El diablo de los números

Sección a cargo de

Javier Cilleruelo

Sumas trigonométricas y congruencias aditivas

por

Moubariz Z. Garaev

1. Introducción

Las sumas trigonométricas y sus estimaciones no triviales son una herramienta básica en la teoría analítica de números que se utiliza para tratar desde problemas aditivos (problema de Waring, problema de Goldbach) hasta el problema de la distribución de los ceros de la función zeta de Riemann. En este artículo[1] vamos a mostrar algunas de sus aplicaciones en la resolución de algunas clases de congruencias aditivas.

Definamos formalmente el concepto de congruencia aditiva de la manera siguiente. Sea $m \geq 2$ un número entero y $\lambda \in \mathbb{Z}$. La congruencia

$$u + v \equiv \lambda \pmod{m}, \tag{1}$$

donde u, v son variables que recorren los sistemas de enteros

$$u = u_1, u_2, \ldots, u_N; \quad v = v_1, v_2, \ldots, v_M,$$

se llama congruencia aditiva. El problema consiste en demostrar (cuando sea posible) que esta congruencia admite soluciones y obtener (cuando sea posible) una fórmula asintótica para el número de soluciones, cuando $m \to \infty$.

Algunos ejemplos de congruencias aditivas que en teoría de números tienen un gran interés son los siguientes:

1) Sean $m = p$ primo, $N = N(p) < p$ un entero positivo y g una raíz primitiva módulo p (ver la definición en la sección 4). El problema consiste en investigar la

[1]Este artículo es una versión del minicurso que el autor impartió, en 2008, a estudiantes del Primer Encuentro en Teoría de Números en Venezuela.

distribución de las potencias $g, g^2, g^3, \ldots, g^N$ en intervalos de longitud dada M. Es decir, investigar la solubilidad de la congruencia

$$g^x - y \equiv 0 \pmod{p}, \qquad 1 \le x \le N, \quad L+1 \le y \le L+M$$

y encontrar una fórmula asintótica para el número de sus soluciones.

2) Dado un entero x coprimo con m, se denota por x^* al menor entero positivo tal que $xx^* \equiv 1 \pmod{m}$. Sea $N = N(m) < m$. Un problema importante es el estudio de la distribución de los números $\{x^* : \ (x,m) = 1, \ 1 \le x \le N\}$ en intervalos de longitud dada. En otras palabras, investigar la solubilidad de la congruencia

$$x^* - y \equiv 0 \pmod{m}, \quad 1 \le x \le N, \quad L+1 \le y \le L+M$$

y encontrar una fórmula asintótica para el número de sus soluciones. Los casos más finos de este problema se resuelven como consecuencias de estimaciones espectaculares de Karatsuba [9] y de Korolev [10] de las sumas trigonométricas análogas a las sumas de Kloosterman (ver la sección 5).

3) Sea $m = p$ un número primo y sea n un entero positivo. Investigar la solubilidad de la ecuación

$$x^n + y^n \equiv \lambda \pmod{p}, \quad 1 \le x, y \le p-1,$$

y encontrar una formula asintótica para el número de sus soluciones.

Consideremos otros ejemplos de congruencias aditivas que son de gran importancia. En lo que sigue, $\mathbb{Z}_m$ denota el anillo de las clases residuales módulo m. En el caso $m = p$ este anillo es un cuerpo y se denota por $\mathbb{F}_p$.

El conjunto $A \subset \mathbb{Z}_m$ se dice que es una base aditiva para $\mathbb{Z}_m$ de orden a lo más k si toda clase residual de $\mathbb{Z}_m$ se puede representar como suma de k elementos de A.

4) El análogo del problema de Waring para congruencias consiste en investigar los valores de k y N para los que la congruencia

$$x_1^n + \cdots + x_k^n \equiv \lambda \pmod{m}, \qquad 1 \le x_1, \ldots, x_k \le N$$

tiene solución. Este problema fue iniciado y resuelto por Karatsuba en 1961 (ver [1, Capítulo 3]).

5) Sean $m = p$ un primo y $N = N(n,p) < p$ un entero positivo. Estudiar la solubilidad y encontrar una fórmula asintótica para el número de soluciones de la siguiente ecuación modular, análoga a la ecuación de Fermat:

$$x^n + y^n + z^n \equiv 0 \pmod{p}, \qquad 1 \le x, y, z \le N.$$

6) Sea $\varepsilon > 0$. Encontrar un número entero $k = k(\varepsilon) > 0$, lo más pequeño posible, tal que para cualquier primo $p \ge p_0(\varepsilon)$ el conjunto

$$\{x^* \pmod{p} : \ 1 \le x \le [p^\varepsilon]\}$$

forme una base aditiva para $\mathbb{F}_p$ de orden a lo más k. Utilizando los resultados de Karatsuba, Shparlinski [11] demostró la existencia de tal número k de tamaño $k = O(\varepsilon^{-3})$. Glibichuk [7] redujo la cota superior hasta $k = O(\varepsilon^{-2})$.

7) Para cualquier $\varepsilon > 0$ existe un entero $k = k(\varepsilon)$ tal que el conjunto

$$\{g^x \pmod p : \ 1 \leq x \leq [p^\varepsilon]\}$$

forma una base aditiva para $\mathbb{F}_p$ del orden a lo más k. La resolución de este problema sigue de las estimaciones suma-producto de Bourgain, Katz y Tao [3], y de Bourgain, Glibichuk y Konyagin [2] (ver la sección 8).

8) La conjetura de Garaev, Luca y Shparlinski [6] afirma que existe un entero positivo k tal que para cualquier número primo p el conjunto

$$\{n! \pmod p : \ 1 \leq n \leq p\}$$

forma una base aditiva para el cuerpo $\mathbb{F}_p$ de orden a lo más k. Éste es un problema abierto.

2. Sumas Trigonométricas

La mayoría de los problemas que mencionamos en la introducción se resuelven utilizando estimaciones de ciertas sumas trigonométricas. Sean N un número entero grande y $f : [1, N] \to \mathbb{R}$ una función dada. La suma

$$\sum_{n=1}^{N} e^{2\pi i f(n)} = \sum_{n=1}^{N} \cos(2\pi f(n)) + i \sum_{n=1}^{N} \operatorname{sen}(2\pi f(n))$$

se llama suma trigonométrica. De la igualdad $|e^{2\pi i f(n)}| = 1$ se sigue la estimación trivial

$$\Big|\sum_{n=1}^{N} e^{2\pi i f(n)}\Big| \leq N.$$

El problema es obtener una estimación de la forma

$$\Big|\sum_{n=1}^{N} e^{2\pi i f(n)}\Big| \leq N\Delta$$

con $\Delta = \Delta(N)$ tan pequeño como sea posible. En particular, nosotros queremos que se cumpla que $\Delta = \Delta(N) \to 0$ cuando $N \to \infty$.

3. Lemas de Vinogradov

El punto de partida que relaciona las congruencias con las sumas trigonométricas es la siguiente identidad elemental:

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

Los siguientes lemas se pueden encontrar en los primeros trabajos de Vinogradov. El Lema 1 conecta el problema de solubilidad y la fórmula asintótica para el número de soluciones de la congruencia (1) con estimaciones de ciertas sumas trigonométricas. Los Lemas 2 y 3 son estimaciones sencillas pero muy útiles en las aplicaciones.

Lema 1. *Sean $m \geq 2$ entero, y u, v números que recorren los sistemas de enteros*

$$u = u_1, u_2, \ldots, u_N; \qquad v = v_1, v_2, \ldots, v_M.$$

Supongamos que

$$\max_{1 \leq a \leq m-1} \left| \sum_u e^{2\pi i a u/m} \right| \leq R; \qquad \sum_{a=1}^{m-1} \left| \sum_v e^{2\pi i a v/m} \right| \leq D.$$

Entonces, para cualquier entero λ el número T de soluciones de la congruencia

$$u + v \equiv \lambda \pmod{m}$$

se puede representar en la forma

$$T = \frac{NM}{m}\Big(1 + \theta \frac{RD}{NM}\Big)$$

para algún $-1 \leq \theta \leq 1$.

Demostración. Sustituimos en (2) $x = u + v - \lambda$:

$$\frac{1}{m} \sum_{a=0}^{m-1} e^{2\pi i a(u+v-\lambda)/m} = \begin{cases} 1, & \text{si } u + v \equiv \lambda \pmod{m}, \\ 0, & \text{si } u + v \not\equiv \lambda \pmod{m}. \end{cases}.$$

Sumando esta identidad para $u = u_1, u_2, \ldots, u_N$ y $v = v_1, v_2, \ldots, v_M$ tenemos

$$T = \sum_u \sum_v \frac{1}{m} \sum_{a=0}^{m-1} e^{2\pi i a(u+v-\lambda)/m} = \frac{1}{m} \sum_{a=0}^{m-1} \sum_u \sum_v e^{2\pi i a(u+v-\lambda)/m}.$$

Separando el término $a = 0$ se obtiene

$$T = \frac{NM}{m} + \text{Error}, \tag{3}$$

donde

$$\text{Error} = \frac{1}{m} \sum_{a=1}^{m-1} \left(\sum_u e^{2\pi i a u/m} \right) \left(\sum_v e^{2\pi i a v/m} \right) e^{-2\pi i a \lambda/m}.$$

Por las hipótesis del lema,

$$|\text{Error}| \leq \frac{1}{m} \sum_{a=1}^{m-1} \left| \sum_u e^{2\pi i a u/m} \right| \left| \sum_v e^{2\pi i a v/m} \right| \leq \frac{R}{m} \sum_{a=1}^{m-1} \left| \sum_v e^{2\pi i a v/m} \right| \leq \frac{RD}{m}.$$

Entonces, para algún θ con $|\theta| \leq 1$ se cumple que Error $= \theta RD/m$, que junto con (3) implica la afirmación. □

Lema 2. *Sea m un entero positivo y sea a un entero coprimo con m. Entonces*

$$\left|\sum_{u=0}^{m-1}\sum_{v=0}^{m-1}\nu(u)\varrho(v)e^{2\pi iauv/m}\right| \leq \sqrt{mUV},$$

donde $\nu(u), \varrho(v)$ son números complejos y

$$\sum_{u=0}^{m-1}|\nu(u)|^2 = U, \quad \sum_{v=0}^{m-1}|\varrho(v)|^2 = V.$$

Demostración. Tenemos

$$S := \sum_{u=0}^{m-1}\sum_{v=0}^{m-1}\nu(u)\varrho(v)e^{2\pi iauv/m} = \sum_{u=0}^{m-1}\nu(u)\left(\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right).$$

Aplicando la desigualdad de Cauchy-Schwarz a la suma sobre u, deducimos que

$$|S|^2 \leq \left(\sum_{u=0}^{m-1}|\nu(u)|^2\right)\sum_{u=0}^{m-1}\left|\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right|^2 = U\sum_{u=0}^{m-1}\left|\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right|^2. \quad (4)$$

Observemos que

$$\sum_{u=0}^{m-1}\left|\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right|^2 = \sum_{u=0}^{m-1}\left(\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right)\overline{\left(\sum_{v'=0}^{m-1}\varrho(v')e^{2\pi iauv'/m}\right)}$$
$$= \sum_{u=0}^{m-1}\sum_{v=0}^{m-1}\sum_{v'=0}^{m-1}\varrho(v)\overline{\varrho(v')}e^{2\pi iau(v-v')/m} = \sum_{v=0}^{m-1}\sum_{v'=0}^{m-1}\varrho(v)\overline{\varrho(v')}\sum_{u=0}^{m-1}e^{2\pi iau(v-v')/m}.$$

Como $(a,m)=1$, según (2) el último sumatorio es igual a cero cuando $v \neq v'$ e igual a m cuando $v = v'$. Entonces,

$$\sum_{u=0}^{m-1}\left|\sum_{v=0}^{m-1}\varrho(v)e^{2\pi iauv/m}\right|^2 = m\sum_{v=0}^{m-1}|\varrho(v)|^2. \quad (5)$$

Combinando (5) con (4), concluimos la afirmación. □

En las hipótesis del Lema 1 aparece el requisito

$$\sum_{a=1}^{m-1}\left|\sum_{v}e^{2\pi iav/m}\right| \leq D,$$

donde v recorre el sistema de números enteros $v_1, v_2, \ldots, v_M$. Sucede que si este sistema coincide con una sucesión de números enteros consecutivos se puede tener una buena estimación para la suma indicada.

Lema 3. *Para cualquier entero $M \geq 1$ se cumple la desigualdad*

$$\sum_{a=1}^{m-1} \left| \sum_{y=1}^{M} e^{2\pi i a y/m} \right| < m \log m.$$

Para demostrar el Lema 3 hay que observar que para $1 \leq a \leq m/2$ se cumple

$$\left| \sum_{y=1}^{M} e^{2\pi i a y/m} \right| \leq \frac{1}{\operatorname{sen}(\pi a/m)} \leq \frac{m}{2a}.$$

La demostración completa la dejamos al lector como ejercicio.

4. Algunas aplicaciones de Lemas de Vinogradov

Recordemos que un número entero $g \not\equiv 0 \pmod p$ se denomina raíz primitiva módulo el número primo p si todos los números $g^1, g^2, \ldots, g^{p-1}$ son distintos entre sí módulo p. Gauss demostró que para cualquier módulo primo p existen exactamente $\phi(p-1)$ raíces primitivas distintas módulo p, donde $\phi(x)$ es la función de Euler.

En teoría analítica de números una cantidad considerable de congruencias están conectadas con raíces primitivas. Uno de los resultados de Vinogradov (publicado en 1926) afirma que si $N \leq p-1$ y $M \leq p$ son enteros positivos, entonces la cantidad T de los números de la sucesión

$$g, g^2, g^3, \ldots, g^N$$

cuyos mínimos residuos positivos módulo p son menores que M se expresa por la fórmula

$$T = \frac{NM}{p} + O(p^{1/2} \log^2 p).$$

Sobre la demostración de este resultado hablaremos más adelante. Ahora vamos a considerar una aplicación sencilla de los lemas de Vinogradov.

4.1. Diferencias de las potencias de una raíz primitiva

El problema de la distribución de diferencias de potencias de una raíz primitiva módulo un primo p aparece en trabajos de Cilleruelo, Garaev, García, Ka-Lam Kueh, Konyagin, Rudnick, Shkredov, Vajaitu, Zaharescu y otros matemáticos. Como un ejemplo de la aplicación de los lemas de Vinogradov vamos a demostrar la siguiente afirmación.

Afirmación 1. *Existe una constante c tal que para cualquier entero λ la congruencia*

$$g^x - g^y \equiv \lambda \pmod p$$

se satisface para algunos enteros positivos $x \leq cp^{3/4}$, $y \leq cp^{3/4}$.

Esta afirmación fue demostrada en 2002/3 independentemente por Garaev y Ka-Lam Kueh, por Konyagin, y por Shkredov. La conjetura, que se atribuye a Odlyzco, afirma que se puede sustituir $cp^{3/4}$ por $cp^{1/2+\varepsilon}$ para cualquier $\varepsilon > 0$ y alguna constante $c = c(\varepsilon) > 0$.

Vamos a seguir las ideas de [5]. Podemos asumir que p es un número grande y que $\lambda \not\equiv 0 \pmod p$, ya que la afirmación es trivial en caso contrario. Consideremos la congruencia aditiva ternaria

$$g^x - g^y - \lambda g^{p-1-z} g^{p-1-t} \equiv 0 \pmod p; \qquad 1 \le x, y, z, t \le 2[p^{3/4}]. \tag{6}$$

Si demostramos que esta congruencia tiene soluciones, esto implicará que la congruencia

$$g^{x+z+t} + g^{y+z+t} \equiv \lambda \pmod p$$

también tiene soluciones y de aquí se seguirá la afirmación con $c = 6$.

Con este fin, aplicamos el Lema 1 para los sistemas de enteros

$$u = g^{p-1-z} g^{p-1-t}; \qquad 1 \le z, t \le 2[p^{3/4}],$$
$$v = g^x - g^y; \qquad 1 \le x, y \le 2[p^{3/4}].$$

Denotemos $L = 2[p^{3/4}]$. Cuando n recorre los enteros del intervalo $1 \le n \le L$, los números g^n (así como los números g^{p-1-n}) recorren sistemas de números enteros distintos módulo p. Entonces, según el Lema 2, tenemos

$$\max_{1 \le a \le p-1} \left| \sum_u e^{2\pi i a u/p} \right| \le \sqrt{pL^2} = p^{1/2} L.$$

Por otro lado (ver la igualdad (5))

$$\sum_{a=1}^{p-1} \left| \sum_v e^{2\pi i a v/p} \right| = \sum_{a=1}^{p-1} \left| \sum_{x=1}^{L} e^{2\pi i a g^x/p} \right|^2 \le pL.$$

Entonces, por el Lema 1, el número T de soluciones de la congruencia (6) satisface

$$T = \frac{L^4}{p} \left(1 + \theta \frac{p^{3/2}}{L^2} \right); \quad |\theta| \le 1.$$

En particular, tenemos $T > 0$.

4.2. Distribución de las potencias de una raíz primitiva

Ahora demostremos el resultado de Vinogradov que mencionamos al inicio de esta sección.

Afirmación 2. *Sean $N \le p-1$, $M \le p$ enteros positivos. Entonces la cantidad T de los términos de la sucesión*

$$g, g^2, g^3, \ldots, g^N$$

cuyos mínimos residuos positivos módulo p son menores o iguales que M se expresa por la fórmula

$$T = \frac{NM}{p} + O(p^{1/2}\log^2 p).$$

Demostración. En el Lema 1 tomemos $m = p$, y los sistemas de enteros

$$u = g, g^2, \ldots, g^N; \quad v = 1, 2, \ldots, M.$$

Entonces, combinando el Lema 1 con el Lema 3, deducimos que

$$T = \frac{NM}{p} + O(R\log p),$$

donde

$$R = \max_{1\le a\le p-1} \left| \sum_{x=1}^{N} e^{2\pi i a g^x/p} \right|.$$

Para concluir la demostración basta con probar que

$$\left| \sum_{x=1}^{N} e^{2\pi i a g^x/p} \right| = O(p^{1/2}\log p).$$

Esta estimación se puede establecer a través de los siguientes pasos.

Paso 1. Sean $1 \le a \le p-1$, $1 \le b \le p-2$. Veamos primero que el módulo de la suma

$$S(a,b) = \sum_{x=1}^{p-1} e^{2\pi i(\frac{ag^x}{p} + \frac{bx}{p-1})}$$

no depende de a. De hecho, sea t un entero tal que $a \equiv g^t \pmod p$. Entonces

$$|S(a,b)| = \left| \sum_{x=1}^{p-1} e^{2\pi i(\frac{g^{x+t}}{p} + \frac{bx}{p-1})} \right|.$$

Haciendo el cambio de variable $x \mapsto x - t$ obtenemos que $|S(a,b)| = |S(1,b)|$. Utilizando esta observación deducimos que

$$(p-1)|S(a,b)|^2 = \sum_{a=1}^{p-1} |S(a,b)|^2 = \sum_{a=0}^{p-1} \left| \sum_{x=1}^{p-1} e^{2\pi i(\frac{ag^x}{p} + \frac{bx}{p-1})} \right|^2 = p(p-1).$$

Entonces, $|S(a,b)| = p^{1/2}$.

Paso 2. Observemos que

$$\sum_{x=1}^{N} e^{2\pi i a g^x/p} = \sum_{x=1}^{p-1} e^{2\pi i a g^x/p} \left(\frac{1}{p-1} \sum_{b=1}^{p-1} \sum_{z=1}^{N} e^{2\pi i b(x-z)/(p-1)} \right),$$

ya que la expresión dentro del paréntesis es cero o uno dependiendo de si $N < x < p$ o $1 \leq x \leq N$. Entonces,

$$\left|\sum_{x=1}^{N} e^{2\pi i a g^x/p}\right| \leq \frac{1}{p-1}\sum_{b=1}^{p-1}\left|\sum_{x=1}^{p-1} e^{2\pi i(\frac{ag^x}{p}+\frac{bx}{p-1})}\right|\left|\sum_{z=1}^{N} e^{2\pi i\frac{bz}{p-1}}\right|.$$

Paso 3. La demostración se termina combinando el Paso 1 y el Paso 2 con el Lema 3. □

Nota. El resultado de Vinogradov es no trivial cuando NM es más grande que $p^{3/2}\log^2 p$. Se puede demostrar (ver [4]) que de hecho se cumple

$$T = \frac{NM}{p} + O(p^{1/2}\log^2(NMp^{-3/2}+2)),$$

que es un resultado no trivial cuando NM es más grande que $p^{3/2}$.

4.3. Ecuación de Fermat en $\mathbb{F}_p$

Sea $n \geq 2$ un número entero. Utilizando la existencia de raíces primitivas en $\mathbb{F}_p$ se puede demostrar fácilmente que la cantidad de elementos distintos módulo p de las potencias

$$1^n, 2^n, \ldots, (p-1)^n$$

es igual a $(p-1)/d$, donde $d = (n, p-1)$. Vamos a aplicar los lemas de Vinogradov para investigar la congruencia ternaria aditiva

$$x^n + y^n + z^n \equiv 0 \pmod{p}; \qquad 1 \leq x, y, z \leq p-1. \tag{7}$$

Afirmación 3. *El número T de soluciones de la congruencia* (7) *se representa de la forma*

$$T = \frac{(p-1)^3}{p}\left(1 + \theta\frac{n^2p^{1/2}}{p-1}\right); \qquad |\theta| \leq 1.$$

En particular, si $n < (p-1)^{1/2}p^{-1/4}$, dicha congruencia admite soluciones.

Demostración. El Lema 1 aplicado a los sistemas de enteros

$$u = 1^n, 2^n, \ldots, (p-1)^n,$$

$$v = y^n + z^n; \qquad 1 \leq y, z \leq p-1,$$

sugiere obtener estimaciones superiores para

$$V := \max_{1\leq a\leq p-1}\left|\sum_{x=1}^{p-1} e^{2\pi i a x^n/p}\right|$$

y para

$$W := \sum_{a=1}^{p-1} \left| \sum_{y=1}^{p-1} \sum_{z=1}^{p-1} e^{2\pi i a(y^n+z^n)/p} \right| \le \sum_{a=1}^{p-1} \left| \sum_{y=1}^{p-1} e^{2\pi i a y^n/p} \right|^2 .$$

La expresión W se estima fácilmente, como en (5). Existen varios métodos para estimar el valor V. Nosotros vamos a utilizar el Lema 2. Para cualquier número t coprimo con p se cumple

$$\sum_{x=1}^{p-1} e^{2\pi i a x^n/p} = \sum_{x=1}^{p-1} e^{2\pi i t^n x^n/p}.$$

Entonces, tomando la suma sobre $1 \le t \le p-1$, tenemos

$$\sum_{x=1}^{p-1} e^{2\pi i a x^n/p} = \frac{1}{p-1} \sum_{x=1}^{p-1} \sum_{t=1}^{p-1} e^{2\pi i t^n x^n/p} = \frac{1}{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \nu(u)\nu(v) e^{2\pi i a u v/m},$$

donde $\nu(u)$ es el número de soluciones de la congruencia

$$t^n \equiv u \pmod p, \quad 1 \le t \le p-1.$$

El Lema 2 implica

$$\left| \sum_{x=1}^{p-1} e^{2\pi i a x^n/p} \right| \le \frac{p^{1/2} U}{p-1}; \qquad U = \sum_{u=0}^{p-1} \nu(u)^2.$$

Observemos que U es igual al número de soluciones de la congruencia

$$x^n \equiv y^n \pmod p; \qquad 1 \le x, y \le p-1.$$

Para cada y fijo existen a lo más n posibilidades para x. Entonces $U \le n(p-1)$ y tenemos

$$\max_{1 \le a \le p-1} \left| \sum_{x=1}^{p-1} e^{2\pi i a x^n/p} \right| \le n p^{1/2}.$$

Acerca de W, agregando y restando a la suma el término con $a = 0$, obtenemos fácilmente que $W \le (p-1)^2 n$. Entonces, aplicando el Lema 1 concluimos la demostración. □

Afirmación 4. *Sea $\lambda \not\equiv 0 \pmod p$. El número T de soluciones de la congruencia*

$$x^n + y^n \equiv \lambda \pmod p; \qquad 1 \le x, y \le p-1,$$

se representa en la forma

$$T = \frac{(p-1)^2}{p} \left(1 + \theta \frac{n^2 p^{1/2}}{p-1} \right); \qquad |\theta| \le 1.$$

La demostración sigue de la misma manera que la demostración de la Afirmación 3, observando que $T = T_1/(p-1)$, donde T_1 es el número de soluciones de la congruencia

$$x^n + y^n \equiv \lambda z^n \pmod p, \qquad 1 \le x, y, z \le p-1.$$

5. Sumas de Kloosterman y sus análogas

Sean a, b enteros, $(a, m) = 1$. En teoría de números la suma

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

se llama suma de Kloosterman. Por trabajos de Weil se sabe que cuando $m = p$ es un primo, se cumple la estimación

$$|S(a, b; p)| \leq 2p^{1/2}.$$

Esta última estimación implica (recordemos los Pasos 2 y 3 de la sección 4) la siguiente estimación de la suma incompleta de Kloosterman: para cualquier $1 \leq N < p$, se tiene

$$\sum_{x=1}^{N} e^{2\pi i a x^*/p} \leq 2p^{1/2} \log p.$$

Utilizando esta estimación se puede demostrar que, para cualquier constante $0 < c < 1$ y para cualquier $\varepsilon > 0$, si $p^{1/2+\varepsilon} < N < p$ y $M > cp$ entonces el número T de las soluciones de la congruencia

$$x^* - y \equiv 0 \pmod{p}$$

se puede representar como

$$T = \frac{NM}{p}\Big(1 + O(p^{-\delta})\Big); \quad \delta = \delta(\varepsilon) > 0.$$

En 1995 Karatsuba [9] obtuvo impresionantes resultados en esta dirección. Por ejemplo, para cualquier número pequeño fijo $\varepsilon > 0$, Karatsuba obtuvo estimaciones no triviales para sumas de la forma

$$W = \sum_{x} e^{2\pi i a x^*/m},$$

donde x recorre los enteros coprimos con m en el intervalo $[1, m^{\varepsilon}]$. Utilizando las estimaciones de Karatsuba, Shparlinski [11] demostró que para cualquier $\varepsilon > 0$ el conjunto

$$\{x^* \pmod{p} : \ 1 \leq x \leq [p^{\varepsilon}]\}$$

forma una base aditiva para $\mathbb{F}_p$ de orden a lo más k para algún $k = O(\varepsilon^{-3})$. Glibichuk [7] redujo esta cota hasta $k = O(\varepsilon^{-2})$.

Las ideas de Karatsuba y sus resultados fueron utilizados y complementados por Korolev [10]. Sea X la cantidad de números enteros menores o iguales que N y coprimos con m. Korolev demostró que si $(a, m) = 1$ y si α, β son números reales dados con $0 \leq \alpha < \beta < 1$, entonces el número T de soluciones de la desigualdad

$$\alpha \leq \left\{\frac{ax^* + bx}{m}\right\} < \beta, \quad 1 \leq x \leq N, \quad (x, m) = 1,$$

se representa de la forma

$$T = (\beta - \alpha)X + O(N\Delta),$$

donde

$$\Delta = (\log N)^{-5/24}(\log m)^{1/6}(\log\log m)^{49/24}.$$

Notemos que dicha desigualdad es equivalente a la congruencia

$$ax^* + bx - y \equiv 0 \pmod{m}, \qquad 1 \le x \le N, \quad (x,m) = 1; \quad \alpha m \le y < \beta m.$$

El lector puede ver una información completa en [1, Capítulo 12].

6. Estimación de Weil

Ya hemos visto cómo estimar la suma trigonométrica

$$\sum_{x=1}^{p} e^{2\pi i a x^n/p}.$$

Una estimación más general y más profunda se debe a Weil.

Afirmación 5. *Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio de grado $n \ge 1$ con coeficientes enteros, $a_n \not\equiv 0 \pmod{p}$. Entonces,*

$$\left| \sum_{x=1}^{p} e^{2\pi i f(x)/p} \right| \le np^{1/2}.$$

Utilizando esta afirmación uno puede deducir la siguiente estimación (otra vez recordemos los Pasos 2 y 3 de la sección 4).

Afirmación 6. *Sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio de grado $n \ge 2$ con coeficientes enteros, $a_n \not\equiv 0 \pmod{p}$. Entonces, para cualquier entero positivo $N \le p$ se cumple*

$$\left| \sum_{x=1}^{N} e^{2\pi i f(x)/p} \right| \le np^{1/2} \log p.$$

Con la ayuda de la Afirmación 5 el lector puede demostrar sin dificultad que si $1 \le N \le p-1$, entonces el número T de soluciones de la congruencia

$$x^n + y^n + z^n \equiv 0 \pmod{p}, \qquad 1 \le x, y, z \le N,$$

se representa de la forma

$$T = \frac{N^3}{p}\Big(1 + \theta \frac{n^2 p^{3/2} \log p}{N^2}\Big); \qquad |\theta| \le 1.$$

7. Una congruencia aditiva con factoriales

En [6], Garaev, Luca y Shparlinski aplicaron sumas trigonométricas para investigar varias congruencias aditivas con factoriales. Uno de sus resultados afirma que cualquier clase residual λ módulo p se representa de la forma

$$n!\, m! + n_1! + n_2! + \cdots + n_{47}! \equiv \lambda \pmod{p},$$

donde

$$\max\{n, m, n_1, \ldots, n_{47}\} \leq Cp^{1350/1351}; \qquad C > 0.$$

Para demostrar esta afirmación se utiliza, en particular, la siguiente estimación de una suma doble trigonométrica con factoriales:

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

Recordemos que la conjetura es que existe un entero positivo k tal que para cualquier número primo p el conjunto

$$\{n! \pmod{p} : \ 1 \leq n \leq p\}$$

forma una base aditiva para $\mathbb{F}_p$ de orden a lo más k.

8. Métodos combinatorios

Sea p un número primo grande. Recordemos que para cualquier raíz primitiva g se cumple la estimación

$$\max_{1\leq a\leq p-1} \left| \sum_{x=1}^{N} e^{2\pi i a g^x/p} \right| = O(p^{1/2} \log p).$$

En particular, utilizando las técnicas propuestas se puede deducir que para cualquier $\varepsilon > 0$ existe un entero $k = k(\varepsilon)$ tal que toda clase residual se puede representar como suma de k elementos del conjunto $\{g^x \pmod{p} : \ x \leq N\}$, donde $N = [p^{1/2+\varepsilon}]$. En otras palabras, este conjunto es una base aditiva para $\mathbb{F}_p$ de orden a lo más k. La pregunta natural es si se puede obtener la misma afirmación para un número N de orden más pequeño que $p^{1/2+\varepsilon}$. Utilizando métodos combinatorios, Glibichuk [7] demostró que si $A, B \subset \mathbb{F}_p$ con $|A||B| > 2p$, entonces el conjunto $AB = \{ab : \ a \in A,\ b \in B\}$ es una base aditiva para $\mathbb{F}_p$ de orden a lo más 8. En particular, tomando

$$A = B = \{g^x \pmod{p} : \ 1 \leq x \leq [1{,}5p^{1/2}]\},$$

se sigue que el conjunto $\{g^x \pmod{p} : \ x \leq 3p^{1/2}\}$ es una base aditiva para $\mathbb{F}_p$ de orden a lo más 8 (de hecho, Glibichuk demostró una afirmación más fina, ver [7, Corolario 5]).

Ahora recordemos la famosa estimación suma-producto de Bourgain, Katz y Tao [3], y Bourgain, Glibichuk y Konyagin [2]: para cualquier constante $0 < c < 1$ existe $\delta = \delta(c) > 0$ tal que si $A \subset \mathbb{F}_p$ con $|A| < p^c$, entonces

$$|A + A| + |AA| > |A|^{1+\delta}.$$

Tomando $A = \{g^x \pmod p : 1 \leq x \leq [p^{\varepsilon_0}]\}$ con un pequeño $\varepsilon_0 > 0$, iterando la estimación de suma-producto y aplicando el resultado de Glibichuk obtenemos que para cualquier fijo $\varepsilon > 0$ existe un entero $k = k(\varepsilon)$ tal que el conjunto

$$\{g^x \pmod p : \ 1 \leq x \leq [p^{\varepsilon}]\}$$

forma una base aditiva para $\mathbb{F}_p$ de orden a lo más k. En relación con estos resultados también es preciso mencionar el importante trabajo de Glibichuk y Konyagin [8].

Agradecimiento. El autor agradece a los profesores Javier Cilleruelo, Fernando Chamizo y Víctor García sus valiosos comentarios.

Referencias

[1] G. I. Arkhipov, V. N. Chubarikov y A. A. Karatsuba, «Trigonometric Sums in Number Theory and Analysis», Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

[2] J. Bourgain, A. A. Glibichuk y S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order,* J. London Math. Soc. (2) **73** (2006), 380–398.

[3] J. Bourgain, N. Katz y T. Tao, *A sum-product estimate in finite fields, and applications,* Geom. Func. Anal. **14** (2004), 27–57.

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

[5] M. Z. Garaev y K.-L. Kueh, *Distribution of special sequences modulo a large prime,* Int. J. of Math. and Math. Sci. **50** (2003), 3189–3194.

[6] M. Z. Garaev, F. Luca y I. E. Shparlinski, *Exponential sums and congruences with factorials*, J. Reine Angew. Math. **584** (2005), 29–44.

[7] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem,* Math. Notes **79** (2006), 356–365.

[8] A. A. Glibichuk y S. V. Konyagin, *Additive properties of product sets in fields of prime order,* Centre de Recherches Mathématiques, CRM Proceedings and Lecture Notes, 43, 279–286 (2007).

[9] A. A. Karatsuba, *Fractional parts of functions of a special form,* Izvestiya: Mathematics **59**:4 (1995), pp. 721–740.

[10] M. A. Korolev, *Incomplete Kloosterman sums and their applications,* Izvestiya: Mathematics **64**:6 (2000), pp. 1129–1152.

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

[12] I. M. Vinogradov, «An introduction to the theory of numbers», Pergamon Press, London & New York, 1955.

[13] I. M. Vinogradov, «Selected Works» (in Russian), Moscow, 1952.

M. Z. Garaev, Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

Correo electrónico: garaev@matmor.unam.mx

Página web: http://www.matmor.unam.mx/~garaev