LEY DE RECIPROCIDAD CUADRÁTICA Y CUESTIONES RELACIONADAS CON CUADRADOS

Mary Alejandra Cuadrado Chica

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
MONTERÍA
2021

LEY DE RECIPROCIDAD CUADRÁTICA Y CUESTIONES RELACIONADAS CON CUADRADOS

Mary Alejandra Cuadrado Chica

Trabajo presentado como requisito parcial para optar al título de
Matemático

Asesor:
Ph. D. Jerson Manuel Borja Soto

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
MONTERÍA
2021

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA

Los jurados abajo firmantes certifican que han leído y que aprueban el trabajo de grado titulado: **LEY DE RECIPROCIDAD CUADRÁTICA Y CUESTIONES RELACIONADAS CON CUADRADOS**, el cual es presentado por la estudiante **Mary Alejandra Cuadrado Chica**.

Fecha: Septiembre 2021

Asesor: _____

Ph. D. Jerson Manuel Borja Soto

Jurado: _____

M.Sc. Sergio Miguel Avilez Ortiz

Jurado: _____

Ph. D. Luis Enrique Benítez Babilonia

Yolima Chica
Y Angie Cuadrado

Resumen

En el presente trabajo tratamos acerca de residuos cuadráticos y la ley de reciprocidad cuadrática. Se muestra la caracterización de los enteros que se pueden representar como suma de dos cuadrados, y hacemos un estudio del respectivo problema modular, que plantea caracterizar y contar la cantidad de enteros módulo n que pueden ser representados como suma de dos cuadrados módulo n.

Palabras claves: Símbolo de Legendre, Reciprocidad Cuadrática, Suma de Dos Cuadrados, Suma de Dos Cuadrados Módulo n.

Abstract

In this work we deal with quadratic residues and the law of quadratic reciprocity. We show the characterization of integers that can be represented as the sum of two squares, and we also study the corresponding modular problem, which states the study of the characterization and counting of the integers modulo n that can be represented as a sum of two squares modulo n.

Keywords: Legendre Symbol, Quadratic reciprocity, Sum of Two Squares, Sum of Two Squares Modulo n.

Agradecimientos

Inicialmente le agradezco a Dios por guiarme, ser mi apoyo espiritual; por llenarme de fuerza en los momentos más difíciles y no permitirme desfallecer. Le agradezco a mi padre, Juan, por enseñarme a tener fortaleza y a mi madre Yolima, por su apoyo y amor incondicional, sus palabras de aliento y porque es mi excelente ejemplo a seguir. Le agradezco a mi hermana, Angie por levantarme para estudiar cuando ya me había quedado dormida muchas veces y por pasar conmigo cada momento, a mi novio, Jesús, por ser una motivación más a lo largo de esta carrera y en mi vida, por apoyarme moralmente y ayudarme a levantarme cada vez que caigo. Le agradezco a la Universidad de Córdoba por brindarme una educación de calidad y en particular al Departamento de Matemáticas y Estadística, y sus profesores, en especial, al los profesores Dairo Díaz, Ricardo Gúzman, Jimmy Lloreda, Carlos Banquet, Carlos Reales, Abraham Arenas, Jorge Reyes, Sergio Avilez y Luis Benítez, porque me ayudaron a descubrir que las matemáticas son un mundo del cuál cuando entras ya no quieres salir, además sus enseñanzas me ayudaron a crecer como estudiante y como persona, me enseñaron a valorar el tiempo y a tener mucha disciplina. Finalmente quiero agradecer a mi asesor Jerson Borja, pues me ha enseñado a querer aprender más, a no conformarme con lo que se me diga, además de compartir conmigo algunos de sus conocimientos y a ser un ejemplo a seguir como matemático y a todas esas personas que no mencioné con ánimo de no extenderme, pero que aportaron mucho para que yo pudiera estar aquí; a mis amigas Pao, Lina, Luisa, Camila, Herlys y Maryliana, quienes han significado mucho para mí y a mis demás compañeros.

Montería, Colombia — Mary Alejandra Cuadrado Chica

Junio de 2021

Índice general

Introducción

En el presente trabajo se muestran algunos resultados relacionados con congruencias cuadráticas y el problema diofántico de representar enteros como suma de dos cuadrados. Específicamente, tratamos sobre residuos cuadráticos y la ley de reciprocidad cuadrática; el teorema de Euler sobre representación de enteros como suma de dos cuadrados, y la representación modular de enteros como suma de dos cuadrados.

Si hablamos de jerarquía, para Gauss, la matemática es la reina de las ciencias, la teoría de números es la reina de las matemáticas, y la ley de reciprocidad cuadrática, una *joya de su corona*. Gauss la llamaba *Teorema Aureum*, y es uno de los resultados más útiles en teoría de números. Más aún, sería acertado decir que la teoría de números moderna, empezó precisamente, con el descubrimiento de la ley de reciprocidad cuadrática.

Esta joya fue enunciada por Euler en 1754 y probada por Gauss por primera vez en 1796; y, de hecho, a lo largo de su vida, Gauss publicó seis demostraciones de esta, e incluso después de su muerte, fueron halladas dos demostraciones más entre sus documentos. Este problema ha sido de gran interés para muchos matemáticos y, actualmente, posee más de cien demostraciones, muchas de las cuáles difieren de otras por pequeños detalles. Ferdinand Eisenstein fue uno de los discípulos más destacados de Gauss, quien realizó cinco demostraciones de la ley de reciprocidad cuadrática. En este trabajo, conoceremos una de las demostraciones de Eisenstein.

La ley de reciprocidad cuadrática se aplica naturalmente en el cálculo de símbolos de Legendre; ella facilita dichos cálculos, y esto es debido a que aunque tengamos que calcular el símbolo de Legendre entre dos números lo suficientemente grandes, al usar

este teorema se reducen a pequeñas cifras.

Otro de los problemas que históricamente ha recibido gran interés es el de representación de enteros como suma de cuadrados. Cuando decimos que un entero n es el resultado de la suma de dos cuadrados, nos referimos a que n se puede expresar como la suma $a^2 + b^2$, donde a y b son enteros; por ejemplo, $8 = 2^2 + (-2)^2$. En la *Aritmética* de Diofanto aparece el siguiente problema: "ningún primo de la forma $4n+3$ puede escribirse como suma de dos cuadrados", y este es uno de los resultados que estudiaremos en el presente trabajo.

Seguramente todos recordamos a Pitágoras por el famoso teorema que recibe su nombre, que establece que en un triángulo rectángulo, la suma de los cuadrados de los catetos es igual al cuadrado de la hipotenusa. Así, si z es la longitud de la hipotenusa, x e y las longitudes de los catetos, entonces $x^2 + y^2 = z^2$. Observe que la longitud de la hipotenusa al cuadrado z^2 es, en particular, un número que se puede escribir como suma de dos cuadrados. Una terna de enteros (x, y, z) que satisface la ecuación $x^2 + y^2 = z^2$ es llamada una *terna pitagórica*.

Otro teorema que estudiaremos en este trabajo, es el Teorema de Fermat para suma de dos cuadrados, que afirma que cualquier primo que sea de la forma $4k + 1$ se puede representar como suma de dos cuadrados. Este teorema fue enviado por Fermat en una carta el 25 de diciembre de 1640 para Mersenne. Sin embargo, Fermat no proporcionó una demostración del teorema en ese momento. Años después se volvió a conocer el resultado cuando Euler dio la primera prueba basada en el método del descenso infinito; Euler resolvió el problema de determinar cuáles son los enteros que se pueden representar como suma de dos cuadrados de enteros.

Finalmente, también estudiaremos el problema de determinar los enteros que se pueden representar como suma de dos cuadrados módulo n, donde n es un entero positivo. Si definimos A_n como el conjunto que contiene a todos los enteros módulo n que pueden representarse como suma de dos cuadrados módulo n, el interrogante que guía nuestro estudio en este contexto es, ¿cuántos elementos tiene A_n?

En el 2014, Joshua Harrington, Lenny Jones y Alicia Lamarche [8], lograron dar

una respuesta al siguiente interrogante: ¿cuáles son los enteros positivos n tales que todo entero módulo n puede expresarse como suma de dos cuadrados módulo n?, en su demostración se utiliza reciprocidad cuadrática y ternas pitagóricas. Tiempo después, en el 2017, Rob Burns [3] dio una descripción del conjunto de los enteros módulo n que se pueden representar como suma de dos cuadrados y estudió su tamaño $|A_n|$, y el comportamiento del cociente $\frac{|A_n|}{n}$ cuando n tiende a infinito. Poco después, los matemáticos Fabián Arias, Jerson Borja y Luis Rubio generalizaron este concepto a cualquier polinomio de grado k, y en particular dieron respuesta al interrogante planteado para algunos polinomios de la forma $c_1x^k+\cdots+c_tx^k$, entre otros, estudiaron el tamaño A_n de estos conjuntos, y dieron formas explícitas de calcular cuántos enteros se pueden representar con esos polinomios módulo n.

Capítulo 1

Preliminares

En este capítulo introduciremos algunas definiciones y teoremas que son necesarios para entender este trabajo; los conceptos presentados aquí se cubren típicamente en los cursos básicos de teoría de números, teoría de grupos y anillos. Con el fin de no extendernos demasiado, no se incluyen las demostraciones de los teoremas; sin embargo, cualquier demostración, y más conceptos y teoría relacionados pueden consultarse en [1, 2, 3, 4, 6, 7, 9, 10, 11].

1.1. Divisibilidad en los enteros

A continuación se enuncian definiciones y teoremas relacionados con divisibilidad de enteros que serán de gran utilidad en el desarrollo del trabajo.

Teorema 1 (Algoritmo de la división)**.** *Sean a y b enteros con $b > 0$. Entonces existen enteros únicos q y r tales que*

$$a = qb + r,$$

donde $0 \leq r < b$. Los enteros q y r son llamados, respectivamente, ***el cociente*** *y* ***el residuo*** *en la división de a por b.*

Definición 2. Sean a y b enteros. Decimos que a **divide a** b, lo que denotamos $a \mid b$, si existe un entero k tal que $b = ak$. En este caso también decimos que b **es múltiplo de** a, que a **es un factor de** b, o que b **es divisible por** a.

La relación de divisibilidad entre enteros tiene las propiedades enunciadas en la siguiente proposición.

Proposición 3. *Sean a, b, c, n enteros. Entonces*

1. $a \mid a$;
2. *si* $a \mid b$, $b \mid c$, *entonces* $a \mid c$;
3. $na \mid nb$;
4. *si* $n \mid a$ *y* $n \mid b$, *entonces* $n \mid (ax + by)$ *para cualesquiera enteros* x *e* y;
5. *si* $a \mid b$ *y* $b \neq 0$, *entonces* $|a| \leq |b|$.

Definición 4 (Máximo común divisor)**.** Sean a y b enteros positivos. Decimos que d es **el máximo común divisor de a y b**, lo que se denota por $d = \text{mcd}(a, b)$, si se satisfacen las siguientes condiciones:

1. $d > 0$;
2. $d \mid a$ y $d \mid b$;
3. si c es un entero tal que $c \mid a$ y $c \mid b$, entonces $c \leq d$.

Definición 5. Sean a y b enteros que no son ambos cero. Decimos que a y b son **primos relativos** si $\text{mcd}(a, b) = 1$.

Teorema 6 (Lema de Euclides)**.** *Sean a, b y c enteros. Si $a \mid bc$ y $\text{mcd}(a, b) = 1$, entonces $a \mid c$.*

Definición 7 (Números primos)**.** Un entero p es llamado **primo** si $p > 1$ y los únicos divisores positivos de p son 1 y p. Un entero mayor que 1 que no es primo es llamado **compuesto**.

Teorema 8 (Teorema fundamental de la aritmética)**.** *Todo entero $n > 1$ puede expresarse como producto de primos. Esta representación es única excepto por el orden de los factores.*

Como consecuencia del teorema fundamental de la aritmética, todo entero $n > 1$ puede expresarse de manera única en la forma

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

donde $p_1 < p_2 < \cdots < p_k$ son primos y $r_i > 0$ para $i = 1, 2, \ldots, k$. Esta representación de n es llamada la **forma estándar** de n.

Teorema 9 (Euclides)**.** *Existen infinitos números primos.*

Definición 10. Una ecuación de la forma $p(x_1, x_2, ..., x_n) = 0$, donde $p(x_1, x_2, ..., x_n)$ es un polinomio de coeficientes enteros y con las variables restringidas a tomar valores enteros se denomina una **ecuación diofántica**.

1.2. Congruencias

La teoría de las congruencias es una rama de la teoría de números, que fue comenzada por Gauss al introducir una notación para simplificar los problemas de divisibilidad, que permite ser operada como una igualdad. Definiremos a continuación estos conceptos y enunciaremos algunos resultados importantes.

Definición 11 (Congruencia módulo m)**.** Sean a, b, m enteros, con $m > 0$. Decimos que a **es congruente con** b **módulo** m y escribimos $a \equiv b \pmod{m}$, si $m|(a - b)$. Es decir $a \equiv b \pmod{m}$ es equivalente a decir que $m|a - b$.

En el caso particular de que $b = 0$, $a \equiv 0 \pmod{m}$ si y solamente si $m|a$.

Dados $a \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$, por el Teorema 1 existen r y q enteros únicos, con $0 \leq r < n$ y $a = nq + r$, dicho de otra manera, $a \equiv r \pmod{n}$. Diremos que r es el residuo de a módulo n y lo denotaremos así $r := a \pmod{n}$.

Teorema 12. *La relación de congruencia es una relación de equivalencia.*

Teorema 13. *Sean a, b, m enteros, con $m > 0$. Entonces $a \equiv b \pmod{m}$, si y sólo si, a y b tienen el mismo residuo al dividirlos por m.*

Teorema 14. *Sean a, b, c, d, m enteros. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces: $ax + cy \equiv bx + dy \pmod{m}$, para cualesquiera enteros x e y; $ac \equiv bd \pmod{m}$; $a^n \equiv b^n \pmod{m}$, para cualquier entero positivo n y $f(a) \equiv f(b) \pmod{m}$, para todo polinomio f con coeficientes enteros.*

Teorema 15. *Sean $a, b, c, m \in \mathbb{Z}$. Si $c > 0$, entonces $a \equiv b \pmod{m}$ si y sólo si $ca \equiv cb \pmod{cm}$.*

Teorema 16 (Ley de cancelación)**.** *Sean $a, b, c, m \in \mathbb{Z}$ y $d = \text{mcd}(m, c)$. Si $ac \equiv bc \pmod{m}$, entonces*

$$a \equiv b \pmod{\frac{m}{d}}.$$

En otras palabras, este Teorema nos dice que, un factor común c, se puede cancelar siempre que el módulo se divida por $\text{mcd}(m, c)$.

Corolario 17. *Sean a, b, c, m enteros, con $m > 0$. Si $ac \equiv bc \pmod{m}$ y $\text{mcd}(m, c) = 1$, entonces $a \equiv b \pmod{m}$.*

Teorema 18. *Sean a, b, m enteros. Si $a \equiv b \pmod{m}$, entonces $\text{mcd}(a, m) = mcd(b, m)$. Además si $a \equiv b \pmod{m}$, $d|m$ y $d|a$, entonces $d|b$.*

Teorema 19. *Sean a, b, m enteros, con $m > 0$. Si $a \equiv b \pmod{m}$ y si $0 \leq |b-a| < m$, entonces $a = b$.*

Definición 20. Sea a un entero. Se define la **clase de equivalencia de a módulo m** y se denota $\overline{a}$ al conjunto de todos los enteros x tales que $x \equiv a \pmod{m}$. Este conjunto está formado por todos los enteros de la forma $a + mq$, donde $q = 0, \pm 1, \pm 2, ...$ Estas clases se llaman también **clases residuales módulo m.**

Teorema 21. *Sea m un entero positivo. Las clases de equivalencia módulo m tienen las siguientes propiedades:*

1. *Sean $a, b \in \mathbb{Z}$. Entonces, $\overline{a} = \overline{b}$, si y sólo si $a \equiv b \pmod{m}$.*

2. *Dos enteros x e y pertenecen a la misma clase residual si, y solamente si, $x \equiv y \pmod{m}$.*

3. *Las clases residuales módulo m, es decir, $\overline{1}, \overline{2}, ..., \overline{m}$ son disjuntas y su unión da $\mathbb{Z}$.*

Definición 22. Sea m un entero. El conjunto $\{a_1, a_2, \ldots, a_m\}$ es llamado un **sistema completo de residuos módulo** m si cada entero es congruente módulo m a exactamente uno de los a_i con $i \in \{1, 2, \ldots, m\}$.

Definición 23. Sea p un número primo, entonces el conjunto

$$\{-(p-1)/2, -(p-3)/2, \ldots, -1, 1, 2, \ldots, (p-1)/2\},$$

es llamado el **conjunto de residuos mínimos módulo** p.

Teorema 24. *Sean k, m enteros. Si $\text{mcd}(k, m) = 1$ y $\{a_1, a_2, ..., a_m\}$ es un sistema completo de residuos módulo m, entonces $\{ka_1, ka_2, ..., ka_m\}$ también es un sistema completo de residuos módulo m.*

Definición 25. Llamaremos $\mathbb{Z}_m$ al conjunto cociente de $\mathbb{Z}$ con respecto a la relación de congruencia módulo m. Los elementos que pertenecen a $\mathbb{Z}_m$ son las clases de equivalencia módulo m. Note que $\mathbb{Z}_m$ es finito, más preciso, tiene orden m, es decir, tiene exactamente m elementos.

Definición 26. Sean a, b, m enteros con $m > 0$. Una congruencia de la forma

$$ax \equiv b \pmod{m},$$

es llamada una **congruencia lineal** y tiene como solución a cualquier entero x_0 que satisfaga $ax_0 \equiv b \pmod{m}$.

Teorema 27. *Sean a, b, n enteros con $n > 0$. La congruencia lineal $ax \equiv b($ mód n$)$ tiene solución si y solo si $d \mid b$, donde $d = \text{mcd}(a, n)$. Más aún, si $d \mid b$, entonces esta congruencia tiene exactamente d soluciones mutuamente incongruentes módulo n, es decir, que no son congruentes entre sí. Además, si x_0 es una solución de la congruencia lineal, entonces cualquier otra solución es de la forma*

$$x = x_0 + \frac{n}{d}t.$$

Teorema 28 (Teorema Chino del residuo)**.** *Sean $n_1, n_2, \ldots, n_r$ enteros positivos tales que* $\text{mcd}(n_i, n_j) = 1$ *para $i \neq j$. Entonces el sistema de congruencias lineales*

$$\begin{cases} x \equiv a_1 \pmod{n_1}; \\ x \equiv a_2 \pmod{n_2}; \\ \quad \vdots \\ x \equiv a_r \pmod{n_r}; \end{cases}$$

tiene una solución simultánea, la cual es única módulo el producto $n_1 n_2 \cdots n_r$.

Teorema 29 (Pequeño teorema de Fermat)**.** *Sean a un entero y p primo. Si $p \nmid a$, es decir, p no divide a a, entonces $a^{p-1} \equiv 1 \pmod{p}$.*

Teorema 30 (Teorema de Wilson)**.** *Para todo número primo p se tiene que*

$$(p-1)! \equiv -1 \pmod{p}.$$

Este último teorema nos ayudara más adelante, así mismo, lo contenido en esta sección, son definiciones básicas de Teoría de números que son fundamentales para comprender este trabajo.

1.3. El grupo multiplicativo $\mathbb{Z}_p^*$

Definimos la adición y la multiplicación de los elemento de $\mathbb{Z}_p$ como sigue: Dados $\overline{m}$ y $\overline{n}$ en $\mathbb{Z}_p$,

$$\overline{m} + \overline{n} = \overline{m+n}$$

$$\overline{m} \cdot \overline{n} = \overline{m \cdot n}.$$

Entonces $\mathbb{Z}_p$ es un grupo multiplicativo. Por conveniencia denotaremos la clase $\overline{0}$ simplemente por 0 y cualquier otra clase de equivalencia, por su residuo más pequeño, lo que nos permite escribir $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Sea $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Lema 31. *Sea p un número primo. Entonces $\mathbb{Z}_p^*$ es un grupo multiplicativo abeliano, es decir,*

1. *Para cada* a *y* $b \in \mathbb{Z}_p^*$ *se cumple que* $a \cdot b \in \mathbb{Z}_p^*$;

2. *Para* a, b *y* $c \in \mathbb{Z}_p^*$, *se tiene que* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

3. *Para cada* $a \in \mathbb{Z}_p^*$ *existe un elemento* $e \in \mathbb{Z}_p^*$ *tal que y* $a \cdot e = e \cdot a = a$;

4. *Para cada* $a \in \mathbb{Z}_p^*$, *existe* a' *tal que* $a \cdot a' = a' \cdot a = e$;

5. *Para cada* a *y* $b \in \mathbb{Z}_p^*$, *se cumple que* $a \cdot b = b \cdot a$.

Demostración. Sean r, m y $n \in \mathbb{Z}_p^*$, luego, $m \neq 0$ y $n \neq 0$, por lo que $mn \neq 0$. Ahora, como $m \cdot n = (m \cdot n) \in \mathbb{Z}_p^*$, se cumple (1). Note que

$$(r \cdot m) \cdot n = r \cdot m \cdot n = r \cdot (m \cdot n).$$

Además

$$m \cdot 1 = 1 \cdot m = m.$$

Por otro lado, ya que p es primo, dado $m \in \mathbb{Z}_p^*$, se tiene que $p \nmid m$ y por el pequeño teorema de Fermat $m^{p-1} \equiv 1 \pmod{p}$, así

$$mm^{p-2} = m^{p-1} \equiv 1 \pmod{p}.$$

Lo cual significa en $\mathbb{Z}_p^*$ que $m \cdot m^{p-2} = 1$ módulo p, es decir, cualquier elemento $m \in \mathbb{Z}_p^*$ posee un inverso. Ahora,

$$m \cdot n = (m \cdot n) = (n \cdot m) = n \cdot m.$$

De lo anterior concluimos que $\mathbb{Z}_p^*$ es un grupo abeliano junto con la operación producto. □

Definición 32. Si H es un subconjunto de un grupo G cerrado bajo la operación binaria de G y si H es en él mismo un grupo bajo esta operación inducida, entonces H es un **subgrupo** de G.

Examinaremos esta estructura en un contexto general. Para cualquier x en un grupo G, definimos **el orden del elemento** x como el entero positivo n más pequeño tal que $x^n = 1$ y denotado como $ord(x) = n$. Consideremos el conjunto $\{x^0, x^1, \ldots, x^{n-1}\}$.

Note que $x^a \neq x^b$ para cada $a, b \in \{0, 1, \ldots, n-1\}$. De no ser así, entonces, digamos que existen s y t en $\{0, 1, \ldots, n-1\}$ tales que $x^s = x^t$, entonces $x^s x^{-t} = 1$ y así $x^{s-t} = 1$. Pero como el $ord(x) = n$, se tiene que $n < s - t < s \leq n - 1$, lo cual es una contradicción. Así que todos los elementos en dicho conjunto son distintos. Este conjunto se denota por G' y es un subgrupo abeliano de G junto con la operación $\cdot$ de G. Además, G' es cíclico generado por x.

Teorema 33 (Lagrange)**.** *Sean G un grupo finito y H un subgrupo de G. Entonces el orden de H divide al orden de G.*

Demostración. Véase [6, página 112]. □

Lema 34. *Sean G un grupo finito y $a \in G$. Entonces el orden de a divide al orden del grupo G.*

Lema 35. *Sea G un grupo con identidad 1 y sea $a \in G$. Si a tiene orden finito $m > 0$, entonces $a^k = 1$ si y solo si $m \mid k$.*

Demostración. Supongamos que $a^k = 1$. Como a tiene orden $m > 0$, por el algoritmo de la división existen elementos únicos q y r de G tales que $k = mq + r$, con $0 \leq r < m$. Ahora, por hipótesis $a^k = 1$, de donde

$$1 = a^k = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r = a^r.$$

Tenemos así que $a^r = 1$ y además $0 \leq r < n$, pero como $m = ord(a)$, m es el entero más pequeño tal que $a^m = 1$. Por consiguiente $r = 0$. Así $m \mid k$.

Recíprocamente supongamos que $m \mid k$. Luego $k = mt$ para algún $t \in G$. Así $a^k = a^{mt} = (a^m)^t = 1$. Lo que termina la prueba. □

Lema 36. *Suponga que x e y son elementos del grupo abeliano $\langle G, \cdot \rangle$. Además, suponga que $ord(x) = a; ord(y) = b$ y $\text{mcd}(a, b) = 1$. Entonces $ord(xy) = ab$.*

Demostración. Sea $ord(xy) = j$. Entonces j es el menor entero tal que $(xy)^j = 1$. Observe que

$$(xy)^{ab} = x^{ab} y^{ab} = (x^a)^b (y^b)^a = 1.$$

Como $ord(ab) = j$, por el lema anterior $j \mid ab$. Note que $1 = (xy)^j = x^j y^j$, de donde $x^j y^j = 1$, así que $(x^j y^j)a = 1^a$, por lo que $(x^a)^j y^{aj} = 1$ y en consecuencia $y^{aj} = 1$, además, ya que $ord(y) = b$, por el lema anterior $b \mid aj$ y como $\text{mcd}(a, b) = 1$, por el lema de Euclides $b \mid a$. Ahora, como $x^j y^j = 1$, tenemos que $x^{bj}(y^b)^j = 1^b = 1$, de donde $x^{bj} = 1$ y nuevamente por el lema anterior $a \mid bj$ y ya que $\text{mcd}(a, b) = 1$ se obtiene que $a \mid j$.

Afirmamos que si $a \mid c, b \mid c$ y $\text{mcd}(a, b) = 1$, entonces $ab \mid c$.

Como a y b son primos relativos, $ax_0 + by_0 = 1$, para algunos enteros x_0 e y_0. Multiplicando toda la igualdad por c tenemos que $acx_0 + bcy_0 = c$. Además, $c = ar$ y $c = bs$, de donde $a(bs)x_0 + b(ar)y_0 = c$, y así $ab(sx_0 + ry_0) = c$. Por lo tanto $ab \mid c$.

De la afirmación y el hecho de que $j \mid ab$ concluimos que $ab = j$. □

Teorema 37. *El grupo multiplicativo $\mathbb{Z}_p^*$ es cíclico, es decir, existe un elemento $a \in \mathbb{Z}_p^*$ tal que cualquier elemento de $\mathbb{Z}_p^*$ se deja escribir de la forma a^n para algún entero n. El elemento a es llamado generador de $\mathbb{Z}_p^*$.*

Demostración. Como $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, entonces $\mathbb{Z}_p^*$ tiene exactamente $p - 1$ elementos, esto es, $|\mathbb{Z}_p^*| = p - 1$. Sea k el máximo orden de los elementos de $\mathbb{Z}_p^*$, lo que hacemos es observar cual es el orden de cada elemento de $\mathbb{Z}_p^*$ y escogemos el mayor de ellos. Consideremos el polinomio $\lambda^k - 1$ en el grupo multiplicativo $\mathbb{Z}_p$. Como sabemos, el orden de un elemento a es el entero positivo n más pequeño tal que $a^n = 1$, así que para cada elemento $x \in \mathbb{Z}_p^*$ el orden de x divide a k. Por lo tanto, cada uno de estos elemento es un cero en el polinomio $\lambda^k - 1$, lo cual implica que $k \geq p - 1$. Pero el orden de un elemento de un grupo no puede ser más grande que el orden del grupo. Así que $k = p - 1$, y cualquier elemento cuyo orden es k es generador de $\mathbb{Z}_p^*$. □

1.4. Funciones multiplicativas

A continuación daremos un par de definiciones y teoremas que serán útiles más adelante.

Definición 38. Una función cuyo dominio es el conjunto de los enteros positivos es llamada **función aritmética**.

Definición 39. Sean m y n enteros positivos con $\text{mcd}(m,n) = 1$ y f una función aritmética. Diremos que f es una **función multiplicativa** si $f(nm) = f(n)f(m)$.

Definición 40. Una función aritmética f es **completamente multiplicativa** si dados dos enteros cualesquiera m y n se cumple que $f(nm) = f(n)f(m)$.

Note que, si f es una función multiplicativa, podemos determinarla con los valores de potencias de primos conocidos. Sabemos que si $n > 1$, por el Teorema fundamental de la aritmética, $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, donde $p_i \neq p_j$ para $i \neq j$ y $a_i > 0$ para cada $i, j \in \{1, 2, \ldots, r\}$. Así que, los $p_i^{a_i}$ son primos relativos dos a dos, como f es multiplicativa

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_r^{a_r}).$$

Si f es una función multiplicativa que no es idénticamente cero, entonces existe un entero n tal que $f(n) \neq 0$. Pero $f(n) = f(n \cdot 1) = f(n)f(1)$, así que $f(1) = 1$. Por lo tanto, si f es multiplicativa y $f \not\equiv 0$, entonces $f(1) = 1$.

Teorema 41. *Sea f una función aritmética tal que $f(1) = 1$. Entonces f es multiplicativa si y solamente si*

$$f\left(\prod_{i=1}^{k} p_i^{n_i}\right) = \prod_{i=1}^{k} f(p_i^{n_i})$$

para todos los primos p_i y todos los enteros $n_i \geq 1$.

1.5. Números complejos y raíces $n-$ésimas de la unidad

Sabemos que $\mathbb{R}^2$ consiste de todas las parejas ordenadas (x, y), donde x e y son números reales. De modo que el sistema de números complejos $\mathbb{C}$ es precisamente $\mathbb{R}^2$ junto con las operaciones suma de vectores, producto escalar por un número real $(a, b) + (c, d) = (a + c, b + d)$, $x(a, b) = (ax, bx)$ con $x \in \mathbb{R}$ y la multiplicación definida como $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. El punto unitario en el eje y, $(0, 1)$ es denotado por $i = \sqrt{-1}$ y el eje y es llamado **eje imaginario** mientras que el eje x es el **eje real**. De modo que un número complejo $(a, b) = (a, 0) + b(0, 1) = a + ib$.

Definición 42. Sea $z \in \mathbb{C}$. Se define $e^{iz} = \cos z + i \sin z$ y $e^{-iz} = \cos z - i \sin z$.

Sumando las dos igualdades anteriores tenemos que:

$$e^{iz} + e^{-iz} = \cos z + i \sin z + \cos z - i \sin z = 2 \cos z,$$

de donde $\cos z = \dfrac{e^{iz} + e^{-iz}}{2}$. Ahora, si restamos estas igualdades obtenemos

$$e^{iz} - e^{-iz} = \cos z + i \sin z - \cos z + i \sin z = 2i \sin z,$$

así, $\sin z = \dfrac{e^{iz} - e^{-iz}}{2i}$.

Definición 43. Sean $z \in \mathbb{C}$ y $n \in \mathbb{N}$. Diremos que w es una raíz n-ésima de z si $w^n = z$.

Teorema 44. *Sean $z \in \mathbb{C}$ y $n \in \mathbb{N}$, con $z \neq 0$. Entonces z tiene exactamente n raíces n-ésimas.*

Definición 45 (Raíces $n-$ésimas de la unidad)**.** Un número complejo ζ es llamado **raíz $n-$ésima de la unidad** si $\zeta^n = 1$ para algún entero $n > 0$. Si n es el entero más pequeño tal que $\zeta^n = 1$, entonces ζ es llamado **raíz primitiva $n-$ésima de la unidad de orden n.**

Las raíces $n-$ésimas de la unidad son: $1, e^{2\pi i/n}, e^{(2\pi i/n)2}, \cdots, e^{(2\pi i/n)(n-1)}$. Las raíces primitivas $n-$ésimas de la unidad son $e^{(2\pi i/n)k}$, donde $\text{mcd}(k, n) = 1$. Además, si ζ es una raíz primitiva, entonces las otras raíces primitivas son de la forma ζ^s, donde s y n son primos relativos.

Capítulo 2

Ley de reciprocidad cuadrática

En este capítulo definiremos el concepto de residuo cuadrático y mostraremos una de las pruebas de la ley de reciprocidad cuadrática debidas a Eisenstein. Mostraremos igualmente varios ejemplos, aplicaciones y resultados importantes como el criterio de Euler para residuos cuadráticos, el lema de Gauss, entre otros.

2.1. Residuos cuadráticos y el símbolo de Legendre

La teoría de las congruencias nos da una ventaja importante; la relación $\equiv$ se puede interpretar como un $=$. En este sentido, una congruencia módulo n, que es una relación de divisibilidad, se puede ver como una ecuación pero en $\mathbb{Z}_n$. Con esta idea en mente, definimos un *residuo cuadrático*.

Definición 46. Sean a un entero y p un primo impar con mcd $(a, p) = 1$. Diremos que a es **residuo cuadrático módulo** p si existe un entero x tal que

$$x^2 \equiv a \pmod{p}. \tag{2.1.1}$$

En otras palabras, a es un residuo cuadrático módulo p si la congruencia (2.1.1) tiene solución. En caso contrario, diremos que a es no-residuo cuadrático módulo p.

Para $p = 2$ el problema de resolver la congruencia (2.1.1) es sencillo, pues si se supone que mcd $(a, 2) = 1$, entonces a es impar e inmediatamente la congruencia

(2.1.1) tiene solución, pues basta tomar $x = 1$. En lo que resta de este capítulo, a menos que se especifique lo contrario, p representará un número primo impar.

Ejemplo 1. En este ejemplo, hallemos los residuos y los no-residuos cuadráticos módulo 13. Para averiguar cuántos enteros en $\{1, 2, \ldots, 12\}$ son residuos cuadráticos módulo 13, debemos averiguar si la congruencia $x^2 \equiv a \pmod{13}$ tiene solución, cuando a recorre al conjunto $\{1, 2, \ldots, 12\}$; por ejemplo, para $a = 1$, tenemos que $12^2 \equiv 1 \pmod{13}$ y $1^2 \equiv 1 \pmod{13}$. Para el resto de elementos observemos la siguiente tabla:

x	1	2	3	4	5	6	7	8	9	10	11	12
a	1	4	9	3	12	10	10	12	3	9	4	1

Esta tabla nos indica por ejemplo que, para $a = 3$ existe 4 tal que $4^2 \equiv 3 \pmod{13}$.

Observamos a partir de la tabla anterior que $1, 3, 4, 9, 10$ y 12 son los residuos cuadráticos módulo 13, mientras que $2, 5, 6, 7, 8$ y 11 son los no-residuos cuadráticos módulo 13.

Definición 47. Sean a un entero y p un primo impar con $\text{mcd}(a, p) = 1$. Definimos el **símbolo de Legendre** (a/p) como sigue:

$$(a/p) = \begin{cases} 1, & \text{si } a \text{ es residuo cuadrático módulo } p; \\ -1, & \text{si } a \text{ es no-residuo cuadrático módulo } p. \end{cases}$$

Dados un entero a y un primo impar p, si $p \mid a$, diremos que $(a/p) = 0$.

Lema 48. *Sean $a, b \in \mathbb{Z}$ y p un primo impar. Entonces $(a/p) = (b/p)$ si y solo si $(a/p) \equiv (b/p) \pmod{p}$.*

Demostración. Observe que en el caso en que por ejemplo $(a/p) = 0$, tenemos para la primera implicación que $(a/p) = (b/p) = 0$ y ya que $p \mid 0$, se sigue que $(a/p) \equiv (b/p) \pmod{p}$. Para la otra implicación, por reducción al absurdo supongamos que $(a/p) \neq (b/p)$; tenemos que $(a/p) \equiv (b/p) \pmod{p}$, esto es, $p \mid (b/p)$, pero el valor (a/b) no puede ser cero por la suposición que acabamos de ser, así que $p \mid 1$ o $p \mid -1$, lo cual es absurdo.

Primero supongamos que $p \nmid a$, $p \nmid b$ y $(a/p) = (b/p)$. Como $(a/p) \equiv (a/p) \pmod{p}$, entonces $(a/p) \equiv (b/p) \pmod{p}$.

Recíprocamente supongamos por reducción al absurdo que $(a/p) \equiv (b/p) \pmod{p}$ y que $(a/p) \neq (b/p)$. Luego, $p \mid (a/p) - (b/p)$, así, $p \mid 2$ o bien $p \mid (-2)$ en cualquier caso esto es imposible puesto que p es un número primo impar. □

Proposición 49. *Sean $a, b \in \mathbb{Z}$ y p un primo impar. Entonces*

1. *Criterio de Euler: $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.*

2. *$(ab/p) = (a/p)(b/p)$.*

3. *Si $a \equiv b \pmod{p}$, entonces $(a/p) = (b/p)$.*

Demostración. Primero observemos que si $p \mid a$, entonces $(a/p) = 0$ y $a \equiv 0 \pmod{p}$, lo cual implica que $a^{(p-1)/2} \equiv 0 \pmod{p}$ y por lo tanto se obtiene que $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.

Por otro lado, si $p \mid a$, entonces $p \mid ab$ y $(ab/p) = 0 = (a/p)(b/p)$. Además, si $a \equiv b \pmod{p}$, entonces $p \mid a - b$, y se sigue que $p \mid b$. Así, $(a/p) = 0 = (b/p)$.

Para el resto de la prueba podemos suponer que $p \nmid a$ y $p \nmid b$.

1. Por el pequeño teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$, de donde

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}. \tag{2.1.2}$$

   Consideremos los siguientes casos; si a es residuo cuadrático módulo p, entonces existe un entero x, con $0 \leq x \leq p-1$ tal que $x^2 \equiv a \pmod{p}$, de donde $(a/p) = 1$, y ya que $x < p$, por el pequeño teorema de Fermat, $x^{p-1} \equiv 1 \pmod{p}$. Así,

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \equiv (a/p) \pmod{p}.$$

   Luego, $a^{(p-1)/2} - 1 \equiv 0 \pmod{p}$.

   Ahora supongamos que a es no-residuo cuadrático módulo p, por definición $(a/p) = -1$, esto significa que la congruencia $x^2 \equiv a \pmod{p}$ no tiene solución para ningún x y en $\mathbb{Z}_p^*$, esto quiere decir que la ecuación $x^2 = a$ no tiene solución.

Ahora, sea $h \in \{1, 2, \ldots, p-1\} \subseteq \mathbb{Z}_p^*$. Observe que, por ser $\mathbb{Z}_p^*$ grupo, existe $h^{-1} \in \mathbb{Z}_p^*$ tal que $hh^{-1} = 1$, así que

$$hk = a,$$

donde $k := h^{-1}a$ y $h \neq k$, pues de ser iguales, tendríamos que h es solución de la ecuación $x^2 = a$ en $\mathbb{Z}_p^*$ y esto no es posible.

Ahora, para $h \in \{1, \ldots, p-1\}$ dividimos este conjunto en $(p-1)/2$ parejas h, k tales que $hk = a$. De este modo

$$1 \cdot 2 \cdots (p-1) = h_1k_1 \cdot h_2k_2 \cdots h_{(p-1)/2}k_{(p-1)/2} = \underbrace{a \cdot a \cdots a}_{(p-1)/2-veces} = a^{(p-1)/2} \ \ en\ \mathbb{Z}_p^*.$$

En congruencias, esto significa que $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$. Ahora, por el teorema de Wilson $(p-1)! \equiv -1 \pmod{p}$, se desprende que

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Por lo tanto $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.

2. Nótese que $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}$. Por la parte anterior, tenemos que

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

   así que $(ab/p) \equiv (a/p)(b/p) \pmod{p}$ y por lo tanto $(ab/p) = (a/p)(b/p)$.

3. En el caso en que a es residuo cuadrático módulo p tenemos que $(a/p) = 1$. Entonces existe un entero x tal que $x^2 \equiv a \pmod{p}$. Como $a \equiv b \pmod{p}$, resulta que $x^2 \equiv b (\mathrm{mod}\ p)$ y así $(b/p) = 1 = (a/p)$. Ahora, si a es no-residuo cuadrático módulo p, entonces para cualquier entero x, $x^2 \not\equiv a (\mathrm{mod}\ p)$, y como $a \equiv b (\mathrm{mod}\ p)$, se sigue que $x^2 \not\equiv b \pmod{p}$. En consecuencia, b es no-residuo cuadrático módulo p y $(b/p) = -1 = (a/p)$.

□

Por la Proposición 49, dado un entero a y un primo impar p, para determinar (a/p), basta con descomponer a como producto de primos, $a = \pm p_1p_2 \cdots p_r$ y hallar $(\pm 1/p)$ y (p_i/p) para $i = 1, 2, \ldots, r$, puesto que

$$(a/p) = (\pm 1/p)(p_1/p)(p_2/p) \cdots (p_r/p).$$

Es claro que $(1/p) = 1$. Veremos criterios para determinar $(-1/p)$, $(2/p)$ y (q/p) cuando q sea impar.

Corolario 50. *Hay tantos enteros módulo p que son residuos cuadráticos, como enteros módulo p que son no-residuos cuadráticos módulo p. Más precisamente, en el conjunto* $\{1, 2, \ldots, p-1\}$*, la cantidad de residuos cuadráticos es igual a la cantidad de no-residuos cuadráticos.*

Demostración. Sean a un entero con $\text{mcd}(a, p) = 1$. Consideremos a los enteros

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

Ahora, si x e y son enteros con $1 \leq x \leq (p-1)/2$ y $1 \leq y \leq (p-1)/2$ tales que $x^2 \equiv y^2 \pmod{p}$, entonces

$$(x+y)(x-y) = x^2 - y^2 \equiv 0 \pmod{p}.$$

Así que $p \mid x^2 - y^2$ y como p es un primo impar, se sigue que $p \mid x+y$ o $p \mid x-y$ y por tanto, $x \equiv y \pmod{p}$ o $x \equiv -y \pmod{p}$. Pero $x \equiv -y \pmod{p}$ no puede ocurrir ya que, de hacerlo, $p \mid x+y$. Luego, $p \leq x+y$, pero, por otro lado tenemos que, $1 < x+y < 2(p-1)/2 = p-1$, lo cual nos lleva a una contradicción. Por lo tanto $x \equiv y \pmod{p}$ y en consecuencia $x = y$. Nótese que x e y son arbitrarios en $1, 2, \ldots, (p-1)/2$, esto es, si tenemos dos elementos diferentes en

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

deben ser incongruentes modulo p. Además, $(p-k)^2 \equiv k^2 \pmod{p}$, es decir, que los cuadrados de los números $1, 2, \ldots, (p-1)/2$, son congruentes con los cuadrados de los números $(p+1)/2, \ldots, p-1$. Por lo tanto, todo residuo cuadrático en $1, 2, \ldots, p-1$ es congruente módulo p a exactamente uno de los números en $1^2, 2^2, \ldots, ((p-1)/2)^2$. Así la congruencia $a^{(p-1)/2} \equiv 1 (\text{mod } p)$ tiene exactamente $(p-1)/2$ soluciones para $a \in \{1, 2, \ldots, p-1\}$ módulo p. Así, por la parte (1) de la Proposición 49, hay exactamente $(p-1)/2$ residuos cuadráticos módulo p, y por lo tanto hay $p-1-(p-1)/2 = (p-1)/2$ no-residuos cuadráticos módulo p. □

Ejemplo 2. Determinemos si 22 es residuo cuadrático módulo 5, y si 40 es residuo cuadrático módulo 3. En efecto, como $5 \nmid 22$, por el pequeño teorema de Fermat tenemos

$$22^4 \equiv 1 \pmod{5}.$$

Así que $22^2 \equiv 1 \pmod{5}$ o $22^2 \equiv -1 \pmod{5}$. Pero $22^2 = 484$, así que $22^2 \equiv -1 \pmod{5}$ y por la Proposición 49 tenemos que $22^2 \equiv (22/5) \pmod{5}$, de donde $5 \mid (22/5) + 1$ y ya que 5 es primo, $(22/5) + 1 = 0$. Por lo tanto $(22/5) = -1$, esto es, 22 es no-residuo cuadrático módulo 5.

Por otro lado, puesto que $3 \mid 30$, se tiene que $40 \equiv 10 \pmod{3}$ y por la Proposición 49 obtenemos que $(40/3) = (10/3)$. Además, puesto que $10 = 5 \cdot 2$, nuevamente, por la Proposición 49, tenemos $(10/3) = (5/3)(2/3)$. Además, $2^{(3-1)/2} = 2 \equiv (2/3) \pmod{3}$ y $5^{(3-1)/2} = 5 \equiv (5/3) \pmod{3}$; pero estas últimas congruencias son posibles únicamente si $(2/3) = (5/3) = -1$. Así

$$\left(\frac{40}{3}\right) = \left(\frac{10}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{5}{3}\right) = (-1)(-1) = 1.$$

En consecuencia, 40 es residuo cuadrático módulo 3.

Del ejemplo anterior podemos observar que 2 y 5 son no-residuos cuadráticos módulo 3; sin embargo, su producto es residuo cuadrático módulo 3. Esta es una de las propiedades que estudiaremos más adelante.

Corolario 51. *Sea p un número primo impar. Entonces*

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

Demostración. Por el Corolario 50 hay $\dfrac{p-1}{2}$ residuos cuadráticos módulo p y hay $\dfrac{p-1}{2}$ no-residuos cuadráticos módulo p. Así que

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

□

Corolario 52. *El producto de dos residuos cuadráticos es un residuo cuadrático; el producto de dos no-residuos cuadráticos es un residuo cuadrático, y el producto de un residuo cuadrático con un no-residuo cuadrático es un no-residuo cuadrático.*

Demostración. Sean $a, b \in \mathbb{Z}$ y p primo con mcd $(a, p) =$ mcd $(b, p) = 1$. Si a y b son residuos cuadráticos, entonces $(a/p) = 1$ y $(b/p) = 1$. Por la Proposición 49 obtenemos que $(ab/p) = (a/p)(b/p) = (1)(1) = 1$. Así, el producto de dos residuos cuadráticos es un residuo cuadrático.

Si a y b son no-residuos cuadráticos, entonces $(a/p) = -1$, $(b/p) = -1$ y nuevamente, por la Proposición 49 tenemos que $(ab/p) = (a/p)(b/p) = (-1)(-1) = 1$. Esto muestra que el producto de dos no-residuos cuadráticos es un residuo cuadrático.

Por último, si a es un residuo cuadrático y b un no-residuo cuadrático, entonces tenemos que $(a/p) = 1$ y $(b/p) = -1$. Luego, por la la Proposición 49 se sigue que $(ab/p) = (a/p)(b/p) = (1)(-1) = -1$. □

2.2. El carácter cuadrático de -1

Usando los resultados que tenemos hasta el momento acerca de residuos cuadráticos y el símbolo de Legendre, podemos caracterizar los primos impares p tales que -1 es residuo cuadrático módulo p. Comenzamos con la siguiente consecuencia de la Proposición 49.

Corolario 53. *Si p es un primo impar, entonces $(-1/p) = (-1)^{(p-1)/2}$.*

Demostración. Basta con tomar $a = -1$ en la primera parte de la Proposición 49. □

Los primos impares se dividen en dos tipos: los de la forma $4k+1$ y los de la forma $4k + 3$. Usando esto, podemos reformular el Corolario 53 de la siguiente manera.

Corolario 54. *Si p es un número primo, entonces la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.*

Demostración. Si la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución, por definición, se tiene que $(-1)^{(p-1)/2} = (-1/p) = 1$, de donde $\dfrac{p-1}{2} = 2j$, para algún entero j. Así, $p - 1 = 4j$ para algún entero j, esto es, $p \equiv 1 \pmod{4}$.

Recíprocamente, si $p \equiv 1 \pmod 4$, entonces $p = 4k + 1$ para algún entero k y se sigue que $(-1/p) = (-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1$. En consecuencia, -1 es un residuo cuadrático módulo p, es decir, la congruencia $x^2 \equiv -1 \pmod p$ tiene solución. □

A partir del Corolario 54 podemos observar que -1 es un residuo cuadrático de los primos de la forma $4k + 1$, es decir, $5, 13, 17, 29, \ldots$. Además, -1 es no-residuo cuadrático de los primos de la forma $4k + 3$, es decir, $3, 7, 11, 19, \ldots$.

Usando el Corolario 53 podemos hacer una prueba de la existencia de infinitos primos de la forma $4k + 1$, como mostramos a continuación.

Proposición 55. *Existen infinitos primos de la forma* $4k + 1$.

Demostración. Por reducción al absurdo, supongamos que hay un número finito de primos de la forma $4k+1$, digamos $p_1, p_2, \ldots, p_m$, y definamos $M = (2p_1p_2 \cdots p_m)^2+1$, con $M \in \mathbb{Z}$. Sea p un divisor primo de M. Entonces -1 es un residuo cuadrático módulo p, pues la congruencia $x^2 \equiv -1 \pmod p$ tiene a $x = 2p_1p_2 \cdots p_m$ como una solución. Se sigue que p es de la forma $4k + 1$, y por lo tanto se tiene que $p = p_i$, para algún $i \in \{1, 2, \ldots, m\}$. Pero, en tal caso se sigue que $p \mid (2p_1p_2 \cdots p_m)^2$ y, en consecuencia, p divide a $M - (2p_1p_2 \cdots p_m)^2 = 1$, lo cual es una contradicción. Esto termina la prueba. □

2.3. El lema de Gauss

El lema de Gauss es usualmente un paso crucial en muchas de las demostraciones de la ley de reciprocidad cuadrática, y esta no es la excepción en la prueba que presentaremos en este trabajo. Damos, a continuación, la definición del número $\mu(a, p)$ y luego de un ejemplo, procedemos a enunciar y demostrar el lema de Gauss.

Definición 56. Sean a un entero y p un primo impar con $\text{mcd}(a, p) = 1$. Consideremos el conjunto $S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$. Definimos $\mu(a, p)$ como el número de elementos de S que tienen residuo mínimo negativo módulo p.

Ejemplo 3. Si $p = 7$, entonces $\dfrac{p-1}{2} = \dfrac{7-1}{2} = 3$. Luego, el conjunto de residuos mínimos es $\{-3, -2, -1, 1, 2, 3\}$. Además, para $a = 3$ tenemos que el conjunto S es $S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\} = \{3, 6, 9\}$; donde, $3 \equiv 3 \pmod 7$, $6 \equiv -1 \pmod 7$ y $9 \equiv 2 \pmod 7$. Así, $\mu(3, 7) = 1$.

Lema 57 (Lema de Gauss)**.** *Sean a un entero y p un primo impar tal que $p \nmid a$. Entonces*

$$(a/p) = (-1)^{\mu(a,p)}.$$

Demostración. Para cada $l \in \{1, 2, \ldots, (p-1)/2\}$, sea m_l el residuo mínimo que es congruente con la. Así $\mu(a, p)$ es igual a la cantidad de m_l que son negativos.

Afirmamos que $|m_l| \neq |m_k|$, si $l \neq k$. En efecto, por reducción al absurdo, supongamos que $|m_l| = |m_k|$. Entonces $m_l = m_k$ o $m_l = -m_k$, lo que quiere decir que $la \equiv ka \pmod p$ o $la \equiv -ka \pmod p$. Como $p \nmid a$, se sigue que $l \equiv k \pmod p$ o $l \equiv -k \pmod p$. Ahora, como $l, k \in \{1, 2, \ldots, (p-1)/2\}$, tenemos que $l \not\equiv k \pmod p$, así que $l \equiv -k \pmod p$, es decir, $p \mid k + l$. Pero tenemos también que

$$2 \leq l + k \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1,$$

lo cual es absurdo.

Hemos mostrado que los elementos $|m_l|$ son todos distintos, lo que implica la igualdad de conjuntos siguiente:

$$\{|m_l| : l \in \{1, 2, \ldots, (p-1)/2\}\} = \{1, 2, \ldots, (p-1)/2\}. \tag{2.3.1}$$

Ahora bien, tenemos las congruencias

$$1a \equiv m_1 \pmod p, 2a \equiv m_2 \pmod p, \ldots, \left(\frac{p-1}{2}\right)a \equiv m_{\frac{p-1}{2}} \pmod p,$$

que al multiplicarlas miembro a miembro obtenemos

$$((p-1)/2)!a^{(p-1)/2} \equiv \left(\prod_{l=1}^{(p-1)/2} m_l\right) \pmod p.$$

En el miembro de la derecha de la congruencia anterior extraemos los signos de todos los m_l que sean negativos, que en total son $\mu(a, p)$, para obtener que

$$((p-1)/2)!a^{(p-1)/2} \equiv (-1)^{\mu(a,p)} \left(\prod_{l=1}^{(p-1)/2} |m_l|\right) \pmod p.$$

Puesto que tenemos la igualdad

$$\{|m_l| : l \in \{1, 2, \ldots, (p-1)/2\}\} = \{1, 2, \ldots, (p-1)/2\},$$

resulta que $\prod_{l=1}^{(p-1)/2} |m_l| = \prod_{l=1}^{(p-1)/2} l = ((p-1)/2)!$, por lo que obtenemos

$$((p-1)/2)!a^{(p-1)/2} \equiv (-1)^{\mu(a,p)}((p-1)/2)! \pmod{p}.$$

Como mcd $((p-1)/2)!, p) = 1$, podemos cancelar $((p-1)/2)!$ de la congruencia anterior y obtener que $a^{(p-1)/2} \equiv (-1)^{\mu(a,p)} \pmod{p}$. Gracias a la Proposición 49 tenemos que $a^{(p-1)/2} \equiv (a/p) \pmod{p}$. Así $(a/p) \equiv (-1)^{\mu(a,p)} \pmod{p}$, lo que significa que p divide a $(a/p) - (-1)^{\mu(a,p)}$; pero $(a/p) - (-1)^{\mu(a,p)} \in \{0, 2, -2\}$, y como p es un primo impar, necesariamente se sigue que $(a/p) - (-1)^{\mu(a,p)} = 0$, esto es, $(a/p) = (-1)^{\mu(a,p)}$. □

Ejemplo 4. Usemos el Lema de Gauss para determinar $\left(\frac{5}{7}\right)$. Tenemos que $a = 5$, $p = 7$, $S = \{5, 10, 15\}$, y el sistema de residuos mínimos es $\{-3, -2, -1, 1, 2, 3\}$. Como $5 \equiv -2 \pmod{7}, 10 \equiv 3 \pmod{7}$ y $15 \equiv 1 \pmod{7}$, resulta que $\mu(5, 7) = 1$ y por el lema de Gauss, $(5/7) = (-1)^{\mu(5,7)} = -1$. Así, 5 es un no-residuo cuadrático módulo 7.

Ahora usaremos el lema de Gauss para dar una caracterización de los primos que tienen a 2 como residuo cuadrático. Los primos impares tienen cuatro formas posibles dependiendo de su residuo al dividirlos entre 8, las cuales son $8k + 1, 8k + 3, 8k + 5$ y $8k + 7$.

Proposición 58. *Sea p un primo impar. Entonces 2 es residuo cuadrático módulo p si y solo si p tiene la forma $8k+1$ o la forma $8k+7$. Esta información se resume en la fórmula siguiente:*

$$(2/p) = (-1)^{(p^2-1)/8}$$

Demostración. Sea p un primo impar. Los enteros $1, 2, \ldots, (p-1)/2$ son primos relativos dos a dos. Como p es impar, $\text{mcd}(2, p) = 1$, así que los enteros

$$2 = 2 \cdot 1, 4 = 2 \cdot 2, \ldots, p - 1 = 2 \cdot \frac{p-1}{2}, \tag{2.3.2}$$

son primos relativos dos a dos. Para hallar los elementos de la lista (2.3.2) que tiene residuo mínimo negativo módulo p, basta con hallar los elementos en (2.3.2) que exceden $(p-1)/2$, que son los mismos que exceden $\frac{p}{2}$. Para $1 \leq m \leq \frac{p-1}{2}$ se cumple que $2m < \frac{p}{2}$ si y solo si $m < \frac{p}{4}$.

Para un entero a, denotemos por $\lfloor a \rfloor$ al mayor entero menor o igual que a. Entonces hay $\lfloor \frac{p}{4} \rfloor$ enteros que en (2.3.2) que son más pequeños que $\frac{p}{2}$. Luego, $(p-1)/2 - \lfloor \frac{p}{4} \rfloor$ es el número de enteros en (2.3.2) que exceden a $p/2$, esto es, $\mu(2,p) = (p-1)/2 - \lfloor \frac{p}{4} \rfloor$. Ahora, tenemos los siguientes casos:

1. si $p = 8k+1$, entonces

$$\mu(2,p) = \frac{8k+1-1}{2} - \left\lfloor \frac{8k+1}{4} \right\rfloor = \frac{8k}{2} - \left\lfloor \frac{8k}{4} + \frac{1}{4} \right\rfloor = 4k - 2k = 2k. \quad (2.3.3)$$

2. si $p = 8k+3$, entonces

$$\mu(2,p) = \frac{8k+3-1}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = \frac{8k+2}{2} - \left\lfloor \frac{8k}{4} + \frac{3}{4} \right\rfloor = 2k+1. \quad (2.3.4)$$

3. si $p = 8k+5$, tenemos que

$$\mu(2,p) = \frac{8k+5-1}{2} - \left\lfloor \frac{8k+5}{4} \right\rfloor = \frac{8k+4}{2} - \left\lfloor \frac{8k}{4} + 1 + \frac{1}{4} \right\rfloor = 2k+1. \quad (2.3.5)$$

4. si $p = 8k+7$, obtenemos

$$\mu(2,p) = \frac{8k+7-1}{2} - \left\lfloor \frac{8k+7}{4} \right\rfloor = \frac{8k+6}{2} - \left\lfloor \frac{8k}{4} + 1 + \frac{3}{4} \right\rfloor = 2k+2. \quad (2.3.6)$$

Por el Lema de Gauss, $(2/p) = (-1)^{\mu(2,p)}$. Así, de (2.3.3) y (2.3.6) tenemos que $(2/p) = (-1)^{\mu(2,p)} = 1$. Por lo que, 2 es residuo cuadrático módulo p si $p = 8k+1$ o $p = 8k+7$. Por otro lado, de (2.3.4) y (2.3.5) $(2/p) = (-1)^{\mu(2,p)} = -1$ si y solo si p es de la forma $8k+3$ o $8k+5$.

Nótese que, si p es de la forma $8k+1$ o $8k-1$ (equivalentemente de la forma $8k+7$), entonces $p = 8k+1 \equiv 1 (\text{mod } 8)$ ó $p = 8k-1 \equiv 7 (\text{mod } 8)$ entonces

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k + 1 - 1}{8} = 8k^2 \pm 2k$$

Se sigue que $\dfrac{p^2-1}{8}$ es par y $(2/p) = (-1)^{(p^2-1)/8} = (-1)^{8k^2 \pm 2} = 1$. Por otro lado, si p es de la forma $8k+3$ o $8k-3$ (equivalentemente $8k+5$), entonces,

$$\frac{8k^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 9 - 1}{8} = 8k^2 \pm 6k + 1.$$

Luego $(2/p) = (-1)^{(p^2-1)/8} = (-1)^{8k^2 \pm 6k+1} = -1$. En cualquier caso tenemos que $(2/p) = (-1)^{(p^2-1)/8}$. □

Ejemplo 5. Como $7 \equiv 7 (\text{mod } 8)$ y $17 \equiv 1 (\text{mod } 8)$, 2 es residuo cuadrático módulo 7 y módulo 17. De hecho, $3^3 \equiv 2 (\text{mod } 7)$ y $6^2 \equiv 2 (\text{mod } 17)$.

Por otro lado, como $19 \equiv 3 (\text{mod } 8)$ y $5 \equiv 5 (\text{mod } 8)$, resulta que 2 es no-residuo cuadrático módulo 19 y módulo 5.

Ejemplo 6. Calculemos el símbolo de Legendre de 18 módulo 43. Tenemos que $18 = 3^2 \cdot 2$ y $43 = 8(5) + 3$, así que

$$(18/43) = ((3^2 \cdot 2)/43) = (3/43)^2(2/43) = 1 \cdot (-1) = -1.$$

Se sigue que 18 es no-residuo cuadrático módulo 43.

Ejemplo 7. En este ejemplo encontramos el valor del símbolo de $(-72/131)$. Observemos que $131 = 128 + 3 = 8(16) + 3$, así que $(2/121) = -1$. Por otro lado

$$(-1/131) = (-1)^{(131-1)/2} = (-1)^{65} = -1.$$

Luego,

$$(-72/131) = (((-1)3^2 2^2 2)/131) = (-1/131)(3/131)^2(2/131)^2(2/131) = (-1)(-1) = 1.$$

Vemos así que -72 es residuo cuadrático módulo 131.

2.4. La ley de reciprocidad cuadrática

Ya sabemos cómo determinar $(-1/p)$ y $(2/p)$. La parte principal de la ley de reciprocidad cuadrática permite relacionar (p/q) con (q/p) cuando p y q son primos impares. A continuación, enunciamos la Ley de reciprocidad cuadrática, y luego iremos abriendo el camino para realizar su demostración.

Teorema 59 (Ley de reciprocidad cuadrática)**.** *Sean p y q primos impares distintos. Entonces,*

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

2.4.1. La función $f(z) = e^{2\pi iz} - e^{-2\pi iz}$

Sea z un número complejo. Sabemos que $\operatorname{sen} z = \frac{e^{iz}-e^{-iz}}{2i}$; utilizaremos esto para definir una función de esta manera, $e^{iz} - e^{-iz} = 2i \operatorname{sen} z$. Consideremos la función compleja

$$f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \operatorname{sen}(2\pi z). \tag{2.4.1}$$

Proposición 60. *Sea z un número complejo. La función f definida en* (2.4.1) *tiene las siguientes propiedades:*

1. $f(z+1) = f(z)$;
2. f *es impar;*
3. *si r es un número real y $2r \notin \mathbb{Z}$, entonces $f(r) \neq 0$.*

Demostración. En efecto, tenemos:

1. $f(z+1) = e^{2\pi i(z+1)} - e^{-2\pi i(z+1)} = e^{2\pi iz}e^{2\pi i} - e^{-2\pi iz}e^{-2\pi i} = e^{2\pi iz} - e^{-2\pi iz} = f(z)$.
2. $f(-z) = e^{2\pi i(-z)} - e^{-2\pi i(-z)} = e^{-2\pi iz} - e^{2\pi iz} = -(e^{2\pi iz} - e^{-2\pi iz}) = -f(z)$.
3. Por último, por contrarrecíproco supongamos que $f(r) = 0$. Entonces tenemos que $\operatorname{sen}(2\pi r) = 0$. Así que, $2\pi r = \pi k$, para algún entero k, de donde $2r = k \in \mathbb{Z}$. □

De la parte 1 de la Proposición 60 se deduce que si $j \in \mathbb{Z}$, entonces $f(z+j) = f(z)$ para todo $z \in \mathbb{C}$.

A continuación, probaremos una identidad importante que involucra a $f(z)$, pero antes necesitamos el siguiente lema algebraico.

Lema 61. *Sea $n \in \mathbb{Z}$. Si $n > 0$ es impar, entonces*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y), \quad \textit{donde} \quad \zeta = e^{2\pi i/n}.$$

Demostración. Inicialmente supongamos que $y = 1$. Ahora, note que $x^n - 1 = 0$ si y solamente si, x es una raíz $n-$ésima de la unidad, esto es, $x = \zeta^k$, donde $k \in \{0, 1, \ldots, n-1\}$. Así

$$x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1}) = \prod_{k=0}^{n-1}(x-\zeta^k). \tag{2.4.2}$$

Por otro lado,

$$\prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k}) = \prod_{k=0}^{n-1}\zeta^k(x-\zeta^{-2k}) = \zeta^{0+1+2+\cdots+n-1}\prod_{0}^{n-1}(x-\zeta^{-2k}). \tag{2.4.3}$$

Ahora,$\zeta^{0+1+2+\cdots+n-1} = \zeta^{n(n-1)/2} = \left(\zeta^n\right)^{(n-1)/2} = 1$. Además

$$\{\zeta^k : k \in \{0, 1, \ldots, n-1\}\} = \{\zeta^{-2k} : k \in \{0, 1, \ldots, n-1\}\}.$$

Luego, (2.4.3) se transforma en lo siguiente:

$$\prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k}) = \prod_{k=0}^{n-1}(x-\zeta^{-2k}) = \prod_{k=0}^{n-1}(x-\zeta^k). \tag{2.4.4}$$

De (2.4.2) y (2.4.4), concluimos que $x^n - 1 = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k})$.

Ahora, sea $z = \frac{x}{y}$, por lo anterior

$$z^n - 1 = \left(\frac{x}{y}\right)^n - 1 = \prod_{k=0}^{n-1}\left(\zeta^k\left(\frac{x}{y}\right) - \zeta^{-k}\right).$$

Así, multiplicando en la igualdad anterior por y^n tenemos que

$$\begin{aligned} x^n - y^n &= y^n \prod_{k=0}^{n-1}\left(\zeta^k\frac{x}{y} - \zeta^{-k}\right) \\ &= \left(\zeta^0 x - \zeta^{-0}y\right)\cdots\left(\zeta^{n-1}x - \zeta^{-(n-1)}y\right) \\ &= \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k}y). \end{aligned}$$

□

Proposición 62. *Si n es un entero positivo impar, entonces*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right) f\left(z-\frac{k}{n}\right).$$

Demostración. En efecto,

$$f(nz) = e^{2\pi izn} - e^{-2\pi izn} = (e^{2\pi iz})^n - (e^{-2\pi iz})^n,$$

tomando $x = e^{2\pi iz}$ e $y = e^{-2\pi iz}$ en el Lema 61, obtenemos que para $\zeta = e^{2\pi i/n}$

$$\begin{aligned} f(nz) &= \prod_{k=0}^{n-1} (\zeta^k e^{2\pi iz} - \zeta^{-k} e^{-2\pi iz}) \\ &= \prod_{k=0}^{n-1} (e^{2k\pi i/n} e^{2\pi iz} - e^{2k\pi i/n} e^{-2\pi iz}) \\ &= \prod_{k=0}^{n-1} (e^{2\pi i(z+k/n)} - e^{-2\pi i(z+k/n)}) \\ &= \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right) \\ &= f(z) \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right). \end{aligned} \tag{2.4.5}$$

De la parte (1) de 60 se sigue que $f(z+\frac{k}{n}) = f(z+\frac{k}{n}-1) = f(z+\frac{k-n}{n}) = f(z-\frac{n-k}{n})$,

$$\begin{aligned} \prod_{k=1}^{(n-1)/2} f\left(z - \frac{k}{n}\right) &= f\left(z - \frac{1}{n}\right) \cdots f\left(z - \frac{\frac{n-1}{2} - 1}{n}\right) f\left(z - \frac{\frac{n-1}{2}}{n}\right) \\ &= f\left(z - \frac{1}{n}\right) \cdots f\left(z - \frac{1}{2} + \frac{3}{2n}\right) f\left(z - \frac{1}{2} + \frac{1}{2n}\right). \end{aligned}$$

Además

$$\begin{aligned} \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) &= \prod_{k=(n+1)/2}^{n-1} f\left(z - \frac{n-k}{n}\right) \\ &= f\left(z - \frac{n - \frac{n+1}{2}}{n}\right) f\left(z - \frac{n - \frac{n+1}{2} + 1}{n}\right) \cdots f\left(z - \frac{n - n + 1}{n}\right) \\ &= f\left(z - \frac{1}{2} + \frac{1}{2n}\right) f\left(z - \frac{1}{2} + \frac{3}{2n}\right) \cdots f\left(z - \frac{1}{n}\right). \end{aligned}$$

De lo anterior y (2.4.5), obtenemos que

$$\begin{aligned} \frac{f(nz)}{f(z)} &= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) \\ &= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=1}^{(n-1)/2} f\left(z - \frac{k}{n}\right) \\ &= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right). \end{aligned}$$

□

Proposición 63. *Si p es un primo impar, a un entero y $p \nmid a$, entonces*

$$\prod_{r=1}^{(p-1)/2} f\left(\frac{ra}{p}\right) = (a/p) \prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p}\right).$$

Demostración. Sea m_r el residuo mínimo de ra módulo p, donde r es un elemento del conjunto $\{1, 2, \ldots, (p-1)/2\}$. Así, $ra \equiv m_r \pmod{p}$. Luego, para cada r, existe un entero j tal que $ra = m_r + pj$, de donde, $\dfrac{ra}{p} = \dfrac{m_r}{p} + j$. Entonces

$$f\left(\frac{ra}{p}\right) = f\left(\frac{m_r}{p} + j\right) = e^{2\pi i m_r/p} e^{2\pi ij} - e^{-2\pi i m_r/p} e^{-2\pi ij} = f\left(\frac{m_r}{p}\right).$$

Multiplicando todas éstas igualdades cuando r recorre $\{1, 2, \ldots, (p-1)/2\}$, y usando el hecho de que f es impar obtenemos lo siguiente

$$\begin{aligned}
\prod_{r=1}^{(p-1)/2} f\left(\frac{ra}{p}\right) &= \prod_{r=1}^{(p-1)/2} f\left(\frac{m_r}{p}\right) \\
&= \prod_{r=1, m_r>0}^{(p-1)/2} f\left(\frac{m_r}{p}\right) \prod_{r=1, m_r<0}^{(p-1)/2} f\left(\frac{m_r}{p}\right) \\
&= \prod_{r=1, m_r>0}^{(p-1)/2} f\left(\frac{|m_r|}{p}\right) \prod_{r=1, m_r<0}^{(p-1)/2} -f\left(\frac{|m_r|}{p}\right) \\
&= (-1)^{\mu(a,p)} \prod_{r=1, m_r>0}^{(p-1)/2} f\left(\frac{|m_r|}{p}\right) \prod_{r=1, m_r<0}^{(p-1)/2} f\left(\frac{|m_r|}{p}\right) \\
&= (a/p) \prod_{r=1}^{(p-1)/2} f\left(\frac{|m_r|}{p}\right) \\
&= (a/p) \prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p}\right),
\end{aligned}$$

donde la igualdad de los productos en el último paso se da gracias a la igualdad de conjuntos $\{|m_r| : r \in \{1, 2, \ldots, (p-1)/2\}\} = \{1, 2, \ldots, (p-1)/2\}$. □

Observamos a partir de la Proposición 63 que

$$(a/p) = \frac{\prod_{r=1}^{(p-1)/2} f\left(\frac{ra}{p}\right)}{\prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p}\right)}.$$

2.4.2. Demostración de la ley de reciprocidad cuadrática

Ahora estamos en posición de realizar la prueba de la ley de reciprocidad cuadrática. Sean p y q primos impares. Usando la Proposición 63 obtenemos que,

$$(q/p) = \frac{\prod_{r=1}^{(p-1)/2} f\left(\frac{rq}{p}\right)}{\prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p}\right)} = \frac{f\left(\frac{q}{p}\right) f\left(\frac{2q}{p}\right) \cdots f\left(\frac{(p-1)q}{2p}\right)}{f\left(\frac{1}{p}\right) f\left(\frac{2}{p}\right) \cdots f\left(\frac{p-1}{2p}\right)} = \prod_{r=1}^{(p-1)/2} \frac{f\left(\frac{rq}{p}\right)}{f\left(\frac{r}{p}\right)}. \tag{2.4.6}$$

Por la Proposición 62 tenemos

$$\frac{f(q(\frac{r}{p}))}{f(\frac{r}{p})} = \prod_{k=1}^{(q-1)/2} f\left(\frac{r}{p} + \frac{k}{q}\right) f\left(\frac{r}{p} - \frac{k}{q}\right). \tag{2.4.7}$$

Se sigue de (2.4.7) y (2.4.6) que

$$(q/p) = \prod_{r=1}^{(p-1)/2} \prod_{k=1}^{(q-1)/2} f\left(\frac{r}{p} + \frac{k}{q}\right) f\left(\frac{r}{p} - \frac{k}{q}\right) = \prod_{k=1}^{(q-1)/2} \prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p} + \frac{k}{q}\right) f\left(\frac{r}{p} - \frac{k}{q}\right). \tag{2.4.8}$$

Análogamente,

$$(p/q) = \prod_{k=1}^{(q-1)/2} \frac{f\left(\frac{kp}{q}\right)}{f\left(\frac{k}{q}\right)} = \prod_{k=1}^{(q-1)/2} \prod_{r=1}^{(p-1)/2} f\left(\frac{k}{q} + \frac{r}{p}\right) f\left(\frac{k}{q} - \frac{r}{p}\right). \tag{2.4.9}$$

Ahora, como f es impar se tiene $f\left(\frac{r}{q} - \frac{k}{p}\right) = -f\left(\frac{k}{p} - \frac{r}{q}\right)$, y dividiendo (2.4.8) entre (2.4.9) resulta lo siguiente:

$$\frac{(q/p)}{(p/q)} = \frac{\prod_{k=1}^{(q-1)/2} \prod_{r=1}^{(p-1)/2} f\left(\frac{r}{p} + \frac{k}{q}\right) f\left(\frac{r}{p} - \frac{k}{q}\right)}{\prod_{k=1}^{(q-1)/2} \prod_{r=1}^{(p-1)/2} f\left(\frac{k}{q} + \frac{r}{p}\right) f\left(\frac{k}{q} - \frac{r}{p}\right)} = \prod_{k=1}^{(q-1)/2} \prod_{r=1}^{(p-1)/2} (-1) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Finalmente tenemos

$$(q/p)(p/q) = (p/q)^2(-1)^{(p-1)(q-1)/4} = (-1)^{(p-1)(q-1)/4}.$$

Esto termina la prueba de la ley de reciprocidad cuadrática. En el siguiente resultado hacemos una reinterpretación de la ley de reciprocidad cuadrática.

Corolario 64. *Sean p y q primos impares. Entonces*

1. $(p/q) = (q/p)$ *si y solo si* $p \equiv 1 \pmod 4$ *o si* $q \equiv 1 \pmod 4$*;*

2. $(p/q) = -(q/p)$ *si y solo si* $p \equiv 3 \pmod 4$ *y* $q \equiv 3 \pmod 4$.

Demostración. Note que $(p-1)(q-1)/4$ es par si y solamente si p o q es de la forma $4k+1$. En este caso, por la ley de reciprocidad cuadrática, $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4} = (-1)^{(4k)(q-1)/4} = 1$, y multiplicando en ambos lados por (q/p) obtenemos que $(p/q) = (q/p)$.

Ahora, si p y q son ambos de la forma $4k+3$, entonces $(p-1)(q-1)/4$ es impar. Entonces $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4} = -1$ y por lo tanto $(p/q) = -(q/p)$. □

Tenemos la siguiente equivalencia de la ley de reciprocidad cuadrática.

Proposición 65. *Sean* p *y* q *primos impares distintos y* $a \geq 1$ *entero. Entonces, las siguientes afirmaciones son equivalentes:*

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

2. Si $p = q + 4a$ *y* $p \nmid a$, *entonces* $(a/p) = (a/q)$.

Demostración. Supongamos que se cumple 1. Como $4a - p \equiv 4a \pmod p$, por la parte 3. de la Proposición 49 tenemos que $(4a/p) = ((4a-p)/p)$. Luego

$$(a/p) = (2/p)^2(a/p) = (4a/p) = ((4a-p)/p) = (-q/p) = (-1/p)(q/p) = (-1)^{(p-1)/2}(q/p).$$

En la última igualdad usamos el Corolario 53. En forma análoga, puesto que $4a+q \equiv 4a \pmod q$, se tiene que $((2a+q)/q) = (4a/q)$ y entonces

$$(a/q) = (2/q)^2(a/q) = (4a/q) = ((4a+q)/q) = (p/q). \tag{2.4.10}$$

Por hipótesis,

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4},$$

así que

$$(q/p) = (p/q)^2(q/p) = (p/q)(-1)^{(p-1)(q-1)/4}. \tag{2.4.11}$$

Luego,

$$\begin{aligned}(a/p) = (-1)^{(p-1)/2}(q/p) &= (-1)^{(p-1)/2}(p/q)(-1)^{(p-1)(q-1)/4} \\ &= (p/q)(-1)^{((p-1)(q-1)/4+(p-1)/2)} \\ &= (p/q)(-1)^{(2(p-1)+(p-1)(q-1))/4} \\ &= (p/q)(-1)^{(p-1)(q+1)/4}.\end{aligned}$$

Afirmamos que $(p-1)(q+1)/4$ es par. Observemos que

$$(p-1)(q+1)/4 = (q+4a-1)(q+1)/4.$$

Siendo q primo, tenemos dos casos que consideramos a continuación. Primero, si $q = 4k+1$ para algún $k \in \mathbb{Z}$, entonces

$$\begin{aligned}\frac{(q+4a-1)(q+1)}{4} &= \frac{(4k+1+4a-1)(4k+1+1)}{4} \\ &= \frac{4(k+a)(4k+2)}{4} \\ &= 2(2k+1)(k+a).\end{aligned}$$

Ahora, si $q = 4k+3$ para algún $k \in \mathbb{Z}$, entonces

$$\frac{(q+4a-1)(q+1)}{4} = \frac{(4k+3+4a-1)(4k+3+1)}{4} = 2(2k+2a+1)(k+1).$$

Luego obtenemos que

$$(a/p) = (p/q)(-1)^{(p-1)(q+1)/4} = (p/q) = (a/q). \tag{2.4.12}$$

De (2.4.10) y (2.4.12) obtenemos $(a/q) = (p/q) = (a/p)$.

Ahora probemos que 2 implica 1. Notemos que $p > q$. Observemos también que

$$(p/q) = ((q+4a)/q) = (4a/q) = (4/q)(a/q) = (2/q)^2(a/q) = (a/q)$$

y como $p = q+4a$, $p-q = 4a$ y $p-q \equiv -q \pmod{p}$, se sigue que

$$(p/q) = (a/q) = (a/p) = (4a/p) = ((p-q)/p) = (-q/p) = (-1/p)(q/p) = (-1)^{(p-1)/2}(q/p).$$

Ahora, para el primo p tenemos las siguientes dos posibilidades. Primero, si $p = 4k+1$ para algún $k \in \mathbb{Z}$, entonces

$$(p/q) = (q/p)$$

y así

$$(p/q)(q/p) = 1 = (-1)^{4k(q-1)/2} = (-1)^{(p-1)(q-1)/4}.$$

Por otro lado, si $p = 4k + 3$ para algún entero k, entonces

$$(p/q) = -(q/p).$$

Luego

$$(p/q)(q/p) = -1 = (-1)^{(2k+1)(q-1)/2} = (-1)^{(p-1)(q-1)/4}.$$

Esto termina la prueba. □

Finalizamos esta sección con el siguiente ejemplo.

Ejemplo 8. Calculemos el símbolo de Legendre (1234/4567). Como $1234 = 2 \cdot 617$, tenemos que $(1234/4567) = (2/4567) \cdot (617/4567)$. Note que,

$$4567 = 4560 + 7 = 8(570) + 7,$$

es decir, 4567 es un primo de la forma $8k + 7$, así, $(2/4567) = 1$. Tenemos así que $(1234/4567) = (617/4567)$.

Como 4567 y 617 son primos, por la Ley de reciprocidad cuadrática tenemos

$$(617/4567)(4567/617) = (-1)^{((617-1)/2)((4567-1)/2)} = (-1)^{(308)(2283)} = 1,$$

por lo que $(617/4567) = (4567/617)$. Observemos que $4567 \equiv 248 \pmod{617}$, de donde $(4567/617) = (248/617) = (2^3 \cdot 31/617)$

$$(4567/617) = ((2^3 \cdot 31)/617) = (2/617)^3(31/617).$$

Como $617 = 8(77)+1$, resulta que $(2/617) = 1$. Así $(4567/617) = (31/617)$. Como 31 y 617 son primos, nuevamente por la ley de reciprocidad cuadrática tenemos

$$(31/617)(617/31) = (-1)^{((31-1)/2)((617-1)/2)} = (-1)^{(15)(308)} = 1.$$

Luego, $(31/617) = (617/31)$. Puesto que $617 \equiv 28 \pmod{31}$, obtenemos por la Proposición 49 que $(617/31) = (28/31)$. Ahora

$$(28/31) = (7/31)(4/31) = (7/31)(2/31)^2 = (7/31).$$

Otra vez, 31 y 7 son primos, así que por la ley de reciprocidad cuadrática,

$$(7/31)(31/7) = (-1)^{((31-1)/2)((7-1)/2)} = (-1)^{(15)(3)} = -1,$$

obteniendo así que $(7/31) = -(31/7)$. Pero $31 \equiv 3 \pmod 7$, así que $(31/7) = (3/7)$. Continuamos aplicando ley de reciprocidad cuadrática a 3 y 7, como sigue:

$$(3/7)(7/3) = (-1)^{((3-1)/2)((7-1)/2)} = (-1)^{(1)(3)} = -1,$$

por lo que $(3/7) = -(7/3)$. Como $7 \equiv 1 \pmod 3$, se sigue que $(7/3) = (1/3)$ y como $1^2 \equiv 1 \pmod 3$, resulta que $(1/3) = 1$. Finalmente, unimos todo lo calculado:

$$(1234/4567) = (617/4567) = (31/617) = (7/31) = -(3/7) = -\left(-(7/3)\right) = (1/3) = 1.$$

Capítulo 3

Sumas de cuadrados en los enteros

En este capítulo estudiamos el problema de caracterizar a los enteros que se pueden representar como suma de dos cuadrados. También, estudiamos la función $r(n)$, que determina de cuántas formas se puede representar un entero n como suma de dos cuadrados y realizamos algunos ejemplos.

3.1. Representación de enteros como suma de dos cuadrados

En esta sección presentamos la caracterización de los enteros n tales que la ecuación diofántica:

$$n = x^2 + y^2, \tag{3.1.1}$$

tiene solución para $x, y \in \mathbb{Z}$. Para $n = 0$, la única solución de (3.1.1) es $x = 0, y = 0$. Además, (3.1.1) no tiene solución si $n < 0$. Geométricamente, para $n > 0$ fijo, la ecuación (3.1.1) representa una circunferencia centrada en $(0, 0) \in \mathbb{R}^2$ y de radio $\sqrt{n}$. Así, n puede ser representado como suma de dos cuadrados de enteros si y solo si existe un punto de coordenadas enteras (x, y) en tal circunferencia. Nótese que si el punto (x, y) está en el primer cuadrante y satisface la ecuación (3.1.1), entonces $(-x, y), (x, -y)$ y $(-x, -y)$ también son soluciones de la ecuación (3.1.1), y ya que las soluciones solo difieren en los signos, esas soluciones no son esencialmente distintas.

Claramente, no todos los círculos de radio n contienen puntos de coordenadas enteras.

El resultado principal de esta sección es el siguiente:

Teorema 66. *Sea n un entero con forma estándar $n = p_1^{a_1} \cdots p_r^{a_r}$. Entonces n puede expresarse como suma de dos cuadrados si y solo si para cada primo p_i de la forma $4k+3$, el exponente a_i es par.*

Todo entero (no negativo) n se puede descomponer como producto de un cuadrado perfecto y un entero libre de cuadrado. Otra manera de expresar el Teorema 66 es diciendo que n puede expresarse como suma de dos cuadrados si y solo si en la parte libre de cuadrado de n no aparecen primos de la forma $4k+3$.

Para lograr la demostración del Teorema 66, probaremos algunos resultados intermedios, que conforman partes importantes de su demostración. De hecho, el siguiente resultado es la prueba de la parte "solo si" del teorema.

Lema 67. *Sean n y k enteros con $n > 0$, y p un primo impar de la forma $4k+3$. Si n es divisible por p y n es suma de dos cuadrados, entonces la potencia de p en la forma estándar de n es par.*

Demostración. Sea $n = x^2 + y^2$ para algunos enteros x e y. Note que si $p \mid n$, entonces $n \equiv 0 \pmod{p}$. Se sigue que $x^2 \equiv -y^2 \pmod{p}$. Afirmamos que $x \equiv y \equiv 0 \pmod{p}$. En efecto, por reducción al absurdo asumamos que $p \nmid y$. Como $\mathbb{Z}_p^*$ es un grupo multiplicativo, existe el inverso de y módulo p, digamos que este es w. Esto quiere decir que $yw \equiv 1 \pmod{p}$. Multiplicando a ambos lados de la congruencia $x^2 \equiv -y^2 \pmod{p}$ por w^2 obtenemos que

$$(xw)^2 \equiv -(wy)^2 (\text{mod } p) \quad y \quad -(wy)^2 \equiv -1 \pmod{p},$$

lo que quiere decir que -1 es residuo cuadrático módulo p, pero esto contradice el Corolario 54 puesto que p es un primo de la forma $4k+3$. Esta contradicción muestra que $y \equiv 0 \pmod{p}$. En forma análoga se tiene que $x \equiv 0 \pmod{p}$.

Ahora, puesto que $p \mid x$ y $p \mid y$, se sigue que $p^2 \mid x^2$ y $p^2 \mid y^2$ y por lo tanto $p^2 \mid x^2 + y^2$, es decir, $p^2 \mid n$.

Luego, existe un entero positivo d_1 tal que $n = p^2 d_1$. Si $p \nmid d_1$, entonces la potencia de p en la factorización de n es 2. Por otro, lado supongamos que $p \mid d_1$. Tenemos que $x = px_1$ e $y = py_1$ para algunos enteros x_1 e y_1. Luego,

$$p^2 d_1 = n = x^2 + y^2 = p^2 x_1^2 + p^2 y_1^2,$$

de donde $d_1 = x_1^2 + y_1^2$. Tenemos, por lo tanto, que d_1 es suma de dos cuadrados y $p \mid d_1$. Por un argumento similar al de arriba concluimos que $p \mid x_1$, $p \mid y_1$ y que $d_1 = p^2 d_2$ para algún entero positivo d_2. Así tenemos que $n = p^4 d_2$.

Continuando con este proceso, después de un número finito r de pasos tendremos una representación de n en la forma $n = p^{2r} d_r$ donde $p \nmid d_r$. Esto muestra que la potencia de p en la forma estándar de n es par. □

Lema 68. *Sean p y q primos. Entonces*

1. *Si $p = 4j + 1$ y $q = 4k + 1$ para algunos enteros j y k, entonces $pq = 4m + 1$ para algún entero m.*

2. *Si $p = 4j + 1$ y $q = 4k + 3$, para algunos enteros j y k, entonces $pq = 4m + 3$ para algún entero m.*

3. *Si ambos p y q son de la forma $4k + 3$, entonces pq es de la forma $4k + 1$.*

Demostración.

1. Supongamos que p y q son ambos de la forma $4k + 1$, luego, $pq = (4j+1)(4k+1) = 16jk + 4j + 4k + 1 = 4(4jk + j + k) + 1 = 4m + 1$, para $m := 4jk + j + j \in \mathbb{Z}$.

2. Si $p = 4j+1$ y $q = 4k+3$, entonces $pq = (4j+1)(4k+3) = 16jk+12j+4k+3$, así $pq = 4(4jk + 3j + k) + 1 = 4m + 1$, donde $m := 4jk + 3j + k \in \mathbb{Z}$.

3. Supongamos que p y q son de la forma $4j+3$ y $4k+3$ respectivamente, entonces $pq = (4j + 3)(4k + 3) = 16jk + 12j + 12k + 9 = 16jk + 12k + 12k + 8 + 1$. Así $pq = 4(4jk + 3j + 3k + 2) + 1 = 4m + 1$, donde $m := 4jk + 3j + 3k + 2 \in \mathbb{Z}$. □

Corolario 69. *Ningún número de la forma $4k + 3$ puede representarse como suma de dos cuadrados.*

Demostración. Sea n un entero de la forma $4k+3$, para algún entero k. Supongamos, por reducción al absurdo que n puede representarse como suma de dos cuadrados. Por la observación del Teorema 66 podemos descomponer a n como producto de un entero cuadrado perfecto y un entero libre de cuadrado, digamos que $n = (p_1 p_2 \cdots p_s)(p_{s+1}^{a_{s+1}} \cdots p_r^{a_r})^2$, donde los p_i son primos distintos para $i = 1, 2, \ldots, s$ y $a_i > 0$ para cada i y además, por el Lema 67, en la parte libre de cuadrados de n no aparecen primos de la forma $4k+3$. Note que $p_1 = 4k_1 + 3$ y $p_2 = 4k_2 + 3$, entonces, por la tercera parte del lema anterior, $p_1 p_2 = 4k' + 1$. Ahora, como p_3 es libre de cuadrado, también es de la forma $4k_3 + 1$ y ya que $p_1 p_2$ es de la forma $4k' + 1$, se sigue que $p_1 p_2 p_3$ es de la forma $4k'' + 1$. Así mostramos que $p_1 p_2 \cdots p_s$ es de la forma $4k+1$. Por otro lado, si $p_i^{a_i}$ de la forma $4k+1$, el cuadrado de $p_i^{a_i}$ también tiene la forma $4k+1$; si algún $p_{i_0}^{a_{i_0}}$ es de la forma $4k_{i_0} + 3$, entonces

$$(p_{i_0}^{a_{i_0}})^2 = (4k_{i_0} + 3)(4k_{i_0} + 3) = 16k_{i_0}^2 + 24k_{i_0} + 9 = 4(4k_{i_0}^2 + 6k_{i_0} + 2) + 1,$$

así que el cuadrado de los $p_i^{a_i}$ que son de la forma $4k+3$ también es de la forma $4k+1$. Por lo tanto, $n = (p_1 p_2 \cdots p_s)(p_{s+1}^{a_{s+1}} \cdots p_r^{a_r})^2$ es la forma $4k+1$, lo cual es absurdo, porque n es de la forma $4k+3$. □

Corolario 70. *Ningún número primo p de la forma $4k+3$ es representable como suma de dos cuadrados.*

Demostración. Supongamos por reducción al absurdo que $p = x^2 + y^2$ para algunos enteros x e y. En el lema 67 tomamos $n = p$, así que se concluye que $p^2 \mid p$, lo que es una contradicción. □

Los resultados que siguen prueban la parte "si" del Teorema 66.

Lema 71. *Si n y m son enteros que se pueden representar como suma de dos cuadrados, entonces el producto nm también.*

Demostración. Si $n = a^2 + b^2$ y $m = c^2 + d^2$, entonces

$$\begin{aligned}(ac + bd)^2 + (ad - bc)^2 &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= nm.\end{aligned}$$

□

La siguiente es una consecuencia inmediata por inducción del Lema 71.

Corolario 72. *El producto de un número finito de enteros que se pueden representar como suma de dos cuadrados también se puede representar como suma de dos cuadrados.*

Asumamos que n es un entero positivo y que en la forma estándar de n los primos de la forma $4k + 3$ aparecen con exponente par. Observemos que si 2 divide a n, entonces la potencia de 2 que divide a n puede expresarse como suma de dos cuadrados. En efecto, digamos que la potencia de 2 que divide a n es 2^r. Si r es par, entonces

$$2^r = \left(2^{r/2}\right)^2 + 0^2,$$

mientras que si r es impar, entonces

$$2^r = 2^{r-1} + 2^{r-1} = \left(2^{(r-1)/2}\right)^2 + \left(2^{(r-1)/2}\right)^2.$$

Si p es un primo de la forma $4k + 3$ que divide a n, entonces la potencia de p que aparece en la forma estándar de n es par, digamos p^s donde s es par. Tenemos que $p^s = \left(p^{s/2}\right)^2 + 0^2$.

Para terminar la prueba del Teorema 66, basta mostrar que todo primo de la forma $4k + 1$ que divide a n se puede expresar como suma de dos cuadrados, pues tendríamos que n es producto de enteros que se pueden expresar como suma de dos cuadrados, así que por el Corolario 72, n también se expresaría como suma de dos cuadrados.

Lema 73. *Todo primo de la forma $4k + 1$ es suma de dos cuadrados.*

Demostración. Sea p un primo de la forma $4k+1$. Luego, por el Corolario 54, existe $x_0 \in \{0, 1, \ldots, p-1\}$ tal que $x_0^2 \equiv -1 \pmod{p}$. Ahora, sea $m = \lfloor \sqrt{p} \rfloor$, así que $m < \sqrt{p} < m+1$ pues al ser p primo se tiene que $\sqrt{p}$ es irracional. Por lo que $m^2 < p < (m+1)^2$. Consideremos los números de la forma $a - bx_0$ donde los enteros a y b son tales que $0 \leq a, b \leq m$. Note que si ponemos a variar a a y fijamos b, tenemos a los $m+1$ números $-bx_0, 1-bx_0, 2-bx_0, \ldots, m-bx_0$ y de manera similar si fijamos a y ponemos a variar a b tenemos a los $m+1$ números $a, a-x_0, a-2x_0, \ldots, a-mx_0$, de modo que en total tenemos $(m+1)^2$ números $a - bx_0$. Ahora, como $p < (m+1)^2$, deben existir a_1, b_1, a_2, b_2 con las condiciones anteriores, tales que $(a_1, b_1) \neq (a_2, b_2)$ y $a_1 - b_1x_0 \equiv a_2 - b_2x_0 \pmod{p}$, así $a_1 - a_2 \equiv (b_1 - b_2)x_0 \pmod{p}$. Sean $a = a_1 - a_2$ y $b = b_1 - b_2$, note que a y b no pueden ser ambos cero, pues de ser así, tendríamos que $a_1 = a_2, b_1 = b_2$ y en consecuencia $(a_1, b_1) = (a_2, b_2)$ lo cual contradice lo supuesto. Además ya que $0 \leq a_1 \leq m$ y $0 \leq a_2 \leq m$, tenemos que $-m \leq a_2 < 0$ y en consecuencia $-m \leq a_1 - a_2 \leq m$, por lo tanto $|a| \leq m$ y de manera similar $|b| \leq m$. De esta manera $a \equiv bx_0 \pmod{p}$, de donde $a^2 \equiv b^2x_0^2 \pmod{p}$ y como $x_0^2 \equiv -1 \pmod{p}$, obtenemos que $a^2 \equiv -b^2 \pmod{p}$, por lo tanto $p \mid (a^2+b^2)$, así $a^2+b^2 = jp$ para algún entero positivo j. Por otro lado, como $|a| \leq m$ y $|b| \leq m$, obtenemos que $a^2 \leq m^2$ y $b^2 \leq m^2$, de manera que $a^2 + b^2 \leq 2m^2 < 2p$, donde $jp = a^2 + b^2 < 2p$. Así que necesariamente $j = 1$ y $a^2 + b^2 = p$. □

Ahora veamos algunos ejemplos. Si n es un entero positivo con forma estándar $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, entonces, para que n pueda ser representado como suma de dos cuadrados es suficiente y necesario que los p_i que sean de la forma $4k+3$ tengan potencia par, y tenemos el siguiente algoritmo para determinar una de tales representaciones:

Algoritmo para representar n como suma de dos cuadrado:

Entrada: n entero positivo.

- Represente a n como producto de un cuadrado perfecto y un entero libre de cuadrado: $n = cl$, donde c es una cuadrado perfecto y l es libre de cuadrado.
- Verifique que l no es divisible por ningún primo de la forma $4k+3$. En caso

contrario, n no se representa como suma de dos cuadrados.

- Represente cada primo que divide a l como una suma de dos cuadrados.
- Use repetidas veces el Lema 71 para hallar la representación de n como suma de dos cuadrados.

Salida: $n = a^2 + b^2$.

Ejemplo 9. Consideremos el entero $n = 16200$. La descomposición estándar de n es $n = 2^3 3^4 5^2$, y de aquí obtenemos

$$n = (2 \cdot 3^2 \cdot 5)^2 \cdot 2 = 90^2 \cdot 2.$$

La parte libre de cuadrado de n es $l = 2$, y observamos que no es divisible por ningún primo de la forma $4k + 3$. Además, $2 = 1^2 + 1^2$. Usando el Lema 71 obtenemos que

$$n = 90^2(1^2 + 1^2) = (90^2 + 0^2)(1^2 + 1^2) = (90 - 0)^2 + (90 + 0)^2 = 90^2 + 90^2.$$

Otra forma en la que podemos encontrar una representación de n como suma de dos cuadrados es la siguiente:

$$\begin{aligned} n = 2^3 3^4 5^2 &= (2^2 + 2^2)(3^4 + 0^2)(4^2 + 3^2) = (18^2 + 18^2)(4^2 + 3^2) \\ &= (18 \cdot 4 - 18 \cdot 3)^2 + (18 \cdot 3 + 18 \cdot 4)^2 \\ &= 18^2 + 126^2 \end{aligned}$$

Ejemplo 10. Consideremos $n = 26741 = 11^2 \cdot 13 \cdot 17$. La parte libre de cuadrado de n es $l = 13 \cdot 17$; 13 y 17 son primos de la forma $4k + 1$, así que n se puede representar como suma de dos cuadrados. Ahora, $13 = 2^2 + 3^2$ y $17 = 1^2 + 4^2$, así que

$$\begin{aligned} n = 11^2 \cdot 13 \cdot 17 &= 11^2 \cdot (2^2 + 3^2) \cdot (1^2 + 4^2) = 11^2 \cdot [(2 - 12)^2 + (8 + 3)^2] \\ &= 11^2 \cdot [10^2 + 11^2] \\ &= 110^2 + 121^2. \end{aligned}$$

Ejemplo 11. Consideremos $n = 61773872875$. Descomponiendo a n en producto de potencias de primos, tenemos que $n = 5^3 \cdot 13^5 \cdot 11^3$, y observamos que el primo 11 que es de la forma $4k + 3$ aparece con potencia 3. Por el Teorema 66 se sigue que n no se puede representar como suma de dos cuadrados.

En los ejemplos anteriores observamos que es necesario conocer la forma estándar del entero n que deseamos representar como suma de dos cuadrados. Computacionalmente es costoso determinar la forma estándar de un entero dado n. El siguiente algoritmo en *Python* determina todas las posibles representaciones de un entero n como suma de dos cuadrados de enteros no negativos. Primero definimos una función $r_{pos}(n)$ que calcula las representaciones de n como suma de dos cuadrados de enteros no negativos,

```
   import math


def r_pos(n):#Calcula las representaciones de n como suma de dos
cuadrados de enteros no negativos
  m=round(math.sqrt(n))
  for i in range(m+1):
    for j in range(m+1):
      if n==((i**2)+(j**2)):
        print(i,j)
```

Ahora, definimos el $card_r(n)$ que cuenta de cuantas formas se puede representar n como suma de dos cuadrados de enteros no negativos y cuales son,

```
      def card_r(n):
  L=[]
  m=round(math.sqrt(n))
  for i in range(m+1):
    for j in range(m+1):
      if n==((i**2)+(j**2)):
        L.append((i,j))
      else:
        L=L
  return len(L)

#print(card_r(n))
```

Con este algoritmo podemos determinar de cuántas formas se puede representar un entero como suma de dos cuadrados y cuáles son esas representaciones. En la Tabla 3.1 se refleja lo dicho anteriormente donde $r'(n)$ denota al número de representaciones como suma de dos cuadrados en los enteros positivos y el cero. Observe que algunas de las representaciones de enteros como suma de dos cuadrados no nos esencialmente diferentes, pues únicamente varía el orden. En la sección siguiente tratamos la función $r(n)$ que determina el número de representaciones como suma de dos cuadrados de n.

3.2. La función $r(n)$

De la sección anterior podemos observar que hay enteros que tienen más de una representación en suma de dos cuadrados; por ejemplo $7^2 + 14^2 = 245 = 14^2 + 7^2$. Vamos a considerar representaciones de un entero n como suma de dos cuadrados, a cualquier par de enteros a y b tales que $n = a^2 + b^2$. El orden será contado como

n	$r'(n)$	representaciones como suma de dos cuadrados
245	2	$7^2+14^2,\ 14^2+7^2$
394	2	$13^2+15^2,\ 15^2+13^2$
400	4	$0^2+20^2,\ 12^2+16^2,\ 16^2+12^2,\ 20^2+0^2$
450	3	$3^2+21^2,\ 15^2+15^2,\ 21^2+3^2$
505	4	$8^2+21^2,\ 12^2+19^2,\ 19^2+12^2,\ 21^2+8^2$
640	2	$8^2+24^2,\ 24^2+8^2$
773	2	$17^2+22^2,\ 22^2+17^2$
833	2	$7^2+28^2,\ 28^2+7^2$
976	2	$20^2+24^2,\ 24^2+20^2$
1025	6	$1^2+32^2, 8^2+31^2, 20^2+25^2, 25^2+20^2, 31^2+8^2, 32^2+1^2$
1189	4	$10^2+33^2, 17^2+30^2, 30^2+17^2, 33^2+10^2$
2509	4	$3^2+50^2, 22^2+45^2, 45^2+22^2, 3^2+50^2$
100017	2	$216^2+231^2, 231^1+216^2$

Tabla 3.1: Representación de algunos enteros como suma de dos cuadrados

diferente; por ejemplo, $5=2^2+1^2$ y $5=1^2+2^2$ serán consideradas como diferentes; también tenemos $5=(-1)^2+2^2$, $5=1^2+(-2)^2=(-1)^2+(-2)^2$. Diremos así que 5 tiene al menos 5 diferentes representaciones como suma de dos cuadrados.

Definición 74. Definimos la función $r:\mathbb{Z}^+\cup\{0\}\to\mathbb{Z}^+\cup\{0\}$, como la función que a cada entero no negativo n le asigna el número de representaciones como suma de dos cuadrados.

Ejemplo 12. Podemos representar a 5 como suma de dos cuadrados, como sigue, $5=(1)^2+(2)^2,(-1)^2+(2)^2,(1)^2+(-2)^2,(-1)^2+(-2)^2,(2)^2+(1)^2,(-2)^2+(1)^2$, también $5=(2)^2+(-1)^2,(-2)^2+(-1)^2$, por lo tanto $r(5)=8$.

Ejemplo 13. Sea n un entero de la forma $4k+3$. Luego, por el Corolario 69, n no se puede representar como suma de dos cuadrados. Así que $r(n)=0$.

Definición 75. Sea $n \in \mathbb{Z}^+$. Definimos $\chi(n)$ de la siguiente manera

$$\chi(n) = \begin{cases} 0, & \text{si } n \text{ es par;} \\ (-1)^{(n-1)/2}, & \text{si } n \text{ es impar.} \end{cases}$$

Así, $\chi(n)$ toma los valores $1, 0, -1, 0, 1, \ldots$, para $n = 1, 2, 3, 4, 5, \ldots$.

Lema 76. *La función $\chi(n)$ es completamente multiplicativa.*

Demostración. Sean n y m enteros positivos. Consideremos los siguientes casos:

1. Si m es par o n es par, digamos $m = 2k$, entonces el producto mn es par, por lo que $\chi(mn) = 0$. Además, por definición de χ, tenemos que $\chi(m) = 0$. Así $\chi(mn) = 0 = 0 \cdot \chi(n) = \chi(n)\chi(m)$.

2. Si ambos m y n son impares, entonces el producto mn es impar y por consiguiente existen enteros k_1, k_2 y k_3 tales que $m = 2k_1 + 1$, $n = 2k_2 + 1$ y $mn = 2k_3 + 1$. Tenemos por definición que $\chi(n) = (-1)^{(n-1)/2}$, $\chi(m) = (-1)^{(m-1)/2}$, luego

$$\chi(m)\chi(n) = (-1)^{(m-1)/2}(-1)^{(n-1)/2} = (-1)^{m+n-2} = (-1)^{2k_1-1+2k_2-1-2} = 1 \tag{3.2.1}$$

y por otro lado

$$\chi(mn) = (-1)^{2k_3+1-1} = 1. \tag{3.2.2}$$

Así, de (3.2.1) y (3.2.2) obtenemos que $\chi(mn) = \chi(m)\chi(n)$.

Así, χ es completamente multiplicativa. □

Sea n un entero positivo. Definamos $\delta(n) = \sum_{d|n} \chi(d)$.

Lema 77. *Sea n un entero positivo. Si $n = 2^\alpha N$, donde N es impar, entonces $\delta(n) = \delta(N)$.*

Demostración. Si $n = 2^\alpha N$, donde N es impar. Podemos descomponer a N como sigue, $N = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, donde los p_i's son primos distintos y los a_i's positivos. Por

definición de $\chi, \chi(2) = \chi(2^2) = \cdots = \chi(2^\alpha) = 0$ y

$$\begin{aligned}
\delta(n) &= \sum_{d|n} \chi(d) \\
&= \chi(2) + \cdots + \chi(2^\alpha) + \chi(p_1) + \cdots + \chi(p_1 \cdots p_r) + \chi(p_1^2) + \cdots + \chi(N) \\
&= 0 + \cdots + 0 + \chi(p_1) + \cdots + \chi(p_r) + \chi(p_1^2 p_2) + \cdots + \chi(N) \\
&= \sum_{d|N} \chi(d) \\
&= \delta(N).
\end{aligned}$$

□

Lema 78. $\prod_{i=1}^{r}(1 + x_i + \cdots + x_i^{a_i}) = \sum x_1^{t_1} \cdots x_r^{t_r}$, *donde la suma se toma sobre todas las tuplas* $(t_1, \ldots, t_r)$ *tales que* $0 \leq t_i \leq a_i$ *para* $i = 1, \ldots, r$.

Demostración. Procedamos por inducción sobre r. Si $r = 1$, tenemos que

$$\sum_{t_1=0}^{a_1} x_1^{t_1} = x_1^0 + x_1 + \cdots + x_1^{a_1} = 1 + x_1 + \cdots + x_1^{a_1} = \prod_{i=1}^{1}(1 + x_1 + \cdots + x_1^{a_1}).$$

Supongamos que el resultado se satisface para r y veamos que se cumple para $r + 1$. Luego,

$$\begin{aligned}
\prod_{i=1}^{r+1}(1 + x_i + \cdots + x_i^{a_i}) &= \prod_{i=1}^{r}(1 + x_i + \cdots + x_i^{a_i})(1 + x_{r+1} + \cdots + x_{r+1}^{a_{r+1}}) \\
&= \sum_{\substack{(t_1,\ldots,t_r) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r}} x_1^{t_1} \cdots x_r^{t_r}(1 + x_{r+1} + \cdots + x_{r+1}^{a_{r+1}}) \\
&= \sum_{\substack{(t_1,\ldots,t_r) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r}} x_1^{t_1} \cdots x_r^{t_r} + \cdots + \sum_{\substack{(t_1,\ldots,t_r) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r}} x_1^{t_1} \cdots x_r^{t_r} x_{r+1}^{a_{r+1}} \\
&= \sum_{\substack{(t_1,\ldots,t_{r+1}) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r \\ t_{r+1}=0}} x_1^{t_1} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}} + \cdots + \sum_{\substack{(t_1,\ldots,t_{r+1}) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r \\ t_{r+1}=a_{r+1}}} x_1^{t_1} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}} \\
&= \sum_{\substack{(t_1,\ldots,t_{r+1}) \\ 0 \leq t_i \leq a_i \\ i=1,\ldots,r+1}} x_1^{t_1} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}}
\end{aligned}$$

□

Supongamos que n es impar. Escribamos a n en su forma estándar, agrupando las potencias de primos que son de la forma $4k + 1$ y también a las potencias de primos

de la forma $4k+3$, esto es, $n = p_1^{a_1} \cdots p_r^{a_r}$, entonces

$$\begin{aligned}\sum_{d|n} \chi(d) &= \sum \chi(p_1^{t_1} \cdots p_r^{t_r}) \\ &= \sum \chi(p_1^{t_1}) \cdots \chi(p_r^{t_r}) \\ &= \prod_{i=1}^{r} (\chi(1) + \chi(p_i) + \cdots + \chi(p_i^{a_i})) \\ &= \prod_{i=1}^{r} (\chi(1) + \chi(p_i) + \cdots + \chi(p_i)^{a_i})\end{aligned}$$

Sin pérdida de generalidad, sean $p_1, \ldots, p_w$ los de la forma $4k+1$ y $p_{w+1}, \ldots, p_r$ los de la forma $4k+3$. Luego

$$\begin{aligned}\sum_{d|n} \chi(d) &= \prod_{i=1}^{w} (\chi(1) + \chi(p_i) + \cdots + \chi(p_i)^{a_i}) \prod_{i=w+1}^{r} (\chi(1) + \chi(p_i) + \cdots + \chi(p_i)^{a_i}) \\ &= \prod_{i=1}^{w} (1 + 1 + \cdots + 1) \prod_{i=w+1}^{r} \left(1 + (-1) + (-1)^2 + \cdots + (-1)^{a_i}\right) \\ &= \prod_{i=1}^{w} (a_i + 1) \prod_{i=w+1}^{r} \left(\frac{1 - (-1)^{a_i+1}}{2}\right) \\ &= \prod_{i=1}^{w} (a_i + 1) \prod_{i=w+1}^{r} \left(\frac{1 + (-1)^{a_i}}{2}\right)\end{aligned}$$

Si algún primo de la forma $4k+3$ aparece con exponente impar, automáticamente $\delta(n) = 0$. Si todos los a_i son pares para $i = w+1, \ldots, r$, entonces

$$\delta(n) = \prod_{i=1}^{w} (a_i + 1)\,.$$

Teorema 79. *Sea $n \in \mathbb{Z}^+$. Entonces $r(n) = 4\delta(n)$.*

La demostración de este teorema no será incluida en este trabajo, pues en ella se incluyen conceptos y resultados importantes del dominio euclidiano de los enteros gaussianos, e incluir esta prueba extiende mucho más el trabajo. Una prueba de este resultado se puede consultar en [7, Theorem 278, página 314].

Ejemplo 14. ¿De cuántas formas se puede representar 3840 como suma de dos cuadrados?

Lo primero que debemos hacer es descomponer a 3840 como producto de potencias de primos. Tenemos que $3840 = 2^8 \cdot 3 \cdot 5$. Observemos que el único primo de la forma

$4k+3$ en esta descomposición es 3 y la potencia de 3 es $a_1 = 1$ impar, de donde $\delta(3840) = 0$ y en consecuencia $r(3840) = 0$.

Ejemplo 15. ¿Es posible determinar de cuántas formas se puede expresar 35114625 como suma de dos cuadrados?

Para responder a esta cuestión descompondremos a 35114625 como producto de potencia de primos, así, $35114625 = 3^2 5^3 7^4 13$. Los primos en la descomposición que son de la forma $4k+3$ son 7 y 3 y sus potencias son 4 y 2 respectivamente, es decir, son pares. Podemos decir entonces que $a_1 = 3$ y $a_2 = 1$, de donde,

$$\delta(35114625) = \prod_{i=1}^{2}(a_i + 1) = (a_1 + 1)(a_2 + 1) = (3 + 1)(1 + 1) = 4 \cdot 2 = 8.$$

Así, por el Teorema 79, obtenemos que

$$r(35114625) = 4\delta(35114625) = 4(8) = 32.$$

Por lo tanto 35114625 tiene 32 representaciones como suma de dos cuadrados.

Capítulo 4

Problema modular de representación de enteros como suma de dos cuadrados

En este capítulo seguiremos las ideas desarrolladas en [1], centradas en el estudio del polinomio x^2+y^2 y en el conjunto A_n de todos los enteros módulo n que se pueden representar como suma de dos enteros módulo n.

4.1. Algunos conceptos preliminares

Consideremos la siguiente congruencia polinomial

$$x^2 + y^2 \equiv a \pmod{n}, \tag{4.1.1}$$

donde a y n son enteros con $n > 0$. Como la congruencia (4.1.1) tiene solución para a si, y solo si, tiene solución para $a + qn$ para cualquier entero q, podemos asumir que a pertenece a un sistema completo de residuos módulo n. Usaremos el sistema de residuos $I_n = \{0, 1, \ldots, n-1\}$.

Definición 80. Sea n un entero positivo. El conjunto A_n se define como sigue:

$$A_n := \{a \in I_n : x^2 + y^2 \equiv a \pmod{n} \text{ es soluble}\}.$$

Además, se define $\alpha(n)$ como el número de elementos de A_n, es decir, $\alpha(n) = |A_n|$.

Así, podemos decir que A_n es el conjunto de todos los elementos en I_n que pueden ser representados como suma de dos cuadrados módulo n, y $\alpha(n)$ cuenta la cantidad de estos enteros.

Nuestros objetivos principales consisten en estudiar los siguientes problemas relacionados con A_n y $\alpha(n)$:

1. Dar una descripción explícita de A_n para todo n.

2. Encontrar una fórmula (explícita o recursiva) para $\alpha(n)$.

3. Determinar o describir todos los valores de n tales que $\alpha(n) = n$.

Definición 81. Sea $n \in \mathbb{Z}^+$. Diremos que el polinomio $x^2 + y^2$ es **sobreyectivo** en n, si, para cada $a \in I_n$, la congruencia 4.1.1 tiene solución.

El problema del numeral 3 es, con esta definición, equivalente a determinar los valores de n tales que el polinomio $x^2 + y^2$ es sobreyectivo en n.

4.2. Familias multiplicativas

Para una familia arbitraria de conjuntos no vacíos $\{A_n\}_{n\in\mathbb{Z}^+}$, donde $A_n \subseteq I_n$ para todo n, definimos la **función asociada a** $\{A_n\}_n$, $\alpha : \mathbb{Z}^+ \to \mathbb{Z}^+$, mediante $\alpha(n) = |A_n|$ para todo n. Note que $A_1 \neq \varnothing$ y $A_1 \subseteq I_1 = \{0\}$, así que $\alpha(1) = |A_1| = 1$.

Lo primero que haremos es definir condiciones adecuadas sobre la familia $\{A_n\}_n$ para que la función asociada α sea multiplicativa. Si n y m son enteros tales que $1 \leq m \leq n$, definimos

$$\begin{aligned} A_n(m) :&= \{s \in I_n : s \equiv a \pmod{m} \text{ para algún } a \ \in A_m\} \\ &= \{a + jm : a \in A_m, 0 \leq j < n/m\}. \end{aligned}$$

Definición 82. Llamamos a una familia $\{A_n\}_n$ **multiplicativa**, si dados m_1 y m_2 primos relativos y $n = m_1 m_2$, se cumple la igualdad $A_n = A_n(m_1) \cap A_n(m_2)$.

La condición de multiplicatividad sobre la familia de conjuntos $\{A_n\}_n$ garantiza que la función asociada α es multiplicativa.

Lema 83. *Si $\{A_n\}_n$ es una familia multiplicativa, entonces la función asociada α es multiplicativa.*

Demostración. Sea $n = m_1 m_2$ donde m_1 y m_2 son primos relativos. Definamos

$$B(a, m_1) := \{a + jm_1 : 0 \leq j < m_2\}.$$

Note que, dados a y $b \in A_{m_1} \subseteq I_{m_1}$, por definición de sistema completo de residuos, si $a \neq b$ entonces $a \not\equiv b \pmod{m_1}$. Ahora, si $x_0 \in B(a, m_1) \cap B(b, m_1)$, se tiene que $x_0 \equiv a \pmod{m_1}$ y $x_0 \equiv b \pmod{m_1}$, y por tanto $a \equiv b \pmod{m_1}$, lo cual es imposible. Así que para $a, b \in A_{m_1}$ con $a \neq b$,

$$B(a, m_1) \cap B(b, m_1) = \varnothing.$$

Por otro lado, para $a \in A_{m_1}$, si $y_0 \in A_n(m_1)$, por definición de $A_n(m_1)$, tenemos que $y_0 = a + jm_1$, con $0 \leq j < \frac{n}{m_1} = m_2$, así que $y_0 \in B(a, m_1) \subseteq \bigcup_{a \in A_{m_1}} B(a, m_1)$. Además, si $w_0 \in \bigcup_{a \in A_{m_1}} B(a, m_1)$, existe $a_0 \in A_{m_1}$ tal que $w_0 = a_0 + jm_1$, donde $0 \leq j < m_2 = \frac{n}{m_1}$, de donde $w_0 \in A_n(m_1)$. Hemos mostrado que los conjuntos $B(a, m_1)$ forman una partición de $A_n(m_1)$. De manera similar, los conjuntos análogos $B(b, m_2)$ forman una partición de $A_n(m_2)$. Entonces,

$$\begin{aligned} A_n(m_1) \cap A_n(m_2) &= \left(\bigcup_{a \in A_{m_1}} B(a, m_1) \right) \cap \left(\bigcup_{b \in A_{m_2}} B(b, m_2) \right) \\ &= \bigcup_{a \in A_{m_1}, b \in A_{m_2}} \Big(B(a, m_1) \cap B(b, m_2) \Big). \end{aligned}$$

Además, $c \in B(a, m_1) \cap B(b, m_2)$ si, y solamente si, $c \equiv b \pmod{m_2}$ y además, $c \equiv a \pmod{m_1}$. Por el teorema Chino del Residuo, el sistema de congruencias

$$\begin{cases} x \equiv a \pmod{m_1}; \\ x \equiv b \pmod{m_2}, \end{cases}$$

tiene exactamente una solución en I_n. Esto significa que $B(a, m_1) \cap B(b, m_2)$ tiene exactamente un elemento. Tenemos también que para $a \in A_{m_1}$ y $b \in A_{m_2}$ los conjuntos

$B(a, m_1) \cap B(b, m_2)$ son disjuntos dos a dos, entonces

$$|A_n(m_1) \cap A_n(m_2)| = \left| \bigcup_{a \in A_{m_1}, b \in A_{m_2}} \Big(B(a, m_1) \cap B(b, m_2) \Big) \right| = |A_{m_1}| \cdot |A_{m_2}|.$$

Ahora, como la familia $\{A_n\}_n$ es multiplicativa, tenemos que

$$\alpha(m_1 m_2) = \alpha(n) = |A_n| = |A_n(m_1) \cap A_n(m_2)| = |A_{m_1}| \cdot |A_{m_2}| = \alpha(m_1)\alpha(m_2).$$

En consecuencia, la función asociada α es multiplicativa. □

El recíproco del Lema 83 no siempre es cierto; veamos el siguiente ejemplo. Para $n = 80$, tenemos que

$$A_{80} = \{0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 21, 24, 25, 26, 29, 32, 33, 34, 36, 37, 40,$$
$$41, 42, 45, 48, 49, 50, 52, 53, 56, 57, 58, 61, 64, 65, 66, 68, 69, 72, 73, 74, 77\}.$$

Además, sabemos que $80 = 16 \cdot 5$, donde, $\text{mcd}(16, 5) = 1$. Podemos observar que $\alpha(80) = 45 = 9 \cdot 5 = \alpha(16) \cdot \alpha(5)$. Al hacer los cálculos, encontramos que

$A_n(m)$	Elementos en $A_n(m)$
$A_{80}(16)$	$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 21, 24, 25, 26, 29, 32, 33, 34, 36, 37, 40, 41, 42, 45, 48, 49, 50, 52$ $53, 56, 57, 58, 61, 64, 65, 66, 68, 69, 72, 73, 74, 77$
$A_{80}(5)$	$0, 1, 2, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 22, 24, 25, 26, 27, 29, 30, 31, 32, 34, 35, 36, 37, 39, 40$ $41, 42, 44, 45, 46, 47, 49, 50, 51, 52, 54, 55, 56, 57, 59, 60, 61, 62, 64, 65, 66, 67, 69, 70, 71, 72, 74, 75, 76, 77, 79$

Tabla 4.1: Elementos de $A_n(m)$

Sin embargo, $A_{80}(16) \cap A_{80}(5) = \{0, 1, 2, 4, 5, 9, 10, 16, 17, 20, 21, 24, 25, 26, 29, 32, 34, 36, 37, 40, 41, 42, 45, 49, 50, 52, 56, 57, 61, 64, 65, 66, 69, 72, 74, 77\}$, y podemos notar que $8 \in A_{80}$ pero $8 \notin A_{80}(16) \cap A_{80}(5)$. Por lo tanto A_{80} no es multiplicativa, sin embargo $\alpha(80) = \alpha(16)\alpha(5)$.

Ahora definimos dos condiciones sobre $\{A_n\}_n$ que son suficientes para que $\{A_n\}_n$ sea multiplicativa.

MT1: Para m y n enteros, si $m \mid n$ y $a \in A_n$, entonces $a \pmod m \in A_m$, donde $a \pmod m$ representa al residuo de a al dividirlo m.

MT2: Si $n = m_1 m_2$, donde $\text{mcd}(m_1, m_2) = 1$ y si $a_1 \in A_{m_1}, a_2 \in A_{m_2}$ y a es la única solución en I_n del sistema de congruencias $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$, entonces $a \in A_n$.

Note que si $\{A_n\}_n$ satisface la **MT1** y $m \mid n$, entonces $A_n \subseteq A_n(m)$. En efecto, si $a \in A_n$, por el algoritmo de la división podemos escribir $a = mq + r$ para algunos enteros q y r, donde $0 \leq r < m$. Luego, por la condición **MT1** $r = a \pmod m \in A_m$ y $a \equiv r \pmod m$. Además, como $m \mid n$, $n = mt$ para algún entero t, y además $n \geq 0, m \geq 0, a \geq 0$ y $r \geq 0$, entonces $q \geq 0$. Note también, que si $q \geq t$, entonces $mq + r \geq mt + r \geq n$, así que $a \geq n$ lo cual contradice el hecho de que $a \in A_n \subseteq I_n$, de donde, debe ocurrir que $0 \leq q < t = n/m$. Se sigue que $a \in A_n(m)$.

Lema 84. *Si $\{A_n\}_n$ satisface las condiciones **MT1** y **MT2**, entonces $\{A_n\}_n$ es multiplicativa.*

Demostración. Sea $n = m_1 m_2$ donde $\text{mcd}(m_1, m_2) = 1$. Como $\{A_n\}_n$ satisface la condición **MT1**, $m_1 \mid n$ y $m_2 \mid n$, entonces $A_n \subseteq A_n(m_1)$ y $A_n \subseteq A_n(m_2)$. Así, $A_n \subseteq A_n(m_1) \cap A_n(m_2)$. Resta probar la otra inclusión. Sea $a \in A_n(m_1) \cap A_n(m_2)$. Entonces existen $a_1 \in A_{m_1}$ y $a_2 \in A_{m_2}$ tales que $a \equiv a_1 \pmod{m_1}$ y $a \equiv a_2 \pmod{m_2}$ y, como $\{A_n\}_n$ satisface la **MT2**, se sigue que $a \in A_n$. Así $A_n = A_n(m_1) \cap A_n(m_2)$ y por tanto $\{A_n\}_n$ es multiplicativa. □

Si asumimos que la familia $\{A_n\}_n$ satisface las condiciones **MT1** y **MT2**, entonces, por los Lemas 83 y 84, la función asociada α es multiplicativa. Así que, para determinar el valor de α en todos los enteros positivos, es suficiente determinar $\alpha(p^n)$ para todo primo p y $n \geq 1$. Esto nos lleva a estudiar los conjuntos A_{p^n} para potencias de primos p^n.

La condición **MT1** sobre la familia $\{A_n\}_n$ implica que si p es primo y $n \geq 1$, entonces $A_{p^n} \subseteq A_{p^n}(p^{n-1})$. Para $n \geq 1$, definimos $N_{p^n} := A_{p^n}(p^{n-1}) \setminus A_{p^n}$ y llamamos a estos conjuntos, los $N-$**conjuntos** del primo p.

Notemos que

$$\begin{aligned} A_{p^n} &= A_{p^n}(p^{n-1}) \setminus N_{p^n} = \{a + jp^{n-1} : a \in A_{p^{n-1}}, 0 \leq j < p\} \setminus N_{p^n} \\ &= \{a + a_{n-1}p^{n-1} : a \in A_{p-1}, a_{n-1} \in \{0, 1, \dots p-1\}\} \setminus N_{p^n}. \end{aligned}$$

Esto nos muestra una manera recursiva de determinar los elementos de A_{p^n}. Usaremos esta representación más adelante.

Lema 85. *Sea p un número primo y $n \geq 1$. Entonces*

$$\alpha(p^n) = p\alpha(p^{n-1}) - |N_{p^n}|.$$

Demostración. Como p es primo y $p^{n-1} \mid p^n$, por definición de los $A_n(m)$, tenemos que

$$\begin{aligned} A_{p^n}(p^{n-1}) &= \{a + jp^{n-1} : a \in A_{p^{n-1}}, 0 \leq j < p\} \\ &= \{a, a + p^{n-1}, a + 2p^{n-1}, \dots, a + (p-1)p^{n-1} : a \in A_{p^{n-1}}\}. \end{aligned}$$

Luego, por cada $a \in A_{p^{n-1}}$ hay p elementos en $A_{p^n}(p^{n-1})$ y como la cantidad de elementos de $A_{p^{n-1}}$ es $|A_{p^{n-1}}|$, tenemos que

$$|A_{p^n}(p^{n-1})| = p|A_{p^{n-1}}|.$$

Además, por definición de la función α, $|A_{p^{n-1}}| = \alpha(p^{n-1})$. Así que

$$|A_{p^n}(p^{n-1})| = p \cdot |A_{p^{n-1}}| = p\alpha(p^{n-1}),$$

además, $N_{p^n} = A_{p^n}(p^{n-1}) \setminus A_{p^n}$, se sigue que $A_{p^n} = A_{p^n}(p^{n-1}) \setminus N_{p^n}$ y por tanto

$$\alpha(p^n) = |A_{p^n}(p^{n-1}) \setminus N_{p^n}| = |A_{p^n}(p^{n-1})| - |N_{p^n}| = p\alpha(p^{n-1}) - |N_{p^n}|. \qquad \square$$

4.3. La familia multiplicativa asociada a $x^2 + y^2$

Por el resto de este capítulo, la familia $\{A_n\}_n$ consistirá de los conjuntos A_n formados por los elementos $a \in I_n$ tales que la congruencia $x^2 + y^2 \equiv a \pmod{n}$ es soluble. Nos referimos a la función asociada α a esta familia $\{A_n\}_n$, como la función asociada a $x^2 + y^2$.

Proposición 86. *La familia $\{A_n\}_n$ asociada a x^2+y^2 es multiplicativa. En particular, la función asociada a x^2+y^2 es multiplicativa.*

Demostración. En efecto, sabemos que para cada $n \in \mathbb{N}$, A_n es el conjunto de los $a \in I_n$ tales que la congruencia $x^2+y^2 \equiv a \pmod{n}$ tiene solución. Ahora, si $m \in \mathbb{Z}^+$ con $m \mid n$ y $a \in A_n$, por definición de congruencia, $n \mid (x^2+y^2-a)$. Luego $m \mid (x^2+y^2-a)$ y así, $a \in A_m$. Hemos mostrado que la familia de $\{A_n\}_n$ satisface la condición **MT1**.

Ahora, supongamos que $x_1^2+x_2^2 \equiv a_1 \pmod{m_1}$ y $y_1^2+y_2^2 \equiv a_2 \pmod{m_2}$, donde $x_i, y_j \in \mathbb{Z}$, m_1 y m_2 son primos relativos con $n = m_1m_2$ y $a_i \in I_m$, para $i = 1, 2$. Sea a la única solución en I_n del sistema de congruencias $x \equiv a_1 \pmod{m_1}$ y $x \equiv a_2 \pmod{m_2}$. Ahora, por el teorema chino del residuo, para cada $j = 1, 2$ existe $c_j \in \mathbb{Z}$ tal que $c_j \equiv x_j \pmod{m_1}$ y $c_j \equiv y_j \pmod{m_2}$. Así, $c_1^2+c_2^2 \equiv x_1^2+x_2^2 \equiv a_1 \equiv a \pmod{m_1}$ y $c_1^2+c_2^2 \equiv y_1^2+y_2^2 \equiv a_2 \equiv a \pmod{m_2}$. Tenemos que $c_1^2+c_2^2 \equiv a \pmod{m_1}$ y $c_1^2+c_2^2 \equiv a \pmod{m_2}$ y así $c_1^2+c_2^2 \equiv a \pmod{n}$, lo que muestra que $a \in A_n$. Hemos mostrado que $\{A_n\}_n$ satisface la condición **MT2**. Por los Lemas 83 y 84 se obtiene lo que se desea. □

Ahora estudiaremos la función multiplicativa α y los conjuntos A_{p^n} asociados con x^2+y^2. Para determinar el valor de α en potencias de primos, necesitamos entender los conjuntos A_{p^n} y N^{p^n}. Los siguientes lemas dan propiedades útiles de estos conjuntos.

Lema 87. *Sea $\{A_n\}_n$ la familia asociada al polinomio x^2+y^2. Sea p un primo impar. Suponga que $a \in A_{p^n}$ y*

$$m_1^2+m_2^2 \equiv a \pmod{p^n},$$

donde m_1 y m_2 son enteros y suponga que p no divide a alguno de los m_i. Entonces $a+jp^n \in A_{p^{n+1}}$ para todo j tal que $0 \leq j < p$.

Demostración. Supongamos que $m_1^2+m_2^2 \equiv a \pmod{p^n}$. Entonces existe un entero w tal que $m_1^2+m_2^2 = a+wp^n$. Sin pérdida de generalidad supongamos que $p \nmid m_1$. Sea $0 \leq j < p$. Como $p \nmid m_1$, se sigue que $p \nmid 2m_1$ y la congruencia $2m_1x+w \equiv j \pmod{p}$ tiene solución para $x \in \mathbb{Z}$; así, existen enteros d y e tales que $2m_1d+w = j+ep$.

Ahora

$$(m_1 + dp^n)^2 = m_1^2 + 2m_1dp^n + d^2p^{2n} = m_1^2 + 2m_1dp^n + p^{n+1}d^2p^{n-1},$$

de donde

$$(m_1 + dp^n)^2 \equiv m_1^2 + 2m_1dp^n \pmod{p^{n+1}}.$$

Luego,

$$(m_1 + dp^n)^2 + m_2^2 \equiv m_1^2 + 2m_1dp^n + m_2^2 \pmod{p^{n+1}},$$

y ya que $m_1^2 + m_2^2 = a + wp^n$, para el módulo p^{n+1} tenemos

$$\begin{aligned}(m_1 + dp^n)^2 + m_2^2 &= a + wp^n + 2m_1dp^n \\ &= a + (w + 2m_1d)p^n \\ &= a + (j + ep)p^n \\ &= a + jp^n + ep^{n+1} \\ &= a + jp^n \pmod{p^{n+1}}.\end{aligned}$$

Por lo tanto, $a + jp^n \in A_{p^{n+1}}$. □

A continuación mostramos que el lema anterior también se cumple para el caso en que $p = 2$.

Lema 88. *Sea $\{A_n\}_n$ la familia asociada al polinomio $x^2 + y^2$. Suponga que $a \in A_{2^n}$ y $m_1^2 + m_2^2 \equiv a \pmod{2^n}$, donde m_1 y m_2 son enteros, y suponga que alguno de los m_i es impar y que $n \geq 3$. Entonces $a + j2^n \in A_{2^{n+1}}$, para todo j tal que $j \in \{0, 1\}$.*

Demostración. Como $m_1^2 + m_2^2 \equiv a \pmod{2^n}$, existe un entero k tal que $m_1^2 + m_2^2 = a+2^nk$. Consideremos el polinomio $f(x) = m_1x+k-j$, donde $j \in \{0, 1\}$ y supongamos sin pérdida de generalidad que $2 \nmid m_1$ y ya que $\text{mcd}(m_1, 2) = 1$ y $1 \mid 0$, por el Teorema 27, la congruencia $f(x) \equiv 0 \pmod 2$ tiene una solución, así que digamos, existen enteros d y s tales que $m_1d + k = j + 2s$. Ahora

$$(m_1 + d2^{n-1})^2 = m_1^2 + 2^ndm_1 + 2^{2(n-1)}d^2 = m_1^2 + 2^ndm_1 + 2^{n+1}2^{n-3}d^2,$$

así, $(m_1 + d2^{n-1})^2 \equiv m_1^2 + 2^n dm_1 \pmod{2^{n+1}}$. De esta manera

$$\begin{aligned}(m_1 + d2^{n-1})^2 + m_2^2 &\equiv m_1^2 + m_2^2 + 2^n dm_1 \pmod{2^{n+1}} \\ &\equiv a + 2^n k + 2^n dm_1 \pmod{2^{n+1}} \\ &= a + 2^n(k + dm_1) \pmod{2^{n+1}} \\ &\equiv a + 2^n(j + 2s) \pmod{2^{n+1}} \\ &\equiv a + 2^n j \pmod{2^{n+1}}.\end{aligned}$$

En consecuencia $a + 2^n j \in A_{2^{n+1}}$. □

Para conocer la forma explícita de los elementos de A_{p^n}, falta ver como son los elementos de N_{p^n} y es lo que analizaremos a continuación.

Lema 89. *Sea p un número primo y considere los $N-$conjuntos N_{p^n} asociados al polinomio $x^2 + y^2$. Entonces*

$$N_{p^n} \subseteq \{p^2 a : a \in N_{p^{n-2}}\},$$

para todo $n > 3$.

Demostración. Sea $b \in N_{p^n} = A_{p^n}(p^{n-1}) \setminus A_{p^n}$. Entonces $b = c + jp^{n-1}$ para algún $c \in A_{p^{n-1}}$ y $0 \leq j < \frac{p^n}{p^{n-1}} = p$. Así, existen enteros m_1 y m_2 tales que $m_1^2 + m_2^2 \equiv c \pmod{p^{n-1}}$. Como $n > 3$, $n - 1 > 2$ y así $n - 1 \geq 1$. Si $p \nmid m_i$ para algún i, entonces por el Lema 87, $b = c + jp^{n-1} \in A_{p^n}$, lo cual es una contradicción ya que $b \in N_{p^n} = A_{p^n}(p^{n-1}) \setminus A_{p^n}$. Se sigue que $p \mid m_i$ para todo $i = 1, 2$, de modo que $m_1 = pk_1$ y $m_2 = pk_2$ para algunos enteros k_1 y k_2. Así que $m_1^2 + m_2^2 = p^2(k_1^2 + k_2^2)$, esto es, $p^2 \mid m_1^2 + m_2^2$. Por otro lado, de $m_1^2 + m_2^2 \equiv c \pmod{p^{n-1}}$ tenemos que $p^{n-1} \mid m_1^2 + m_2^2 - c$ y como $n - 1 > 2$, también obtenemos que $p^{n-1} = p^2 p^t$ donde $t = n-3$. De modo que $p^2 \mid p^{n-1}$ y de esta manera $p^2 \mid (m_1^2 + m_2^2 - (m_1^2 + m_2^2 - c)) = c$, con lo cual obtenemos la congruencia

$$\left(\frac{m_1}{p}\right)^2 + \left(\frac{m_2}{p}\right)^2 \equiv \frac{c}{p^2} \pmod{\frac{p^{n-1}}{p^2}},$$

así

$$\left(\frac{m_1}{p}\right)^2 + \left(\frac{m_2}{p}\right)^2 \equiv \frac{c}{p^2} \pmod{p^{n-3}}.$$

Por lo tanto $\dfrac{c}{p^2} \in A_{p^{n-3}}$. Afirmamos que $c/p^2 + jp^{n-3} \in N_{p^{n-2}}$. En caso contrario, si $q_1^2 + q_2^2 \equiv c/p^2 + jp^{n-3} \pmod{p^{n-2}}$ para algunos enteros q_1 y q_2, multiplicando por p^2 en toda la congruencia, tenemos que

$$(pq_1)^2 + (pq_2)^2 \equiv c + jp^{n-1} \pmod{p^n},$$

de donde

$$(pq_1)^2 + (pq_2)^2 \equiv b \pmod{p^n}.$$

De ahí $b \in A_{p^n}$ y esto es una contradicción. De modo que $c/p^2 + jp^{n-1} \in N_{p^{n-2}}$. Así, si $a := c/p^2 + jp^{n-3}$, entonces $a \in N_{p^{n-2}}$ y $b = c + jp^{n-1} = p^2a$. Esto termina la prueba. □

Lema 90. *Considere los $N-$conjuntos N_{2^n} asociados al polinomio x^2+y^2. Entonces $N_{2^n} \subseteq \{2^2a : a \in N_{2^{n-2}}\}$, para todo $n > 3$.*

Demostración. Deseamos que cualquier elemento de N^{2^n} tenga la forma $2^2 \cdot a$ para algún $a \in N^{2^{n-2}}$ y $n > 3$.

En efecto, sea $m \in N_{2^n} = A_{2^n}(2^{n-1}) \setminus A_{2^n}$, esto es, $m = c + j2^{n-1}$, para algún $c \in A_{2^{n-1}}$ y $0 \leq j < 2$. Como $c \in A_{2^{n-1}}$, por definición, c es suma de cuadrados módulo 2^{n-1}, esto es, existen enteros m_1 y m_2 tales que $m_1^2 + m_2^2 \equiv c \pmod{2^{n-1}}$, así que

$$2^{n-1} \mid (m_1^2 + m_2^2) - c. \tag{4.3.1}$$

Observe que m_1 y m_2 son ambos pares, pues, si alguno de los dos no lo fuera, por el Lema 88 obtendríamos que $m \in A_{2^n}$, pero esto no puede ocurrir porque $m \in N^{2^n} = A_{2^n}(2^{n-1}) \setminus A_{2^n}$, de donde existen enteros t_1 y t_2 tales que $m_1 = 2t_1$ y $m_2 = 2t_2$. Por lo que $m_1^2 + m_2^2 = 2^2(t_1^2 + t_2^2)$ y así

$$2^2 \mid (m_1^2 + m_2^2). \tag{4.3.2}$$

Además $2^{n-1} = 2^{n-3+2} = 2^2 2^{n-3} = 2^2 t$, para $t = 2^{n-3} \in \mathbb{Z}^+(n > 3, n-3 > 0)$, entonces

$$2^2 \mid 2^{n-1}. \tag{4.3.3}$$

De (4.3.1) y (4.3.3) obtenemos que $2^2 \mid (m^1 + m^2 - c)$ y de ésta última y de (4.3.2) obtenemos que $2^2 \mid (m_1^2 + m_2^2 - (m_1^2 + m_2^2 - c)) = c$. De todo lo anterior, obtenemos la congruencia

$$\left(\frac{m_1}{2}\right)^2 + \left(\frac{m_2}{2}\right)^2 \equiv \left(\frac{c}{2^2}\right) \left(\mod \frac{2^{n-1}}{2^2}\right).$$

Por lo que $c/2^2 \in A_{2^{n-3}}$. Note también que $c/2^2 + j^2 n - 3 \in N_{2^{n-2}}$, pues en caso contrario $c/2 + j2^{n-3}$ sería suma de dos cuadrados módulo 2^{n-2}, esto es, $q_1^2 + q_2^2 \equiv c/2^2 + j2^{n-3} \pmod{2^{n-2}}$ para algunos enteros q_1 y q_2, multiplicamos por 2^2 y obtenemos que $(2q_1)^2 + (2q_2)^2 \equiv c + j2^{n-1} \pmod{2^n}$, esto es, $m = c + j2^{n-1} \in A_{2^n}$, lo cual es una contradicción. Por lo tanto $c/2^2 + j2^{n-3} \in N_{2^{n-2}}$. Así $a := c/2^2 + j2^{n-2} \in N_{2^{n-2}}$ y $m = c + j2^{n-1} = 2^2 \cdot a$. □

Ahora definiremos una condición sobre el primo p tal que la inclusión inversa en el Lema 89 se satisfaga.

Definición 91. Sea p un número primo. Decimos que un entero no negativo e es un **exponente de** p **en** $x^2 + y^2$, si cuando p^e divide a un entero de la forma $m_1^2 + m_2^2$, se tiene que el cociente $(m_1^2 + m_2^2)/p^e$ es también de la forma $q_1^2 + q_2^2$ para algunos enteros q_1 y q_2.

Lema 92. *Las siguientes afirmaciones son verdaderas.*

1. *Si $p = 2$ o p es un primo tal que $p \equiv 1 \pmod 4$, entonces 1 es un exponente de p en el polinomio $x^2 + y^2$.*

2. *Si p es un primo y $p \equiv 3 \pmod 4$, entonces 2 es un exponente de p en el polinomio $x^2 + y^2$.*

Demostración. 1. Si $p = 2$ o $p \equiv 1 \pmod 4$ y $p \mid (m_1^2 + m_2^2)$. Entonces existe un entero s tal que $m_1^2 + m_2^2 = ps$. Por otro lado si, $m_1^2 + m_2^2 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, por el Teorema 66 para cada $i = 1, 2, \ldots, r$, los p_i que sean de la forma $4k_i + 3$ deben tener potencia par. Sin pérdida de generalidad suponemos que $p_1 = p$ y obtenemos que

$$s = p_1^{a_1 - 1} \ldots p_r^{a_r},$$

sigue sucediendo que cada p_i que sea de la forma $4k_i + 3$ tiene potencia par, así que nuevamente, por el Teorema 66, $s = s_1^2 + s_2^2$ para algunos enteros s_1 y s_2, así,

$$\frac{m_1^2 + m_2^2}{p} = s = s_1^2 + s_2^2.$$

2. Supongamos ahora, que $p \equiv 3 \pmod 4$ con $p^2 \mid (m_1^2 + m_2^2)$. Entonces existe un entero t tal que $m_1^2 + m_2^2 = p^2 t$. Por otro lado, $m_1^2 + m_2^2 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ para p_i primos distintos y $a_i > 0$ para cada $i = 1, 2, \ldots, r$ y por el Teorema 66, cada p_j que sea de la forma $4k + 3$ debe tener potencia par. Supongamos, sin pérdida de generalidad, que $p_1 = p$, así tenemos que $p_1^{a_1 - 2} p_2^{a_2} \cdots p_r^{a_r} = t$. Ya que $p_1 = p$, entonces a_1 es par y así $a_1 - 2$ también es par y Por el Teorema 66 $t = v_1^2 + v_2^2$ para enteros v_1 y v_2. Así,

$$\frac{m_1^2 + m_2^2}{p^2} = t = v_1^2 + v_2^2. \qquad \square$$

Lema 93. *Si e es un exponente de un primo p en el polinomio $x^2 + y^2$, entonces todo entero positivo múltiplo de e también es un exponente de p en $x^2 + y^2$.*

Demostración. Sean e un exponente de p en $x^2 + y^2$, $c = ek$ para algún entero k. Afirmamos que si $c \mid (m_1^2 + m_2^2)$, entonces

$$\frac{m_1^2 + m_2^2}{p^c} = t_1^2 + t_2^2,$$

para algunos enteros t_1 y t_2. Verifiquémoslo por inducción sobre k. Si $k = 1$, entonces $c = e$ y como e es un exponente de p en $x^2 + y^2$, existen t_1' y t_2' enteros tales que

$$\frac{m_1^2 + m_2^2}{p^c} = (t_1')^2 + (t_2')^2.$$

Supongamos que el resultado se satisface para k y que $c \mid (m_1^2 + m_2^2)$ donde $c = e(k+1)$. Luego

$$\frac{m_1^2 + m_2^2}{p^c} = \frac{m_1^2 + m_2^2}{p^{ek} p^e} = \left(\frac{m_1^2 + m_2^2}{p^e} \right) \frac{1}{p^{ek}} = \frac{(t_1') + (t_2')^2}{p^{ek}}.$$

Finalmente como por hipótesis inductiva, ek es un exponente de $x^2 + y^2$, entonces existen enteros $t_1^2 + t_2^2$ tales que $(t_1') + (t_2')^2)/(p^{ek}) = t_1^2 + t_2^2$ y así

$$\frac{m_1^2 + m_2^2}{p^c} = t_1^2 + t_2^2. \qquad \square$$

Lema 94. *Sea p un número primo. Para los $N-$conjuntos asociados al polinomio x^2+y^2 se cumple que*

$$\{p^2a : a \in N_{p^{n-2}}\} \subseteq N_{p^n}$$

para todo $n > 2$.

Demostración. Supongamos que e es un exponente del primo p en x^2+y^2 con $e \mid 2$. Debemos probar que todo elemento de $\{p^2a : a \in N_{p^{n-2}}\}$ pertenece a N_{p^n}. Veámoslo por reducción al absurdo; supóngase que existe $a \in N_{p^{n-2}}$ tal que $p^2a \notin N_{p^n} = A_{p^n}(p^{n-1}) \setminus A_{p^n}$. Entonces $p^2a \in A_{p^n}$. Luego, existen enteros m_1 y m_2 tales que $m_1^2+m_2^2 \equiv p^2a \pmod{p^n}$. Por el Lema 93, como $e \mid 2$ entonces 2 también es un exponente de p en x^2+y^2. Así que,

$$\frac{m_1^2+m_2^2}{p^2} = c_1^2+c_2^2,$$

para algunos enteros c_1 y c_2. De esta manera,

$$c_1^2+c_2^2 = \frac{m_1^2+m_2^2}{p^2} \equiv \frac{p^2a}{p^2} \pmod{\frac{p^n}{p^2}},$$

así,

$$c_1^2+c_2^2 \equiv a \pmod{p^{n-2}}.$$

En consecuencia, $a \in A_{p^{n-2}}$. Esto es una contradicción, pues por como definimos A_n, $a \in N_{p^{n-2}} = A_{p^{n-2}}(p^{n-3}) \setminus A_{p^{n-2}}$. Por lo tanto, se tiene que $p^2a \in N_{p^n}$, para todo $a \in N_{p^{n-2}}$. □

Una aplicación de los Lemas 89 y 94 nos dice que para todo $n > 3$ se tiene que

$$N_{p^n} = \{p^2a : a \in N_{p^{n-2}}\}. \tag{4.3.4}$$

Para un conjunto de enteros A, mA denota el conjunto $\{ma : a \in A\}$. Entonces $N_{p^n} = p^2N_{p^{n-2}}$ para todo $n > 3$. Por lo tanto, si $n = 2q+r$, donde $q \geq 0$ y $r \in \{2,3\}$, tenemos que

$$N_{p^n} = p^2N_{p^{n-2}} = p^4N_{p^{n-4}} = \cdots = p^{2q}N_{p^r}. \tag{4.3.5}$$

Definamos $n_r := |N_{p^r}|$, para $r \in \{2,3\}$. Por (4.3.5) se sigue que si $n > 1$ y $n \equiv r \pmod 2$, donde $r \in \{2,3\}$, entonces $|N_{p^n}| = |N_{p^r}| = n_r$.

Proposición 95. *Sea p un número primo. Entonces*

$$\alpha(p^n) = p\alpha(p^{n-1}) - n_r, \tag{4.3.6}$$

para todo $n > 1$ tal que $n \equiv r \pmod 2$, donde $r \in \{2, 3\}$.

Demostración. En efecto, por el Lema 85 tenemos que $\alpha(p^n) = p\alpha(p^{n-1}) - |N_{p^n}|$. Como $|N_{p^n}| = |N_{p^r}| = n_r$, se sigue que $\alpha(p^n) = p\alpha(p^{n-1}) - n_r$. □

4.4. La función α asociada a $x^2 + y^2$

En esta sección hallamos fórmulas explícitas para $\alpha(p^n)$, donde p es primo y $n \geq 1$. Empezamos con el siguiente resultado:

Lema 96. *Para todo número primo p, tenemos que $\alpha(p) = p$.*

Demostración. Recordemos que para p primo, A_p es el conjunto de todos los $a \in I_p$ tales que la congruencia

$$x^2 + y^2 \equiv a \pmod p,$$

tiene solución, es decir, todos los $a \in I_p$ tales que a es suma de dos cuadrados módulo p. Mostraremos que todo elemento en $I_p = \{0, 1, \ldots, p-1\}$ se puede expresar como suma de dos cuadrados módulo p.

En efecto, sabemos que hay $\frac{p+1}{2}$ elementos en I_p que son cuadrados módulo p. Entonces, para cada $a \in I_p$ hay $\frac{p+1}{2}$ elementos $s \in I_p$ tales que la congruencia

$$a - x^2 \equiv s \pmod p, \tag{4.4.1}$$

tiene solución. Note que $2\frac{p+1}{2} = p + 1$, pero hay exactamente p elementos en $I_p = \{0, 1, \ldots, p-1\}$, así que existe un elemento s_0 en I_p satisfaciendo simultáneamente las congruencias $a - x^2 \equiv s_0 \pmod p$ y $y^2 \equiv s_0 \pmod p$ tienen solución para $x, y \in I_p$. Se sigue que $x^2 + y^2 \equiv a \pmod p$. Esto muestra que $a \in A_p$ para cualquier $a \in I_p$. □

Por el Lema 96, $\alpha(p) = p$ y $A_p = I_p$ para todo primo p.

4.4.1. Cálculo de $\alpha(2^n)$

En esta sección calculamos $\alpha(2^n)$ para todo $n \geq 1$. Por el Lema 92, el primo 2 tiene exponente 1 en $x^2 + y^2$. Ahora, por el Lema 96, $\alpha(2) = 2$ y $A_2 = \{0, 1\}$.

Primero calculamos los $N-$conjuntos y N_4 y N_8. Vamos Considerar el conjunto $I_4 = \{0, 1, 2, 3\}$. En la siguiente tabla mostramos las sumas de cuadrados módulo 4:

$+$	0^2	1^2	2^2	3^2
0^2	0	1	0	1
1^2	1	2	1	2
2^2	0	1	0	1
3^2	1	2	1	2

Tabla 4.2: Suma de dos cuadrados módulo 4

De la Tabla 4.2 observamos que $A_4 = \{0, 1, 2\}$. La siguiente tabla contiene las sumas de cuadrados módulo 8:

$+$	0^2	1^2	2^2	3^2	4^2	5^2	6^2	7^2
0^2	0	1	4	1	0	1	4	1
1^2	1	2	5	2	1	2	5	2
2^2	4	5	0	5	4	5	0	5
3^2	1	2	5	2	1	2	5	2
4^2	0	1	4	1	0	1	4	1
5^2	1	2	5	2	1	2	5	2
6^2	4	5	0	5	4	5	0	5
7^2	1	2	5	2	1	2	5	2

Tabla 4.3: Suma de dos cuadrados módulo 8

Observamos que $A_8 = \{0, 1, 2, 4, 5\}$. Ahora, recordando que

$$A_4(2) = \{a + 2j : a \in A_2 \text{ y } j \in \{0, 1\}\} \text{ y } A_8(4) = \{a + 4j : a \in A_4 \text{ y } j \in \{0, 1\}\}$$

obtenemos que

$$A_4(2) = \{0, 1, 2, 3\},\ N_4 = A_4(2) \setminus A_4 = \{3\}$$

y

$$A_8(8) = \{0, 1, 2, 4, 5, 6\},\ N_8 = A_8(4) \setminus A_8 = \{6\}.$$

De este modo resulta que $n_2 = |N_{2^2}| = 1$ y $n_3 = |N_{2^3}| = 1$. Por la Proposición 95, resulta que para todo $n > 1$, vale la fórmula de recurrencia

$$\alpha(2^n) = 2\alpha(2^{n-1}) - 1.$$

Ya estamos en posición de calcular $\alpha(2^n)$.

Lema 97. *Para todo $n \in \mathbb{Z}^+$, $\alpha(2^n) = 2^{n-1} + 1$.*

Demostración. Veámoslo por inducción sobre n. En efecto, si $n = 1$, entonces por el Lema 96, $\alpha(2^1) = 2 = 2^{1-1} + 1$. Supongamos que para algún $k \in \mathbb{Z}^+$ se tiene $\alpha(2^k) = 2^{k-1} + 1$. Entonces $k + 1 > 1$ y por lo tanto

$$\alpha(2^{k+1}) = 2\alpha(2^k) - 1 = 2(2^{k-1} + 1) - 1 = 2^k + 2 - 1 = 2^{(k+1)-1} + 1.$$

Se sigue por inducción que $\alpha(2^n) = 2^{n-1} + 1$, para todo $n \geq 1$. □

Ahora, daremos una descripción explícita de los conjuntos A_{2^n} para todo $n \geq 1$. Primero que todo, determinaremos N_{2^n} para todo $n \geq 2$. Note que $N_{2^2} = \{3\}$ y $N_{2^3} = \{6\}$. Para $n > 3$, podemos escribir $n = 2q + r$, donde $r \in \{2, 3\}$. Por (4.3.5) tenemos que $N_{2^n} = \{2^{2q}a : a \in N_{2^r}\} = \{2^{n-r}a : a \in N_{2^r}\}$.

Lema 98. *Para todo $n \geq 2$, $N_{2^n} = \{3 \cdot 2^{n-2}\} = \{2^{n-2} + 2^{n-1}\}$.*

Demostración. Probemos que $\{2^{n-r}a : a \in N_{2^r}\} = \{3 \cdot 2^{n-2}\}$. Primero, supongamos que $r = 2$. Entonces $N_{2^2} = \{3\}$, así que $\{2^{n-2}a : a \in N_{2^2}\} = \{2^{n-2} \cdot 3\} = \{3 \cdot 2^{n-2}(1 + 2)\}$.

Por otro lado, si $r = 3$, entonces $\{2^{n-3}a : a \in N_{2^3}\} = \{2^{n-3} \cdot 6\} = \{3 \cdot 2^{n-2}\}$.

Finalmente, como $3 \cdot 2^{n-2} = (1+2)2^{n-2} = 2^{n-2} + 2^{n-1}$ se sigue que $\{2^{n-2} + 2^{n-1}\} = \{3 \cdot 2^{n-2}\} = N_{2^n}$. Esto termina la prueba. □

Para $n \geq 2$ tenemos que

$$A_{2^n} = A_{2^n}(2^{n-1}) \setminus N_{2^n} = \{a + a_{n-1}2^{n-1} : a \in A_{2^{n-1}}, a_{n-1} \in \{0,1\}\} \setminus N_{2^n}.$$

Proposición 99. *Sea $n \in \mathbb{Z}^+$, $n \geq 2$. Entonces A_{2^n} consiste de todos los elementos de la forma*

$$a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1}, \tag{4.4.2}$$

donde

1. *$a_0, a_1, a_2, \ldots, a_{n-1} \in \{0,1\}$ y*
2. *los dos primeros a_i's no nulos no son consecutivos.*

Demostración. Procedamos por inducción sobre n. Para $n = 2$, tenemos que $A_{2^2} = \{0,1,2\}$, y tenemos que

$$0 = 0 + 0 \cdot 2, \quad 1 = 1 + 0 \cdot 2 \text{ y } \ 2 = 0 + 1 \cdot 2.$$

Claramente estas representaciones de $0, 1$ y 2 satisfacen las condiciones 1 y 2. Por inducción, supongamos que la afirmación se satisface para n y sea $x \in A_{2^{n+1}}$. Luego, $x = a + a_n 2^n$ donde $a \in A_{2^n}$, $a_n \in \{0,1\}$. Como $a \in A_{2^n}$, por la hipótesis de inducción podemos representar a a en la forma

$$a = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1},$$

donde $a_0, a_1, a_2, \ldots, a_{n-1} \in \{0,1\}$ y los dos primeros a_i's no nulos no son consecutivos. Luego

$$x = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1} + a_n 2^n,$$

donde $a_0, a_1, \ldots, a_{n-1}, a_n \in \{0,1\}$. Supongamos, por reducción al absurdo, que los dos primeros a_i's no nulos en la representación de x son consecutivos. Esto no puede ocurrir con a_i y a_{i+1} para $i \leq n-2$ por la hipótesis de inducción. Necesariamente debe ser $a_{n-1} = 1$ y $a_n = 1$; pero esto significaría que $x = 2^{n-1} + 2^n$, es decir, $x \in N_{2^{n+1}}$, lo que contradice que $x \in A_{2^{n+1}}$.

Veamos ahora por inducción sobre n que un elemento que tiene la forma $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1}$ y que satisface las con las condiciones (1) y (2), pertenece

a A_{2^n}. En efecto, para $n = 1$, sea $x = a_0$, con $a_0 \in \{0, 1\}$. Ya que $A_{2^1} = A_2 = \{0, 1\}$, se sigue inmediatamente que $x \in A_{2^1}$. Supongamos que el resultado se cumple para n y veamos que se cumple para $n+1$. Ahora, sea $x = a_0 + a_1\dot{2} + \cdots + a_{n-1} \cdot 2^{n-1} + a_n \cdot 2^n$, donde se cumplen (1) y (2). Luego

$$x = (a_0 + a_1 \cdot 2 + \cdots + a_{n-1} \cdot 2^{n-1}) + a_n \cdot 2^n = a + a_n 2^n,$$

donde $a = a_0 + a_1 \cdot 2 + \cdots + a_{n-1} \cdot 2^{n-1}$. Como se cumple que $a_i \in \{0, 1\}$ para cada $i \in \{0, 1, \ldots, n\}$, en particular $a_i \in \{0, 1\}$, para $i \in \{0, 1, \ldots, n-1\}$, $a_n \in \{0, 1\}$ y los dos primeros $a_i's$ no nulos, no son consecutivos, así que, por la hipótesis de inducción, $a \in A_{2^n}$ y además $a_n \in \{0, 1\}$. Ahora, observe que $x \notin N_{2^{n+1}}$, pues de ser así x tendría la forma $2^{n-1} + 2^n$ y esto ocurriría solamente si todos los $a_i's$ son nulos para $0 \leq i < n-1$ y $a_{n-1} = a_n = 1$, lo cual contradice lo supuesto. Por lo tanto $x \in A_{2^{n+1}}$. □

Con la descripción de A_{2^n} en la Proposición 99, podemos calcular $\alpha(2^n)$ como se muestra a continuación.

Corolario 100. *Para todo $n \in \mathbb{Z}^+$, $\alpha(2^n) = 2^{n-1} + 1$.*

Demostración. Para $n = 1$ ya sabemos que $\alpha(2) = 2^{1-1} + 1$ porque $A_2 = \{0, 1\}$. Para $n \geq 2$, hay 2^{n-i} elementos de la forma $2^{i-2} + 2^{i-1} + a_i 2^i + \ldots + a_{n-1} 2^{n-1}$ para $2 \leq i \leq n$. Así,

$$\alpha(2^n) = 2^n - \sum_{i=2}^{n} 2^{n-i} = 2^n - (2^{n-1} - 1) = 2^{n-1} + 1. \qquad \square$$

4.4.2. Cálculo de $\alpha(p^n)$ donde p es un primo impar

Ahora, calcularemos $\alpha(p^n)$ donde p es un primo impar. Pero antes tenemos el siguiente lema.

Lema 101. *Sea p un primo impar. Consideremos los $N-$conjuntos asociados a $x^2 + y^2$, entonces,*

$$N_{p^2} \subseteq \{jp : 0 < j < p\} \text{ y } N_{p^3} = \{jp^2 : j \notin A_p, 0 < j < p\}.$$

Demostración. Sean p un primo impar y $a \in A_p$, con $a \neq 0$. Luego, existen enteros m_1 y m_2 tales que $m_1^2 + m_2^2 \equiv a \pmod{p}$, luego $p \mid (m_1^2 + m_2^2 - a)$. Observe que si $p \mid m_1$ y $p \mid m_2$, entonces $p \mid (m_1^2+m_2^2)$ y en consecuencia $p \mid a$, así que $p \leq a$. Por otro lado, ya que $a \in A_p \subseteq I_p$, se tiene que $0 \leq a < p$, lo cual es una contradicción. De modo que p no puede dividir simultáneamente a ambos m_1 y m_2. Por lo que podemos suponer sin pérdida de generalidad que $p \nmid m_1$. Luego, por el Lema 87, se sigue que $a + jp \in A_{p^2}$, para todo $0 \leq j < p$. Por lo tanto, si $a + jp \in N_{p^2}$, con $0 \leq j < p$, entonces $a = 0$ y $N_{p^2} \subseteq \{jp : 0 \leq j < p\}$. Además, $0 \in A_{p^2}$, así que $0 \notin N_{p^2}$ y en consecuencia $N_{p^2} \subseteq \{jp : 0 < j < p\}$.

Por otro lado, si $j \in A_p$, existen enteros m_1 y m_2 tales que $m_1^2 + m_2^2 \equiv j \pmod{p}$. Multiplicando por p^2 en la congruencia obtenemos que $(pm_1)^2+(pm_2)^2 \equiv jp^2 \pmod{p^3}$ y por lo tanto $jp^2 \in A_{p^3}$. De donde $N_{p^3} \subseteq \{jp^2 : j \notin A_p, 0 < j < p\}$.

Finalmente si $m_1^2 + m_2^2 \equiv jp^2 \pmod{p^3}$ y $\frac{m_1^2+m_2^2}{p^2} = q_1^2 + q_2^2$ para algunos enteros m_1, m_2, q_1 y q_2, entonces en la congruencia anterior dividimos por p^2 y obtenemos que $q_1^2 + q_2^2 \equiv j \pmod{p}$. Así que $j \in A_p$ si y solamente si $jp^2 \in A_{p^3}$ y por lo tanto $N_{p^3} = \{jp^2 : j \notin A_p, 0 < j < p\}$. □

Proposición 102. *Sea p un número primo tal que $p \equiv 3 \pmod{4}$ y $n \geq 2$. Entonces $N_{p^2} = \{jp : 0 < j < p\}$ y $N_{p^3} = \varnothing$. La fórmula de recurrencia para $\alpha(p^n)$ está dada por*

$$\alpha(p^n) = \begin{cases} p\alpha(p^{n-1}), & \text{si } n \text{ es impar;} \\ p\alpha(p^{n-1}) - p + 1, & \text{si } n \text{ es par.} \end{cases}$$

Una fórmula explicita para $\alpha(p^n)$ es

$$\alpha(p^n) = \begin{cases} \frac{p}{p+1}(p^n + 1), & \text{si } n \text{ es impar;} \\ \frac{1}{p+1}(p^{n+1} + 1), & \text{si } n \text{ es par.} \end{cases}$$

Demostración. Por lo anterior, esto se reduce a probar que $\{jp : 0 < j < p\} \subseteq N_{p^2}$, esto es, $jp \notin A_{p^2}$ si $0 < j < p$. Supongamos por reducción al absurdo que $jp \in A_{p^2}$. Entonces existen enteros m_1 y m_2 tales que $m_1^2 + m_2^2 \equiv jp \pmod{p^2}$. Luego existe un entero w tal que $m_1^2+m_2^2 = jp+wp^2 = p(j+wp)$. Lo cual implica que $p \mid m_1^2+m_2^2$. Y ya

que $p \equiv 3 \pmod 4$, se tiene que el exponente de p en la descomposición en potencias de primos de $m_1^2+m_2^2$ debe ser par. En particular, $p^2 \mid m_1^2+m_2^2$, así que $m_1^2+m_2^2 = p^2c$ para algún entero c y $p^2c = jp + wp^2$, luego, $p(c-w) = j$ y en consecuencia $p \mid j$, lo cual es una contradicción. Hemos mostrado que $N_{p^2} = \{jp : 0 < j < p\}$. Por otro lado, note que si $x_0 \in N_{p^3}$ entonces $x_0 = jp^2$ con $0 < j < p$ y $j \notin A_p$. Pero $A_p = I_p$, por o que no existe j tal que $jp^2 \in N_{p^3}$, esto es, $N_{p^3} = \varnothing$. Además tenemos que $n_2 = |N_{p^2}| = p-1$ y $n_3 = |N_{p^3}| = 0$. Por la Proposición 95, si $n > 1$ es impar

$$\alpha(p^n) = p\alpha(p^{n-1}) - n_3 = p\alpha(p^{n-1}) - 0 = p\alpha(p^{n-1}).$$

Note que esta fórmula también es válida para $n = 1$ puesto que $\alpha(p) = p$. Si n es par, entonces,

$$\alpha(p^n) = p\alpha(p^{n-1}) - n_2 = p\alpha(p^{n-1}) - (p-1) = p\alpha(p^{n-1}) - p + 1.$$

Así obtenemos la siguiente fórmula de recurrencia para $\alpha(p^n)$:

$$\alpha(p^n) = \begin{cases} p\alpha(p^{n-1}), & \text{si } n \text{ es impar;} \\ p\alpha(p^{n-1}) - p + 1, & \text{si } n \text{ es par.} \end{cases} \tag{4.4.3}$$

Veamos por inducción sobre n que si n es par, entonces $\alpha(p^n) = \frac{1}{p+1}(p^{n+1}+1)$ y si n es impar, $\alpha(p^n) = \frac{p}{p+1}(p^n+1)$. Si $n = 1$, n es impar, luego,

$$\alpha(p^1) = p\alpha(p^{1-1}) = p \cdot 1 = p = p\frac{p^1+1}{p+1}.$$

Si $n = 2$, n es par, así que por la fórmula de recurrencia,

$$\alpha(p^2) = p\alpha(p^{2-1}) - p + 1 = p \cdot p - p + 1 = p^2 + p + 1 = (p^2 - p + 1)\frac{p+1}{p+1} = \frac{p^3+1}{p+1}.$$

Supongamos que el resultado se satisface para $n+1$. Consideremos dos casos:

1. Si $n+1$ es impar, n es par y por la fórmula de recurrencia, tenemos que

$$\alpha(p^{n+1}) = p\alpha(p^n) = p\frac{p^{n+1}+1}{p+1}.$$

2. Si $n+1$ es par, entonces n es impar y

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

y como n es impar, $p^n + 1 = (p+1)(p^{n-1} - p^{n-2} + p^{n-3} - \cdots + 1)$. Luego, la ecuación anterior se transforma en

$$\begin{aligned}
\alpha(p^{n+1}) &= p\left(\frac{p((p+1)(p^{n-1} - p^{n-2} + p^{n-3} - \cdots + 1))}{p+1}\right) - p + 1 \\
&= p(p(p^{n-1} - p^{n-2} + p^{n-3} - \cdots + 1)) - p + 1 \\
&= p^{n+1} - p^n + p^{n-1} - \cdots + p^2 - p + 1 \\
&= \frac{p+1}{p+1}(p^{n+1} - p^n + p^{n-1} - \cdots + p^2 - p + 1) \\
&= \frac{p^{n+2}+1}{p+1}.
\end{aligned}$$

Así se deduce la fórmula explicita

$$\alpha(p^n) = \begin{cases} \frac{p}{p+1}(p^n+1), & \text{si } n \text{ es impar;} \\ \frac{1}{p+1}(p^{n+1}+1), & \text{si } n \text{ es par.} \end{cases}$$

□

Sea p un número primo tal que $p \equiv 3 \pmod 4$. Podemos dar una descripción del conjunto A_{p^n} para $n \geq 1$. Recordemos, por la observación del Lema 84, tenemos que A_{p^n} puede representarse en la siguiente forma

$$A_{p^n} = \{a + a_{n-1}p^{n-1} : a \in A_{p^{n-1}}, a_{n-1} \in \{0, 1, \ldots, p-1\}\} \setminus N_{p^n}. \tag{4.4.4}$$

Proposición 103. *Sea $n \geq 2$. Entonces A_{p^n} consiste en todos los enteros de la forma*

$$a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_{n-1} \cdot p^{n-1}, \tag{4.4.5}$$

donde

1. *$a_0, a_1, a_2, \ldots, a_{n-1} \in \{0, 1, \ldots, p-1\}$ y*
2. *el primer subíndice i tal que $a_i \neq 0$ es par.*

Demostración. Procedamos por inducción sobre n; para $n = 2$, por la fórmula (4.4.4), $A_{p^2} = \{a + a_1 p : a \in A_p, a_1 \in \{0, 1, \ldots, p-1\}\}$, luego, cada elemento de A_p^2 es de la forma $x = a_0 + a_1 p$, donde $a_1 = a \in \{0, 1, \ldots p-1\}$. Además a_0 no puede ser 0, pues

de ser así $x \in N_{p^2}$ lo cual contradice que $x \in A_{p^2}$. Supongamos que la afirmación se satisface para n. Ahora, sea $x \in A_{p^{n+1}}$, luego, por (4.4.4),

$$x = a + a_n p^n,$$

donde $a \in A_{p^n}$ y $a_n \in \{0, 1, \ldots, p-1\}$. Como $a \in A_{p^n}$, por hipótesis inductiva, $a = a_0 + a_1 \cdot p + a_2 \cdot^2 + \cdots + a_{n-1} p^{n-1}$, así $x = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_n \cdot p^n$, donde cada $a_i \in \{0, 1, \ldots, p-1\}, i = 0, 1, \ldots, n$.

Falta mostrar que el primer subíndice i tal que $a_i \neq 0$ es par. Supongamos por reducción al absurdo que el primer subíndice i, tal que $a_i \neq 0$ es impar. Esto no puede ocurrir para $0 \leq i \leq n-1$ por la hipótesis de inducción así que necesariamente $x = a_n \cdot p^n$, así que n es impar y $0 < a_n \leq p - 1 < p$, es decir, $x \in N_{p^{n+1}}$, lo cual contradice el hecho de que $x \in A_{p^{n+1}}$.

Veamos ahora que un elemento que tiene la forma (4.4.5) pertenece a A_{p^n}. Ahora, afirmamos que

$$N_{p^n} = \begin{cases} \varnothing, & \text{si } n > 1 \text{ es impar;} \\ \{jp^{n-1} : 0 < j < p\}, & \text{si } n \text{ es par.} \end{cases}$$

Nuevamente por inducción sobre n, para $n = 3$ tenemos ya probado anteriormente que $N_{p^3} = \varnothing$ y $N_{p^2} = \{jp : 0 < j < p\}$. Supongamos que la afirmación se satisface para n. Ahora, si $n+1$ es par, entonces $n-1$ también es par y $N_{p^{n-1}} = \{jp^{n-2} : 0 < j < p\}$. Además sabemos que $N_{p^n} = p^2 N_{p^{n-2}}$ para $n > 3$, de donde,

$$N_{p^{n+1}} = p^2 N_{p^{n-1}} = p^2 \{jp^{n-2} : 0 < j < p\} = \{jp^n; 0 < j < p\}.$$

Por otro lado, si $n+1$ es impar, tenemos que $n-1$ es impar y $N_{p^{n-1}} = \varnothing$. Así que $N_{p^{n+1}} = p^2 N_{p^{n-1}} = p^2 \varnothing = \varnothing$. Esto implica que un elemento de la forma (4.4.5) están en A_{p^n} si y solo si su primer elemento diferente de cero es de la forma $a_i p^i$ con i par. □

Proposición 104. *Sea p un número primo impar tal que $p \equiv 1 \pmod 4$. Entonces, $N_{p^2} = N_{p^3} = \varnothing$. Más aún, $\alpha(p^n) = p^n$ para todo $n \geq 1$.*

Demostración. Si existiera $x_0 \in N_{p^3}$ entonces $x_0 = jp^2$ con $0 < j < p$ y $j \notin A_p$. Pero si $j \notin A_p$ entonces $j \notin I_p$ y por lo tanto no existe $0 < j < p$ tal que $jp^2 \in N_{p^3}$. Por lo tanto $N_{p^3} = \varnothing$. Para probar que $N_{p^2} = \varnothing$, resta probar que $jp \in A_{p^2}$ si $0 < j < p$. En efecto, si $0 < j < p$, entonces por el Lema 96, existen enteros w_1, w_2 y w tales que $w_1^2 + w_2^2 = j + wp$. Como $p \equiv 1 \pmod 4$, por el Teorema de 66, el producto $p(w_1^2 + w_2^2)$ es suma de dos cuadrados, esto es $p(w_1^2 + w_2^2) = m_1^2 + m_2^2$. Por lo tanto $m_1^2 + m_2^2 = p(w_1^2 + w_2^2) = p(j + wp) = jp + wp^2$. Así hemos probado $A_{p^2} = I_{p^2}$ y por tanto $N_{p^2} = \varnothing$.

Por la Proposición 95, se sigue la fórmula recurrente

$$\alpha(p^n) = \begin{cases} p, & \text{si } n = 1; \\ p\alpha(p^{n-1}), & \text{si } n > 1. \end{cases}$$

Veamos que $\alpha(p^n) = p^n$. Si $n = 1$, entonces $\alpha(p^1) = p^1$. Supongamos que la afirmación se satisface para $n > 1$. Ahora, $\alpha(p^{n+1}) = p\alpha(p^n) = p \cdot p^n = p^{n+1}$. □

4.4.3. Cálculo de $\alpha(n)$ y A_n

Hasta este momento, en este capítulo, hemos estudiado varias cuestiones relacionadas con la familia de conjuntos no vacíos $\{A_n\}_{n \in \mathbb{Z}^+}$ asociada al polinomio $x^2 + y^2$, y la función asociada a ella. Vimos que esta familia es multiplicativa, así como la función asociada y calculamos el valor de $\alpha(p^n)$ donde p es primo, $n \geq 1$; y también caracterizamos los elementos en A_{p^n}. En esta subsección analizaremos un poco más la familia de conjuntos A_n, para calcular A_n, donde n no es necesariamente potencia de primo y mostramos algunos ejemplos.

Lema 105. *Sean m_1 y m_2 enteros positivos, primos relativos tales que $1 \leq m_1 m_2 \leq n$. Entonces, $A_n(m_1 m_2) = A_n(m_1) \cap A_n(m_2)$.*

Demostración. Para la primera inclusión, sea $y \in A_n(m_1 m_2)$, luego $y = a + jm_1 m_2$, donde $a \in A_{m_1 m_2}$ y $0 \leq j < n/m_1 m_2$. Podemos reescribir a y como sgue, $y = a + j_1 m_1$ y $y = a + j_2 m_2$, donde $j_1 = jm_2$ y $j_2 = jm_1$, multiplicamos por m_2 en la primera desigualdad y por m_1 en la segunda desigualdad y obtenemos que $0 \leq j_1 < n/m_1$

y $0 \leq j_2 < n/m_2$. Además, ya que $a \in A_{m_1m_2} = A_{m_1m_2}(m_1) \cap A_{m_1m_2}(m_2)$, entonces $a \in A_{m_1m_2}(m_1)$ y $a \in A_{m_1m_2}(m_2)$, por lo que $a = b + im_1$, donde $b \in A_{m_1}$, $0 \leq i < m_2$ y $a = c + km_2$, con $c \in A_{m_2}$ $0 \leq k < m_1$, por MT1 jm_1 y km_2 están en A_{m_1} y A_{m_2} respectivamente y por lo tanto $a \in A_{m_1}$ y $a \in A_{m_2}$. Así $\in A_n(m_1) \cap A_n(m_2)$.

Sea $x \in A_n(m_1) \cap A_n(m_2)$. Entonces $x = a + jm_1 = b + im_2$, donde $a \in A_{m_1}$ y $b \in A_{m_2}$, con $0 \leq j < n/m_1, 0 \leq i < n/m_2$. Entonces, tenemos que, $x \equiv a \pmod{m_1}$ y $x \equiv b \pmod{m_2}$. Luego, por el teorema chino del residuo, existe un único c con $0 \leq c < m_1m_2$ tal que $c \equiv a \pmod{m_1}$ y $c \equiv b \pmod{m_2}$. Además, $x \equiv c \pmod{m_1m_2}$, lo que quiere decir que $x = c + k(m_1m_2)$, donde $0 \leq k < n/(m_1m_2)$. Observar que si $k \geq n/(m_1m_2)$, entonces $km_1m_2 \geq n$, así que $c + k(m_1m_2) \geq c + n$, luego, $x \geq c+n = a+tm_1+n \geq a+m$. Por otro lado, tenemos que $0 \leq j < n/m_1$, entonces $0 \leq jm_1 < n$, así $0 \leq a \leq a + jm_1 < a + n$, por lo que $a \leq x < a + n$. De modo que la desigualdad $x \geq a + n$ no puede ocurrir. Por lo tanto $0 \leq k < n/(m_1m_2)$ y en consecuencia $x \in A_n(m_1m_2)$. □

Corolario 106. *Sean $m_1, m_2, \ldots, m_r$ enteros positivos, primos relativos dos a dos, tales que $1 \leq m_1 \cdots m_r \leq n$. Entonces,*

$$A_n(m_1 \cdots m_r) = A_n(m_1) \cap \cdots A_n(m_r).$$

Demostración. Procedamos por inducción sobre r, para el caso base; si $r = 1$, tenemos que $A_n(m_1) = A_n(m_1)$. Supongamos que la afirmación se satisface para r y sean $m_1, m_2, \ldots, m_r, m_{r+1}$ primos relativos dos a dos y $1 \leq m_1 \cdots m_{r+1} \leq n$, veamos que $A_n(m_1 \cdots m_{r+1}) = A_n(m_1) \cap A_n(m_{r+1})$. En efecto, podemos asociar $m_1 \cdots m_r m_{r+1}$ como sigue $(m_1 \cdots m_r)m_{r+1}$, llamemos $m := m_1 \cdots m_r$. Ahora, podemos observar que como $m_1, m_2, \ldots, m_{r+1}$ son primos relativos dos a dos, entonces m y m_{r+1} son primos relativos, además $1 \leq mm_{r+1} \leq n$. Luego, por el lema anterior

$$\begin{aligned} A_n(m_1 \cdots m_r m_{r+1}) = A_n(mm_{r+1}) &= A_n(m) \cap A_n(m_{r+1}) \\ &= A_n(m_1 \cdots m_r) \cap A_n(m_{r+1}) \\ &= A_n(m_1) \cap \cdots \cap A_n(m_r) \cap A_n(m_{r+1}). \end{aligned}$$ □

Proposición 107. *Sea n un entero positivo, con $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, donde los p_i son primos distintos y los $a_i > 0$ para $i = 1, 2, \ldots, r$. Entonces*

$$A_n = A_n(p_1^{a_1}) \cap A_n(p_2^{a_2}) \cap \cdots \cap A_n(p_r^{a_r})$$

Demostración. Observemos que $A_n = A_n(n)$, por el corolario anterior, tenemos que

$$A_n = A_n(n) = A_n(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) = A_n(p_1^{a_1}) \cap A_n(p_2^{a_2}) \cap \cdots \cap A_n(p_r^{a_r}). \qquad \square$$

Ejemplo 16. Veamos que números se pueden representar como suma de dos cuadrados módulo 6 y módulo 18, esto es equivalente a encontrar los elementos de A_6 y A_{18} utilizando el método.

Calculemos A_6 con este método. Note que $6 = 2 \cdot 3$ y es más fácil hallar A_2 y A_3. Ya sabemos que $A_2 = \{0, 1\}$. Para hallar A_3 consideremos la siguiente tabla, que muestra las sumas de cuadrados módulo 3:

$+$	0^2	1^2	2^2
0^2	0	1	1
1^2	1	2	2
2^2	1	2	2

Tabla 4.4: Suma de dos cuadrados módulo 3

Así que $A_3 = \{0, 1, 2\}$. Ahora, por definición, sabemos que $A_6(2) = \{a + 2j : a \in A_2 \text{ y } 0 \leq j < 6/2\} = \{0 + 2 \cdot 0, 0 + 2 \cdot 1, 0 + 2 \cdot 2, 1 + 2 \cdot 0, 1 + 2 \cdot 1, 1 + 2 \cdot 2\}$. De manera similar $A_6(3) = \{a + 3j : a \in A_3 \text{y } 0 \leq j < 6/3\} = \{0 + 3 \cdot 0, 0 + 3 \cdot 1, 1 + 3 \cdot 0, 1 + 3 \cdot 1, 2 + 3 \cdot 0, 2 + 3 \cdot 1\}$. Así

$$A_6(2) = \{0, 1, 2, 3, 4, 5\} \text{ y } A_6(3) = \{0, 1, 2, 3, 4, 5\}.$$

Finalmente

$$A_6 = A_6(2) \cap A_6(3) = \{0, 1, 2, 3, 4, 5\}.$$

Ahora, para A_{18} tenemos que, $18 = 9 \cdot 2$, ya sabemos que $A_2 = \{0, 1\}$, para hallar A_{18} observemos la siguiente tabla

+	0^2	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2	11^2	12^2	13^2	14^2	15^2	16^2	17^2
0^2	0	1	4	9	16	7	0	13	10	9	10	13	0	7	16	9	4	1
1^2	1	2	5	10	17	8	1	14	11	10	11	14	1	8	17	10	5	2
2^2	4	5	8	13	2	11	4	17	14	13	14	17	4	11	2	13	8	5
3^2	9	10	13	0	7	16	9	4	1	5	1	4	9	16	7	0	13	10
4^2	16	17	2	7	14	5	16	13	8	13	8	13	16	5	14	7	2	17
5^2	7	8	10	15	4	13	7	2	15	2	15	2	7	13	4	15	10	8
6^2	0	1	4	9	16	7	0	13	10	9	10	13	0	7	16	9	4	1
7^2	13	14	17	4	11	2	13	8	5	4	5	8	13	2	11	4	17	14
8^2	10	11	14	1	8	15	10	5	2	1	2	5	10	15	8	1	14	11
9^2	9	10	13	0	7	16	9	4	1	5	1	4	9	16	7	0	13	10
10^2	10	11	14	1	8	15	10	5	2	1	2	5	10	15	8	1	14	11
11^2	13	14	17	4	11	2	13	8	5	4	5	8	13	2	11	4	17	14
12^2	0	1	4	9	16	7	0	13	10	9	10	13	0	7	16	9	4	1
13^2	7	8	10	15	4	13	7	2	15	2	15	2	7	13	4	15	10	8
14^2	16	17	2	7	14	5	16	13	8	13	8	13	16	5	14	7	2	17
15^2	9	10	13	0	7	16	9	4	1	5	1	4	9	16	7	0	13	10
16^2	4	5	8	13	2	11	4	17	14	13	14	17	4	11	2	13	8	5
17^2	1	2	5	10	17	8	1	14	11	10	11	14	1	8	17	10	5	2

Tabla 4.5: Suma de dos cuadrados módulo 18

Podemos observar que

$$A_{18} = \{0, 1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 16, 17\}.$$

Consideremos la siguiente tabla para hallar los elementos que se dejan expresar como suma dos cuadrados módulo 9,

+	0^2	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2
0^2	0	1	4	0	7	7	0	4	1
1^2	1	2	5	1	8	8	1	5	2
2^2	4	5	8	4	2	2	4	8	5
3^2	0	1	4	0	7	7	0	4	1
4^2	7	8	2	7	5	5	7	2	8
5^2	7	8	2	7	5	5	7	2	8
6^2	0	1	4	0	7	7	0	4	1
7^2	4	5	8	4	2	2	4	8	5
8^2	1	2	5	1	8	8	1	5	2

Tabla 4.6: Suma de dos cuadrados módulo 9

De modo que $A_9 = \{0, 1, 2, 4, 5, 7, 8\}$. Sabemos por definición que $A_{18}(9) = \{a + 9j : a \in A_9 \text{ y } 0 \leq j < 2\}$, así que j tiene dos opciones: 0 y 1. Así que los elementos de $A_{18}(9) = \{0+9\cdot 0, 0+9\cdot 1, 1+9\cdot 0, 1+9\cdot 1, 2+9\cdot 0, 2+9\cdot 1, 4+9\cdot 0, 4+9\cdot 1, 5+9\cdot 0, 5+9\cdot 1, 7+9\cdot 0, 7+9\cdot 1, 8+9\cdot 0, 8+9\cdot 1\} = \{0, 9, 1, 10, 2, 11, 4, 13, 5, 14, 7, 16, 8, 17\}$. De manera similar tenemos que $A_{18}(2) = \{a + 2j : a \in A_2 \ y \ 0 \leq j < 9\}$, esto es,

$$A_{18}(2) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}.$$

Observamos de lo anterior que

$$A_{18}(9) \cap A_{18}(2) = 0, 1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 16, 17 = A_{18}.$$

Diseñamos un programa sencillo en Phyton que nos permite calcular A_n para cualquier entero positivo n. Inicialmente definimos $C(k, n)$ al conjunto de los residuos cuadráticos de i^k módulo n, cuando i recorre a I_n, $(k = 2)$:

```
def C(k,n): #Calcula los residuos de i^k cuando i recorre  I_n
  P=[]
  for i in range(n):
    s=(i**k)%n
    if s not in P:
      P.append(s)
    else:
      P=P
  return sorted(P)
```

Continuamos, definiendo ahora $S(k, n)$ que calcula los residuos de $i^k + j^k$ módulo n, cuando i y j recorren los elementos de I_n:

```
 def S(k,n): #Calcula los residuos de i^k+j^k
  R=[]
  L=C(k,n)
  for i in L:
    for j in L:
      s=(i+j)%n
      if s not in R:
        R.append(s)
      else:
        R=R
  return sorted(R)
for n in range(1, n):
  print(n, (S(2,n)))
```

Este algoritmo calcula cuántos elementos tiene A_n para $n = 1, 2, \ldots$, pero si en la última linea reemplazamos $print(n, (S(2, n)))$, por $print(n, len(S(2, n)))$, obtendremos cuáles son esos elementos.

A continuación presentamos una taba con la información obtenida de A_n para $n = 12, 14, 18, 22, \ldots$

A_n	$\alpha(n)$	A_n	$\alpha(n)$	A_n	$\alpha(n)$	A_n	$\alpha(n)$	A_n	$\alpha(n)$	A_n	$\alpha(n)$
A_{12}	9	A_{14}	14	A_{18}	14	A_{22}	22	A_{24}	15	A_{25}	25
A_{26}	26	A_{27}	21	A_{28}	21	A_{30}	30	A_{32}	17	A_{35}	35
A_{36}	21	A_{40}	25	A_{50}	50	A_{56}	35	A_{62}	62	A_{63}	49
A_{64}	33	A_{65}	65	A_{66}	66	A_{68}	51	A_{69}	69	A_{70}	70
A_{72}	35	A_{75}	75	A_{77}	77	A_{81}	61	A_{84}	63	A_{85}	85
A_{89}	89	A_{90}	70	A_{92}	69	A_{94}	94	A_{99}	77	A_{100}	75
A_{120}	75	A_{140}	105	A_{157}	157	A_{221}	221	A_{258}	258	A_{284}	213
A_{290}	290	A_{314}	314	A_{350}	350	A_{368}	207	A_{420}	315	A_{469}	469

Tabla 4.7: Elementos en A_n

Terminamos este trabajo con el siguiente teorema, que caracteriza todos los n tales que el polinomio $x^2 + y^2$ es sobreyectivo en n, es decir, que $\alpha(n) = n$.

Teorema 108. *Sean $n \in \mathbb{Z}^+$. Entonces, el polinomio $x^2 + y^2$ es sobreyectivo en n si y solamente si*

1. *$4 \nmid n$ y*
2. *si p es un número primo con $p \equiv 3 \pmod 4$, entonces $p^2 \nmid n$.*

Demostración. Supongamos que $x^2 + y^2$ es sobreyectivo en n. Entonces

1. Si $4 \mid n$, entonces $n = 4j$ para algún entero j. Como $x^2 + y^2$ es sobreyectivo en n, se tiene que $n - 1 \in A_n$ y en consecuencia existen enteros u y v tales que $u^2 + v^2 \equiv n - 1 \pmod n$. Además $n - 1 \equiv -1 \pmod n$, así que $u^2 + v^2 \equiv -1 \pmod n$. Luego, existe un entero l tal que

$$u^2 + v^2 = -1 + ln = -1 + l(4j) = 4jl - 4 + 3 = 4(jl - 1) + 3 = 4k + 3,$$

   donde $k := jl - 1 \in \mathbb{Z}$. Pero esto es imposible ya que por el Corolario 69, ningún número de la forma $4k + 3$ puede expresarse como suma de dos cuadrados. En consecuencia $4 \nmid n$.

2. Sea p un primo con $p \mid n$, $p \equiv 3 \pmod 4$ y supongamos por reducción al absurdo que $p^2 \mid n$. Como $x^2 + y^2$ es sobreyectivo en n, se tiene que la congruencia $x^2 + y^2 \equiv p \pmod n$ tiene solución, digamos, que existen a y b enteros tales que $a^2 + b^2 \equiv p \pmod n$. De este modo $a^2 + b^2 = p + nt$ para algún entero t. Por otro lado, como $p^2 \mid n$, entonces $n = p^2 s$ para algún entero s y así

$$a^2 + b^2 = p + nt = p + p^2 st = p(1 + pst) = pr,$$

   donde $r := 1 + st \in \mathbb{Z}$. Así que si $m := pr$, tenemos que $p^2 \nmid m$ y m se puede representar como suma de dos cuadrados, pero esto contradice el Teorema 66.

Recíprocamente, supongamos que se satisfacen (1) y (2) y sea $n = 2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ donde los p_i's son primos impares distintos y $a_i > 0$ para cada $i \in \{1, 2, \ldots, r\}$. Veamos que $\alpha(n) = n$. Como $\alpha(n)$ es multiplicativa, tenemos que

$$\alpha(n) = \alpha(2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}) = \alpha(2^{a_0})\alpha(p_1^{a_1})\alpha(p_2^{a_2})\cdots\alpha(p_r^{a_r}).$$

Para los p_i que son de la forma $4k_i + 1$, por la Proposición 104 tenemos que $\alpha(p_i^{a_i}) = p_i^{a_i}$. Para 2^{a_0}, por el Lema 97, $\alpha(2^{a_0}) = 2^{a_0-1} + 1$, pero como $4 \nmid n$, entonces $a_0 = 0$ o $a_0 = 1$;si $a_0 = 0$, entonces $\alpha(2^{a_0}) = \alpha(2^0) = \alpha(1) = 1 = 2^{a_0}$ y si $a_0 = 1$, entonces $\alpha(2^{a_0}) = \alpha(2) = 2 = 2^{a_0}$. Y para los p_i que son la forma $4k_i + 3$, como $p_i^2 \nmid n$, se tiene que $a_i = 1$. Por el Lema 96, $\alpha(p_i^{a_1}) = \alpha(p_i) = p_i = p_i^{a_i}$. Así

$$\alpha(n) = \alpha(2^{a_0})\alpha(p_1^{a_1})\alpha(p_2^{a_2})\cdots\alpha(p_r^{a_r}) = 2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} = n. \qquad \square$$

Futuros estudios

En este trabajo hemos estudiado, entre otras cosas, la representación de enteros como suma de dos cuadrados módulo n, para cualquier entero positivo n. En el futuro se podrá estudiar la representación de enteros como imagen de cualquier polinomio de grado $k > 2$. Siguiendo [1], será interesante estudiar el comportamiento de $\alpha(n)$ cuando A_n es el conjunto de, por ejemplo, todos los enteros de forma $a^3 + b^3$ módulo n, entre otros. Además, se puede estudiar el comportamiento del cociente $\alpha(n)/n$ cuando n tiende a infinito y A_n es el conjunto de todos los enteros positivos que se pueden expresar como imagen de un polinomio módulo n.

Bibliografía

[1] F. Arias, J. Borja, L. Rubio, *Counting integers representable as images of polynomials modulo n*. Journal of Integer Sequences, Vol. 22 (2019).

[2] T. Apostol, *Introduction to analytic number theory*. Springer-Verlag, New York, 1976.

[3] R. Burns, *Representing numbers as the sum of squares and powers in the ring* $\mathbb{Z}_n$, preprint, 2017. Disponible en https://arxiv.org/abs/1708.03930.

[4] D. Burton, *Elementary number theory*. McGraw-Hill, New York, 2002.

[5] E. Cardenal, *La Gema de la Reina: Una breve revisión histórica de la ley de reciprocidad cuadrática*. Lecturas matemáticas, Universidad nacional de Colombia, Bogotá, 2002.

[6] J. Fraleigh, *A first course in abstract algebra* . Addison- Wesley, Massachusetts, 1982.

[7] G. H. Hardy, E. M. Wright, D. Brown, J. Silverman, *An introduction to the theory of numbers*. Oxford university press, England, 1979.

[8] J. Harrington, L. Jones, A. Lamarche, *Representing Integers as the Sum of Two Squares in the Ring* $\mathbb{Z}_n$. Journal of Integer Sequences, Vol. 17(2014).

[9] K. Ireland, M. Rosen, *A classical introduction to modern number theory*. Springer-Verlag, New York, 1990.

[10] M. Pineda, G. Villa, *El campo de los números complejos*. Departamento de matemáticas, Universidad autónoma metropolitana- Iztapalapa.

[11] G. Rubiano, L. Jiménez, J. Gordillo, *Teoría de números para principiantes*. Universidad nacional de Colombia, Bogotá, 2004.

[12] M. Wong, *Representing integers as sums of squares*, 2009. Disponible en http://www.math.uchicago.edu/ may/VIGRE/VIGRE2009/REUPapers/Wong.pdf