Divulgaciones Matemáticas Vol. 12 No. 2(2004), pp. 171–180

Contando con Sumas de Gauss

Counting with Gauss' Sums

José O. Araujo (jaraujo@exa.unicen.edu.ar)
Laura B. Fernández (lfernan@exa.unicen.edu.ar)
Fac. de Ciencias Exactas, UNICEN
Tandil, 7000 Buenos Aires, Argentina

Resumen

En este trabajo presentamos una aplicación de las sumas de Gauss para la determinación del número de puntos de ciertas cuádricas sobre un cuerpo finito.
Palabras y frases clave: sumas de Gauss, formas cuadráticas, cuadrados.

Abstract

In this work we present an aplication of Gauss' sums to the determination of the number of points of certain quadrics over a finite field.
Key words and phrases: Gauss' sums, quadratic forms, squares.

1 Introducción

Gauss introdujo y estudió las sumas que llevan su nombre, usándolas, entre otras cosas, para dar una demostración de la ley de reciprocidad cuadrática (ver [2] o [4]). Esta ley fue descubierta empíricamente por Euler y demostrada en forma parcial por el mismo Euler.
El material de divulgación que presentamos a continuación podría resultar atractivo a la hora de mostrar algunas aplicaciones de las sumas de Gauss, en este caso, para calcular el número de soluciones de un tipo de ecuaciones de congruencias módulo un número primo impar.

Recibido 2004/10/01. Revisado 2004/11/18. Aceptado 2004/11/19.
MSC (2000): Primary 11A07.

2 El problema

Los temas relativos a congruencias y sus propiedades básicas pueden encontrarse en [3], [4] o [5].
Como ya dijimos, nos hemos interesado en número de soluciones de una ecuación de congruencias, más precisamente, por el número de puntos de una cuádrica asociada a una forma cuadrática sobre el cuerpo de restos módulo un número primo impar.
Notaremos con p un número primo impar, y con $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ el cuerpo de restos módulo el primo p.
Consideremos $q(x_1, \ldots, x_n)$ una forma cuadrática sobre $\mathbb{Z}_p$, es decir una función de las variables $x_1, \ldots, x_n$ que tiene la forma:

$$q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \qquad (a_{ij} \in \mathbb{Z}_p) \qquad [1]$$

El problema a tratar en estas notas es el siguiente:

¿Cuántos puntos tiene la cuádrica dada por $q(x_1, \ldots, x_n) = k$, $(k \in \mathbb{Z}_p)$*?*

En particular, tendríamos el caso de lo que podríamos llamar *superficies esféricas* dadas por las ecuaciones:

$$x_1^2 + \cdots + x_n^2 = k$$

El número de puntos de las superficies esféricas fue presentado en [1]. El caso general no es muy diferente si tenemos en cuenta que toda forma cuadrática puede ser expresada como:

$$\sum_{i=1}^{n} a_i x_i^2$$

mediante un cambio lineal de coordenadas.

3 Preliminares

3.1 Los cuadrados

En el cuerpo $\mathbb{Z}_p$, indicaremos con $\mathcal{C}$ el conjunto de elementos no nulos que son un cuadrado en $\mathbb{Z}_p$ (*cuadrados no nulos*), y con $\mathcal{N}$ el conjunto de elementos que no son un cuadrado en $\mathbb{Z}_p$(*no cuadrados*). Se tiene:

$$\mathbb{Z}_p = \{0\} \cup \mathcal{C} \cup \mathcal{N}$$

Elegimos como sistema de representante de restos módulo p al conjunto:

$$\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\right\}$$

Resulta claro que hay $\frac{p-1}{2}$ cuadrados no nulos, dados por:

$$(\pm 1)^2, (\pm 2)^2, \ldots, \left(\pm \frac{p-1}{2}\right)^2$$

En consecuencia se tiene:

$$|\mathcal{C}| = \frac{p-1}{2} = |\mathcal{N}|$$

Observemos que si $a \in \mathcal{C}$ y $b \in \mathcal{N}$ se verifican:

$$a\mathcal{C} = \{am : m \in \mathcal{C}\} = \mathcal{C} \quad \text{y} \quad a\mathcal{N} = \{am : m \in \mathcal{N}\} = \mathcal{N}$$
$$b\mathcal{C} = \{bm : m \in \mathcal{C}\} = \mathcal{N} \quad \text{y} \quad b\mathcal{N} = \{bm : m \in \mathcal{N}\} = \mathcal{C}$$

Para establecer estas identidades, tendremos en cuenta los siguientes hechos que se comprueban sin mayor dificultad:
El producto de dos cuadrados es un cuadrado.
El producto de un cuadrado no nulo por un no cuadrado es un no cuadrado.
El producto por un elemento no nulo determina una biyección en Z_p.
Ahora, $a\mathcal{C} \subseteq \mathcal{C}$ y la aplicación dada por $m \to am$ es inyectiva, resulta $a\mathcal{C} = \mathcal{C}$ y consecuentemente $a\mathcal{N} = \mathcal{N}$.
Por otra parte, $b\mathcal{C} \subseteq \mathcal{N}$, la aplicación dada por $m \to bm$ es inyectiva y $|\mathcal{C}| = |\mathcal{N}|$, resulta $b\mathcal{C} = \mathcal{N}$ y $b\mathcal{N} = \mathcal{C}$.

3.2 Las formas cuadráticas.

No vamos a tratar en detalle lo relativo a diagonalización de formas cuadráticas. Enunciaremos y usaremos un resultado que garantiza una diagonalización de una forma cuadrática con coeficientes en un cuerpo.
Dada una forma cuadrática $q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ sobre $\mathbb{Z}_p$, existe una matriz simétrica $B = [b_{ij}] \in \mathbb{Z}_p^{n \times n}$ tal que:

$$q(x_1, \ldots, x_n) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} B \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Es claro que:

$$b_{ij} = \frac{a_{ij} + a_{ji}}{2}$$

La forma cuadrática $q(x_1, \ldots, x_n)$ se dice *no singular* si B es inversible.
El teorema de diagonalización al que nos referimos anteriormente se basa en el siguiente resultado que presentamos sin demostración.

Lema 3.1. *Sea K un cuerpo y $B \in K^{n\times n}$ una matriz simétrica. Existe una matriz inversible $U \in K^{n\times n}$ tal que $UB\,{}^tU$ es una matriz diagonal.*

En el enunciado del lema ${}^tU$ indica la matriz traspuesta de U. La demostración del lema no difiere de la que suele darse en un curso de algebra lineal para matrices simétricas reales.

Teorema 3.2. *Una forma cuadrática no singular con coeficientes en Z_p puede ser representada por una expresión de la forma:*

$$x_1^2 + \cdots + x_m^2 + e\left(x_{m+1}^2 + \cdots + x_n^2\right)$$

donde m es un entero entre 0 y n, $e \in N$.

Demostración Consideremos la expresión de la forma cuadrática como:

$$q(z_1, \ldots, z_n) = \begin{bmatrix} z_1 & \ldots & z_n \end{bmatrix} B \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

En virtud del lema, existe una matriz inversible U tal que $D = UB\,{}^tU$ es una matriz diagonal. En las coordenadas $y_1, \ldots, y_n$ dado por:

$$\begin{bmatrix} y_1 & \ldots & y_n \end{bmatrix} = \begin{bmatrix} z_1 & \ldots & z_n \end{bmatrix} U^{-1}$$

la expresión de q es:

$$\begin{bmatrix} y_1 & \ldots & y_n \end{bmatrix} D \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = d_1 y_1^2 + \cdots + d_n y_n^2$$

donde los d_i son los elementos en la diagonal principal de D. Como B es no singular, $d_i \neq 0$ para $i = 1, \ldots, n$. Reordenando la expresión, si fuera necesario, podemos suponer que para algún índice m se cumple que $d_1, \ldots, d_m \in \mathcal{C}$ y $d_{m+1}, \ldots, d_n \in \mathcal{N}$. Fijado $e \in \mathcal{N}$, se tiene:

$$\begin{array}{ll} d_i = k_i^2 & \text{si} \quad i \leq m \\ d_i = ek_i^2 & \text{si} \quad m < i \end{array}$$

En el sistema de coordenadas dado por $x_i = k_i y_i$ se tiene la expresión buscada.
■

3.3 El número de puntos

Fijado $e \in \mathcal{N}$ y $m \leq n$, en lo que sigue estudiaremos el número de puntos en la hipersuperficie de ecuación:

$$x_1^2 + \cdots + x_m^2 + e\left(x_{m+1}^2 + \cdots + x_n^2\right) = k \qquad (k \in \mathbb{Z}_p)$$

Notemos con $c_{m,k}$ el número de tales puntos. Resulta claro que:

$$\begin{array}{ll} c_{m,k} = c_{m,1} & \text{si} \quad k \in \mathcal{C} \\ c_{m,k} = c_{m,e} & \text{si} \quad k \in \mathcal{N} \end{array}$$

pues basta multiplicar los puntos en una de las hipersuperficies por un escalar apropiado para obtener los puntos en la otra hipersuperficie.
Los p^n puntos en $\mathbb{Z}_p^n$ pueden ser agrupados según el valor la forma cuadrática, de donde:

$$p^n = c_{m,0} + \frac{p-1}{2} c_{m,1} + \frac{p-1}{2} c_{m,e}$$

Notar que $c_{m,1} = c_{n-m,e}$, $c_{m,e} = c_{n-m,1}$ y $c_{m,0} = c_{n-m,0}$.

3.4 El caso $n = 2$

Para simplificar la notación, usaremos x, y en lugar de x_1, x_2. En este caso tenemos las ecuaciones:

$$\begin{array}{rll} e\left(x^2 + y^2\right) = k & \text{si} & m = 0 \\ x^2 + ey^2 = k & \text{si} & m = 1 \\ x^2 + y^2 = k & \text{si} & m = 2 \end{array}$$

Proposición 3.3. *Si $n = 2$ y $k \neq 0$, entonces $c_{m,k} = c_{m,1}$.*

Demostración Bastará ver que, en este caso, $c_{m,1} = c_{m,e}$. Dado que $c_{0,1} = c_{2,e}$ y $c_{0,e} = c_{2,1}$, podemos probar la afirmación para $m \geq 1$.
Mostremos primero que $c_{m,1}$ y $c_{m,e}$ no son cero, lo cual es claro si $m = 1$. Si $m = 2$, resulta evidente que $c_{2,1} \neq 0$. Si $c_{2,e}$ fuera igual a cero, la suma de dos cuadrados tendría que ser nuevamente un cuadrado, entonces serían cuadrados: $1, 2 = 1 + 1, 3 = 2 + 1, \ldots$ es decir $\mathbb{Z}_p \subseteq \mathcal{C}$, lo cual es un absurdo.
Indiquemos con $x^2 + \delta y^2 = k$ a una de las ecuaciones, siendo $\delta = e$ si $m = 1$ y $\delta = 1$ si $m = 2$.

Fijemos $(x, y) \in \mathbb{Z}_p^2$ tal que:

$$x^2 + \delta y^2 = e$$

La transformación lineal σde $\mathbb{Z}_p^2$ dada por:

$$\sigma\,(u, v) = (xu - \delta yv, yu + xv)$$

es biyectiva, pues su determinate es $x^2 + \delta y^2 = e$. Además de la identidad:

$$(xu - \delta yv)^2 + \delta\,(yu + xv)^2 = \left(u^2 + \delta v^2\right)\left(y^2\delta + x^2\right) = \left(u^2 + \delta v^2\right) e$$

se sigue que σ transforma las soluciones de la ecuación $u^2 + \delta v^2 = 1$ en soluciones de la ecuación $u^2 + \delta v^2 = e$ y a su vez soluciones de esta última en soluciones de la ecuación $u^2 + \delta v^2 = e^2$. En conclusión $c_{m,1} \leq c_{m,e} \leq c_{m,e^2} = c_{m,1}$, y así queda demostrada la proposición. ■

Corolario 3.4. *Si $n = 2$, entonces:*

Si $p = 4h + 1$	$c_{0,0} = c_{2,0} = 2p - 1$	$c_{0,1} = c_{2,1} = p - 1$
	$c_{1,0} = 1$	$c_{1,e} = c_{1,1} = p + 1$
Si $p = 4h - 1$	$c_{0,0} = c_{2,0} = 1$	$c_{0,1} = c_{2,1} = p + 1$
	$c_{1,0} = 2p - 1$	$c_{1,e} = c_{1,1} = p - 1$

Para tratar el caso general, usaremos la siguiente suma de Gauss:

$$\alpha = \sum_{x=0}^{p-1} \zeta^{x^2}$$

donde ζ es una raíz p-ésima primitiva de la unidad.
Podemos escribir:

$$\alpha = 1 + 2\sum_{k \in \mathcal{C}} \zeta^k$$

y tenemos además la identidad:

$$0 = 1 + \sum_{k \in \mathcal{C}} \zeta^k + \sum_{k \in \mathcal{N}} \zeta^k$$

Por otra parte:

$$\begin{aligned} \alpha^2 &= \sum_{(x,y) \in \mathbb{Z}_p} \zeta^{x^2+y^2} \\ &= c_{2,0} + c_{2,1} \sum_{k \in \mathcal{C}} \zeta^k + c_{2,e} \sum_{k \in \mathcal{N}} \zeta^k \\ &= c_{2,0} - c_{2,1} \end{aligned}$$

luego, de las identidades del corolario, se sigue que:

$$\alpha^2 = (-1)^{\frac{p-1}{2}}\, p$$

identidad que fue probada por Gauss.

Consideremos ahora la suma de Gauss:

$$\beta = \sum_{x=0}^{p-1} \zeta^{ex^2}$$

Se tiene:

$$\beta = 1 + 2\sum_{k\in\mathcal{N}} \zeta^k$$

es decir, $\beta = -\alpha$, además:

$$\textstyle\sum_{k\in\mathcal{C}} \zeta^k = \frac{\alpha-1}{2} \quad \text{y} \quad \sum_{k\in\mathcal{N}} \zeta^k = -\frac{\alpha+1}{2}$$

Por otra parte:

$$\alpha^m\beta^{n-m} = \left(\textstyle\sum_{(x_1,\ldots,x_m)\in\mathbb{Z}_p^m} \zeta^{x_1^2+\cdots+x_m^2}\right)\left(\sum_{(x_{m+1},\ldots,x_n)\in\mathbb{Z}_p^{n-m}} \zeta^{e\left(x_{m+1}^2+\cdots+x_n^2\right)}\right)$$

es decir

$$\begin{aligned}\alpha^m\beta^{n-m} &= \sum_{(x_1,\cdots,x_n)\in\mathbb{Z}_p^n} \zeta^{x_1^2+\cdots+x_m^2+e\left(x_{m+1}^2+\cdots+x_n^2\right)} \\ &= c_{m,0} + c_{m,1}\sum_{k\in\mathcal{C}}\zeta^k + c_{m,e}\sum_{k\in\mathcal{N}}\zeta^k \\ &= c_{m,0} + c_{m,1}\frac{\alpha-1}{2} - c_{m,e}\frac{\alpha+1}{2}\end{aligned}$$

Luego:

$$2\,(-1)^{m-n}\,\alpha^n = 2c_{m,0} + (c_{m,1} - c_{m,e})\,\alpha - (c_{m,1} + c_{m,e})$$

Teniendo en cuenta la paridad de n, resulta:

$$\alpha^n = \begin{cases} (-1)^{\frac{p-1}{2}k}\, p^k & \text{si} \quad n = 2k \\ (-1)^{\frac{p-1}{2}k}\, p^k\alpha & \text{si} \quad n = 2k+1 \end{cases}$$

de donde, si $n = 2k$:

$$2\,(-1)^{\frac{p-1}{2}k+m}\, p^k = 2c_{m,0} - c_{m,1} - c_{m,e} \quad \text{y} \quad c_{m,1} = c_{m,e}$$

y si $n = 2k + 1$:

$$2\left(-1\right)^{\frac{p-1}{2}k+m-1} p^k = c_{m,1} - c_{m,e} \quad \text{y} \quad 2c_{m,0} = c_{m,1} + c_{m,e}$$

De las identidades establecidas y recordando que:

$$p^n = c_{m,0} + \frac{p-1}{2} c_{m,1} + \frac{p-1}{2} c_{m,e}$$

se tienen los sistemas lineales:

$$\begin{bmatrix} 2 & p-1 & p-1 \\ 2 & -1 & -1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} c_{m,0} \\ c_{m,1} \\ c_{m,e} \end{bmatrix} = \begin{bmatrix} 2p^{2k} \\ 2\left(-1\right)^{\frac{p-1}{2}k+m} p^k \\ 0 \end{bmatrix} \text{ si } n = 2k$$

y si $n = 2k + 1$,

$$\begin{bmatrix} 2 & p-1 & p-1 \\ 2 & -1 & -1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} c_{m,0} \\ c_{m,1} \\ c_{m,e} \end{bmatrix} = \begin{bmatrix} 2p^{2k+1} \\ 0 \\ 2\left(-1\right)^{\frac{p-1}{2}k+m-1} p^k \end{bmatrix}$$

La resolución de estos sistemas da lugar a la siguiente conclusión.

Teorema 3.5. *Si n es un número par:*

$$c_{m,0} = p^{n-1} + \left(-1\right)^{\frac{p-1}{4}n+m} p^{\frac{n-2}{2}} \left(p-1\right)$$
$$c_{m,e} = c_{m,1} = p^{n-1} - \left(-1\right)^{\frac{p-1}{4}n+m} p^{\frac{n-2}{2}}$$

Si n es un número impar:

$$c_{m,0} = p^{n-1}$$
$$c_{m,1} = p^{n-1} - \left(-1\right)^{\frac{(p-1)(n-1)}{4}+m} p^{\frac{n-1}{2}}$$
$$c_{m,e} = p^{n-1} + \left(-1\right)^{\frac{(p-1)(n-1)}{4}+m} p^{\frac{n-1}{2}}$$

Finalizamos esta nota con algunas preguntas para el lector

1. ¿Qué ocurre cuando $p = 2$?

2. ¿Dónde pueden fracasar los argumentos previos cuando $p = 2$?

El *grupo ortogonal* O_q asociado con la forma cuadrática q está dado por los endomorfismos de $\mathbb{Z}_p^n$ $(p \neq 2)$ que conservan la forma, es decir:

$$O_q = \left\{\sigma \in End\left(\mathbb{Z}_p^n\right) : q\left(\sigma\left(x\right)\right) = q\left(x\right), \forall x \in \mathbb{Z}_p^n\right\}$$

En particular, si $b(x,y)$ denota la forma bilineal simétrica asociada con q, y $r \in \mathbb{Z}_p^n$ es tal que $q(r) \neq 0$ la transformación dada por:

$$\sigma_r(x) = x - 2\frac{b(x,r)}{q(r)}r$$

es un elemento de O_q llamada *reflexión con raíz* r.
Algunas propiedades de las reflexiones, que se establecen sin mayor dificultad, son las siguientes:

i) Si $\lambda \in Z_p$, $\lambda \neq 0$, entonces $\sigma_{\lambda r} = \sigma_r$.

ii) $\sigma_r^2 = id_{\mathbb{Z}_p^n}$.

iii) Existe una base de $\mathbb{Z}_p^n$ tal que la matriz asociada a σ_r es la matriz diagonal:

$$\begin{bmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

En particular $\det(\sigma_r) = -1$ y $tr(\sigma_r) = n-1$.

iv) $\forall \tau \in O_q$ se verifica $\tau\sigma_r\tau^{-1} = \sigma_{\tau(r)}$.

A partir *i)* la raíz de una reflexión puede ser tomada de modo que $q(r) = 1$ ó $q(r) = e$.
Podemos destacar dos subgrupos O_q^1 y O_q^e de O_q, el primero es el que generan las reflexiones σ_r con $q(r) = 1$, el segundo es el generado por las reflexiones σ_r con $q(r) = e$. Por *iv)* ambos son subgrupos normales de O_q.
En relación con el grupo ortogonal dejamos las siguientes preguntas:

3. ¿Es transitiva la acción de O_q sobre las cuádricas $q(x) = k$?

4. ¿Cuál es el orden O_q?

5. ¿Cuál es el número de reflexiones en O_q?

6. ¿Qué puede decirse de los subgrupos $O_q^1 \times O_q^e$ y $O_q^1 \cap O_q^e$?

7. ¿Qué puede decir de órdenes de los subgrupos O_q^1 y O_q^e.

Referencias

[1] Aguado, J. L., Araujo, J. O. *La ecuación* $x_1^2 + \cdots x_n^2 \equiv k$ mód p. Revista de Educación Matemática, UMA, Vol. 17 No. 2 (2002), 3–17.

[2] Ivorra Castillo, C. *Teoría de Números*, 2004.
URL: `www.uv.es/~ivorra/Libros/Numeros.pdf`

[3] Le Veque, W. J. *Teoria Elemental de los Números*, Herreros Hnos., México, 1968.

[4] Narkiewicz, W. *Number Theory*, World Scientific Publishing Co., Singapore, 1983.

[5] Vinogradov, I. *Fundamentos de la Teoría de los Números*, Ed. Mir, 1977.