ALGUNOS PROBLEMAS ADITIVOS EN RESIDUOS CUADRÁTICOS MÓDULO P

Trabajo de grado presentado como requisito
parcial para optar al título de Matemático

JOHN HERMES CASTILLO GÓMEZ
OLMER FOLLERO SOLARTE
ANDRÉS LARRAÍN HUBACH

Director
CARLOS ALBERTO TRUJILLO SOLARTE

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2003

TABLA DE CONTENIDO

	INTRODUCCIÓN	...1
1	PRELIMINARES	...4
1.1	Residuos cuadráticos módulo p	...4
1.2	La estructura algebráica de los residuos cuadráticos	...8
1.3	Sumas de Gauss y sumas de Jacobi	...9
1.4	Ley de reciprocidad cuadrática	..14
2	SUMAS Y DIFERENCIAS DE RESIDUOS CUADRÁTICOS	..19
2.1	La ecuación $x^2 + y^2 \equiv n(\mathrm{mod}\, p)$	..19
2.2	La función $\sigma_p(n)$	..22
2.3	La ecuación $x^2 - y^2 \equiv n(\mathrm{mod}\, p)$	..28
2.4	La función $\delta_p(n)$	..30
3	CUADRADOS EN PROGRESIÓN ARITMÉTICA	..35
3.1	Ternas pitagóricas	..35
3.2	La ecuación $a(a+d)(a+2d)(a+3d) = x^2$	..39
3.3	Solución paramétrica de la ecuación $x^2 + y^2 - xy = z^2$	..46
3.4	Residuos cuadráticos en progresión aritmética	..48
3.5	Residuos cuadráticos consecutivos	..51
4	ALGUNOS PROBLEMAS RELACIONADOS	..60
4.1	Residuos cuadráticos y progresiones aritméticas	..60
4.2	Base minimal de residuos cuadráticos	..62
4.3	Residuos cuadráticos y conjuntos de Sidon	..64
4.4	Otros problemas	..65
	BIBLIOGRAFÍA	..67

Introducción

En las matemáticas es muy común que algunas de las propiedades más interesantes de ciertos tipos de números, cuya definición se fundamenta en una determinada operación, aparezcan cuando se analizan dichos números mediante una operación distinta y con preguntas parecidas. Los números primos son un ejemplo latente de esta afirmación: su definición se basa enteramente en el concepto de multiplicación, y del teorema fundamental de la aritmética, se sigue que todo natural puede descomponerse como producto de ellos, pero ¿qué pasa aditivamente?. En los años 30, *Vinogradov* demostró que todo número suficientemente grande es la suma de tres primos y ésto es lo mejor conocido hasta ahora. Posteriormente *Chen* probó un resultado más fuerte, sin embargo usa conceptos más complicados. La famosa conjetura de *Golbach* sigue sin resolverse y no parece haber esperanzas de una pronta respuesta. Analizando el *Teorema Fundamental de la Aritmética* y la *Conjetura de Golbach* se observa que ambas exponen el mismo concepto pero con diferente operación: se desea saber si los primos son una base multiplicativa y aditiva para los números naturales. Sin embargo, con respecto a la suma, hay una pregunta adicional y es: ¿Cuántos primos es necesario sumar como máximo en cada caso, de forma que se obtengan todos los enteros positivos?. Con este enfoque surgen preguntas muy importantes e interesantes las cuales no existirían si se restringieran los primos a un análisis exclusivamente multiplicativo.

En este trabajo se siguió un proceso parecido partiendo de otros números famosos:los cuadrados, obtenidos de multiplicar cada entero positivo por sí mismo. De los griegos se sabe que algunas tripletas de cuadrados satisfacen la llamada identidad pitagórica $x^2+y^2=z^2$ con $x, y, z \in \mathbb{Z}^+$ la cual constituye la base del teorema de Pitágoras, indiscutiblemente el resultado más famoso de todas las matemáticas y también el que tiene la mayor cantidad de demostraciones. Comenzando aquí se planteó la pregunta: ¿Cuántas tripletas de cuadrados satisfacen la identidad pitagórica en un campo finito con p elementos?. Obviamente, en este contexto, cuadrado es otra cosa completamente distinta, estos cuadrados se llaman

residuos cuadráticos y no son más que el residuo módulo p de multiplicar cada elemento de $\mathbb{Z}_p - \{0\}$ por sí mismo.

Sorpresivamente, a pesar del radical cambio de contexto, se logró probar que cada residuo cuadrático es la suma de otros dos residuos cuadráticos mediante identidades relacionadas con las ternas pitagóricas normales. Asi se abrió un mundo completo de preguntas interesantes siguiendo la misma filosofía: si en los cuadrados se hace una determinada observación ¿qué sucede en los residuos cuadráticos?

Se empezó por un teorema de *Fermat* el cual afirma que los números primos de la forma $4k+1$ son los únicos representables como suma de dos cuadrados. Utilizando varios conceptos inherentes a la teoría de ecuaciones sobre campos finitos se logró probar que en $\mathbb{Z}_p$ todos sus elementos son representables como suma de residuos cuadráticos y además se encontró el número exacto de representaciones de cada elemento de $\mathbb{Z}_p$.

El mismo Fermat demostró que no existen cuatro cuadrados en progresión aritmética. Las demostraciones de esa afirmación son casi siempre muy complicadas y se basan en construcciones artificiosas. Revisando la literatura matemática encontramos un artículo de Tamás Erdelyi en donde el autor prueba de una manera bastante elegante y consisa de este resultado. Siendo posiblemente la única demostración sencilla conocida, se decidió exponerla aquí procurando explicar lo mejor posible cada paso.

Posteriormente, se analizó el comportamiento de los residuos cuadráticos con respecto a progresiones aritméticas, encontrando nuevamente resultados bastante más interesantes, en particular el hecho de que dado cualquier entero positivo n por grande que sea, existe un primo p de forma que en $\mathbf{Z}_p$ existe una progresión aritmética de longitud n constituida enteramente por residuos cuadráticos.

Como siempre sucede en matemáticas, una solución produce más preguntas, por lo que el último capítulo se dedica a plantear varios problemas abiertos basados en el comportamiento de los residuos cuadráticos respecto al comportamiento aditivo de los cuadrados. Destaca, entre otros, el problema de la base minimal que dice: dado un primo p ¿cual es la menor cantidad de residuos cuadráticos que forman una base aditiva de orden 2 para $\mathbf{Z}_p$?, Con respecto a este difícil problema se realizaron

numerosas búsquedas computacionales obteniéndose que, a medida que p crece, posiblemente existe un subconjunto de residuos cuadráticos de tamaño aproximado $2\sqrt{p}$ que satisface el problema. Una demostración de la conjetura anterior mejoraría obstensiblemente el conocimiento con respecto a las bases aditivas en campos finitos. Lamentablemente sólo argumentos heurísticos permiten sospechar su veracidad.

Se espera con este estudio abrir tópicos para nuevos trabajos de grado basados no sólo en este tema sino en el método de analizar preguntas análogas entre sistemas numéricos distintos.

Queremos expresarle un especial agradecimiento a nuestro director Carlos A. Trujillo por su constante apoyo, su guía y sus consejos. Gracias a él logramos iniciarnos en la investigación matemática y nos dimos cuenta de que la matemática es mucho más que acumular conocimiento de libros.

1 Preliminares

En este capítulo se presentan los fundamentos teóricos necesarios para el desarrollo de los temas subsecuentes. Con el deseo de hacer el manuscrito lo más completo posible se demuestran los resultados más importantes en esta teoría, tales como la ley de reciprocidad cuadrática y las identidades que relacionan las sumas de Gauss con las sumas de Jacobi.

Los libros [1] , [7] , [8] constituyen las referencias fundamentales, ver también la Tesis de Maestría [9] .

1.1 Residuos cuadráticos módulo p

Sean p un primo impar y a un entero no divisible por p.

> Se dice que a es un *residuo cuadrático módulo* p, denotado aRp, si la congruencia
>
> $$x^2 \equiv a (\mathrm{mod}\, p) \tag{1.1}$$
>
> tiene solución. En caso contrario, es decir si la congruencia (1.1) no tiene solución, a se llama un *no residuo cuadrático módulo* p, denotado aNp.

Es claro que para determinar todos los residuos (y no residuos) cuadráticos módulo p, es suficiente considerar la congruencia (1.1) para todo a tal que $1 \leq a \leq p-1$.

Como es usual, $\mathbb{Z}_p$ representa el único campo (salvo isomorfismos) con p elementos y $\mathbb{Z}_p^*$ corresponde al grupo de unidades de $\mathbb{Z}_p$. Es decir

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\},$$

$$\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}.$$

Por otro lado, en $\mathbb{Z}_p^*$ el subconjunto de todos los residuos cuadráticos y el de los no residuos cuadráticos módulo p se representan mediante R_p y N_p, respectivamente.

Ejemplo 1.1. En $\mathbb{Z}_{13}^*$, se tiene que

$$R_{13} = \{1, 3, 4, 9, 10, 12\},$$

$$N_{13} = \{2, 5, 6, 7, 8, 11\}.$$

Puesto que

$$1^2 \equiv 1(\mathrm{mod}\,13), \quad 2^2 \equiv 4(\mathrm{mod}\,13), \quad 3^2 \equiv 9(\mathrm{mod}\,13), \quad 4^2 \equiv 3(\mathrm{mod}\,13),$$

$$5^2 \equiv 12(\mathrm{mod}\,13), \quad 6^2 \equiv 10(\mathrm{mod}\,13), \quad 7^2 \equiv 10(\mathrm{mod}\,13), \quad 8^2 \equiv 12(\mathrm{mod}\,13),$$

$$9^2 \equiv 3(\mathrm{mod}\,13), \quad 10^2 \equiv 9(\mathrm{mod}\,13), \quad 11^2 \equiv 4(\mathrm{mod}\,13), \quad 12^2 \equiv 1(\mathrm{mod}\,13).$$

Es fácil ver que si x_1 es solución de (1.1) entonces $p - x_1$ también lo es puesto que:

$$x_1^2 \equiv (p - x_1)^2(\mathrm{mod}\,p). \tag{1.2}$$

Además si $x_1^2 \equiv x_2^2(\mathrm{mod}\,p)$ entonces $x_1^2 - x_2^2 \equiv 0\,(\mathrm{mod}\,p)$, luego $x_2 \equiv x_1\,(\mathrm{mod}\,p)$ ó $x_2 \equiv p - x_1\,(\mathrm{mod}\,p)$.

Así, la congruencia (1.1) tiene dos soluciones cuando aRp o no tiene cuando aNp.

Los siguientes resultados muestran que

$$|R_p| = |N_p| = \frac{p-1}{2},$$

para todo primo $p > 2$.

Teorema 1.1.

Para todo primo $p > 2$, existen $(p-1)/2$ residuos cuadráticos módulo p.

Prueba. Al considerar los valores de $1^2, 2^2, ..., (p-1)^2$ módulo p, por la ecuación (1.2) se tiene que:

$$1^2 \equiv (p-1)^2(\mathrm{mod}\,p),$$

$$2^2 \equiv (p-2)^2(\mathrm{mod}\,p),$$

$$\vdots$$

$$(\frac{p-1}{2})^2 \equiv (\frac{p+1}{2})^2(\mathrm{mod}\,p).$$

Luego, la expresión x^2 toma $\frac{p-1}{2}$ valores incongruentes módulo p a medida que x recorre $\mathbb{Z}_p^*$; por lo tanto hay $\frac{p-1}{2}$ residuos cuadráticos módulo p. □

Corolario 1.1.

Para todo primo $p > 2$, existen $(p-1)/2$ no residuos cuadráticos módulo p.

Prueba. En $\mathbb{Z}_p^*$ hay $p-1$ elementos de los cuales $(p-1)/2$ son residuos cuadráticos, de aquí que los restantes deben ser no residuos cuadráticos. □

La siguiente definición caracteriza, de forma sencilla, si un entero a es o no un residuo cuadrático módulo un primo $p > 2$.

Definición 1.1. (Símbolo de Legendre)

Sea $p > 2$ un número primo. Si a es un entero no es divisible por p, se define el *símbolo de Legendre* como

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{Si } aRp \\ -1, & \text{Si } aNp \end{cases}$$

que se lee "Legendre a de p".

Si a es divisible por p se define $\left(\frac{a}{p}\right) = 0$.

Con la ayuda del símbolo de Legendre se puede exponer de manera sencilla el siguiente resultado debido a Euler.

Lema 1.1. (Criterio de Euler)

Sea p un número primo impar. Entonces para todo n, se tiene:

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} (\mathrm{mod}\, p).$$

Prueba. Si $n \equiv 0 (\mathrm{mod}\, p)$ el resultado es trivial ya que ambos miembros son congruentes con $0 (\mathrm{mod}\, p)$. Ahora si se supone que $\left(\frac{n}{p}\right) = 1$, entonces existe un x tal que $x^2 \equiv n \,(\mathrm{mod}\, p)$ y por tanto

$$n^{(p-1)/2} \equiv \left(x^2\right)^{(p-1)/2} = x^{p-1} \equiv 1 = \left(\frac{n}{p}\right) (\mathrm{mod}\, p).$$

Ahora suponemos que $\left(\frac{n}{p}\right) = -1$ y se considera el polinomio

$$f(x) = x^{(p-1)/2} - 1.$$

Como el grado de $f(x)$ es $(p-1)/2$ la congruencia

$$f(x) \equiv 0 (\mathrm{mod}\, p)$$

tiene a lo sumo $(p-1)/2$ soluciones y, como los $(p-1)/2$ residuos cuadráticos son soluciones, entonces los no residuos no son soluciones. Luego

$$n \equiv 1 (\mathrm{mod}\, p) \text{ si } \left(\frac{n}{p}\right) = -1.$$

Ahora, por el pequeño Teorema de Fermat $n^{(p-1)} \equiv 1 (\mathrm{mod}\, p)$, y por la relación anterior se tiene

$$n^{(p-1)/2} \equiv -1 = \left(\frac{n}{p}\right) (\mathrm{mod}\, p). \square$$

Corolario 1.2

$-1 \in R_p$ si, y sólo si $p \equiv 1 \,(\mathrm{mod}\, 4)$

Prueba.

Se sabe que $-1 \in R_p$si, y sólo si $\left(\frac{-1}{p}\right) = 1$.

Ahora por el criterio de Euler $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2}$ ésto es igual a 1 si, y sólo si $(p-1)/2$ es un número par. de donde se sigue el resultado.□

Del corolario anterior se tiene que $-1 \notin R_p$ si, y sólo si $p \equiv 3 \,(\mathrm{mod}\, 4)$.

El siguiente lema establece algunas propiedades del símbolo de Legendre.

Lema 1.2.

Para todo primo p y todo par de enteros a, b, se tiene:

1). $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

2).Si $a \equiv b \,(\mathrm{mod}\, p)$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Prueba. 1). Por el Criterio de Euler se tiene:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\, p),$$
$$\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} (\mathrm{mod}\, p).$$

Luego

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{(p-1)/2} \,(\mathrm{mod}\, p) = \left(\frac{ab}{p}\right),$$

nuevamente por el criterio de Euler.

2). Si $a \equiv b (\mathrm{mod}\, p)$, entonces $x^2 \equiv a (\mathrm{mod}\, p)$ tiene solución sí, y sólo si $x^2 \equiv b (\mathrm{mod}\, p)$ tiene solución y por tanto

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \square$$

1.2 La estructura algebráica de los residuos cuadráticos

Una de la propiedades básicas de los residuos cuadráticos módulo p consiste en que forman un subconjunto de $\mathbb{Z}_p$ con estructura de grupo multiplicativo. Esta propiedad, que se denominará desde ahora *propiedad de grupo*, será de gran utilidad en este trabajo.

Para demostrarla se requiere del siguiente lema:

Lema 1.3.

Para todo primo p, se tienen las siguientes propiedades:

1). El producto de dos residuos cuadráticos así como el de dos no residuos es un residuo cuadrático.

2). El producto de un residuo por un no residuo (cuadrático) es un no residuo cuadrático.

Prueba. 1). Si a y b son residuos cuadráticos entonces

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

de donde ab es un residuo cuadrático. Similarmente, si a y b son no residuos cuadráticos entonces

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1,$$

y por lo tanto

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1$$

de donde ab es un residuo cuadrático.

2). Dados a y b, si uno es un residuo cuadrático y el otro es un no residuo cuadrátco, entonces

$$\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right),$$

luego

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left[-\left(\frac{a}{p}\right)\right] = -\left[\left(\frac{a}{p}\right)\right]^2 = -1,$$

es decir ab es un no residuo cuadrático. □

Teorema 1.2. (Propiedad de grupo)

Para todo primo p, los residuos cuadráticos forman un grupo multiplicatico de orden $\frac{p-1}{2}$.

Prueba. El lema anterior demuestra que R_p es cerrado bajo el producto, además la propiedad asociativa se hereda de $\mathbb{Z}_p$. Puesto que $1^2 \equiv 1 (\mathrm{mod}\, p)$ el elemento identidad de la multiplicación en $\mathbb{Z}_p$ esta en R_p.

Ahora, si a es un residuo cuadrático, $\left(\frac{a}{p}\right) = 1$, entonces

$$\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a^{-1}}{p}\right) = \left(\frac{aa^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1,$$

de esto a^{-1} también es un residuo cuadrático. □

1.3 Sumas de Gauss y sumas de Jacobi

En esta sección se exponen las propiedades principales de los caracteres multiplicativos, el símbolo de Legendre es un caso particular de ellos; también se definen las sumas de Gauss y de Jacobi, y se establecen algunas de sus propiedades fundamentales.

Definición 1.2. (Carácter multiplicativo)

Un *carácter multiplicativo* sobre $\mathbb{Z}_p$ es una función χ de $\mathbb{Z}_p^*$ al conjunto de los números complejos que satisface

$$\chi(ab) = \chi(a)\,\chi(b)\,, \text{ para todo } a, b \in \mathbb{Z}_p^*.$$

En terminos algebráicos, un carácter multiplicativo es un homomorfismo del grupo multiplicativo $\mathbb{Z}_p^*$ en el grupo multiplicativo de los números complejos. El *carácter identidad (o carácter trivial)*, denotado mediante ε se define de tal forma que $\varepsilon(a) = 1$ para todo $a \in \mathbb{Z}_p^*$.

Un caso particular no trivial de carácter multiplicativo es el símbolo de Legendre.

A continuación se establecen varias propiedades de los caracteres.

Lema 1.4.

Sea χ un carácter multiplicativo y $a \in \mathbb{Z}_p^*$, entonces

1). $\chi(1) = 1$.

2). $\chi(a)$ es una raiz p-ésima de la unidad.

3). $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Prueba. 1). $\chi(1) = \chi(1)\chi(1)$, de donde $\chi(1) = 1$.

2). Puesto que $a^{p-1} = 1$ en $\mathbb{Z}_p^*$, se tiene que $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.

3). Es consecuencia inmediata de los puntos anteriores puesto que:

$$1 = \chi(1) = \chi\left(aa^{-1}\right) = \chi(a)\chi(a^{-1}) = \chi(a)\chi(a)^{-1} = \chi(a)\overline{\chi(a)}. \square$$

Lema 1.5.

Sea χ un carácter multiplicativo. Si $\chi \neq \varepsilon$, entonces $\sum_t \chi(t) = 0$, donde la suma es sobre todos los $t \in \mathbb{Z}_p^*$. Si $\chi = \varepsilon$ el valor de la suma es $p - 1$.

Prueba. La última afirmación es inmediata.

Si $\chi \neq \varepsilon$, entonces existe $a \in \mathbb{Z}_p^*$ tal que $\chi(a) \neq 1$. Sea $T = \sum_t \chi(t)$ entonces

$$\chi(a)T = \sum_t \chi(a)\chi(t) = \sum_t \chi(at) = T.$$

La última igualdad se tiene porque at recorre todos los elementos de $\mathbb{Z}_p^*$ a medida que t lo hace. Luego $\chi(a)T = T$ y como $\chi(a) \neq 1$, $T = 0$. $\square$

Corolario 1.3.

Si $\chi(a) = \left(\frac{a}{p}\right)$ entonces $\sum_a \left(\frac{a}{p}\right) = 0$.

Definición 1.3. (Suma de Gauss)

Sean χ un carácter sobre $\mathbb{Z}_p$, $a \in \mathbb{Z}_p$ se define $g_a(\chi) = \sum_t \chi(t)\,\zeta^{at}$, donde la suma es sobre todo t en $\mathbb{Z}_p$, y $\zeta = e^{2\pi i/p}$ (raiz p-ésima de la unidad)[1]. La expresión $g_a(\chi)$ se llama suma de Gauss sobre $\mathbb{Z}_p$ correspondiente al carácter χ (y al elemento a).

Si $\chi(t) = \left(\dfrac{t}{p}\right)$ entonces la expresión $g_a(\chi)$ se denomina *suma cuadrática de Gauss.*

Los siguientes lemas permiten expresar $g_a(\chi)$ en términos de $g_1(\chi)$.

Lema 1.6.

Si $a \neq 0$ y $\chi \neq \varepsilon$ se tiene que $g_a(\chi) = \chi\left(a^{-1}\right) g_1(\chi)$.

Prueba. Sean $a \neq 0$ y $\chi \neq \varepsilon$, entonces

$$\chi(a)\, g_a(\chi) = \chi(a) \sum_t \chi(t)\,\zeta^{at} = \sum_t \chi(at)\,\zeta^{at} = \sum_k \chi(k)\,\zeta^k = g_1(\chi),$$

puesto que cuando t recorre $\mathbb{Z}_p$, $k = at$ también lo hace. $\square$

Lema 1.7.

Si $\chi \neq \varepsilon$,entonces $|g_1(\chi)| = \sqrt{p}$.

Prueba. La idea consiste en evaluar la suma $\sum_a g_a(\chi)\,\overline{g_a(\chi)}$ de dos formas.

Si $a \neq 0$, entonces por el lema anterior

$$\overline{g_a(\chi)} = \overline{\chi\left(a^{-1}\right) g_1(\chi)} = \chi(a)\,\overline{g_1(\chi)},$$

[1]Las raices p-ésimas de la unidad estan dadas por:

$\varpi = e^{(2\pi i+k)/p}$, $k = 0, ..., p-1$. En este caso se toma $k = 0$.

y

$$g_a(\chi) = \chi\left(a^{-1}\right) g_1(\chi).$$

ζDe aquí

$$g_a(\chi)\,\overline{g_a(\chi)} = \chi\left(a^{-1}\right)\chi(a)\, g_1(\chi)\,\overline{g_1(\chi)} = |g_1(\chi)|^2.$$

Dado que $g_0(\chi) = 0$, la suma $\sum_a g_a(\chi)\,\overline{g_a(\chi)}$ tiene el valor $(p-1)\,|g_1(\chi)|^2$.

Por otro lado

$$g_a(\chi)\,\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\,\overline{\chi(y)}\zeta^{ax-ay}.$$

Ahora,

$$p^{-1}\sum_{a=0}^{p-1}\zeta^{a(x-y)} = \delta(x,y)$$

donde

$$\delta(x,y) = \begin{cases} 1, & \text{si } x \equiv y \pmod p \\ 0, & \text{si } x \not\equiv y \pmod p \end{cases}$$

puesto que si $x \equiv y \pmod p$ entonces $\zeta^{a(x-y)} = 1$ para todo a entre 1 y $p-1$.

Si $x \not\equiv y \pmod p$ entonces $\zeta^{a(x-y)} \neq 1$ y

$$\sum_{a=0}^{p-1}\zeta^{a(x-y)} = \frac{(\zeta^{ap}-1)}{(\zeta^a-1)} = 0$$

Sumando en ambos lados sobre a y usando lo anterior se tiene

$$\sum_a g_a(\chi)\,\overline{g_a(\chi)} = \sum_x\sum_y \chi(x)\,\overline{\chi(y)}\delta(x,y)\,p = (p-1)\,p,$$

Por lo tanto $(p-1)\,|g_1(\chi)|^2 = (p-1)\,p$. □

A continuación se definen las sumas de Jacobi y se establecen sus propiedades básicas.

Definición 1.4. (Sumas de Jacobi)

Sean χ y λ dos caracteres sobre $\mathbb{Z}_p$, la expresión

$$J(\chi,\lambda) = \sum_{a+b=1}\chi(a)\lambda(b)$$

se denomina *suma de Jacobi* (correspondiente a los caracteres χ, λ).

$g_1(\chi)$ se denotará por $g(\chi)$.

La relación principal entre sumas de Gauss y sumas de Jacobi se establece en el siguiente teorema.

Teorema 1.3.

Sean χ y λ dos caracteres no triviales, si $\chi\lambda \neq \varepsilon$ entonces

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Prueba. Se tiene que

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_x \chi(x)\zeta^x\right)\left(\sum_y \lambda(y)\zeta^y\right) \\ &= \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y}, \end{aligned}$$

luego

$$g(\chi)g(\lambda) = \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t. \tag{1.3}$$

Si $t = 0$ entonces

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0,$$

puesto que $\chi\lambda \neq \varepsilon$ por hipótesis.

Si $t \neq 0$, se definen x' y y' mediante $x' = tx$ y $y' = ty$. Si $x + y = t$ entonces $x' + y' = 1$. Se sigue que

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi,\lambda),$$

sustituyendo en (1.3) se obtiene

$$g(\chi)g(\lambda) = \sum_t \chi\lambda(t)J(\chi,\lambda)\zeta^t = J(\chi,\lambda)g(\chi\lambda). \square$$

Teorema 1.4.

Sea χ un carácter no trivial entonces

$$J(\chi,\chi^{-1}) = -\chi(-1)$$

Prueba. Se nota

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1, b\neq 0} \chi(a/b) = \sum_{a\neq 1} \chi(a/(1-a)).$$

Considerese $a/(1-a) = c$. Si $c \neq -1$,entonces $a = c/(1+c)$. De ésto se sigue que como a varia en $\mathbb{Z}_p - \{1\}$, c varia en $\mathbb{Z}_p - \{-1\}$.

Y de aquí

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1). \square$$

Corolario 1.4.

Si χ,λ, $\chi\lambda$ no son iguales a ε, entonces $|J(\chi, \lambda)| = \sqrt{p}$.

Prueba. Partiendo del teorema 1.3 y recordando que $|g(\chi)| = \sqrt{p}$ para todo carácter no trivial se sigue el resultado. $\square$

Del teorema y del corolario anteriores se sigue que si $\chi(a) = \left(\frac{a}{p}\right)$ entonces

$$J(\chi, \chi^{-1}) = -\left(\frac{-1}{p}\right) = -(-1)^{(p-1)/2}.$$

1.4 Ley de reciprocidad cuadrática

La ley de reciprocidad cuadrática es uno de los resultados más importantes referentes a residuos cuadráticos y será de gran utilidad en el tercer capítulo.

Teorema 1.5. (Ley de reciprocidad cuadrática)

Si p y q son primos impares distintos, entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Para la prueba de este teorema se necesitan algunos resultados preliminares.

Lema 1.8. (Lema de Gauss)

Supongase que $n \not\equiv 0 (\mathrm{mod}\, p)$ y considerese el menor residuo positivo módulo p de los siguientes $(p-1)/2$ múltiplos de n

$$n,\ 2n,\ 3n, ...,\ \frac{p-1}{2}n.$$

Si m designa el número de residuos que exceden a $p/2$, entonces

$$\left(\frac{n}{p}\right) = (-1)^m.$$

Prueba. Los números

$$n, 2n, 3n, ..., ((p-1)/2)\, n$$

son incongruentes módulo p. Se consideran sus mínimos residuos positivos y se distribuyen en dos conjuntos disjuntos A y B según si los residuos son mayores o menores a $p/2$. Sean

$$A = \{a_1, a_2, ..., a_k\},$$

$$B = \{b_1, b_2, ..., b_m\},$$

donde cada $a_i \equiv tn (\mathrm{mod}\, p)$ para algún $t \leq \frac{p-1}{2}$, $0 < a_i < \frac{p}{2}$ y $b_i \equiv sn (\mathrm{mod}\, p)$ para algún $s \leq \frac{p-1}{2}$ y $\frac{p}{2} < b_i < p$. Se ve que $m + k = \frac{p-1}{2}$ pues A y B son disjuntos. El número m de elementos de B es significativo en este teorema. Se forma un nuevo conjunto C de m elementos restando cada b_i. Entonces

$$C = \{c_1, \cdots, c_m\} \text{ en donde } c_i = p - b_i.$$

Ahora $0 < c_i < \frac{p}{2}$, luego los elementos de C pertenecen al mismo intervalo que los elementos de A. A continuación se ve que A y C son disjuntos.

Suponemos que $c_j = a_i$ para algún i y j. Entonces $p - b_j = a_i$,o $a_i + b_j \equiv 0 (\mathrm{mod}\, p)$. Por consiguiente

$$tn + sn = (t+s)\, n \equiv 0 (\mathrm{mod}\, p)$$

para ciertos s y t con $1 < t < \frac{p}{2}$ y $1 < s < \frac{p}{2}$. Pero ésto es imposible ya que $p \nmid n$ y $0 < t + s < p$. Por consiguiente A y C son disjuntos, luego su unión $A \cup C$ contiene $m + k = (p-1)/2$ enteros en el intervalo $[1, (p-1)/2]$. Luego

$$A \cup C = \{a_1, a_2, ..., a_k, c_1, \cdots, c_m\} = \{1, 2, ..., (p-1)/2\}$$

Se forman ahora el producto de todos los elementos de $A \cup C$ a fin de obtener

$$a_1 a_2 ... a_k c_1 \cdots c_m = \left(\frac{p-1}{2}\right)!$$

Puesto que $c_i = p - b_i$, se tiene

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= a_1 a_2 ... a_k \left(p - b_1\right) ... \left(p - b_m\right) \\ &\equiv (-1)^m a_1 a_2 ... a_k \left(p - b_1\right) ... \left(p - b_m\right) \left(\mathrm{mod}\, p\right) \\ &\equiv (-1)^m n \left(2n\right) ... \left[\frac{p-1}{2}\right] n \left(\mathrm{mod}\, p\right) \\ &\equiv (-1)^m n^{(p-1)/2} \left(\frac{p-1}{2}\right)! \left(\mathrm{mod}\, p\right)\end{aligned}$$

Y finalmente simplificando el factorial se obtiene

$$n^{(p-1)/2} \equiv (-1)^m \left(\mathrm{mod}\, p\right). \square$$

Lema 1.9.

Sean p y q dos primos diferentes, entonces

$$\sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{(p-1)}{2}\frac{(q-1)}{2}.$$

Prueba. Considerese la siguiente función

$$f\left(x, y\right) = qx - py.$$

Si x, y son enteros no cero, entonces $f\left(x, y\right)$ es un entero no cero. Sin embargo, dado que x toma los valores $1, 2, ..., \frac{p-1}{2}$ y y toma los valores $1, 2, ..., \frac{q-1}{2}$, entonces $f\left(x, y\right)$ toma

$$\frac{(p-1)}{2}\frac{(q-1)}{2}$$

valores distintos dos a dos ya que

$$f\left(x, y\right) - f\left(x', y'\right) = f\left(x - x', y - y'\right) \neq 0.$$

Ahora se cuenta el número de valores de $f\left(x, y\right)$ que son positivos y el número de los que son negativos.

Para cada x fijo se tiene $f(x,y) > 0$ si, y sólo si, $y < \frac{qx}{p}$, o $y < [\frac{qx}{p}]$. Por lo tanto, el número de valores positivos es

$$\sum_{x=1}^{(p-1)/2} \left[\frac{qx}{p}\right].$$

Análogamente, el número de valores negativos es

$$\sum_{y=1}^{(q-1)/2} \left[\frac{py}{q}\right].$$

Puesto que el número de valores positivos y negativos es en total

$$\frac{(p-1)}{2}\frac{(q-1)}{2}$$

se termina la prueba. □

Lema 1.10.

Sea m el número definido en el lema de Gauss. Entonces

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod 2.$$

En particular, si n es impar entonces

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2.$$

Prueba. Se considera tn/p y se observa el tamaño de su residuo.

Es decir

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\}, \text{ en donde } 0 < \left\{\frac{tn}{p}\right\} < 1,$$

aquí, $[x], \{x\}$ representan la parte entera y la parte decimal del número real x. Luego

$$tn = p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} = p\left[\frac{tn}{p}\right] + r_t,$$

en donde $0 < r_t < p$. El número $r_t = tn - p\left[\frac{tn}{p}\right]$ es el mínimo residuo positivo de tn módulo p.

Sean

$$A = \{a_1, a_2, ..., a_k\},$$

$$B = \{b_1, b_2, ..., b_m\},$$

en donde cada $a_i \equiv tn(\mathrm{mod}\, p)$ para algún $t \leq (p-1)/2$ y $0 < a_i < p/2$, y cada $b_i \equiv sn(\mathrm{mod}\, p)$ para algún $s \leq (p-1)\,2$ y $p/2 < b_i < p$.

Luego

$$\{r_1, ..., r_{(p-1)/2}\} = \{a_1, ..., a_k, b_1, ..., b_m\}.$$

y como

$$\left\{1, 2, ..., \frac{p-1}{2}\right\} = \{a_1, ..., a_k, c_1, ..., c_m\},$$

donde $c_i = p - b_i$.

Ahora se calculan las sumas de los elementos de estos conjuntos y se obtiene

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j, \tag{1.4}$$

y

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j. \tag{1.5}$$

Si en (1.4) se remplaza r_t por su definición se obtiene

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = n \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right]$$

y de aquí la ecuación (1.5) se puede expresar como

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{t=1}^{(p-1)/2} t$$

y sumando esta ecuación a la anterior

$$\begin{aligned} mp + 2\sum_{i=1}^{k} a_i &= (n+1) \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \\ &= (n+1)\,\frac{p^2-1}{8} - p \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \end{aligned}$$

reduciendo este resultado módulo p se obtiene que

$$m \equiv (n-1)\left(\frac{p^2-1}{8}\right) + \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2. \ \square$$

Ahora se procede con la prueba del Teorema 1.5.

Prueba de la ley de reciprocidad cuadrática. Por el Lema de Gauss y el lema 1.10 se tiene que

$$\left(\frac{q}{p}\right) = (-1)^m,$$

con

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2.$$

Análogamente,

$$\left(\frac{p}{q}\right) = (-1)^n,$$

donde

$$n \equiv \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] \pmod 2.$$

Luego $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$, y lo afirmado por el Teorema 1.5 se sigue del Lema 1.9. □

2 Sumas y diferencias de residuos cuadráticos

Todo primo de la forma $4k+1$ es representable como suma de dos cuadrados (ver [6]). A partir de este resultado surge la siguiente pregunta: ¿cuáles elementos en $\mathbb{Z}_p$ son representables como suma (resta) de dos residuos cuadráticos?. La pregunta anterior equivale a encontrar los valores $n \in \mathbb{Z}_p$, tales que las ecuaciones $x^2 + y^2 \equiv n \pmod{p}$ y $x^2 - y^2 \equiv n \pmod{p}$ tienen solución. El objetivo del capítulo es resolver ambas ecuaciones y posteriormente dar el número de soluciones. Se utiliza extensamente la propiedad de grupo además de las identidades sobre sumas de Jacobi dadas en el primer capítulo.

2.1 La ecuación $x^2 + y^2 \equiv n(\mathrm{mod}\, p)$

El trabajo con respecto a esta ecuación se divide en dos partes, en primer lugar se establece la existencia de soluciones recurriendo a construcciones relacionadas con las ternas pitagóricas y después se hace un conteo de ellas mediante las sumas de Jacobi.

Lema 2.1.

Para todo $n \in \mathbb{Z}_p$, existen $x, y \in \mathbb{Z}_p$ tales que

$$x^2 + y^2 \equiv n(\mathrm{mod}\, p). \tag{2.1}$$

Prueba. Sea $n \in \mathbb{Z}_p^*$, se definen los siguientes conjuntos

$$A = R_p \cup \{0\},$$

$$B = \{n - a(\mathrm{mod}\, p) : a \in A\}.$$

entonces

$$|A| = |R_p| + 1 = \frac{p-1}{2} + 1 = \frac{p+1}{2}.$$

Además dados $a_1, a_2 \in A$ tales que $a_1 \not\equiv a_2 \pmod{p}$, entonces $n - a_1 \not\equiv n - a_2 \pmod{p}$; de ésto

$$|B| = |A| = \frac{p+1}{2}.$$

Ahora bien, como A y B están contenidos en $\mathbb{Z}_p$ y $|B| + |A| = p + 1 > |\mathbb{Z}_p|$, entonces $A \cap B \neq \phi$, es decir existe un $z \in A \cap B$, tal que $z \equiv a_1 (\mathrm{mod}\, p)$ y $z \equiv n - a_2 (\mathrm{mod}\, p)$ donde $a_1, a_2 \in A$, luego $a_1 \equiv n - a_2 (\mathrm{mod}\, p)$, ésto es $a_1 + a_2 \equiv n (\mathrm{mod}\, p)$.

Como a_1 y a_2 están en A, existen $x, y \in \mathbb{Z}_p$, tales que

$$x^2 \equiv a_1 (\mathrm{mod}\, p) \text{ y } y^2 \equiv a_2 (\mathrm{mod}\, p),$$

es decir

$$x^2 + y^2 \equiv n (\mathrm{mod}\, p). \square$$

En la ecuación (2.1), existe la posibilidad de que x ó y sea cero. Es claro que si n es un no residuo cuadrático módulo p, se tiene que x y y son incongruentes con cero módulo p; lo que no se puede garantizar si n es un residuo cuadrático. Con el fin de encontrar soluciones de la ecuación (2.1) en las cuales x y y no sean cero módulo p se hace la siguiente construcción.

Sean $a, b \in \mathbb{Z}_p$ con $p > 5$, se definen:

$$x = a^2 - b^2,$$

$$y = 2ab,$$

$$z = a^2 + b^2,$$

luego:

$$x^2 + y^2 = z^2.$$

Si se toman a y b de forma que $a^2 \not\equiv \pm b^2 (\mathrm{mod}\, p)$ y $a, b \not\equiv 0 (\mathrm{mod}\, p)$ (ésto se puede hacer puesto que $p > 5$), x, y y z son incongruentes con cero módulo p. A partir de esta construcción y recurriendo a la propiedad de grupo de los residuos cuadráticos se demuestra el resultado principal de esta sección.

Teorema 2.1.

Sea $p > 5$. Para todo $n \in \mathbb{Z}_p^*$, existen $x, y \in \mathbb{Z}_p^*$ tales que:

$$x^2 + y^2 \equiv n(\mathrm{mod}\, p).$$

Prueba. Si $n \in N_p$ el resultado es consecuencia de las observaciones siguientes al lema 2.1.

Cuando $n \in R_p$ se procede de la siguiente forma: por la construcción anterior existe al menos una tripleta x, y, z en $\mathbb{Z}_p^*$ tal que $x^2 + y^2 = z^2$.

Por la propiedad de grupo existe $t \in R_p$ con $t \equiv r^2(\mathrm{mod}\, p)$, tal que $z^2 t \equiv z^2 r^2 \equiv (zr)^2 \equiv n(\mathrm{mod}\, p)$, ésto es:

$$x_1^2 + y_1^2 \equiv n(\mathrm{mod}\, p),$$

donde $x_1^2 \equiv x^2 t \equiv x^2 r^2 \equiv (xr)^2 \not\equiv 0(\mathrm{mod}\, p)$ y $y_1^2 \equiv y^2 t \equiv y^2 r^2 \equiv (yr)^2 \not\equiv 0(\mathrm{mod}\, p)$. □

El teorema 2.1. establece que los residuos cuadráticos son una *base aditiva de orden dos para* $\mathbb{Z}_p^*$, es decir: todo elemento de $\mathbb{Z}_p^*$ es suma de dos residuos cuadráticos. El cero no siempre se puede expresar en la forma anterior; de hecho sólo es representable cuando $p \equiv 1(\mathrm{mod}\, 4)$ pues en este caso -1 es un residuo cuadrático de lo cual para todo $r \in R_p, -r \in R_p$ es decir existen $x, y \in \mathbb{Z}_p^*$ con $x^2 \equiv r\,(\mathrm{mod}\, p)$ y $y^2 \equiv -r\,(\mathrm{mod}\, p)$ y por tanto $r + (-r) \equiv x^2 + y^2 \equiv 0(\mathrm{mod}\, p)$.

Ejemplo 2.1. En la siguiente tabla se hace la suma de los residuos cuadráticos de 17. En este caso todos los elementos de $\mathbb{Z}_{17}^*$ aparecen en esta tabla, es decir que todos se pueden expresar como suma de dos residuos cuadráticos.

+	**1**	**2**	**4**	**8**	**9**	**13**	**15**	**16**
1	2	3	5	9	10	14	16	0
2		4	6	10	11	15	0	1
4			8	12	13	0	2	3
8				16	0	4	6	7
9					1	5	7	8
13						9	11	12
15							13	14
16								15

2.2 La función $\sigma_p(n)$

En la sección anterior se demostró que todo elemento de $\mathbb{Z}_p^*$ es representable como suma de dos residuos cuadráticos, ahora se desea encontrar cuantas representaciones tiene un elemento cualquiera de $\mathbb{Z}_p$.

Considere la ecuación $x^2 + y^2 = 1$ sobre el campo $\mathbb{Z}_p$. Se define $N(x^2 + y^2 = 1)$ como el número de parejas $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ tales que $x^2 + y^2 \equiv 1 (\mathrm{mod}\, p)$.

$$N(x^2 + y^2 = 1) = \sum_{a+b \equiv 1 (\mathrm{mod}\, p)} N(x^2 = a) N(x^2 = b),$$

donde la suma se toma sobre todas las parejas a, b en $\mathbb{Z}_p$ tales que $a + b \equiv 1 \,(\mathrm{mod}\, p)$ y $N(x^2 = a)$ es el número de soluciones de la ecuación $x^2 \equiv a \,(\mathrm{mod}\, p)$ en $\mathbb{Z}_p$.

Ahora, si $a \in R_p$, para un $x \in \mathbb{Z}_p^*$ se tiene que $x^2 \equiv (-x)^2 \equiv a \,(\mathrm{mod}\, p)$ y cuando $a \notin R_p$ la ecuación $x^2 \equiv a \,(\mathrm{mod}\, p)$ no tiene solución, por tanto

$$N(x^2 = a) = 1 + \left(\frac{a}{p}\right) = \begin{cases} 2 \text{ si } a \in Rp \\ 0 \text{ si } a \in Np \end{cases}.$$

luego

$$N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b \equiv 1 (\mathrm{mod}\, p)} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Las dos primeras sumas son cero (por el corolario 1.3) y la tercera es una suma de Jacobi cuyo valor es $-(-1)^{\frac{p-1}{2}}$ por la observación posterior al corolario 1.4.

En conclusión

$$N(x^2+y^2=1)=\begin{cases}p-1, & \text{si } p\equiv 1(\text{mod}4)\\ p+1, & \text{si } p\equiv 3(\text{mod}4)\end{cases}$$

Definición 2.1.

Sea $n\in\mathbb{Z}_p$

$$\sigma_p(n)=\#\{(a,b)\in R_p\times R_p : a\leq b \text{ y } n=a+b\}.$$

La función $\sigma_p(n)$ da el número de representaciones de n como suma de dos residuos cuadráticos.

Se estudiará por separado el número de representaciones del cero, de los residuos y no residuos cuadráticos módulo p.

Primero se establece una relación entre $\sigma_p(1)$ y $\sigma_p(r)$ donde $r\in R_p$.

Sea

$$r_1+r_2\equiv 1\,(\text{mod}\,p)\,,\ \text{donde } r_1,r_2\in R_p,$$

una representación para el 1 como suma de residuos cuadráticos. A partir de ésta, como $r\in R_p$ se obtiene que $r_1r+r_2r\equiv r(\text{mod}\,p)$, donde $r_1r,\, r_2r\in R_p$ por la propiedad de grupo. Así, por cada representación para el 1 se obtiene una representación para $r\in R_p$.

Además, sea

$$r_3+r_4\equiv r\,(\text{mod}\,p)\,,\ \text{con } r_3,\, r_4\in R_p$$

$$r_3r^{-1}+r_4r^{-1}\equiv rr^{-1}\equiv 1\,(\text{mod}\,p)\,,$$

donde $r_3r^{-1}, r_4r^{-1}\in R_p$ por la propiedad de grupo. Esto prueba que dada una representación para $r\in R_p$ se obtiene una para 1. Resumiendo

$$\sigma_p(1)=\sigma_p(r) \text{ para todo } r\in R_p$$

Se busca ahora una relación entre $N(x^2+y^2=1)$ y $\sigma_p(1)$. Retomando lo anterior

$$N(x^2+y^2=1)=\sum_{a+b=1}N(x^2=a)N(y^2=b)$$

Como las parejas $(1,0)$, $(-1,0)$, $(0,1)$, $(0,-1)$ son soluciones de $x^2+y^2\equiv 1(\mathrm{mod}\, p)$ se tiene que

$$N(x^2+y^2=1)=4+\sum_{\substack{a+b=1\\ a,b\neq 0}} N(x^2=a)N(y^2=b)$$

Si $a,b\in R_p$ con $a\neq b$ y $a+b=1$ entonces

$$N(x^2=a)N(y^2=b)=4 \text{ y } N(x^2=b)N(y^2=a)=4$$

Así, si la pareja (x,y) con $x\not\equiv y\,(\mathrm{mod}\, p)$ es solución para $x^2+y^2\equiv 1(\mathrm{mod}\, p)$ entonces las parejas $(x,-y),(-x,y),(-x,-y),(y,x),(y,-x),(-y,x),(-y,-x)$ también son soluciones.

De esta forma, *por cada representación para* 1 *como suma de dos residuos cuadráticos diferentes, se obtienen ocho parejas* (x,y) *tales que* $x^2+y^2\equiv 1(\mathrm{mod}\, p)$.

$\sigma_p(1)$ se definió como el número de representaciones de 1 mediante la suma de dos residuos cuadráticos.

Por lo dicho anteriormente:

$$\sum_{\substack{a+b=1\\ a,b\neq 0\\ a\neq b}} N(x^2=a)N(y^2=b)=8\sigma_p(1)$$

Pero si existe una pareja (x,y) con $y\equiv x\,(\mathrm{mod}\, p)$ que sea solución de $x^2+y^2\equiv 1(\mathrm{mod}\, p)$ esto implica que $2x^2\equiv 1(\mathrm{mod}\, p)$; ésto es: la pareja (x,x) es solución para $x^2+y^2\equiv 1(\mathrm{mod}\, p)$, lo que implica que las parejas $(x,-x),(-x,x),(-x,-x)$ también lo son.

Luego, *si existe una representación para* 1 *como suma de un residuo cuadrático consigo mismo, se obtienen sólo cuatro parejas* (x,y) *tales que* $x^2+y^2\equiv 1(\mathrm{mod}\, p)$. Esto es

$$\sum_{\substack{a+b=1\\ a,b\neq 0\\ a\neq b}} N(x^2=a)N(y^2=b)+N(x^2=a)N(y^2=a)=8\sigma_p(1)$$

Lo anterior demuestra el siguiente lema:

Lema 2.2

$$\sum_{\substack{a+b=1\\ a,b\neq 0}} N(x^2=a)N(y^2=b)=\begin{cases} 8\sigma_p(1) \text{ si } \nexists\, a\in R_p \text{ tal que } 2a\equiv 1(\mathrm{mod}\, p)\\ 8\sigma_p(1)-4 \text{ si } \exists\, a\in R_p \text{ tal que } 2a\equiv 1(\mathrm{mod}\, p)\end{cases}$$

Lema 2.3

$2\in R_p$ si, y sólo si existe $a\in R_p$, tal que $2a\equiv 1(\mathrm{mod}\, p)$

Prueba. La existencia de un $a \in R_p$ tal que $2a \equiv 1(\mathrm{mod}\, p)$ implica que $2 \in R_p$, pues 2 sería el inverso multiplicativo de un residuo cuadrático. Además, si $2 \in R_p$, existe un $a \in R_p$ tal que $2a \equiv 1(\mathrm{mod}\, p)$ por la propiedad de grupo.□

Lema 2.4.

Sea p un primo. Entonces:

1). Si $2 \in R_p$ entonces $N(x^2 + y^2 = 1) = 8\sigma_p(1)$.

2). Si $2 \notin R_p$ entonces $N(x^2 + y^2 = 1) = 4 + 8\sigma_p(1)$.

Prueba.

1). Supongase que $2 \in R_p$ entonces existe $a \in R_p$, tal que $2a \equiv 1(\mathrm{mod}\, p)$ y por el lema 2.2

$$N(x^2 + y^2 = 1) = 4 + \sum_{\substack{a+b=1 \\ a,b\neq 0}} N(x^2 = a)N(y^2 = b) = 4 + 8\sigma_p(1) - 4 = 8\sigma_p(1)$$

2) Si $2 \notin R_p$entonces no existe $a \in R_p$, tal que $2a \equiv 1(\mathrm{mod}\, p)$ y por el lema 2.2

$$N(x^2 + y^2 = 1) = 4 + \sum_{\substack{a+b=1 \\ a,b\neq 0}} N(x^2 = a)N(y^2 = b) = 4 + 8\sigma_p(1).\square$$

Para encontrar el valor exacto de $\sigma_p(1)$ se debe entonces determinar cuando $2 \in R_p$.

Lema 2.5.

a). $2 \in R_p$ si, y sólo si $p \equiv \pm 1(\mathrm{mod}\, 8)$.

b). $2 \in N_p$ si, y sólo si $p \equiv \pm 3(\mathrm{mod}\, 8)$.

Prueba. Consideremos las $\frac{p-1}{2}$ congruencias siguientes

$$p - 1 \equiv 1(-1)^1(\mathrm{mod}\, p),$$

$$2 \equiv 2(-1)^2(\mathrm{mod}\, p),$$

$$p - 3 \equiv 3(-1)^3(\mathrm{mod}\, p),$$

$$4 \equiv 4(-1)^4(\mathrm{mod}\, p),$$

$$\vdots$$

$$r \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}}(\mathrm{mod}\, p),$$

en donde r es $p-(p-1)/2$ ó $(p-1)/2$. Multiplicando estas congruencias se observa que cada entero de la izquierda es par. Se obtiene

$$2\cdot 4\cdot 6\cdot\cdots\cdot(p-1)\equiv\left(\frac{p-1}{2}\right)!\,(-1)^{1+2+\cdots+\left(\frac{p-1}{2}\right)}\,(\mathrm{mod}\,p)\,.$$

Esto es

$$2^{\left(\frac{p-1}{2}\right)}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!\,(-1)^{\left(\frac{p^2-1}{8}\right)}\,(\mathrm{mod}\,p)\,.$$

Como

$$\left(\frac{p-1}{2}\right)!\ncong 0\,(\mathrm{mod}\,p)$$

se tiene

$$2^{\left(\frac{p-1}{2}\right)}\equiv(-1)^{\left(\frac{p^2-1}{8}\right)}\,(\mathrm{mod}\,p)\,.$$

Por el criterio de Euler se tiene $2^{\left(\frac{p-1}{2}\right)}\equiv\left(\frac{2}{p}\right)(\mathrm{mod}\,p)$, y como cada uno de estos miembros es 1 o -1, ambos miembros son iguales. □

Lema 2.6.

Sea $p\geq 7$ un número primo, entonces

$$1)\,\text{Si}\;\; p\equiv 1(\mathrm{mod}\,8),\quad \sigma_p(1)=\frac{p-1}{8}.$$
$$2)\,\text{Si}\;\; p\equiv 3(\mathrm{mod}\,8),\quad \sigma_p(1)=\frac{p-3}{8}.$$
$$3)\,\text{Si}\;\; p\equiv 5(\mathrm{mod}\,8),\quad \sigma_p(1)=\frac{p-5}{8}.$$
$$4)\,\text{Si}\;\; p\equiv 7(\mathrm{mod}\,8),\quad \sigma_p(1)=\frac{p+1}{8}.$$

Prueba. Se sabe que

$$N(x^2+y^2=1)=\begin{cases}p-1, & \text{si } p\equiv 1(\mathrm{mod}4)\\ p+1, & \text{si } p\equiv 3(\mathrm{mod}4)\end{cases}$$

Por el lema 2.4 se sigue el resultado.□

Hasta ahora se ha encontrado el valor de $\sigma_p(r)$ para $r\in R_p$. Ahora se encuentra σ_p para los no residuos cuadráticos y para el cero.

Sean $a\in N_p$, $b\in N_p$ y $r_1+r_2\equiv a(\mathrm{mod}\,p)$ una representación para a como suma de elementos de R_p; por lo visto en el primer capitulo, existe $r_3\in R_p$ tal que $b\equiv ar_3(\mathrm{mod}\,p)$ luego $b\equiv r_1r_3+r_2r_3(\mathrm{mod}\,p)$;

ésto es, por cada representación de a existe una de b y viceversa. Así *todos los no residuos cuadráticos tienen igual número de representaciones como suma de elementos de* R_p.

Para finalizar esta sección, el siguiente teorema establece el valor exacto de σ_p en todo elemento de $\mathbb{Z}_p$.

Teorema 2.2.

Sean $p \geq 7$ un número primo, $r \in R_p$ y $n \in N_p$, entonces

$$\begin{aligned}
&1).\ \text{Si } p \equiv 1(\operatorname{mod} 8),\ \sigma_p(r) = \frac{p-1}{8} = \sigma_p(n),\ \sigma_p(0) = \frac{p-1}{4}.\\
&2).\ \text{Si } p \equiv 3(\operatorname{mod} 8),\ \sigma_p(r) = \frac{p-3}{8},\ \sigma_p(n) = \frac{p+5}{8},\ \sigma_p(0) = 0.\\
&3).\ \text{Si } p \equiv 5(\operatorname{mod} 8),\ \sigma_p(r) = \frac{p-5}{8},\ \sigma_p(n) = \frac{p+3}{8},\ \sigma_p(0) = \frac{p-1}{4}.\\
&4).\ \text{Si } p \equiv 7(\operatorname{mod} 8),\ \sigma_p(r) = \frac{p+1}{8} = \sigma_p(n),\ \sigma_p(0) = 0.
\end{aligned}$$

Prueba. El resultado para $\sigma_p(r)$ se sigue del lema 2.6 y de que $\sigma_p(r) = \sigma_p(1)$ como ya se demostró. Ahora se hará la prueba para $\sigma_p(n)$ y $\sigma_p(0)$.

Como $|R_p| = \frac{p-1}{2}$, entonces el número total de sumas de dos elementos de R_p es

$$\binom{\frac{p-1}{2}+1}{2} = \frac{1}{8}\left(p^2-1\right).$$

Dado que existen tantos residuos como no residuos cuadráticos, entonces:

$$\frac{1}{8}\left(p^2-1\right) = \left(\frac{p-1}{2}\right)\left(\sigma_p(r) + \sigma_p(n)\right) + \sigma_p(0). \tag{2.2}$$

1). Si $p \equiv 1(\operatorname{mod} 8)$, entonces $p \equiv 1(\operatorname{mod} 4)$ lo cual implica que $-1 \in R_p$, y con esto, si $b \in R_p$ entonces $-b$ también está en R_p. Es decir, cada uno de los residuos cuadráticos tiene su inverso aditivo en R_p. Así,

$$b + (-b) = (-b) + b \equiv 0(\operatorname{mod} p),$$

luego

$$\sigma_p(0) = \frac{p-1}{4}.$$

Ahora de (2.2) y de lo anterior se tiene

$$\left(\frac{p-1}{2}\right)\sigma_p(n) = \frac{1}{8}\left(p^2-1\right) - \left(\frac{p-1}{2}\right)\left(\frac{p-1}{8}\right) - \left(\frac{p-1}{4}\right),$$

y de aquí

$$\sigma_p(n) = \frac{p-1}{8}.$$

2). Si $p \equiv 3(\mathrm{mod}\, 8)$, entonces $p \equiv 3(\mathrm{mod}\, 4)$ y $-1 \notin R_p$, de donde

$$\sigma_p(0) = 0,$$

y fácilmente se puede ver que

$$\sigma_p(n) = \frac{p+5}{8}.$$

Las partes 3) y 4) se prueban de igual forma. □

2.3 La ecuación $x^2 - y^2 \equiv n(\mathrm{mod}\, p)$

En esta sección, se prueban resultados análogos a los ya obtenidos en sumas de residuos cuadráticos.

Lema 2.7.

Para todo $n \in \mathbb{Z}_p^*$, existen $x, y \in \mathbb{Z}_p$ tales que

$$x^2 - y^2 \equiv n(\mathrm{mod}\, p).$$

Prueba. Se definen los conjuntos

$$A = R_p \cup \{0\},$$

$$B = \{n + t(\mathrm{mod}\, p) : t \in A\},$$

y se procede como en la prueba del lema 2.1. □

Lema 2.8.

Si $n \in \mathbb{Z}_p^*$ entonces el número de parejas $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ tales que $x^2 - y^2 \equiv n(\mathrm{mod}\, p)$ es $p - 1$.

Prueba. Como $x^2 - y^2 = (x-y)(x+y)$. Sean $u = x - y$ y $v = x + y$, luego $x^2 - y^2 = uv$, ahora si se fija v y se varía u en $\mathbb{Z}_p^*$ se obtienen las ecuaciones

$$1.v \equiv n(\mathrm{mod}\, p),$$

$$2.v \equiv n(\mathrm{mod}\, p),$$

$$\vdots$$

$$(p-1).v \equiv n(\mathrm{mod}\, p),$$

cada una de las cuales tiene solución única. Por cada ecuación se resuelve el sistema

$$\begin{cases} u = x - y \\ v = x + y \end{cases}$$

que siempre tiene solución para x y y.

Por lo tanto existen $p-1$ parejas (x, y) que solucionan la ecuación. □

Teorema 2.3.

Sea $p \geq 7$. Para todo $n \in \mathbb{Z}_p^*$, existen $x, y \in \mathbb{Z}_p^*$ tales que

$$x^2 - y^2 \equiv n(\mathrm{mod}\, p).$$

Prueba. En la sección anterior se garantizó la existencia de $x, y, z \in \mathbb{Z}_p^*$ tales que $z^2 + y^2 \equiv x^2(\mathrm{mod}\, p)$ que equivale a $z^2 \equiv x^2 - y^2(\mathrm{mod}\, p)$ luego, si $n \in R_p$ lo afirmado se sigue inmediatamente de esta observación (existe $t \in R_p$ tal que $tz^2 \equiv n\,(\mathrm{mod}\, p)$).

Si $n \in N_p$ se consideran los siguientes casos.

1). $p \equiv 1(\mathrm{mod}\, 4)$.

2). $p \equiv 3(\mathrm{mod}\, 4)$.

En ambos casos se debe mostrar que tanto x como y pueden ser incongruentes con cero módulo p.

En el primer caso, como $-1 \in R_p$, $-y^2$ es un residuo cuadrático y $x^2 - y^2 = x^2 + (-1)y^2 \equiv n(\mathrm{mod}\, p)$.

En el segundo caso, y no es congruente con cero módulo p pues $n \in N_p$. Además, si en todas las $p-1$ parejas que solucionan la ecuación $x^2 - y^2 \equiv n(\mathrm{mod}\, p)$ se tuviera que $x \equiv 0(\mathrm{mod}\, p)$, se concluiría que

todos los no residuos cuadráticos son congruentes módulo p pues $-y^2 \in N_p$ cuando y recorre $\mathbb{Z}_p^*$ lo cual es imposible.

Por lo tanto existe al menos una solución con x y y incongruentes con cero módulo p. □

Ejemplo 2.2. El teorema anterior dice que todo elemento de $\mathbb{Z}_p^*$, $p \geq 7$, se puede expresar como diferencia de dos residuos cuadráticos. En la tabla presentada abajo se hace la diferencia de los resíduos cuadráticos de 17.

−	**1**	**2**	**4**	**8**	**9**	**13**	**15**	**16**
1	0	1	3	7	8	12	14	15
2	16	0	2	6	7	11	13	14
4	14	15	0	4	5	9	11	12
8	10	11	13	0	1	5	7	8
9	9	10	12	16	0	4	6	7
13	5	6	8	12	13	0	2	3
15	3	4	6	10	11	15	0	1
16	2	3	5	9	10	14	16	0

2.4 La función $\delta_p(a)$

Lema 2.9.

Si $a \in \mathbb{Z}_p^*$, el número de soluciones de $x^2 - y^2 \equiv a(\mathrm{mod}\, p)$ esta dado por

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2+a}{p}\right)\right). \tag{2.3}$$

Prueba. La ecuación $x^2 - y^2 \equiv a(\mathrm{mod}\, p)$ es equivalente a $x^2 \equiv a + y^2(\mathrm{mod}\, p)$ la cual tiene solución si, y sólo si $y^2 + a \in R_p$. A cada y que cumpla lo anterior le corresponden las dos soluciones: $x^2 \equiv a + y^2(\mathrm{mod}\, p)$ y $(-x)^2 \equiv a + y^2(\mathrm{mod}\, p)$. Además:

$$1 + \left(\frac{y^2+a}{p}\right) = \begin{cases} 2 \text{ si } y^2 + a \in R_p \\ 0 \text{ si } y^2 + a \notin R_p \end{cases}$$

Cuando y recorre $\mathbb{Z}_p$, la sumatoria (2.3) da el número de soluciones de la ecuación original. □

Este lema y el lema 2.8 implican que:

$$\sum_{y=0}^{p-1}\left(1+\left(\frac{y^2+a}{p}\right)\right)=p-1,$$

ésto implica

$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)=-1. \tag{2.4}$$

Definición 2.2.

Dado un primo p y $a\in\mathbb{Z}_p^*$, $\delta_p(a)$ se define por:

$$\delta_p(a)=\#\left\{r_1-r_2\equiv a(\mathrm{mod}\, p): r_1,r_2\in R_p\right\}.$$

es decir; $\delta_p(a)$ es el número de representaciones de a como resta de dos residuos cuadráticos módulo p.

Teorema 2.3. Sea $p\geq 7$ un número primo, y $a\in\mathbb{Z}_p^*$, entonces

1). Si $p\equiv 1(\mathrm{mod}\, 4)$ se tiene que

$$\delta_p(a)=\begin{cases}\frac{p-5}{4} \text{ si } a\in R_p\\ \frac{p-1}{4} \text{ si } a\notin R_p\end{cases}$$

2). Si $p\equiv 3(\mathrm{mod}\, 4)$ se tiene que

$$\delta_p(a)=\frac{p-3}{4}$$

3). Para todo p

$$\delta_p(0)=\frac{p-1}{2}$$

Prueba.

(Para esta demostración se recurre al concepto de multiconjunto el cual se entiende como una lista donde pueden existir elementos repetidos).

A partir de la ecuación (2.4) se sabe:

$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)=-1, \text{siempre que } a\in\mathbb{Z}_p^*,$$

con el cual se cuenta el número de elementos de los multiconjuntos.

$$A \cap R_p = \{x \in A : x \in R_p\},$$

$$A \cap N_p = \{x \in A : x \in N_p\},$$

$$A_0 = \{x \in A : x \equiv 0 \,(\mathrm{mod}\, p)\},$$

donde

$$A = \left\{y^2 + a : y, a \in \mathbb{Z}_p^*,\ a \text{ fijo}\right\},$$

es un multiconjunto con elementos repetidos módulo p. Como $y^2 + a \equiv (p-y)^2 + a \,(\mathrm{mod}\, p)$ entonces

$$2\delta_p(a) = |A \cap R_p|, \tag{2.5}$$

pues dada una representación para a como resta de elementos de R_p, es decir $x^2 - y^2 \equiv a(\mathrm{mod}\, p)$ donde $x, y \in \mathbb{Z}_p^*$, se tiene que los elementos $y^2 + a$ y $(p-y)^2 + a$ son congruentes con $x^2(\mathrm{mod}\, p)$ y por tanto están en $A \cap R_p$.

Además:

$$|A \cap R_p| + |A \cap N_p| + |A_0| = |A| = p - 1. \tag{2.6}$$

Ahora, se consideran cuatro casos para $a \in \mathbb{Z}_p^*$.

Caso 1. Si $p \equiv 1(\mathrm{mod}\, 4)$ y $a \in R_p$.

En este caso $-1 \in R_p$, y por la propiedad de grupo $-a \in R_p$, ésto es: existen y_1 y y_2 tales que $y_1^2 \equiv y_2^2 \equiv -a \,(\mathrm{mod}\, p)$ por lo tanto existen dos elementos de A congruentes con cero módulo p ($y_1^2 + a$ y $y_2^2 + a$) luego

$$|A_0| = 2,$$

reemplazando en (2.6)

$$|A \cap R_p| + |A \cap N_p| = p - 3. \tag{2.7}$$

Ahora bien, como $a \in R_p$, $\left(\frac{a}{p}\right) = 1$ entonces

$$1 + \sum_{y=1}^{p-1} \left(\frac{y^2 + a}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = -1$$

por tanto

$$\sum_{y=1}^{p-1}\left(\frac{y^2+a}{p}\right)=-2$$

es decir, en A el número de no residuos cuadráticos excede en dos al número de resíduos por tanto

$$|A\cap N_p|=|A\cap R_p|+2,$$

y por (2.7)

$$|A\cap R_p|=\frac{p-5}{2}$$
$$|A\cap N_p|=\frac{p-1}{2}$$

finalmente por (2.5) se concluye $\delta_p(a)=\frac{p-5}{4}$.

Caso 2. $p\equiv 1(\mathrm{mod}\,4)$ y $a\notin R_p$.

En este caso, y^2 no tomará el valor de $-a$ cuando y recorre $\mathbb{Z}_p^*$, luego

$$|A_0|=0,$$

de (2.6) se tiene

$$|A\cap R_p|+|A\cap N_p|=p-1.$$

Además como $a\notin R_p,\left(\frac{a}{p}\right)=-1$. Asi

$$-1+\sum_{y=1}^{p-1}\left(\frac{y^2+a}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)=-1$$
$$\text{por tanto }\sum_{y=1}^{p-1}\left(\frac{y^2+a}{p}\right)=0$$

de donde se obtiene

$$|A\cap N_p|=|A\cap R_p|,$$

entonces

$$|A\cap R_p|=\frac{p-1}{2},$$
$$|A\cap N_p|=\frac{p-1}{2},$$

Nuevamente por (2.5) se sigue que $\delta_p(a) = \frac{p-1}{4}$.

Caso 3. Si $p \equiv 3(\mathrm{mod}\, 4)$ y $a \in R_p$.

En este caso $-1 \notin R_p$, por lo tanto (como en el caso 2)

$$|A_0| = 0,$$

y

$$|A \cap R_p| + |A \cap N_p| = p - 1.$$

Ahora bien como $a \in R_p$, de igual forma que en el caso 1

$$|A \cap N_p| = |A \cap R_p| + 2,$$

entonces

$$|A \cap R_p| = \frac{p-3}{2},$$
$$|A \cap N_p| = \frac{p+1}{2},$$

luego $\delta_p(a) = \frac{p-3}{4}$.

Caso 4. $p \equiv 3(\mathrm{mod}\, 4)$ y $a \notin R_p$

Se tiene nuevamente que

$$|A_0| = 2$$

y por tanto

$$|A \cap R_p| + |A \cap N_p| = p - 3.$$

Además como $a \notin R_p$, entonces

$$|A \cap N_p| = |A \cap R_p|,$$

luego

$$|A \cap R_p| = \frac{p-3}{2},$$
$$|A \cap N_p| = \frac{p-3}{2},$$

de donde $\delta_p(a) = \frac{p-3}{4}$.

Todas las representaciones de 0 como resta de residuos cuadráticos son de la forma $r - r$ con $r \in R_p$, entonces

$$\delta_p(0) = \frac{p-1}{2}. \square$$

3 Cuadrados en progresión aritmética

En este capítulo se demuestra que no es posible tener cuatro cuadrados enteros en progresión aritmética, mientras que para todo k existen infinitos primos para los cuales se tienen k residuos cuadráticos en progresión aritmética.

3.1 Ternas pitagóricas

Definición 3.1 (Terna pitagórica)

Una *terna pitagórica* es una tripleta (x, y, z) de enteros positivos tales que:

$$x^2 + y^2 = z^2$$

Una terna pitagórica (x, y, z) se llama *primitiva* si $mcd(x, y, z) = 1$.

No es difícil probar que todas las ternas pitagóricas se pueden obtener a partir de las ternas primitivas. Si x, y, z es una terna pitagórica con $mcd(x, y, z) = d$ entonces existen enteros x_1, y_1, z_1 con $x = dx_1$, $y = dy_1$ y $z = dz_1$ y $mcd(x_1, y_1, z_1) = 1$. Además como

$$x^2 + y^2 = z^2,$$

se tiene

$$(dx_1)^2 + (dy_1)^2 = (dz_1)^2,$$

por lo tanto

$$x_1^2 + y_1^2 = z_1^2,$$

luego la tripleta (x_1, y_1, z_1) es pitagórica primitiva y la tripleta $(x, y, z) = (dx_1, dy_1, dz_1)$, un múltiplo entero de una terna primitiva. Recíprocamente, mediante cómputo directo es fácil ver que todo múltiplo de una terna primitiva es una terna pitagórica.

Por lo tanto, para caracterizar todas las ternas pitagóricas es suficiente caracterizar las ternas primitivas.

Lema 3.1

Si x, y, z es una terna primitiva entonces $mcd\,(x, y) = mcd\,(x, z) = mcd\,(y, z) = 1$.

Prueba. Suponga que x, y, z es una terna primitiva y que $mcd\,(x, y) \neq 1$. Entonces existe un primo p tal que $p \mid mcd(x, y)$, y de aquí $p \mid x$ y $p \mid y$. Luego, $p \mid (x^2 + y^2) = z^2$. Puesto que $p \mid z^2$ se sigue que $p \mid z$. Esto es una contradicción porque $mcd(x, y, z) = 1$. Luego $mcd(x, y) = 1$.
En forma similar se prueba que $mcd(x, z) = mcd(y, z) = 1$. □

Lema 3.2

Si x, y, z es una terna primitiva, entonces y es par y x impar ó y es impar y x es par (x, y son de paridad opuesta).

Prueba. Sea x, y, z la terna primitiva. Por el lema anterior se sabe que $(x, y) = 1$, entonces x, y no pueden ser los dos pares. También x, y no pueden ser ambos impares, porque si x, y fueran impares se tendría

$$x^2 \equiv y^2 \equiv 1 \,(\mathrm{mod}\, 4)\,,$$

entonces

$$z^2 = x^2 + y^2 \equiv 2 \,(\mathrm{mod}\, 4)\,,$$

que es imposible porque los cuadrados módulo 4 son congruentes con 1 o 0. De aquí y es par y x impar o viceversa. □

Lema 3.3

Si r, s y t son enteros positivos tales que $mcd\,(r, s) = 1$ y $rs = t^2$, entonces existen enteros m y n tal que $r = m^2$ y $s = n^2$.

Prueba. Si $r = 1$ ó $s = 1$, entonces el lema es verdadero. Ahora supongase que $r > 1$ y $s > 1$.

Sean:

$$r = p_1^{a_1} p_2^{a_2} ... p_u^{a_u}, \quad \text{con } a_i > 0,$$

$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} ... p_v^{a_v}, \quad \text{con } a_j > 0,$$

y

$$t = q_1^{b_1} q_2^{b_2} ... q_k^{b_k}, \quad \text{con } b_i > 0,$$

Dado que $mcd(r, s) = 1$ los primos que aparecen en las factorizaciones de r y s son diferentes.

Como $rs = t^2$, se tiene que:

$$p_1^{a_1} p_2^{a_2} ... p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} ... p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} ... q_k^{2b_k}.$$

Del *Teorema Fundamental de la Aritmética* las potencias primas que ocurren en ambos lados de la ecuación son las mismas. Esto es: cada p_i debe ser igual a q_j para algún j, es decir, con los exponentes se tiene que para cada i , $a_i = 2b_j$ para algún j. Así se tiene que $r = m^2$ y $s = n^2$ donde m y n son los enteros

$$m = p_1^{a_1/2} p_2^{a_2/2} ... p_u^{a_u/2},$$

y

$$n = p_{u+1}^{a_{u+1}/2} p_{u+2}^{a_{u+2}/2} ... p_v^{a_v/2}. \square$$

Teorema 3.1 (Caracterización de las ternas pitagóricas primitivas)

Los enteros positivos x, y, z forman una terna pitagórica primitiva, con y par, si, y sólo si existen enteros positivos primos relativos m y n $(m > n)$, con m impar y n par (o viceversa) tales que:

$$x = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2.$$

Prueba. Sea (x, y, z) una terna primitiva, por el lema 3.2, x es impar y y es par, o viceversa. Sin perder generalidad, se supone que y es par. Luego x y z son impares. De aquí, $z+x$ y $z-x$ son pares, entonces existen enteros positivos r y s con $r = (z+x)/2$ y $s = (z-x)/2$.

Dado que $x^2 + y^2 = z^2$, se tiene que $y^2 = z^2 - x^2 = (z+x)(z-x)$. De aquí

$$(y/2)^2 = ((z+x)/2)((z-x)/2) = rs.$$

Note que $mcd(r, s) = 1$.

Ahora, usando el lema 3.3, existen enteros m y n tales que $r = m^2$ y $s = n^2$. Expresando x, y, z en términos de m y n, se tiene que:

$$x = r - s = m^2 - n^2,$$

$$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn,$$

y

$$z = r + s = m^2 + n^2.$$

$mcd(m, n) = 1$, puesto que cualquier divisor de m y n debe dividir también a $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, y además $mcd(x, y, z) = 1$. También se nota que m y n no pueden ser ambos impares, porque si lo fueran, entonces x, y, z son todos pares, contradiciendo la condición $mcd(x, y, z) = 1$.

Como $mcd(m, n) = 1$, m y n no pueden ser ambos pares, suponga que m es par y n es impar. Esto muestra que la terna pitagórica primitiva tiene la forma buscada.

Para ver que toda terna de la forma

$$x = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2,$$

donde m y n son enteros postivos, $m > n, mcd(m,n) = 1$, y $m \not\equiv n (\mathrm{mod}\, 2)$, constituye una terna primitiva primero observar que:

$$\begin{aligned} x^2 + y^2 &= \left(m^2 - n^2\right)^2 + (2mn)^2 \\ &= \left(m^4 - 2m^2n^2 + n^4\right) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= \left(m^2 + n^2\right)^2 \\ &= z^2 \end{aligned}$$

Además, es fácil verificar que x, y y z son primos relativos dos a dos. □

3.2 La Ecuación $a\,(a+d)\,(a+2d)\,(a+3d) = x^2$

Se le atribuye a *Fermat* la primera demostración de la inexistencia de cuatro cuadrados en progresión aritmética. A pesar de ser un resultado clásico, casi todas sus demostraciones son tremendamente complicadas y requieren muchos cálculos. La demostración aqui presentada es tomada del artículo "*On the equation* $a\,(a+d)\,(a+2d)\,(a+3d) = x^2$ " de *Tamás Erdélyi* [3] .

Lo interesante de esta prueba es la ausencia de conceptos distintos a los aprendidos en un curso de matemáticas fundamentales y que constituye una aplicación del método del *Descenso Infinito de Fermat.* Esta técnica se basa en el hecho de que todo subconjunto de los enteros positivos tiene un elemento mínimo. (ver [8]).

La idea de la prueba consiste en que si existieran cuatro cuadrados en progresión aritmética habría una solución para la ecuación

$$a\,(a+d)\,(a+2d)\,(a+3d) = x^2$$

en los enteros positivos. De esta forma, la no existencia de cuatro cuadrados en progresión aritmética se deduce de la no solubilidad en los enteros positivos de la anterior ecuación.

Lema 3.4

Si existen cuatro cuadrados en progresión aritmética, entonces la ecuación

$$a\,(a+d)\,(a+2d)\,(a+3d) = x^2$$

tiene solución en $\mathbb{Z}^+$.

Prueba. Sean A^2, B^2, C^2, D^2 tales que existen a, d con:

$$A^2 = a,$$

$$B^2 = a + d,$$

$$C^2 = a + 2d,$$

$$D^2 = a + 3d,$$

es decir, los cuadrados están en una progresión aritmética de razón d, término inicial a y longitud 4. Se tiene que

$$A^2B^2C^2D^2 = a\,(a+d)\,(a+2d)\,(a+3d) = (ABCD)^2. \;\square$$

Lema 3.5

Las soluciones enteras de la ecuación

$$x^2 + y^2 - xy = z^2$$

vienen dadas por

$$x = t(a-b)\,(a+b)\,, \quad y = ta(a-2b), \quad a, b, t \in \mathbb{Z},\ b \neq 0.$$

La demostración se presenta en la siguiente sección.

Teorema 3.2

La ecuación

$$a\,(a+d)\,(a+2d)\,(a+3d) = x^2 \tag{3.1}$$

no tiene solución en $\mathbb{Z}^+$.

Prueba. En primer lugar se asume que existe una terna de enteros positivos (a, d, x) tal que:

$$a\,(a+d)\,(a+2d)\,(a+3d) = x^2,$$

donde $(a+d)\,(a+2d)$ es minimal.

Se mostrará que existe una terna (A, D, X) de enteros positivos que satisfacen

$$A\,(A+D)\,(A+2D)\,(A+3D) = X^2,$$

y tales que

$$(A+D)\,(A+2D) < (a+d)\,(a+2d)\,.$$

Se puede suponer que $mcd\,(a, d) = 1$ ya que en caso contrario bastaría con dividir (3.1) entre $mcd\,(a, d)$, para obtener una nueva terna donde el término inicial y la razón sean primos relativos.

Resolviendo (3.1) se obtiene

$$a\,(a+d)\,(a+2d)\,(a+3d) = a^4 + 6a^3d + 2a^2d^2 + 9a^2d^2 + 6ad^3 = x^2,$$

sumando d^4 en ambos lados de la igualdad anterior

$$a^4 + 6a^3d + 2a^2d^2 + 9a^2d^2 + 6ad^3 + d^4 = x^2 + d^4,$$

ésto es

$$\left(a^2 + 3ad + d^2\right)^2 = x^2 + \left(d^2\right)^2.$$

Como los enteros $\left(a^2 + 3ad + d^2\right)$, x, d^2 forman una terna pitagórica primitiva por el teorema 3.1 se desprenden los siguientes casos.

Caso 1.

$$a^2 + 3ad + d^2 = u^2 + v^2;\ d^2 = 2uv \tag{3.2}$$

con $u, v \in \mathbb{Z}^+$ y uv es par con $mcd\,(u, v) = 1$.

Caso 2.

$$a^2 + 3ad + d^2 = u^2 + v^2;\ d^2 = u^2 - v^2$$

con $u, v \in \mathbb{Z}^+$ y uv es par con $mcd\,(u, v) = 1$.

Solución del Caso 1. Sin perder generalidad, se puede asumir que u es par.

Como $mcd\,(u, v) = 1$, entonces $mcd\,(2u, v) = 1$ luego por el lema 3.3 y debido a que $d^2 = 2uv$ existen enteros positivos u' y v_1 tales que

$$2u = (u')^2\,,$$

$$v = v_1^2.$$

Nótese que como $2u$ es par entonces u' debe ser par, esto es $u' = 2u_1$, donde $u_1 \in \mathbb{Z}^+$.

De esta forma

$$v = v_1^2,\ u = 2u_1^2.$$

Reemplazando lo anterior en (3.2)

$$a^2 + 3ad + d^2 = 4u_1^4 + v_1^4,\ \text{donde } d = 2u_1v_1.$$

Ahora se considera la siguiente ecuación en a:

$$f\,(a) = a^2 + 6u_1v_1a + 4u_1^2v_1^2 - 4u_1^4 - v_1^4 = 0.$$

El discriminante de $f(a)$ debe ser el cuadrado de un entero puesto que se supuso que había solución entera de (3.1). Así

$$36u_1^2v_1^2 - 4(1)(4u_1^2v_1^2 - 4u_1^4 - v_1^4) = y^2,$$

que se puede escribir como

$$20u_1^2v_1^2 + 16u_1^4 + 4v_1^4 = y^2,$$

dividiendo por 4

$$4u_1^4 + v_1^4 + 5u_1^2v_1^2 = \frac{y^2}{4} = y_1^2,\ \text{donde } y_1 = \frac{y}{2}.$$

Esto es

$$\left(u_1^2 + v_1^2\right)\left(4u_1^2 + v_1^2\right) = y_1^2. \tag{3.3}$$

Observese que $mcd((u_1^2+v_1^2),(4u_1^2+v_1^2))=h=1$. Porque si $h>1$, entonces

$$h \mid \left[\left(4u_1^2+v_1^2\right)-3\left(u_1^2+v_1^2\right)\right]=3u_1^2,$$

$$h \mid \left[4\left(u_1^2+v_1^2\right)-\left(4u_1^2+v_1^2\right)\right]=3v_1^2,$$

y como u_1 y v_1 son primos relativos se tiene que $h=3$ ó $h=1$. Pero el hecho de que $h \mid \left(u_1^2+v_1^2\right)$ implica que $h \neq 3$, pues de otra manera $3 \mid v_1$ y $3 \mid u_1$. Así que h debe ser igual a 1.

Luego, aplicando el lema 3.3 a (3.3) existen enteros positivos e, f tales que

$$u_1^2+v_1^2=e^2,$$

$$4u_1^2+v_1^2=f^2.$$

Si se aplica nuevamente el teorema 3.1 a los dos ecuaciones anteriores:

$$u_1=2u_2v_2, \quad v_1=u_2^2-v_2^2,$$

$$2u_1=2u_3v_3, \quad v_1=u_3^2-v_3^2,$$

con $u_2, v_2, u_3, v_3 \in \mathbb{Z}^+$. Entonces

$$u_3v_3=2u_2v_2,$$

$$u_3^2-v_3^2=u_2^2-v_2^2.$$

Así:

$$\left(u_3^2-v_3^2\right)^2+u_3^2v_3^2=\left(u_2^2-v_2^2\right)+4u_2^2v_2^2.$$

Simplificando términos

$$\left(u_3^2-v_3^2\right)^2+u_3^2v_3^2=\left(u_2^2+v_2^2\right)^2.$$

Haciendo $x=u_3^2,\ y=v_3^2$, por el lema 3.5. las soluciones de esta última ecuación pueden ser expresadas como

$$x=t\left(a_1-b_1\right)\left(a_1+b_1\right),\ y=ta_1(a_1-2b_1),$$

donde t es un entero y $b_1 \neq 0$.

Ahora si se considera que t es un entero divisible entre 3 se tiene:

$$x = \frac{t}{3}(a_1 - b_1)(a_1 + b_1), \quad y = \frac{t}{3}a_1(a_1 - 2b_1),$$

como

$$u_3^2 v_3^2 = xy = \frac{t^2}{9}(a_1 - b_1)(a_1 + b_1)a_1(a_1 - 2b_1),$$

definiendo $a_2 = a_1 - 2b_1$, $b_2 = b_1$ se obtiene:

$$\frac{9u_3^2 v_3^2}{t^2} = a_2(a_2 + b_2)(a_2 + 2b_2)(a_2 + 3b_2).$$

finalmente

$$\begin{aligned}(a_2 + b_2)(a_2 + 2b_2) &< \frac{1}{2}a_2(a_2 + b_2)(a_2 + 2b_2)(a_2 + 3b_2) \\ &= \frac{9}{2t^2}u_3^2 v_3^2 = \frac{9}{2t^2}u_1^2 = \frac{9}{8t^2}4u_1^2 \leq \frac{9}{8t^2}4u_1^2 v_1^2 \\ &= \frac{9}{8}d^2 < d^2 < a^2 + 3ad + 2d^2 = (a + d)(a + 2d)\end{aligned}$$

Así se ha construido una nueva terna que satisface la ecuación (3.1); pero con

$$(a_2 + b_2)(a_2 + 2b_2) < (a + d)(a + 2d)$$

lo que es una contradicción.

Solución Caso 2.

$$a^2 + 3ad + d^2 = u^2 + v^2;\ d^2 = u^2 - v^2;\ u, v \in \mathbb{Z}^+ \text{ y } uv \text{ es par, con } mcd(u, v) = 1.$$

Manipulando la primera ecuación

$$4\left(a^2 + 3ad + d^2\right) = 2[(u + v)^2 + (u - v)^2],$$

$$d^2 = (u + v)(u - v).$$

Puesto que $mcd(u, v) = 1$ y uv es par se tiene que $mcd(u + v, u - v) = 1$.

Aplicando el lema 3.3 se tiene:

$$u + v = x_1^2 \quad \text{y} \quad u - v = x_2^2 \text{ con } x_1, x_2 \in \mathbb{Z}^+ \text{ y } mcd(x_1, x_2) = 1.$$

Con lo anterior $d = x_1 x_2$. Ahora, igual que en el caso 1, se considera la siguiente ecuación

$$f(a) = a^2 + 3x_1 x_2 a + x_1^2 x_2^2 - \frac{1}{2}x_1^4 - \frac{1}{2}x_2^4 = 0.$$

Tomando el discriminante y simplificando términos se tiene que

$$2x_1^4 + 5x_1^2 x_2^2 + 2x_2^4 = y^2 \text{ con } \ y \in \mathbb{Z}^+,$$

ésto es

$$(2x_1^2 + x_2^2)\left(2x_2^2 + x_1^2\right) = y^2.$$

Ya que $mcd(x_1, x_2) = 1$ es imposible que $3 \mid x_1$ y $3 \mid x_2$.

Supongase ahora que $3 \mid x_1$ y $3 \nmid x_2$ o viceversa, entonces

$$2x_1^2 \equiv 0(\mathrm{mod}\, 3), \quad x_2^2 \equiv 1\,(\mathrm{mod}\, 3)\,,$$

$$x_1^2 \equiv 0\,(\mathrm{mod}\, 3)\,, \quad 2x_2^2 \equiv 2\,(\mathrm{mod}\, 3)\,.$$

Luego

$$y^2 = (2x_1^2 + x_2^2)\left(2x_2^2 + x_1^2\right) \equiv 2(\mathrm{mod}\, 3).$$

Esto es imposible pues los únicos cuadrados módulo 3 son 0 y 1. Con ésto se afirma que $3 \nmid x_1$ y $3 \nmid x_2$,

luego $x_1^2 \equiv x_2^2 \equiv 1(\mathrm{mod}\, 3)$.

Y por lo cual $3 \mid \left(2x_1^2 + x_2^2\right)$ y $3 \mid \left(2x_2^2 + x_1^2\right)$.

De donde

$$x_2^2 \left[\frac{2x_1^2 + x_2^2}{3}\right]\left[\frac{2x_2^2 + x_1^2}{3}\right] x_1^2 = x_1^2 x_2^2 y^2 = y_1^2, \text{ donde } y_1 = x_1 x_2 y \in \mathbb{Z}^+.$$

Sea $a_2 = x_2^2$ y $b_2 = \frac{1}{3}\left(x_1^2 - x_2^2\right)$ así

$$a_2\,(a_2 + b_2)\,(a_2 + 2b_2)\,(a_2 + 3b_2) = y_1^2.$$

Es fácil ver que $b_2 \neq 0$, pues de lo contrario $d = 0$ implica una contradicción.

Finalmente

$$\begin{aligned}(a_2+b_2)(a_2+2b_2) &= \frac{1}{9}\left(2x_1^4+2x_2^4+5x_1^2x_2^2\right) = \frac{1}{9}\left(4\left(a^2+3ad+d^2\right)+5d^2\right)\\ &= \frac{1}{9}\left(4\left(a^2+3ad\right)+9d^2\right) < \frac{1}{9}[9\left(a^2+3ad+d^2\right)]\\ &= a^2+3ad+d^2 < a^2+3ad+2d^2\\ &= (a+d)(a+2d).\end{aligned}$$

Por lo tanto se ha encontrado, al igual que en el caso 1 una terna solución de (3.1) tal que

$$(a_2+b_2)(a_2+2b_2) < (a+d)(a+2d). \ \square$$

3.3 Solución paramétrica de la ecuación $x^2+y^2-xy=z^2$

En la sección anterior se necesitó encontrar todas las soluciones de la ecuación $x^2+y^2-xy=z^2$ en números enteros, sin embargo se debía encontrarlas de forma que dependieran de un parámetro t. En esta sección se da una demostración de la fórmula dada en el lema 3.5. Esta prueba es un ejemplo del llamado método de Bachet (en honor a su descubridor *Bachet de Méziriac*) el cual permite, mediante sencillos argumentos geométricos, encontrar todas las soluciones racionales de algunas ecuaciones diofánticas en forma paramétrica. A continuación se explica este método aplicándolo a la ecuación $ax^2+by^2=cz^2$ y posteriormente se hace una adaptación del método para la ecuación anterior.

Se considera la ecuación

$$ax^2+by^2=cz^2 \ , a,b,c\in\mathbb{Z}.$$

En general esta ecuación no tiene por qué tener soluciones, pero si se encuentra una solución (x_0,y_0,z_0) se puede hallar el resto mediante un procedimiento sencillo.

Buscar las soluciones enteras de $ax^2+by^2=cz^2$ es equivalente a buscar las soluciones racionales de $ax_1^2+by_1^2=c$, donde $x_1=\frac{x}{z},\ y_1=\frac{y}{z}$.

Es decir, se han de encontrar los puntos (x,y) de coordenadas racionales sobre la elipse $ax^2+by^2=c$. Supongase que mediante una inspección se ha encontrado un punto (x_0,y_0) de coordenadas racionales sobre la elipse. Ahora se traza una recta que pase por dicho punto y con pendiente $r\in\mathbb{Q}$. Esta recta

cortará la elipse en otro punto (x_0', y_0').

Si $y - y_0 = r(x - x_0)$ es la ecuación de la recta, se sustituye en la ecuación de la elipse, $ax^2 + b(y_0 + r(x - x_0))^2 = c$. Esta ecuación tiene como soluciones x_0 y x_0'.

Ahora bien, la suma de las soluciones de una ecuación de segundo grado con coeficientes racionales es racional. Por tanto, si x_0 es racional, x_0' debe ser racional y sustituyendo en la ecuación de la recta, y_0' también es racional.

Por otra parte, dos puntos de coordenadas racionales sobre la elipse determinan una recta de pendiente racional. Es decir, existe una biyección entre las soluciones enteras de la ecuación original y los puntos x_0', y_0' obtenidos según el método anterior.

Puesto que la ecuación $x^2 + y^2 - xy = 1$ describe una elipse centrada en el origen y rotada $45°$ en sentido contrario a las manecillas del reloj, el método anterior puede ser aplicado para encontrar las soluciones de la ecuación $.x^2 + y^2 - xy = z^2$.

Prueba del Lema 3.5. La ecuación $x^2 + y^2 - xy = z^2$ puede ser transformada en

$$x_1^2 + y_1^2 - x_1 y_1 = 1 \tag{3.4}$$

donde $x_1 = \frac{x}{z}$ y $y_1 = \frac{y}{z}$.

Como el punto $(1, 0)$ es solución de (3.4), y por ser de coordenadas racionales se puede encontrar otro punto (x_0', y_0') de coordenadas racionales. Se considera la recta que pasa por los puntos $(1, 0)$ y $\left(0, \frac{a}{b}\right)$. Dicha recta corta la elipse en otro punto de coordenadas racionales (x_0', y_0').

Ahora bien la ecuación de la recta viene dada por

$$y = \frac{a}{b}(x - 1). \tag{3.5}$$

Reemplazando esto en (3.4)

$$x^2 + \left(\frac{a}{b}(x-1)\right)^2 - x\frac{a}{b}(x-1) = 1,$$

luego

$$\begin{aligned} \frac{a^2}{b^2}(x-1)^2 &= 1 - x^2 + x\frac{a}{b}(x-1) \\ &= -(x-1)(1+x) + (x-1)x\frac{a}{b}, \end{aligned}$$

como el punto que se busca es diferente de $(1,0)$, se puede suponer que $x \neq 1$. Así:

$$\frac{a^2}{b^2}(x-1) = -1 - x + x\frac{a}{b}.$$

De donde

$$x = \frac{a^2 - b^2}{a^2 - ab + b^2},$$

reemplazando este valor en la ecuación (3.5)

$$y = \frac{a(a-2b)}{a^2 - ab + b^2}.$$

Finalmente reemplazando estos valores en la ecuación (3.4) se tiene que

$$\left(a^2 - b^2\right)^2 + \left(a(a-2b)\right)^2 - \left(a^2 - b^2\right)a(a-2b) = \left(a^2 - ab + b^2\right)^2,$$

y de ésto las soluciones de $x^2 + y^2 - xy = z^2$ son de la forma

$$x = \left(a^2 - b^2\right)t,$$

$$y = a(a-2b)t,$$

para $t \in \mathbb{Z}$. $\square$

3.4 Residuos cuadráticos en progresión aritmética

En la sección 3.2 se vió que hay como máximo 3 cuadrados en progresión aritmética. Siguiendo el objetivo del trabajo, se desea ahora investigar el comportamiento de los residuos cuadráticos con respecto a las progresiones aritméticas. Para ésto se plantean y responden las siguientes preguntas:

1. Dado un número natural n, ¿existe un primo p que tenga n residuos cuadráticos en progresión aritmética?

2. Dado un número natural n, ¿existe un primo p que tenga n residuos cuadráticos consecutivos?

3. ¿Cuántas parejas de residuos cuadráticos consecutivos tiene un primo p? ¿Cuántas ternas?

En primer lugar el problema fundamental a tratar será el siguiente:

Dado un conjunto de números primos $\{p_i\}_{i=1}^{k}$ garantizar la existencia de un primo P tal que todos los p_i sean residuos cuadráticos módulo P.

Para no dar una solución inmediata, en donde no se observe realmente las ideas que hay de fondo, se hará un proceso constructivo.

Sean $p_1, p_2, \ldots, p_k$ primos distintos. Para cualquier p_i del conjunto anterior se garantizará la existencia de un primo q_i tal que $p_i \in R_{q_i}$.

Como ya se sabe $-1 \in R_{q_i}$ cuando $q_i \equiv 1 \pmod 4$; si además $q_i \equiv 1 \pmod{p_i}$, por la ley de reciprocidad cuadrática

$$\left(\frac{p_i}{q_i}\right) = (-1)^{(p_i-1)(q_i-1)/4} \left(\frac{q_i}{p_i}\right) = \left(\frac{q_i}{p_i}\right) = 1$$

ya que $(p_i - 1)(q_i - 1)/4$ es par, resumiendo si:

$$q_i \equiv 1 \pmod 4,$$

$$q_i \equiv 1 \pmod{p_i},$$

se tendrá que $p_i \in R_{q_i}$. Estas identidades se satisfacen si

$$q_i \equiv 1 \pmod{4p_i},$$

con lo que finalmente hay que garantizar que existe un primo en la progresión

$$(4p_i)\, n + 1,$$

que se logra usando el siguiente resultado.

Teorema 3.3. (Teorema de Dirichlet)

Si $t > 0$ y $mcd(h, t) = 1$, existe una infinidad de primos de la forma $tn + h$.

La prueba de este resultado se sale de los objetivos del trabajo, pero puede ser encontrada en [1].

Ahora bien, si en el teorema anterior se toma $t = 4p_i$ y $h = 1$, claramente $mcd(h, t) = 1$ y se garantiza la existencia de un primo q_i tal que $p_i \in R_{q_i}$ con $q_i \equiv 1 \pmod{4p_i}$.

Luego, para que un primo q tenga la propiedad de que los primos $p_1, p_2, \ldots, p_k$ sean residuos cuadráticos módulo q, debe cumplirse que

$$q \equiv 1 \,(\mathrm{mod}\, 4p_1)\,,$$

$$q \equiv 1 \,(\mathrm{mod}\, 4p_2)\,,$$

$$\vdots$$

$$q \equiv 1 \,(\mathrm{mod}\, 4p_k)\,.$$

O en forma equivalente

$$q \equiv 1 \,(\mathrm{mod}\, 4p_1p_2 \ldots p_k)\,.$$

que nuevamente, por el teorema anterior, se garantiza su existencia. Así el problema queda resuelto y se enuncia y demuestra de la siguiente forma

Teorema 3.4.

Dado un conjunto de primos $p_1, p_2, \ldots, p_k$, existe un primo q tal que $p_i \in R_q$ para todo $i = 1, 2, \ldots, k$.

Prueba. Sea q un primo en la progresión

$$(4p_1p_2 \ldots p_k)\, n + 1,$$

ahora se demuestra que este q satisface los requisitos.

Sea p_i un primo del conjunto dado. Usando la ley de reciprocidad cuadrática

$$\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right),$$

ya que $q \equiv 1 \,(\mathrm{mod}\, 4)$, además como $q = tp_i + 1$ entonces

$$\left(\frac{q}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1,$$

luego

$$\left(\frac{p_i}{q}\right) = 1.$$

Esto prueba que $p_i \in R_q$ para todo $i = 1, 2, ..., k$. □

Corolario 3.1.

Dado cualquier conjunto de k enteros positivos, $A = \{a_1, a_2, \ldots, a_k\} \subset \mathbb{Z}^+$, existe un primo q ta que $A \subset R_q$.

Prueba. Sean $p_1, p_2, \ldots, p_m$ los primos necesarios para factorizar todos los elementos de A, por el teorema 3.4 existe un primo q tal que ellos son residuos cuadráticos módulo q, por tanto, todo entero que se pueda escribir como producto de ellos, tambien será un residuo cuadrático módulo q.□

Si en el colorario anterior tomamos los elementos del conjunto A como los términos de una progresión aritmética, o como el conjunto de n enteros seguidos, se han resuelto las preguntas, 1) y 2) respectivamente, planteadas al inicio de esta sección.

A continuación se hará un trabajo más preciso a cerca de las preguntas 2) y 3).

3.5 Residuos cuadráticos consecutivos

Al observar los residuos cuadráticos de 17

$$R_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\},$$

se ve que existen tres parejas de éstos que son consecutivos $(1, 2)$, $(8, 9)$, $(15, 16)$.

Pero cuando se ven los resíduos cuadráticos de 5

$$R_5 = \{1, 4\},$$

se observa que no hay ninguna pareja de residuos cuadráticos consecutivos.

Así que tiene sentido preguntarse

¿*Para qué primos existen residuos cuadráticos consecutivos?* y si hay residuos cuadráticos consecutivos,

¿*Cuántas parejas de ellos hay?*

Para resolver los anteriores interrogantes es necesario considerar los siguientes resultados.

Lema 3.6.

Sea $f(x)$ un polinomio que toma valores enteros cuando x es entero.

1). Si a y b son enteros entonces

$$\sum_{x \mod p} \left(\frac{f(ax+b)}{p}\right) = \sum_{x \mod p} \left(\frac{f(x)}{p}\right), \text{ si } mcd(a,p) = 1.$$

2). Para todo a

$$\sum_{x \mod p} \left(\frac{af(x)}{p}\right) = \left(\frac{a}{p}\right) \sum_{x \mod p} \left(\frac{f(x)}{p}\right).$$

3). Si $mcd(a,p) = 1$ entonces

$$\sum_{x \mod p} \left(\frac{ax+b}{p}\right) = 0.$$

4). Sea $f(x) = x(ax+b)$, en donde $mcd(a,p) = mcd(b,p) = 1$. Entonces

$$\sum_{x=1}^{p-1} \left(\frac{f(x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{a+bx}{p}\right) = -\left(\frac{a}{p}\right).$$

Prueba.

1). Sean $x, x_1 \in \mathbb{Z}_p$ tal que $x \not\equiv x_1 (\mathrm{mod}\, p)$. Puesto que $mcd(a,p) = 1$ entonces $ax+b \not\equiv ax_1+b (\mathrm{mod}\, p)$.

Esto es cuando x recorre $\mathbb{Z}_p$ se tiene que $ax+b$ también lo hace.

2). Se sigue de:

$$\left(\frac{af(x)}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{f(x)}{p}\right).$$

3). Sea $f(x) = x$ entonces de la parte 1)

$$\sum_{x \mod p} \left(\frac{ax+b}{p}\right) = \sum_{x \mod p} \left(\frac{x}{p}\right) = 0.$$

4). Considerese el siguiente polinomio

$$g(x) = \frac{f(x)}{x^2} = a + bx^{-1}.$$

Cuando x recorre $\mathbb{Z}_p^*$ se tiene que x^{-1} también lo hace. Así

$$\sum_{x=1}^{p-1} \left(\frac{x(ax+b)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x^2 g(x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{a+bx}{p}\right).$$

Ahora como $mcd(b,p)=1$ entonces por la parte 3) se tiene que

$$\sum_{x \bmod p} \left(\frac{a+bx}{p}\right) = 0,$$

luego

$$\sum_{x=1}^{p-1} \left(\frac{a+bx}{p}\right) = -\left(\frac{a}{p}\right). \square$$

Definición 3.2

Sean $\alpha, \beta \in \{1,-1\}$ y p un primo impar, mediante $N(\alpha,\beta)$ se representa el número de enteros x de $\{1,2,...,p-2\}$ tales que

$$\left(\frac{x}{p}\right) = \alpha \quad \text{y} \quad \left(\frac{x+1}{p}\right) = \beta.$$

Lema 3.7

Sea p un número primo. Entonces

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2} \left\{1+\alpha\left(\frac{x}{p}\right)\right\}\left\{1+\beta\left(\frac{x+1}{p}\right)\right\}.$$

Prueba. Si existe $x \in \{1,2,...,p-2\}$ tal que

$$\left(\frac{x}{p}\right) = \alpha \quad \text{y} \quad \left(\frac{x+1}{p}\right) = \beta, \tag{3.6}$$

entonces para dicho x se tiene que

$$1+\alpha\left(\frac{x}{p}\right) = 1+\beta\left(\frac{x+1}{p}\right) = 2.$$

Luego $\left\{1+\alpha\left(\frac{x}{p}\right)\right\}\left\{1+\beta\left(\frac{x+1}{p}\right)\right\} = 4$, para todo $x \in \{1,2,...,p-2\}$ que satisface (3.6).

Es fácil ver que si

$$\left(\frac{x}{p}\right) \neq \alpha \quad \text{o} \quad \left(\frac{x+1}{p}\right) \neq \beta,$$

entonces $\left\{1+\alpha\left(\frac{x}{p}\right)\right\}\left\{1+\beta\left(\frac{x+1}{p}\right)\right\} = 0$.

Puesto que $N(\alpha,\beta)$ cuenta el número de los x en $\{1,2,...,p-2\}$ que satisfacen (3.6), se puede afirmar que

$$N(\alpha,\beta) = \frac{1}{4}\sum_{x=1}^{p-2} \left\{1+\alpha\left(\frac{x}{p}\right)\right\}\left\{1+\beta\left(\frac{x+1}{p}\right)\right\},$$

de donde se obtiene el resultado. $\square$

Teorema 3.5

Sea p un primo. Entonces

$$4N(\alpha,\beta) = p - 2 - \beta - \alpha\beta - \alpha\left(\frac{-1}{p}\right).$$

En particular

$$N(1,1) = \frac{p - 4 - \left(\frac{-1}{p}\right)}{4}.$$

Prueba. Del lema 3.7

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2}\left\{1 + \alpha\left(\frac{x}{p}\right)\right\}\left\{1 + \beta\left(\frac{x+1}{p}\right)\right\}.$$

Expandiendo esta sumatoria

$$4N(\alpha,\beta) = \sum_{x=1}^{p-2} 1 + \sum_{x=1}^{p-2}\alpha\left(\frac{x}{p}\right) + \sum_{x=1}^{p-2}\beta\left(\frac{x+1}{p}\right) + \sum_{x=1}^{p-2}\alpha\beta\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) \tag{3.7}$$

A partir del lema 3.6, se puede obtener el valor de cada una de las suma anteriores:

$$\sum_{x=1}^{p-2}\alpha\left(\frac{x}{p}\right) = \alpha\sum_{x=1}^{p-2}\left(\frac{x}{p}\right) = -\alpha\left(\frac{-1}{p}\right), \text{ por el corolario 1.3}$$

$$\sum_{x=1}^{p-2}\beta\left(\frac{x+1}{p}\right) = -\beta(\frac{1}{p}) = -\beta,$$

$$\sum_{x=1}^{p-2}\alpha\beta\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \alpha\beta\sum_{x=1}^{p-2}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right).$$

Ahora por la parte 3).del lema 3.3

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x\,(x+1)}{p}\right) = -\left(\frac{1}{p}\right) = -1.$$

Como

$$\sum_{x=1}^{p-2}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right),$$

y debido a que $x = p-1$ implica $x+1 \equiv 0(\mathrm{mod}\, p)$, entonces

$$\sum_{x=1}^{p-2}\alpha\beta\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -\alpha\beta.$$

Reemplazando los resultados de las anteriores sumas en la ecuación (3.7) se obtiene la primera parte del teorema.

La segunda parte se obtiene haciendo $\alpha = \beta = 1$ en el primer resultado. $\square$

El anterior teorema ofrece una forma sencilla de saber cuantos residuos cuadráticos consecutivos tiene un primo dado. Pero surge la siguiente pregunta ¿Cuáles primos tienen esta característica ?. Es decir, ¿para cuáles primos p existe al menos una pareja de elementos consecutivos en R_p?. Todo lo anterior es equivalente a preguntarse para qué primos se tiene que $N(1,1) \geq 1$. Esto se resuelve en el siguiente teorema.

Teorema 3.6

Para todo primo $p \geq 7$ existe al menos una pareja de residuos cuadráticos consecutivos.

Prueba. Como

$$N(1,1) = \frac{p - 4 - \left(\frac{-1}{p}\right)}{4},$$

entonces, claramente $N(1,1) \geq 1$ para todo primo $p \geq 7$. $\square$

Con los dos resultados precedentes se resuelve el problema sobre el número de parejas de dos residuos cuadráticos consecutivos.

¿Es posible obtener un resultado similar para tres residuos cuadráticos consecutivos, y en general, para n residuos cuadráticos consecutivos?

Ahora se realiza una exposición similar a la anterior para tres residuos cuadráticos consecutivos. Como es de esperarse para este caso se necesita una extensión de la definición del número $N(1,1)$.

Definición 3.3

Mediante $N(1,1,1)$ se representa el número de ternas de resíduos cuadráticos consecutivos,

es decir

$$N(1,1,1) = \#\left\{x \in R_p : \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = \left(\frac{x+2}{p}\right) = 1\right\},$$

ó equivalentemente

$$N(1,1,1) = \#\left\{x \in R_p : x, x+1, x+2 \in R_p\right\}.$$

Lema 3.8.

Sea p un primo. Entonces

$$8N(1,1,1) = \sum_{x=1}^{p-2} \left\{1 + \left(\frac{x}{p}\right)\right\} \left\{1 + \left(\frac{x+1}{p}\right)\right\} \left\{1 + \left(\frac{x+2}{p}\right)\right\}.$$

Prueba. Análoga a la demostración del lema 3.7. □

Lema 3.9

Si $p \equiv 3 \pmod 4$ entonces

$$\sum_{x=1}^{p-2} \left(\frac{x}{p}\right) \left(\frac{x+1}{p}\right) \left(\frac{x+2}{p}\right) = 0.$$

Prueba. Sea $y = x + 1$ entonces $x = y - 1, x + 2 = y + 1$. Así

$$\sum_{x=1}^{p-2} \left(\frac{x}{p}\right) \left(\frac{x+1}{p}\right) \left(\frac{x+2}{p}\right) = \sum_{y=2}^{p-1} \left(\frac{y}{p}\right) \left(\frac{y^2-1}{p}\right).$$

Ahora tomando la sumatoria anterior desde 1 se tiene que

$$\sum_{y=2}^{p-1} \left(\frac{y}{p}\right) \left(\frac{y^2-1}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \left(\frac{y^2-1}{p}\right) = \sum_{y=1}^{(p-1)/2} \left(\frac{y^2-1}{p}\right) \left[\left(\frac{y}{p}\right) + \left(\frac{-y}{p}\right)\right]$$

Puesto que cuando y recorre desde 1 hasta $(p-1)/2$, $p - y \equiv -y (\mathrm{mod}\, p)$ recorre desde $p - 1$ hasta $(p+1)/2$.

Como $p \equiv 3 \pmod 4$ entonces $\left(\frac{-1}{p}\right) = -1$, luego $\left(\frac{-y}{p}\right) = -\left(\frac{y}{p}\right)$. Por tanto $\left(\frac{y}{p}\right) + \left(\frac{-y}{p}\right) = 0$, para todo $y \not\equiv 0 (\mathrm{mod}\, p)$. □

Teorema 3.7

Si $p \equiv 3 \pmod 4$ entonces

$$N(1,1,1) = \frac{p - 8 - 3\left(\frac{-1}{p}\right) - 1\left(\frac{-2}{p}\right) - 3\left(\frac{2}{p}\right)}{8}.$$

Prueba. Expandiendo el resultado del lema 3.8

$$\begin{aligned} 8N(1,1,1) = &\sum_{x=1}^{p-3} 1 + \sum_{x=1}^{p-3} \left(\frac{x}{p}\right) + \sum_{x=1}^{p-3} \left(\frac{x+1}{p}\right) + \sum_{x=1}^{p-3} \left(\frac{x+2}{p}\right) \\ &+ \sum_{x=1}^{p-3} \left(\frac{x}{p}\right) \left(\frac{x+1}{p}\right) + \sum_{x=1}^{p-3} \left(\frac{x}{p}\right) \left(\frac{x+2}{p}\right) \\ &+ \sum_{x=1}^{p-3} \left(\frac{x+1}{p}\right) \left(\frac{x+2}{p}\right) + \sum_{x=1}^{p-3} \left(\frac{x}{p}\right) \left(\frac{x+1}{p}\right) \left(\frac{x+2}{p}\right) \end{aligned} \tag{3.8}$$

Ahora se calculan las sumas que aparecen en la expresión anterior. Como $\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$ entonces

$$\sum_{x=1}^{p-3}\left(\frac{x}{p}\right)=-\left(\frac{-2}{p}\right)-\left(\frac{-1}{p}\right), \tag{3.9}$$

$$\sum_{x=1}^{p-3}\left(\frac{x+1}{p}\right)=-\left(\frac{-1}{p}\right)-1, \tag{3.10}$$

$$\sum_{x=1}^{p-3}\left(\frac{x+2}{p}\right)=-1-\left(\frac{2}{p}\right). \tag{3.11}$$

Por la parte 4) del lema 3.6

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+2}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{2x+1}{p}\right)=-1,$$

y ésto implica

$$\sum_{x=1}^{p-3}\left(\frac{x}{p}\right)\left(\frac{x+2}{p}\right)=-1-\left(\frac{-1}{p}\right). \tag{3.12}$$

En la demostración del teorema 3.5 se encontró que

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)=-1,$$

esto implica

$$\sum_{x=1}^{p-3}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)=-1-\left(\frac{2}{p}\right). \tag{3.13}$$

Como

$$\sum_{x=1}^{p-3}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right)=0, \tag{3.14}$$

hace falta calcular

$$\sum_{x=1}^{p-3}\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right),$$

que puede verse como

$$\sum_{x=1}^{p-1}\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right)=\sum_{x=1}^{p-3}\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right).$$

Ahora sea $y=x+1$,

$$\sum_{x=1}^{p-1}\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right)=\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)\left(\frac{y+1}{p}\right)=-\left(\frac{2}{p}\right)-1. \tag{3.15}$$

Reemplazando (3.9)-(3.15) en (3.8), se obtiene el resultado deseado. □

Corolario 3.2.

Sea p un primo congruente con 3 módulo 4, entonces

$$N(1,1,1) = \begin{cases} \frac{p-7}{8}, & \text{si } p \equiv 7 (\text{mod}\, 8) \\ \frac{p-3}{8}, & \text{si } p \equiv 3 (\text{mod}\, 8) \end{cases}$$

Prueba. Reemplazando los Símbolos de Legendre por sus valores en el teorema anterior se obtiene el resultado. □

Lema 3.10.

Si $p \equiv 1 \,(\text{mod}\, 4)$ entonces

$$-\left(\frac{p-3}{2}\right) \leq \sum_{x=1}^{p-2} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right) \leq \left(\frac{p-3}{2}\right).$$

Prueba. Por el lema 3.8

$$\sum_{x=1}^{p-2} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y^2-1}{p}\right).$$

En el capitulo 2 se demostró que

$$\sum_{y=0}^{p-1} \left(\frac{y^2-1}{p}\right) = -1,$$

y como $\left(\frac{-1}{p}\right) = 1$, entonces

$$\begin{aligned} 1 + \sum_{y=1}^{p-1} \left(\frac{y^2-1}{p}\right) - \sum_{y=1}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y^2-1}{p}\right) &= 1 + \sum_{y=1}^{p-1} \left(1 - \left(\frac{y}{p}\right)\right)\left(\frac{y^2-1}{p}\right) \\ &= 1 + 2 \sum_{y \in N_p} \left(\frac{y^2-1}{p}\right) \\ &\leq 1 + 2\delta_p(1) = \frac{p+1}{2} \end{aligned}$$

luego

$$\sum_{y=1}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y^2-1}{p}\right) \geq -\frac{p+3}{2}$$

Con una prueba análoga a la anterior, se llega a que

$$\sum_{y=1}^{p-1} \left(\frac{y}{p}\right)\left(\frac{y^2-1}{p}\right) \leq \frac{p+3}{2}. \; \square$$

Teorema 3.8

Si $p \equiv 1 \pmod 4$ entonces

$$\frac{p-19-6\left(\frac{-1}{p}\right)-2\left(\frac{-2}{p}\right)-6\left(\frac{2}{p}\right)}{16} \leq N(1,1,1) \leq \frac{3p-13-6\left(\frac{-1}{p}\right)-2\left(\frac{-2}{p}\right)-6\left(\frac{2}{p}\right)}{16}$$

Prueba. Se tiene que

$$8N(1,1,1) = p - 8 - 3\left(\frac{-1}{p}\right) - 1\left(\frac{-2}{p}\right) - 3\left(\frac{2}{p}\right) + \sum_{x=1}^{p-2}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right).$$

Ahora utilizando el lema precedente se obtiene el resultado. □

Corolario 3.3.

Sea p un primo. Entonces:

1). Si $p \equiv 1 \pmod 8$ entonces

$$\frac{p-33}{16} \leq N(1,1,1) \leq \frac{3p-27}{16}.$$

2). Si $p \equiv 5 \pmod 8$ entonces

$$\frac{p-17}{16} \leq N(1,1,1) \leq \frac{3p-11}{16}.$$

Prueba. Reemplazar los valores de los símbolos de Legendre para $-1, -2, 2$ en el teorema 3.7. □

Corolario 3.4.

Para todo primo $p \geq 37$ existen tres residuos cuadráticos consecutivos.

Prueba. Usando los resultados de los corolarios 3.2 y 3.3, claramente cuando $p \geq 37$, se tiene $N(1,1,1) \geq 1$. □

4 Algunos problemas relacionados

En este capítulo se destacan los principales resultados obtenidos en la monografía y se establecen algunos problemas relacionados con ellos.

4.1 Residuos cuadráticos y progresiones aritméticas

En el capítulo 3 se resolvieron preguntas tales como:

1. Dado un número natural n, ¿existe un primo p que tenga n residuos cuadráticos en progresión aritmética?

2. Dado un número natural n, ¿existe un primo p que tenga n residuos cuadráticos consecutivos?

Con ésto se logró mostrar varias de las propiedades de los residuos cuadraticos de especial interes para este trabajo.

Algunos problemas que hacen falta para complementar estos resultados sobre residuos cuadráticos en progresiones aritméticas son los siguientes:

Problema 4.1.

Dado un primo p, ¿qué tipo de progresiones aritméticas están contenidas en R_p?

Problema 4.2.

Dado un primo p, ¿cual es la progresión aritmética más larga contenida en R_p?

En la sección 3.4 se encontró la forma de saber cuantas parejas de residuos cuadráticos consecutivos tiene un primo dado; pero cuando se quiso calcular el número de ternas de este tipo, sólo se logró para los primos congruentes con 3 módulo 4. La dificultad encontrada para el caso en que el primo es

congruente con 1 módulo 4 fue determinar el valor exacto para

$$\sum_{x=1}^{p-3}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\left(\frac{x+2}{p}\right).$$

Sin embargo acotando esta suma se logró encontrar un primo a partir del cual siempre existen tres residuos cuadráticos consecutivos.

Aunque con ésto se resuelve parte del problema aún queda la siguiente duda

Problema 4.3.

¿Cuál es el valor exacto de $N(1,1,1)$ para todos los primos?

Aún más, si se desea ir mas lejos, se plantean las siguientes preguntas:

Dado el entero positivo n:

¿A partir de qué primo, siempre existen n residuos cuadráticos consecutivos?

¿Se puede calcular en forma exacta el valor de $N(\underbrace{1,1,\cdots,1}_{n\text{-veces}})$?

Problema 4.4.

Estudiar parejas (ternas, etc) de residuos cuadráticos consecutivos pero con diferencia d, en el lugar de 1. ¿Es posible obtener fórmulas similares a las obtenidas para residuos cuadráticos consecutivos?

En el texto [5], Problema F5, se propone el siguiente problema.

Problema 4.5. (Conjetura de Schur)

Si R (respectivamente N) es el máximo número de residuos cuadráticos consecutivos (no residuos) módulo un primo impar p, entonces A. Brauer demostró que para $p \equiv 3(\mathrm{mod}\,4)$, $R = N < \sqrt{p}$. Por otro lado, si $p = 13$, entonces $N = 4 > \sqrt{13}$, ya que $5, 6, 7, 8$ son todos no residuos de 13. Schur conjeturó que $N < \sqrt{p}$ si p es suficientemente grande. Hudson probó la conjetura de Schur; además él cree que $p = 13$ es la única excepción.

4.2 Base minimal de residuos cuadráticos

Si $p \equiv 1(\mathrm{mod}\, 4)$, sea $A \subseteq \mathbb{Z}_p$, si $A + A = \mathbb{Z}_p$ entonces A se llama una base aditiva de orden dos para $\mathbb{Z}_p$. Cuando $p \equiv 3(\mathrm{mod}\, 4)$, se cambia $\mathbb{Z}_p$ por $\mathbb{Z}_p^*$. Un problema de gran interés consiste en obtener una fórmula para el mínimo número de elementos en una base aditiva de orden dos, es decir se trata de estudiar la función

$$G(p) := Mín\left\{|A| : A \subset \mathbb{Z}_p, \quad A + A = \mathbb{Z}_p\right\}.$$

En el capítulo 2 se demostró que los resíduos cuadráticos forman una base aditiva de orden dos para $\mathbb{Z}_p$ o $\mathbb{Z}_p^*$, según que $p \equiv 1$ o $3(\mathrm{mod}\, 4)$. Esto sugiere estudiar el número mínimo de residuos cuadráticos que forman una base aditiva. Es decir, proponemos estudiar el comportamiento asintótico de la función

$$\rho(p) = Mín\left\{|A| : A \subset R_p, \quad A + A = \mathbb{Z}_p\right\}.$$

Por ejemplo, analizando R_{17} se ve que los conjuntos de la forma $R_{17} - \{r\}$ para cualquier resíduo cuadrático son los únicos subconjuntos propios de R_{17} que siguen siendo base aditiva para $\mathbb{Z}_{17}$, así $\rho(17) = |R_{17}| - 1 = 7$.

Ejemplo 4.1. En la siguiente tabla se da una lista de primos con una cota inferior y superior para $\rho(p)$.

p	$\rho(p)$
17	7
19	entre 6 y 7
23	entre 7 y 8
29	entre 8 y 10
31	entre 8 y 9
37	entre 9 y 12
41	entre 9 y 11
43	entre 9 y 13
47	entre 10 y 15

Como se desea representar todos los elementos de $\mathbb{Z}_p$, si $A \subseteq R_p$ es una base con k elementos entonces el número de sumas de dos elementos (incluyendo repeticiones) de A debe ser mayor que p; ésto es

$$\binom{k+1}{2} \geq p$$

Y de aquí

$$k\,(k+1) \geq 2p.$$

La última desigualdad afirma que para que un conjunto A sea una base para $\mathbb{Z}_p$ su cardinal $|A|$ debe ser mayor o igual que $\sqrt{2p}$. Pero como A es subconjunto de R_p entonces $|A|$ debe ser menor o igual que $\frac{p-1}{2}$. Lo anterior prueba el siguiente resultado.

Lema 4.1.

Para todo primo $p > 7$

$$\sqrt{2p} \leq \rho(p) \leq \frac{p-1}{2}.$$

¿Es posible encontrar una cota superior más pequeña para $\rho(p)$? La cota superior dada en el lema 4.1 es la cota superior trivial para $\rho(p)$.

En la tabla del ejemplo 4.1 se evidencia que posiblemente existe una cota superior para $\rho(p)$ mucho menor que la dada en el lema 4.1. Para valores grandes de p se empieza a ver que parecen existir bases de residuos cuadráticos de tamaño aproximadamente igual a $c\sqrt{p}$, para alguna constante c.

Pregunta abierta 4.1.

¿Existe alguna constante $c > 0$ tal que para p suficientemente grande, $\rho(p)$ y $c\sqrt{p}$ son asintóticamente iguales?. Es decir

$$¿\lim_{p\to\infty} \frac{\rho(p)}{\sqrt{p}} = c?$$

Más aún, quizás sea posible tomar $c = 2$.

Se conocen muy pocas construcciones de bases aditivas para $\mathbb{Z}_p$ cuyo orden asintótico sea de la forma $c\sqrt{p}$.

Una respuesta afirmativa a la pregunta anterior sería un considerable avance en esta teoría, pues además de obtener un nuevo tipo de base asintóticamente pequeña, al conocer la estructura de sus elementos (residuos cuadráticos), su construcción sería más fácil.

4.3 Residuos cuadráticos y conjuntos de Sidon

Un conjunto $A \subseteq \mathbb{Z}_p$ se llama un conjunto de Sidon módulo p, si todas las sumas de dos elementos (incluyendo repetición) son incongruentes módulo p, es decir si

$$x + y \equiv u + v (\mathrm{mod}\, p) \Longrightarrow \{x, y\} = \{u, v\}\,.$$

Es importante estudiar el máximo número de elementos de $\mathbb{Z}_p$ que pueden seleccionarse de tal forma que constituyan un conjunto de Sidon módulo p, es decir se trata de estudiar la función

$$f_2\,(p) = M\acute{a}x\,\{|A| : A \in B_2(\mathrm{mod}\, p)\}\,,$$

donde $B_2\,(\mathrm{mod}\, p)$ representa la clase de todos los conjuntos de Sidon módulo p. Proponemos el problema consistente en estudiar el máximo cardinal de un conjunto de Sidon módulo p consistente de residuos cuadráticos.

Pregunta Abierta 4.2.

Investigar el comportamiento asintótico de la función

$$r_2(p) = M\acute{a}x\,\{|A| : A \subseteq R_p, \quad A \in B_2(\mathrm{mod}\, p)\}\,.$$

Quizás sea posible demostrar que

$$\lim_{N\to\infty} \frac{r_2(p)}{\sqrt{p}} = c,$$

donde $c > 0$ es una constante. ¿Es $c = 1$?.

Un problema relacionado consiste en estudiar conjuntos de residuos cuadráticos cuyas diferencias (sumas) son residuos cuadráticos.

En el texto [5], Problema F8 se menciona lo siguiente:

Gary Ebert solicita encontrar la máxima colección de residuos cuadráticos $r_i (\mathrm{mod}\, p^n)$, $p^n \equiv 1 (\mathrm{mod}\, 4)$, de tal forma que $r_i - r_j$ es un residuo cuadrático para todos los pares (i, j). Es conveniente considerar el problema para $n = 1$, y el problema análogo para sumas.

Problema 4.6.

Estimar las siguientes funciones

$$D(p) = Máx \{|A| : A \subseteq R_p, A - A \subseteq R_p\},$$

$$S(p) = Máx \{|A| : A \subseteq R_p, A + A \subseteq R_p\}.$$

4.4 Otros problemas

Sobre el valor de la suma de todos los residuos cuadráticos, se propone el siguiente problema.

Problema 4.7.

No es difícil demostrar que si $p \equiv 1 (\mathrm{mod}\, 4)$ entonces

$$\sum_{r \in R_p} r = \frac{p(p-1)}{4}.$$

¿Existe una fórmula similar si $p \equiv 3 (\mathrm{mod}\, 4)$? (Ver [1]).

Un problema natural consiste en considerar lo que ocurre con los no residuos cuadráticos.

En el capítulo 2 se demostró que para todo primo $p \geq 7$, todo entero no divisible por p puede expresarse como suma (y como diferencia) de dos residuos cuadráticos, ver teoremas 2.1 y 2.3. Más específicamente:

$$p \equiv 3 (\mathrm{mod}\, 4) \Longrightarrow \mathbb{Z}_p^* = R_p + R_p,$$

$$p \equiv 1 (\mathrm{mod}\, 4) \Longrightarrow \mathbb{Z}_p = R_p + R_p,$$

donde, como es usual $R_p + R_p = \{r + r' : r, r' \in R_p\}$. Además se establecieron resultados sobre el número de representaciones de un entero como suma (y como diferencia) de dos residuos cuadráticos, ver teoremas 2.2 y 2.4.

Problema 4.8.

¿Es posible obtener resultados similares si R_p se reemplaza por N_p?

En el capítulo 3 se obtuvieron algunos resultados sobre residuos cuadráticos en progresión aritmética, por ejemplo se establecieron fórmulas para el número de parejas (y ternas) de residuos cuadráticos consecutivos, ver teoremas 3.5 y 3.6, y se probó que para todo entero k existe un primo p tal que todos los enteros $1, 2, 3, ..., k$ son residuos cuadráticos módulo p, ver teorema 3.4 .

Problema 4.9.

¿Es posible obtener resultados similares cuando se consideran los no residuos cuadráticos?

En general, se trata de identificar hasta qué punto es posible obtener resultados sobre no residuos cuadráticos análogos a los que se obtuvieron en esta monografía.
Finalmente, es importante considerar posibles generalizaciones para módulos no primos.

Problema 4.10.

Intentar generalizar algunos de los resultados y preguntas planteadas en la monografía a módulos no necesariamente primos. Quizás sea conveniente comenzar considerando módulos que son potencias primas.

BIBLIOGRAFÍA

[1] Apostol T.M. *Introducción a la teoría analítica de números.* Editorial Reverté, S.A., Barcelona, 1980.

[2] Cilleruelo J., Córdoba A. *La teoría de los números.* Biblioteca Mondadori, Madrid, 1992.

[3] Erdélyi T. *On the equation* $a\,(a+d)\,(a+2d)\,(a+3d) = x^2$. American Mathematical Monthly, Vol. 107, No. 2 (2000), 166-169.

[4] Gauss C. F. *Disquisitiones Arithmeticae.* Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, 1995.

[5] Guy R. *Unsolved problems in number theory.* Volume I, second edition. Springer Verlag, New York, 1994.

[6] Hardy G. H., Wright E. M. *An introduction to the theory of numbers.* Fifth edition, Oxford Science Publication, London, 1998.

[7] Ireland K. , Rosen M. *A classical introduction to modern number theory.* Springer Verlag.New York. 1982.

[8] Rosen K. H. *Elementary number theory and its applications.* Addison Wesley publishing company.New York.1987.

[9] Trujillo C. A. *Sumas de Gauss y sumas de Jacobi con algunas aplicaciones.* Tesis de maestría.Universidad del Valle.1987.