiguientemente

$$\begin{aligned} \Delta c_1 &\equiv \Delta_3 \pmod{p}, \\ \Delta c_2 &\equiv \Delta_2 \pmod{p}, \\ \Delta c_3 &\equiv \Delta_1 \pmod{p}, \\ \Delta c_0 &\equiv \Delta_4 \pmod{p}. \end{aligned}$$

Al sustituir esto en (2.15) se tiene que la congruencia original se convierte en

$$\Delta y^2 - \Delta_4 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x \pmod{p}, \qquad |x|, |y| \leq M.$$

Ahora bien, como de (2.16), (2.24) y (2.25) se obtiene que para cada M suficientemente grande el valor absoluto de las expresiones en ambos miembros de la congruencia de arriba es menor o igual a $p/2$, necesariamente se debe cumplir que

$$\Delta y^2 - \Delta_4 y = \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x, \qquad |x|, |y| \leq M.$$

Del Lema 2.3 (de Bombieri y Pila) se concluye que el número de soluciones de la congruencia en consideración es a lo más $M^{1/3+o(1)}$.

Caso 3: $\lambda_3 \leq (10M)^{-1}$, $\lambda_4 > 1$. La estimación (2.22) implica que

$$\prod_{i=1}^{3} \lambda_i \leq \rho^{-16} M^{-6+o(1)}.$$

Además, al ser $\lambda_3 \leq (10M)^{-1}$, se tiene que

$$\mathbf{v}_1 = (v_{2,1}, v_{3,1}, \tilde{v}_{2,1}, 0, 0),\ \mathbf{v}_2 = (v_{2,2}, v_{3,2}, \tilde{v}_{2,2}, 0, 0),\ \mathbf{v}_3 = (v_{2,3}, v_{3,3}, \tilde{v}_{2,3}, 0, 0). \quad (2.27)$$

Así pues, apelando a la definición de Γ, se observa que

$$\begin{pmatrix} v_{2,1} & v_{3,1} & \tilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \tilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \tilde{v}_{2,3} \end{pmatrix} \begin{pmatrix} 1 \\ c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \pmod{p}.$$

De esto se sigue a su vez que si $\Delta := \det \begin{pmatrix} v_{2,1} & v_{3,1} & \tilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \tilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \tilde{v}_{2,3} \end{pmatrix}$ entonces $\Delta \equiv 0 \pmod{p}$.

Por otro lado, de acuerdo con (2.17)

$$|\Delta| \ll \lambda_1 \lambda_2 \lambda_3 M^7 \leq \frac{M^{1+o(1)}}{\rho^{16}} < M^{2.6+o(1)}.$$

Así entonces, $\Delta = 0$. De esto y (2.27) se desprende que los vectores $\mathbf{v}_1, \mathbf{v}_2$ y $\mathbf{v}_3$ son linealmente dependientes, lo cual entra en contradicción con la indepedencia lineal del conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_5\}$.

Caso 4: $(10M)^{-1} < \lambda_3 < 1, \lambda_4 > 1$. En este caso, la estimación en (2.22) deviene en

$$\prod_{i=1}^{3} \lambda_i \leq \rho^{-16} M^{-6+o(1)}.$$

Luego, al considerar la desigualdad $\lambda_3 > (10M)^{-1}$, se obtiene que

$$\lambda_1 \lambda_2 < \rho^{-16} M^{-5+o(1)}.$$

Nótese que en este caso se cumple también que $\lambda_1 > (10M^2)^{-1}$: en efecto, pues en otro caso $v_{2,1} = \tilde{v}_{2,1} = v_{1,1} = \tilde{v}_{1,1} = 0$ lo cual conlleva a que $v_{3,1} \equiv 0$

(mód p); de esto y el supuesto de que $M < (\frac{p}{16})^{1/3}$ se colige que $v_{3,1} = 0$, lo que entra en contradicción con el hecho de que $\mathbf{v}_1 \neq (0,0,0,0,0)$.

Otro punto a tener en cuenta en lo que sigue es que de $\lambda_1 > (10M^2)^{-1}$ y $\rho > M^{-1/10}$ se desprende que $\lambda_2 < (10M)^{-1}$. Así entonces,

$$\mathbf{v}_1 = (v_{2,1}, v_{3,1}, \tilde{v}_{2,1}, 0, 0), \qquad \mathbf{v}_2 = (v_{2,2}, v_{3,2}, \tilde{v}_{2,2}, 0, 0).$$

Apelando a la definición de Γ se llega a que

$$\begin{pmatrix} v_{3,1} & \tilde{v}_{2,1} \\ v_{3,2} & \tilde{v}_{2,2} \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \end{pmatrix} \pmod{p}.$$

Luego, en vista de que

$$\Delta := \det \begin{pmatrix} v_{3,1} & \tilde{v}_{2,1} \\ v_{3,2} & \tilde{v}_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}, \tag{2.28}$$

$$\Delta_1 := \det \begin{pmatrix} -v_{2,1} & \tilde{v}_{2,1} \\ -v_{2,2} & \tilde{v}_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^4 < \frac{M^{-1+o(1)}}{\rho^{16}}, \tag{2.29}$$

$$\Delta_2 := \det \begin{pmatrix} v_{3,1} & -v_{2,1} \\ v_{3,2} & -v_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}, \tag{2.30}$$

se infiere que $|\Delta|, |\Delta_1|, |\Delta_2| < p$. Así las cosas, si fuera el caso que $\Delta \equiv 0 \pmod{p}$ entonces $\Delta_1 \equiv \Delta_2 \equiv 0 \pmod{p}$ y, consiguientemente, $\Delta = \Delta_1 = \Delta_2 = 0$. Empero, como de la anulación de los tres determinantes anteriores se deduce que el rango de la matriz

$$\begin{pmatrix} v_{2,1} & v_{3,1} & \tilde{v}_{2,1} & 0 & 0 \\ v_{2,2} & v_{3,2} & \tilde{v}_{2,2} & 0 & 0 \end{pmatrix}$$

es a lo más 1, se acaba de derivar una contradicción con la independencia lineal de $\{\mathbf{v}_1, \mathbf{v}_2\}$. Se colige así que el supuesto $\Delta \equiv 0 \pmod{p}$ está fuera de lugar. Por lo tanto, $p \nmid \Delta$; de la regla de Cramer se sigue que

$$\Delta c_3 \equiv \Delta_1 \pmod{p}, \qquad \Delta c_2 \equiv \Delta_2 \pmod{p}.$$

Tomando estas relaciones en cuenta podemos reescribir (2.15) como

$$\Delta y^2 - a_0 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + b_0 x \pmod{p}, \qquad |x|, |y| \leq M \tag{2.31}$$

para algunos enteros a_0, b_0. Ahora bien, si

$$T := \left\lfloor \left(\frac{p}{M}\right)^{1/3} \rho^{16/3} \right\rfloor$$

entonces resulta claro que $M^{2/3} < T < T^2 < p/2$. Más aún, *el principio de las casillas garantiza la existencia de* $t_0 \in \mathbb{Z} \cap [1, T^2 + 1)$ *tal que*

$$|(t_0 a_0)_p| \leq \frac{p}{T}, \qquad |(t_0 b_0)_p| \leq \frac{p}{T}$$

donde $(x)_p$ *denota al elemento de la clase módulo p de x con menor valor absoluto*[2]. Al multiplicar ambos lados de (2.31) por t_0 se obtiene

$$t_0 \Delta y^2 - (t_0 a_0)_p y \equiv t_0 \Delta_1 x^3 + t_0 \Delta_2 x^2 + (t_0 b_0)_p x \pmod{p}, \qquad |x|, |y| \leq M.$$

De (2.28), (2.29) y (2.30) se desprende que el módulo de las expresiones en sendos lados de la congruencia previa es $pM^{1+o(1)}T^{-1}$; en consecuencia, es válido reemplazarla por la ecuación diofántica

$$t_0 \Delta y^2 - (t_0 a_0)_p y = t_0 \Delta_1 x^3 + t_0 \Delta_2 x^2 + (t_0 b_0)_p x + pz, \qquad |x|, |y| \leq M, \qquad |z| < M^{1+o(1)} T^{-1}.$$

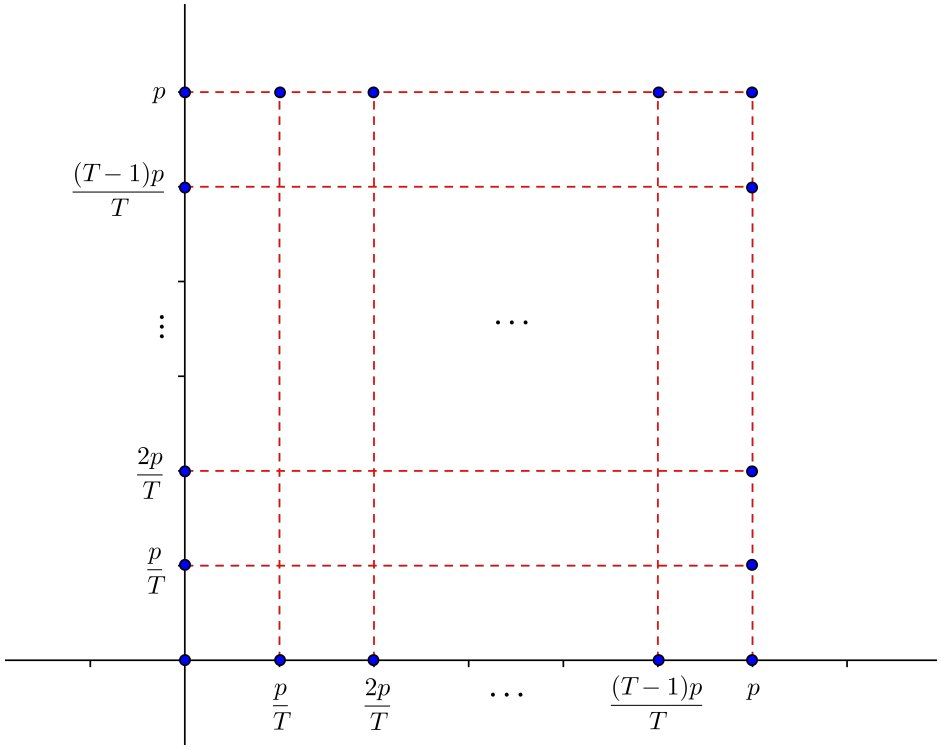
El Lema 2.3 (de Bombieri y Pila) permite concluir así que el número de soluciones de la congruencia en consideración es a lo más

$$\begin{aligned} \left(\frac{M}{T} + 1\right) M^{1/3+o(1)} &\leq \left(\frac{M^{4/3}}{p^{1/3}} \rho^{-16/3} + 1\right) M^{1/3+o(1)} \\ &\leq M^{2/3+o(1)} \leq M^{9/10+o(1)} \leq \left(\frac{M^3}{p}\right)^{1/16} M^{1+o(1)}. \end{aligned}$$

∎

[2]La prueba de este aserto auxiliar viene inmediatamente después de la presente demostración.

Sobre el *aserto auxiliar*: Fijemos $T \in \mathbb{N}_{>2}$. Las rectas verticales $x = \frac{p}{T}$, $x = \frac{2p}{T}$, $\ldots$, $x = \frac{(T-1)p}{T}$, $x = p$ y las rectas horizontales $y = \frac{p}{T}$, $y = \frac{2p}{T}$, $\ldots$, $y = \frac{(T-1)p}{T}$, $y = p$ dan lugar a un embaldosado del cuadrado $[0,p) \times [0,p)$ en T^2 subcuadrados como se muestra en la figura:



Denotemos con $[t]_p$ al menor entero positivo en la clase de congruencia (módulo p) de t. Claramente se tiene que los puntos $([a_0]_p, [b_0]_p)$, $([2a_0]_p, [2b_0]_p)$, $\ldots$, $([(T^2+1)a_0]_p, [(T^2+1)b_0]_p)$ pertenecen todos al cuadrado $[0,p) \times [0,p)$. Supongamos que entre estos puntos no hay dos que sean iguales. Como en tal caso habría T^2+1 puntos distintos del plano y T^2 subcuadrados en el embaldosado de $[0,p) \times [0,p)$, el principio de las casillas indica que uno de los subcuadrados alberga dos de esos T^2+1 puntos. Digamos que esos puntos son $([\ell a_0]_p, [\ell b_0]_p)$ y $([\mathscr{L} a_0]_p, [\mathscr{L} b_0]_p)$ donde $1 \leq \ell < \mathscr{L} \leq T^2+1$. Por la forma en que fueron definidos los subcuadrados se sigue que

$$\left|[\mathscr{L} a_0]_p - [\ell a_0]_p\right| \leq \frac{p}{T} < \frac{p}{2}, \qquad \left|[\mathscr{L} b_0]_p - [\ell b_0]_p\right| \leq \frac{p}{T} < \frac{p}{2}.$$

El resultado se sigue ahora al notar que el elemento de la clase módulo p de $(\mathscr{L} - \ell)a_0$ (resp. $(\mathscr{L} - \ell)b_0$) con menor valor absoluto es $[\mathscr{L}a_0]_p - [\ell a_0]_p$ (resp. $[\mathscr{L}b_0]_p - [\ell b_0]_p$).

2.6. Demostración del Teorema 2.3

Denotemos con $\mathcal{X}$ al conjunto de $x \in [R+1, R+M]$ que satisfacen la congruencia $y^2 \equiv f(x) \pmod p$ para algún $y \in [S+1, S+M]$. Luego, si $X := |\mathcal{X}|$ entonces es claro que

$$I_f(M; R, S) \leq 2X. \tag{2.32}$$

Para $k \in \mathbb{N}$ denotemos mediante $\mathcal{Y}_k$ al conjunto $\{y_1^2 + \cdots + y_k^2 \pmod p \colon S+1 \leq y_1, \ldots, y_k \leq S+M\}$. ¿Qué se puede decir sobre el cardinal de $\mathcal{Y}_k$? Notemos en primer lugar que si consideramos los cambios de variable $y_1 = S + z_1, \ldots, y_k = S + z_k$ entonces resulta que

$$\mathcal{Y}_k = \{z_1^2 + \cdots + z_k^2 + 2S(z_1 + \cdots + z_k) + kS^2 \pmod p \colon 1 \leq z_1, \ldots, z_k \leq M\}.$$

Ergo,

$$|\mathcal{Y}_k| \leq |\{r + 2Ss + kS^2 \colon 1 \leq r \leq KM^2, 1 \leq s \leq kM\}| \leq k^2M^3.$$

Ahora bien, puesto que para cada $(x_1, \ldots, x_k) \in \mathcal{X}^k$ existe $\lambda \in \mathcal{Y}_k$ de tal modo que

$$f(x_1) + \cdots + f(x_k) \equiv \lambda \pmod p,$$

se sigue que

$$X^k \leq \sum_{\lambda \in \mathcal{Y}_k} r(\lambda)$$

donde

$$r(\lambda) := |\{(x_1, \ldots, x_k) \in [R+1, R+M]^k \colon f(x_1) + \cdots + f(x_k) \equiv \lambda \pmod p\}|.$$

De esto y la desigualdad de Cauchy-Schwarz se infiere que

$$X^{2k} \leq |\mathcal{Y}_k| \sum_{\lambda \in \mathcal{Y}_k} r^2(\lambda) \leq k^2 M^3 T_k(R;M) \tag{2.33}$$

donde $T_k(R;M)$ es el número de soluciones de

$$f(x_1)+\cdots+f(x_k) \equiv f(x_{k+1})+\cdots+f(x_{2k}) \pmod{p}, \qquad (x_1,\ldots,x_{2k}) \in [R+1,R+M]^{2k}.$$

La expresión $T_k(R;M)$ fue introducida y estimada en [8, pág. 828] para $R = 0$; pero recurriendo a un cambio de variables resulta fácil convencerse de que la cota ahí obtenida vale también para cualquier otro valor de R. Esbozaremos enseguida la estimación de $T_k(0;M)$ hecha en el trabajo previamente mencionado.

Supongamos que $f(x) = a_m x^m + \cdots + a_1 x + a_0$. La congruencia cuyo número de soluciones $(x_1,\ldots,x_{2k}) \in [1,M]^{2k}$ deseamos estimar se puede reescribir como

$$a_m \left(\sum_{i=1}^{k} x_i^m - \sum_{i=k+1}^{2k} x_i^m \right) + \cdots + a_1 \left(\sum_{i=1}^{k} x_i - \sum_{i=k+1}^{2k} x_i \right) \equiv 0 \pmod{p}. \tag{2.34}$$

Para cada solución $(x_1,\ldots,x_{2k})$, definamos

$$\begin{aligned} \lambda_1 &:= x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k} \\ \lambda_2 &:= x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_{2k}^2 \\ &\vdots \\ \lambda_m &:= x_1^m + \cdots + x_k^m - x_{k+1}^m - \cdots - x_{2k}^m. \end{aligned}$$

Para todo $j \in \{1,2,\ldots,m\}$ se cumple que $\lambda_j \in [-kM^j, kM^j]$; además, dado que $a_m\lambda_m + \cdots + a_1\lambda_1 \equiv 0 \pmod{p}$, se sigue que por cada elección de

$$(\lambda_1,\lambda_2,\ldots,\lambda_{m-1}) \in [-kM,kM] \times [-kM^2,kM^2] \times \cdots \times [-kM^{m-1},kM^{m-1}],$$

el número de posibles valores que λ_m puede asumir es $O(M^m/p+1)$. Así entonces,

$$T_k(0;M) \ll M^{(m-1)m/2}\,(M^m/p+1) \max_{(\lambda_1,\ldots,\lambda_m)} J_{k,m}(\lambda_1,\ldots,\lambda_m;M)$$

donde $J_{k,m}(\lambda_1, \dots, \lambda_m; M)$ denota al número de soluciones en $[1, M]^{2k}$ del sistema de ecuaciones diofánticas

$$\begin{cases} x_1^m + \cdots + x_k^m = x_{k+1}^m + \cdots + x_{2k}^m + \lambda_m \\ \vdots \\ x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k} + \lambda_1 \end{cases}$$

En vista de que para cada vector $(\lambda_1, \dots, \lambda_m)$ la desigualdad $J_{k,m}(\lambda_1, \dots, \lambda_m; M) \leq J_{k,m}(0, \dots, 0; M) =: J_{k,m}(M)$ tiene lugar, se desprende que

$$T_k(0; M) \ll M^{(m-1)m/2} \left(M^m/p + 1\right) J_{k,m}(M).$$

Podemos retomar ahora la estimación de X^{2k}. Al tomar $k = \kappa(m)$, de tal manera que la estimación (2.4) tenga lugar, y considerar la estimación recién obtenida para $T_k(R; M)$ y la desigualdad (2.33) se llega a que

$$X^{2k} \leq M^3(M^m/p + 1)M^{m(m-1)/2}M^{2k-m(m+1)/2+o(1)} \leq (M^m/p + 1)M^{2k+3-m+o(1)}.$$

Por consiguiente,

$$X \leq M(M^3/p)^{1/2k+o(1)} + M^{1-(m-3)/2k+o(1)}$$

y la demostración termina. ∎

2.7. Demostración del Teorema 2.4

En lo que sigue denotaremos $J_f(M; R, S)$ simplemente mediante J. Notemos en primer lugar que es posible definir una función inyectiva entre el conjunto de soluciones de

$$y \equiv f(x) \pmod{p}, \qquad (x, y) \in [R + 1, R + M] \times [S + 1, S + M] \tag{2.35}$$

y el conjunto de soluciones de

$$y + S \equiv f(x) \pmod{p}, \qquad (x, y) \in [R + 1, R + M] \times [1, M].$$

Esto indica que tiene cabida suponer en lo sucesivo que

$$0 \leq S+1 < S+M \leq p.$$

Hagamos $\alpha := \frac{S+1}{p}$, $\beta := \frac{S+M}{p}$ y $\gamma_n := \left\{\frac{f(R+n)}{p}\right\} = \frac{f(R+n)}{p} - \left\lfloor \frac{f(R+n)}{p} \right\rfloor$ para cada $n \in \{1, \dots M\}$. Puesto que

$$f(R+n) \equiv y \pmod{p}$$

para algún $y \in [S+1, S+M]$ si y sólo si $\gamma_n \in [\alpha, \beta]$, se sigue que estimar superiormente el número de soluciones de (2.35) es esencialmente lo mismo que estudiar el cardinal del conjunto $\{n \in \{1, \dots, M\} \colon \gamma_n \in [\alpha, \beta]\}$. De lo anterior y el Lema 2.1 se obtiene que

$$\begin{aligned} J &\ll M(\beta-\alpha) + \frac{M}{K} + \sum_{k=1}^{K} \left(\frac{1}{K} + \min\{\beta-\alpha, 1/k\}\right) \left| \sum_{n=1}^{M} e^{2\pi i k \gamma_n} \right| \\ &\ll \frac{M^2}{p} + \frac{M}{K} + \left(\frac{1}{K} + \frac{M}{p}\right) \sum_{k=1}^{K} \left| \sum_{n=1}^{M} e^{2\pi i \frac{k f(R+n)}{p}} \right| \end{aligned}$$

para todo número natural K. Al estimar mediante el Lema 2.2 la suma interior que figura en el tercer término se llega a que

$$\begin{aligned} J &\ll \frac{M^2}{p} + \frac{M}{K} \\ &+ \left(\frac{1}{K} + \frac{M}{p}\right) M^{1-\frac{m}{2^{m-1}}} \underbrace{\sum_{k=1}^{K} \left(\sum_{-M<\ell_1,\dots,\ell_{m-1}<M} \min\left\{M, \left\| \frac{a}{p} m!\, k\, \ell_1 \cdots \ell_{m-1} \right\|^{-1}\right\}\right)^{2^{1-m}}}_{:=\mathcal{T}} \end{aligned}$$

donde a denota al coeficiente del término principal de f. Para estimar $\mathcal{T}$ consideramos en primera instancia la contribución de los términos de la suma interior que satisfacen $\ell_1 \cdots \ell_{m-1} = 0$; al hacerlo se colige que la estimación previa se puede reescribir como

$$\begin{aligned} J &\ll \frac{M^2}{p} + \frac{M}{K} + \left(\frac{1}{K} + \frac{M}{p}\right) M^{1-\frac{m}{2^{m-1}}} K (M^{m-1})^{2^{1-m}} + \left(\frac{1}{K} + \frac{M}{p}\right) M^{1-\frac{m}{2^{m-1}}} W \\ &\ll \frac{M^2}{p} + \frac{M}{K} + \left(\frac{1}{K} + \frac{M}{p}\right) K M^{1-\frac{1}{2^{m-1}}} + \left(\frac{1}{K} + \frac{M}{p}\right) M^{1-\frac{m}{2^{m-1}}} W \end{aligned} \tag{2.36}$$

donde

$$W := \sum_{k=1}^{K} \left(\sum_{0<|\ell_1|,\dots,|\ell_{m-1}|<M} \min\left\{ M, \left\| \frac{a}{p} m!\, k\, \ell_1 \cdots \ell_{m-1} \right\|^{-1} \right\} \right)^{2^{1-m}}.$$

Así entonces, todo se ha reducido a estimar W. Aplicando la desigualdad de Hölder con $\mathfrak{p} = \frac{2^{m-1}}{2^{m-1}-1}$ y $\mathfrak{q} = 2^{m-1}$ se obtiene que

$$\begin{aligned} W^{2^{m-1}} &\ll \left(\sum_{k=1}^{K} 1 \right)^{2^{m-1}-1} \left(\sum_{k=1}^{K} \sum_{0<|\ell_1|,\dots,|\ell_{m-1}|<M} \min\left\{ M, \left\| \frac{a}{p} m!\, k\, \ell_1 \cdots \ell_{m-1} \right\|^{-1} \right\} \right) \\ &= K^{2^{m-1}-1} \left(\sum_{k=1}^{K} \sum_{0<|\ell_1|,\dots,|\ell_{m-1}|<M} \min\left\{ M, \left\| \frac{a}{p} m!\, k\, \ell_1 \cdots \ell_{m-1} \right\|^{-1} \right\} \right). \end{aligned}$$

Luego, si con S_z denotamos al conjunto

$$\{(k, \ell_1, \dots, \ell_{m-1}) \colon 1 \le k \le K, \quad 0 < |\ell_1|, \dots, |\ell_{m-1}| < M \quad \text{y} \quad z = m!\, k\, \ell_1 \cdots \ell_{m-1}\}$$

entonces

$$\begin{aligned} W^{2^{m-1}} &\ll K^{2^{m-1}-1} \left(\sum_{\substack{|z|<m!KM^{m-1} \\ z\not\equiv 0 \pmod p}} \sum_{(k,\ell_1,\dots,\ell_{m-1})\in S_z} \min\left\{ M, \left\| \frac{a}{p} m!\, k\, \ell_1 \cdots \ell_{m-1} \right\|^{-1} \right\} \right) \\ &\ll K^{2^{m-1}-1} \sum_{\substack{|z|<m!KM^{m-1} \\ z\not\equiv 0 \pmod p}} |S_z| \min\left\{ M, \left\| \frac{a}{p} z \right\|^{-1} \right\} \end{aligned} \tag{2.37}$$

En vista de que $z \in [-m!KM^{m-1}, m!KM^{m-1}]$, la estimación superior clásica para la función aritmética $\tau(N) := \sum_{d\,|\,N} 1$ (ver por ejemplo [16, págs. 343-346]) garantiza que

$$|S_z| \ll (\tau(|z|))^{m-1} \ll e^{c\frac{\log m!KM^{m-1}}{\log\log m!KM^{m-1}}}$$

para alguna constante $c > 0$ y todo M suficientemente grande. Considerando la elección de K implícita en (2.36), esto es $K := \left\lfloor \frac{p}{M} \right\rfloor$, la estimación para $|S_z|$ deviene en

$$|S_z| \ll e^{c\frac{\log m!p^{m-1}}{\log\log m!p^{m-1}}} < p^{o(1)};$$

de lo cual se infiere a su vez que

$$\begin{aligned} W^{2^{m-1}} &\ll K^{2^{m-1}-1}p^{o(1)} \sum_{\substack{|z|<m!KM^{m-1} \\ z\not\equiv 0 \pmod p}} \left\|\frac{a}{p}z\right\|^{-1} && (2.38)\\ &\ll K^{2^{m-1}-1}p^{o(1)}\frac{KM^{m-1}}{p}\sum_{z=1}^{p-1}\left\|\frac{a}{p}z\right\|^{-1} && (2.39)\\ &= K^{2^{m-1}}p^{o(1)}\frac{M^{m-1}}{p}\sum_{z=1}^{p-1}\left\|\frac{z}{p}\right\|^{-1} && (2.40)\\ &\leq 2K^{2^{m-1}}p^{o(1)}\frac{M^{m-1}}{p}\sum_{z=1}^{\frac{p-1}{2}}\frac{p}{z} \\ &\ll K^{2^{m-1}}p^{o(1)}M^{m-1}\log p \\ &\ll K^{2^{m-1}}p^{o(1)}M^{m-1}. \end{aligned}$$

(Nótese que el paso de (2.38) a (2.39) está avalado por la periodicidad de la aplicación $z \mapsto \left\|\frac{a}{p}z\right\|$ y el paso de (2.39) a (2.40) por el hecho de que, al ser a coprimo con p, la aplicación $z \mapsto az$ permuta las clases de congruencia invertibles módulo p y porque la congruencia $u \equiv v \pmod p$ implica que $\left\|\frac{u}{p}\right\| = \left\|\frac{v}{p}\right\|$.) De esto, de la definición de K y de (2.36) se concluye que

$$\begin{aligned} J_f(M;R,S) &\ll \frac{M^2}{p} + M^{1-\frac{1}{2^{m-1}}} + \frac{M}{p}\left(M^{1-\frac{m}{2^{m-1}}}\right)(KM^{\frac{m-1}{2^{m-1}}})p^{o(1)} \\ &= \frac{M^2}{p} + M^{1-\frac{1}{2^{m-1}}}p^{o(1)}. \end{aligned}$$

∎

Glosario

◇ **Caracteres de Dirichlet módulo** m. Si G es un grupo y $\chi\colon G \to \mathbb{C}^*$ es un homomorfismo, entonces se dice que χ es un *caracter* del grupo G.

Sea $m \in \mathbb{N}$. Un *caracter de Dirichlet módulo* m es una función $f\colon \mathbb{Z} \to \mathbb{C}$ de la forma

$$f(n) = \begin{cases} \chi(n \pmod m) & \text{si } (n,m) = 1 \\ 0 & \text{en otro caso.} \end{cases}$$

para algún caracter χ del grupo $(\mathbb{Z}/m\mathbb{Z})^* =: \mathbb{Z}_m^*$. Abusando un poco de la notación, mediante χ se tiende a denotar tanto al caracter de $\mathbb{Z}_m^*$ como al caracter de Dirichlet módulo m determinado por él. Al caracter de Dirichlet módulo m determinado por el homomorfismo $\mathbb{Z}_m^* \to \mathbb{C}^*$ que manda cada elemento de $\mathbb{Z}_m^*$ en el elemento neutro de $\mathbb{C}^*$ se le denomina el *caracter trivial* χ_0.

◇ **Desigualdad de Hölder.** Supóngase que $p, q \in (1, \infty)$ satisfacen $\frac{1}{p} + \frac{1}{q} = 1$. Entonces, para cualesquiera números complejos $a_1, \ldots, a_n, b_1, \ldots, b_n$ se cumple que

$$\sum_{k=1}^{n} |a_k b_k| \leq \left(\sum_{k=1}^{n} |a_k|^p \right)^{1/p} \left(\sum_{k=1}^{n} |b_k|^q \right)^{1/q}$$

Cuando $p = q = 2$ se tiene la célebre desigualdad de Cauchy-Schwarz.

◇ **Identidad de Parseval (versión discreta).** Sea p un número primo. Si $A \subseteq$

$\{1, 2, \ldots, p-1\}$ entonces

$$\frac{1}{p-1}\sum_{\chi}\left|\sum_{c\in A}\chi(c)\right|^2 = |A|.$$

La primera suma es sobre los $p-1$ caracteres de Dirichlet módulo p. Para demostrar esta identidad basta con apelar a la **relación de ortogonalidad** (2.41) y a las manipulaciones usuales:

$$\begin{aligned}\frac{1}{p-1}\sum_{\chi}\left|\sum_{c\in A}\chi(c)\right|^2 &= \frac{1}{p-1}\sum_{\chi}\sum_{c\in A}\chi(c)\sum_{d\in A}\overline{\chi(d)}\\ &= \sum_{c\in A}\sum_{d\in A}\left(\frac{1}{p-1}\sum_{\chi}\chi(cd^*)\right)\\ &= |\{(c,d)\in A\times A\colon c=d\}|\\ &= |A|.\end{aligned}$$

◇ **Irreducibilidad absoluta.** Sean F un campo y $f(x,y)\in F[x,y]$. Se dice que el polinomio f es *absolutamente irreducible* si f es irreducible sobre cada extensión algebraica K de F. He aquí un criterio de irreducibilidad absoluta particularmente relevante a nuestro trabajo: una condición suficiente para la irreducibilidad absoluta del polinomio $y^s - f(x)\in F[x,y]$ es que $(s, \deg(f)) = 1$; para la demostración de este criterio puede consultarse [23, págs. 11-13] o [24, págs. 53-55].

◇ **Relaciones de ortogonalidad.** Sea $m\in\mathbb{N}$. A las identidades

$$\frac{1}{\phi(m)}\sum_{\chi}\chi(a) = \begin{cases}1 & \text{si } a\equiv 1 \pmod m\\ 0 & \text{en otro caso.}\end{cases} \tag{2.41}$$

$$\frac{1}{\phi(m)}\sum_{a\in\mathbb{Z}_m^*}\chi(a) = \begin{cases}1 & \text{si } \chi=\chi_0\\ 0 & \text{en otro caso.}\end{cases} \tag{2.42}$$

se les conoce como *relaciones de ortogonalidad para los caracteres de Dirichlet módulo m*. ϕ es la función indicatriz de Euler; la primera suma es sobre los $\phi(m)$ caracteres de Dirichlet módulo m.

Bibliografía

[1] U. Betke, M. Henk, *&* J. M. Wills, *Successive-minima type inequalities*. Discrete Comput. Geom. **9** (1993), 165-175.

[2] E. Bombieri, *On exponential sums*. Amer. J. of Math. **88** (1966), 71-105.

[3] J. Bourgain, M. Z. Garaev, S. V. Konyagin, *&* I. E. Shparlinski, *On congruences with products of variables from short intervals and applications*. Proc. Steklov Inst. Math. **280** (2013), 67-96.

[4] J. H. H. Chalk *&* R. A. Smith, *On Bombieri's estimate for exponential sums*. Acta Arith. **18** (1971), 191-212.

[5] T. H. Chan *&* I. E. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*. Acta Arith. **142** (2010), 59-66.

[6] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski, *&* A. Zumalacárregui, *Points on curves in small boxes and applications*. Michigan Math. J. **63** (2014), 503-534.

[7] J. Cilleruelo *&* M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*. Geom. Funct. Anal. **21** (2011), 892-904.

[8] J. Cilleruelo, M. Z. Garaev, A. Ostafe, *&* I. E. Shparlinski, *On the concentration of points of polynomial maps and applications*. Math. Z. **272** (2012), 825-837.

[9] J. Cilleruelo, I. E. Shparlinski, & A. Zumalacárregui, *Isomorphism classes of elliptic curves over a finite field in some thin families*. Math. Res. Lett. **19** (2012), 335-343.

[10] P. Erdős & C. Stewart, *On the greatest and least prime factors of n*! + 1. J. London Math. Soc. (Second series) **13** (1976), 513-519.

[11] M. Z. Garaev & J. Hernández, *A note on n*! *modulo p*. Monat. Math. **182** (2017), 23-31.

[12] M. Z. Garaev, F. Luca, & I. E. Shparlinski, *Character sums and congruences with n*!. Trans. Amer. Math. Soc. **356** (2004), 5089-5102.

[13] M. Z. Garaev, *Sumas trigonométricas y congruencias aditivas*. Gaceta R. Soc. Mat. E. **12** (2009), 129-143.

[14] V. C. García, *On the value set of n*!*m*! *modulo a large prime*. Bol. Soc. Mat. Mexicana, **13** (2007), 1-6.

[15] V. C. García, *Representation of residue classes by product of factorials, binomial coefficients, and sum of harmonic sums modulo a prime*. Bol. Soc. Mat. Mexicana, **14** (2008), 165-175.

[16] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*. Sixth edition (revised by D. R. Heath-Brown and J. H. Silverman), Oxford University Press, 2008.

[17] A. Hurwitz, *Übungen zur Zahlentheorie (1891-1918)*. Umschrift zum Barbara Aquilino vervielfältigen als Manuskript Herausgegeben von Herbert Funk und Beat Glaus. ETH-Bibliothek, Zürich, 1993.

[18] H. Iwaniec & E. Kowalski, *Analytic number theory*. Amer. Math. Soc., Providence, RI, USA, 2004.

[19] O. Klurman & M. Munsch, *Distribution of factorials modulo p*. Preprint: arXiv:1505.01198, 2015.

[20] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*. Amer. Math. Soc., Providence, RI, USA, 1994.

[21] B. Rokowska & A. Schinzel, *Sur un problème de M. Erdős*. Elem. Math. **15** (1960), 84-85.

[22] I. Ruzsa, *Sums of finite sets*. In Number Theory (New York Seminar 1991-1995); edited by D.V. Chudnovsky, G.V. Chudnovsky, and M.B. Nathanson. Springer-Verlag NY, 1996, 281-293.

[23] W. M. Schmidt, *Equations over finite fields: an elementary approach*. Lecture Notes in Mathematics, 536, Springer-Verlag Berlin-NY, 1976.

[24] S. A. Stepanov, *Arithmetic of algebraic curves*. Monographs in Contemporary Mathematics, Consultants Bureau, NY, USA, 1994.

[25] T. Tao & V. Vu, *Additive combinatorics*. Cambridge Stud. Adv. Math., 105, Cambridge University Press, 2006.

[26] T. Trudgian, *There are no socialist primes less than* 10^9. Integers **14** (2014), 1-4.

[27] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II.* Duke Math. J. **162** (2013), 673-730.