Números primos de la forma $x^2 + ny^2$

Aprendiz: Mario Andrés Medina Barrera

Mentor: Sergio Zapata Ceballos

Fundación Universitaria Konrad Lorenz

marioa.medinab@konradlorenz.edu.co

Bogotá, DC

Resumen

Los números primos han sido objeto de estudio desde siglos por lo matemáticos, ya sea su infinitud, su patrón o las formas en que se pueden representar. En este artículo nos centraremos en los primos que se pueden representar de la forma $x^2 + ny^2$, donde $n \in \mathbb{N}$. Esto se hará por medio de herramientas de la teoría de números, teoría de grupos, formas cuadráticas y la teoría elemental de género.

1. Motivación e historia del problema

Los carteos de Fermat y Mersenne fueron una serie de correspondencias que tuvieron lugar en el siglo XVII entre los matemáticos Pierre de Fermat y Marin Mersenne sobre los números primos de la forma $p = x^2 + ny^2$, con $n = 1, 2, 3$.

Fermat y Mersenne estaban particularmente interesados en encontrar una fórmula general para determinar cuándo un número de la forma $p = x^2 + ny^2$ es primo. Fermat llegó a la conclusión de que todos los números primos de la forma $p = 4n + 1$ se podían escribir como $x^2 + y^2$. Así Fermat enunció los siguientes tres teoremas, aunque en el tiempo en que los enunció no los demostró.

Teorema 1.1: Un primo p puede ser escrito como $x^2 + y^2$ si y sólo si $p \equiv 1 \ mod(4)$.

Teorema 1.2: Un primo p puede ser escrito como $x^2 + 2y^2$ si y sólo si $p \equiv 1, 3 \ mod(8)$.

Teorema 1.3: Un primo p puede ser escrito como $x^2 + 3y^2$ si y sólo si $p = 3, p \equiv 1 \ mod(3)$.

Otro gran aportador en este problema fue Euler que dedicó gran parte de su vida a probar los teoremas de Fermat y de alguna manera generalizarlos.

Ahora demostraremos el teorema 1.1 haciendo uso de los siguientes lemas.

Lema 1.1: Si $x, y, z, w \in \mathbb{Z}$, entonces $(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$.

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, página 19 (Ejercicio 1).

Lema 1.2: Suponga que N es una suma de dos cuadrados coprimos, y que $q = x^2 + y^2$ es un divisor primo de N, entonces N/q es también una suma de dos cuadrados coprimos.

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, página 10 (Lema 1,4).

Demostración del Teorema 1.1:
($\Longrightarrow$) La demostración en esta dirección es trivial, ya que se tiene x impar y y par o viceversa, en cualquier caso se llega a que $p \equiv 1 \ mod(4)$.

($\Longleftarrow$) Para esta dirección la estrategia de Euler fue usar el paso de descenso(i) y el de reciprocidad(ii), los cuales son

i. Si $p \mid x^2 + y^2$, $mcd(x, y) = 1$, entonces p puede ser escrito como una suma de cuadrados.

ii. Si $p \equiv 1 \ mod(4)$, entonces $p \mid x^2 + y^2$, $mcd(x, y) = 1$.

Para el paso de descenso suponga que $x' = x + pk$ y $y' = y + pl$ para $k, l \in \mathbb{Z}$, entonces p divide a $x'^2 + y'^2$, ya que

$$x'^2 + y'^2 = x^2 + y^2 + 2xpk + 2ypl + p^2k^2 + p^2l^2$$

Entonces podemos elegir un k, l de tal manera que $2|x'| < p$ y $2|y'| < p$ y $p \mid x'^2 + y'^2$. Ahora notese que p no divide a $mcd(x', y')$ ya que implicaría que divide a x y y, después de dividir entre el mcd podemos asumir que $2|x| < p$ y $2|y| < p$ con $p \mid x^2 + y^2$ y $mcd(x, y) = 1$, de esta manera tenemos que el factor primo más grande de $x^2 + y^2$ es p, ya que considere otro $q \mid x^2 + y^2$, entonces $x^2 + y^2 = qpm$, $m \in \mathbb{Z}$ y

$$x^2 + y^2 < \frac{p^2}{2} \Longrightarrow pqm < \frac{p^2}{2} \Longrightarrow qm < \frac{p}{2} < p \Longrightarrow q < p$$

Ahora si todos los divisores menores que p son de la forma $x^2 + y^2$, entonces por el lema 1.1 y el lema 1.2, p también debe ser una suma de cuadrados, si p no es de esa forma se concluye que debe haber un primo q_1 menor que p, que tampoco es de esa forma. Ahora si volvemos a aplicar el procedimiento a partir de $q_1 \mid x^2 + y^2$, $mcd(x, y) = 1$, se llega a que debe haber otro primo q_2 menor a q_1, tal que no es una suma de cuadrados, aplicando nuevamente este procedimiento indefinidamente llegamos a una sucesión infinita de primos descendentes, lo cual es absurdo, entonces se debe cumplir que p es una suma de cuadrados.

Ahora para el paso de reciprocidad se usa el pequeño teorema de Fermat notando que $p = 4k+1$ y tomando cualquier $x \not\equiv 0 \quad mod(p)$, entonces

$$x^{4k} \equiv 1\ mod(p) \Longrightarrow x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1) \equiv 0\ mod(p)$$

y si además $x^{2k} - 1 \not\equiv 0 \quad mod(p)$ para algún x, entonces $x^{2k} + 1 \equiv 0 \quad mod(p)$ y por lo tanto $p \mid x^{2k} + 1$, donde $mcd(x, 1) = 1$, dicho x existe ya que $x^{4k} - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ y tiene máximo $2k < p - 1$ raíces.

Para los demás teoremas 1.2 y 1.3 también se emplea la misma estrategia del paso descendente y el de reciprocidad con sus respectivos ajustes. Ahora tome en consideración los siguientes lemas.

Lema 1.3: Si $x, y, z, w \in \mathbb{Z}$ y $n \in \mathbb{N}$, entonces.

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2$$

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, página 19 (Ejercicio 1).

Lema 1.4: Suponga que N es una suma de la forma $a^2 + nb^2$ y que $q = x^2 + ny^2$ es un divisor primo de N. Entonces N/q es también una suma de la forma $N/q = c^2 + nd^2$.

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, página 19 (Ejercicio 3).

A partir de los anteriores lemas se podría pensar que el paso de descenso es general para cualquier $n \in \mathbb{N}$. Pero nótese que el paso de descenso falla con $n = 5$, porque $3 \mid 21 = 1^2 + 5(2)^2$ pero $3 \neq x^2 + 5y^2$ para $x, y \in \mathbb{Z}$, de esta manera se concluye que el paso de descenso no es general.

Ahora para $p \mid x^2 + ny^2$ con $mcd(x, y) = 1$, se tiene que $x^2 + ny^2 \equiv 0\ mod(p)$ y por lo tanto $x^2 \equiv -ny^2\ mod(p)$. Nótese que $mcd(y, p) = 1$ ya que en el caso $mcd(y, p) = p$ se tiene que $p \nmid x^2 + ny^2$ y para el caso $mcd(y, p) = d < p$ solo es posible que $d = 1$, ya que p es un primo. Ahora al tener que el conjunto $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo (cada elemento tiene inverso multiplicativo), y que $y \in (\mathbb{Z}/p\mathbb{Z})^*$ entonces

$$\begin{aligned} x^2(y^{-1})^2 &\equiv -ny^2(y^{-1})^2\ mod(p) \\ \Longrightarrow (xy^{-1})^2 &\equiv -n\ mod(p) \end{aligned}$$

Esto sugiere que para generalizar el paso de reciprocidad se debe estudiar los residuos cuadrados equivalentes a $-n$ módulo p

$$x^2 \equiv -n\ mod(p)$$

de tal manera que impliquen que $p \mid x^2 + ny^2$ con $mcd(x, y) = 1$.

2. Reciprocidad cuadrática

Para resolver la cuestión anterior definiremos el símbolo de Legendre (a/p), donde a es un entero y p es un primo impar y los residuos cuadráticos módulo p:

Definición de residuo cuadrático: $b \in \mathbb{Z}$ es un residuo cuadrático módulo p, si existe un $x \in \mathbb{Z}$ tal que $x^2 \equiv b \quad mod(p)$.

Definición de símbolo de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ y } a \text{ es un residuo cuadrático modulo } p \\ -1 & p \nmid a \text{ y } a \text{ es un residuo no cuadrático modulo } p \end{cases}$$

Una vez definido el símbolo de Legendre tenemos el siguiente lema.

Lema 2.1:

$$p \mid x^2 + ny^2 \ , \ mcd(x, y) = 1 \Longleftrightarrow \left(\frac{-n}{p}\right) = 1$$

Demostración: ($\Longrightarrow$) Como se mostró anteriormente $p \mid x^2 + ny^2$ con $mcd(x, y) = 1$ implica que

$$(xy^{-1})^2 \equiv -n \ mod(p)$$

y por lo tanto $(-n/p) = 1$.
($\Longleftarrow$) Dado $x_1^2 \equiv -n \ mod(p)$ se tiene que para un $y \in \mathbb{Z}$ con $mcd(y, p) = 1$

$$\begin{aligned} & x_1^2 y^2 \equiv -ny^2 \ mod(p) \\ \Longrightarrow & (x_1 y)^2 \equiv -ny^2 \ mod(p) \\ \Longrightarrow & (x_1 y + p)^2 \equiv -ny^2 \ mod(p) \end{aligned}$$

y por lo tanto denotando $x = x_1 y + p$, se tiene que $p \mid x^2 + ny^2 \ mod(p)$ y $mcd(x, y) = 1$, ya que si $mcd(x, y) \neq 1$, entonces contradeciría $mcd(y, p) = 1$.

Ahora con el lema 2.1 podemos formular la pregunta para que $p \equiv \alpha, \beta, \cdots mod(4n)$ implica que $(-n/p) = 1$ (y por lo tanto a $p \mid x^2 + ny^2$, $mcd(x, y) = 1$), incluso para $n < 0$. Esto es algo sobre lo que Euler ya había hecho conjeturas, tales como

$$\begin{aligned} \left(\frac{3}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1 \ mod(12) \\ \left(\frac{5}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1, \pm 11 \ mod(20) \\ \left(\frac{7}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \ mod(28) \end{aligned}$$

notese que en la segunda equivalencia $11 \equiv -9 \ mod(20)$ y $3 \equiv -25 \ mod(28)$ y por lo tanto

$$\begin{aligned} \left(\frac{3}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1 \ mod(12) \\ \left(\frac{5}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1, \pm 9 \ mod(20) \\ \left(\frac{7}{p}\right) &= 1 \Longleftrightarrow p \equiv \pm 1, \pm 25, \pm 9 \ mod(28) \end{aligned}$$

De esta manera se podría deducir que se cumple que $p \equiv \pm \beta^2 \ mod(4n)$, para algún entero β, pero nótese que en un caso q par se tiene que

$$\left(\frac{6}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1, \pm 5 \ mod(24)$$

donde ± 5 no puede ser transformado a un cuadrado de un impar modulo 24.

A partir de estos resultados Euler conjeturó que para p y q primos impares distintos se cumple que

$$\left(\frac{q}{p}\right) \Longleftrightarrow p \equiv \pm \beta^2 \ mod(4q), \text{ para algún entero } \beta$$

Donde la conjetura anterior es equivalente al siguiente teorema.

Teorema de la reciprocidad cuadrática: Si p y q son primos impares distintos, entonces

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

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, página 14 (Proposición $1,10$).
Ahora por medio del teorema de la reciprocidad cuadrática se puede generalizar el paso de reciprocidad con la siguiente proposición.

Proposición 2.1: Sea n un entero distinto a cero, y sea $\mathcal{X} : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ el homomorfismo del lema 2.2, entonces cuando $D = -4n$ se tiene que si p es un primo impar que no divide a n, entonces las siguientes condiciones son equivalentes:

i. $p \mid x^2 + ny^2$, $gcd(x, y) = 1$.

ii. $(-n/p) = 1$

iii. $[p] \in ker(\mathcal{X}) \subset (\mathbb{Z}/4n\mathbb{Z})^*$

Lema 2.2: Si $D \equiv 0, 1\ mod(4)$ es un entero distinto de cero, entonces hay un único homomorfismo de grupos $\mathcal{X} : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$, tal que para todo primo impar p con $p \nmid D$, $\mathcal{X}([p]) = (D/p)$, además

$$\mathcal{X}([-1]) = \begin{cases} 1 & D > 0 \\ -1 & D < 0 \end{cases}$$

Demostración: Ver prueba en [1]. Capítulo 1, sección 1, páginas $15, 16$ (Lema 1,14).

Demostración de la Proposición 2.1: (i) $\Longleftrightarrow$ (ii) se siguen del lema 2.2 y (ii) $\Longleftrightarrow$ (iii) siguen del hecho de que

$$\left(\frac{-4n}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{-n}{p}\right) = \left(\frac{-n}{p}\right)$$

De esta manera podemos determinar las congruencias $p \equiv \alpha, \beta \cdots mod(4n) \in (\mathbb{Z}/4n\mathbb{Z})$ para que se cumpla que $p \mid x^2 + ny^2$, $mcd(x, y) = 1$. Aunque ya se ha generalizado el paso de reciprocidad, un problema que surge que ya había visto Euler, por ejemplo para el caso $n = 14$ es que el hecho de que hallemos unas condiciones de congruencia $p \equiv \alpha, \beta \cdots mod(4n)$ no quiere decir que estas solo impliquen que $p = x^2 + ny^2$, ya que pueden p puede ser representado por otras formas algebraicas, por ejemplo

$$p = \begin{Bmatrix} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{Bmatrix} \Longleftrightarrow p \equiv 1, 9, 15, 23, 25, 39\ mod(56)$$
$$p = \begin{Bmatrix} x^2 + 5y^2 \\ 2x^2 + 2xy + 3y^2 \end{Bmatrix} \Longleftrightarrow p \equiv 1, 3, 7, 9\ mod(20)$$

3. Formas cuadráticas

Para resolver el problema anterior introduciremos la teoría de las formas cuadráticas desarrollada por Legendre y Gauss. Se dice que una forma cuadrática es una expresión algebraica dada por $ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, la cual se dice además que es primitiva si $mcd(a, b, c) = 1$.
Se dice que un entero m es representado por una forma $f(x, y)$, si la ecuación $m = f(x, y)$ tiene solución entera en x y y, adicionalmente se dice que m es propiamente representado si $mcd(x, y) = 1$, nótese que el tema de estudio es hallar los primos p que son representados por la forma cuadrática $x^2 + ny^2$, antes de continuar definiremos lo que es acción de grupo y de órbita.

Definición de acción de grupo: Sea G un grupo y X un conjunto, entonces una acción de G sobre X es una función, $\phi : G \times X \longrightarrow X$, donde se cumple que $\phi(e, x) = x$ con e siendo el elemento identidad de G y $x \in X$, al igual que $\phi(g, \phi(h, x)) = \phi(g \cdot h, x)$, con $g, h \in G$ y $x \in X$.

Por simplicidad denotaremos a $\phi(g, x)$ donde ϕ es una acción de grupo y $g \in H$, $x \in X$ como gx, o sea $\phi(g, x) = gx$.

Definición de órbita: Sea G un grupo y X un conjunto, donde G actúa sobre X, entonces la órbita $O(x)$ para un $x \in X$, se define como $O(x) = \{gx : g \in G\}$, donde $gx = \phi(g, x)$, siendo ϕ la acción de grupo dada. Cabe resaltar que las órbitas de un conjunto X forman una partición del conjunto X.

Ahora decimos que dos formas $f(x, y)$ y $g(x, y)$ son equivalentes si existe un $h \in \mathrm{GL}(2, \mathbb{Z})$, tal que para la acción de grupos $\phi : \mathrm{GL}(2, \mathbb{Z}) \times X \longrightarrow X$ (X es el conjunto de formas cuadráticas primitivas) se cumpla que

$$\phi\left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} \times g(x, y)\right) = g(px + qy, rx + sy) = f(x, y)$$

$$h = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

De donde se sigue que la equivalencia de formas es una relación de equivalencia, ya que al definir dos formas cuadráticas primitivas x y y, tal que $x \sim y \iff \exists\, g \in \mathrm{GL}(2, \mathbb{Z})$, tal que $gx = y$, puede ser traducido a la definición de órbita, donde de todas las formas cuadráticas primitivas y equivalentes a una forma cuadrática primitiva x, se tiene que $y \in O(x)$, donde el conjunto de orbitas $O(x)$ forman una partición del conjunto X y por lo tanto una relación de equivalencia.

Es importante notar que formas equivalentes representan los mismos números. Ahora denotamos como Gauss una equivalencia propia, donde $h \in \mathrm{SL}(2, \mathbb{Z})$ y una equivalencia impropia donde $h \in \mathrm{GL}(2, \mathbb{Z})/\mathrm{SL}(2, \mathbb{Z})$.

Ahora definiremos el discriminante de una forma $ax^2 + bxy + cy^2$ como $D = b^2 - 4ac$, ahora denotanto el discriminante de $f(x, y)$ como D y el discriminante de $g(x, y)$ como D', entonces se se cumple que si $f(x, y)$ y $g(x, y)$ son equivalentes, entonces $D = (ps - qr)^2 D' = D'$. Ahora para una forma $f(x, y)$ con discriminante D, se tiene la siguiente identidad

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

donde si se cumple que $D > 0$, entonces $f(x, y)$ representa tanto a enteros negativos y positivos, mientras que si $D < 0$ se tiene que $f(x, y)$ representa o solo enteros negativos o positivos dependiendo del signo de a, de esta manera definimos las formas definidas postivas o definidas negativas. De esto surge el siguiente lema y corolario.

Lema 3.1: Sea $D \equiv 0, 1\ mod(4)$ un entero y m un entero impar coprimo con D. Entonces m es propiamente representado por una forma primitiva de descriminante D si y sólo si D es un residuo cuadrático módulo m.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 24 (Lema 2,5).

Corolario 3.1: Sea n un entero y sea p un primo impar que no divide a n, entonces $(-n/p) = 1$ si y sólo si p es representado por una forma primitiva de discriminante $-4n$.

Demostración: Se sigue inmediatamente del lema 3.2, ya que $-4n$ es un residuo cuadrático módulo n, si y sólo si $(-4n/p) = (-n/p) = 1$.

Este corolario es un importante avance a la hora de generalizar el paso de descenso, pero nótese del corolario anterior que hay muchas formas cuadráticas con discriminante $-4n$, para solucionar este problema introducimos las formas reducidas definidas positivas, las cuales se definen como una forma $ax^2 + bxy + cy^2$ donde se cumple que

$$|b| \leq a \leq c, \text{ y } b \geq 0 \text{ si se cumple que } |b| = a \text{ o } a = c$$

De este definición se tiene el siguiente teorema.

Teorema 3.1: Cada forma primitiva definida positiva es propiamente equivalente a una única forma reducida.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, páginas $25, 26$ (Teorema 2,8).

Ahora se sigue por la definición de discriminante y de forma reducida positiva los siguientes resultados.

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \Longrightarrow a \leq \sqrt{(-D)/3}$$

$$|b| \le a$$

$$b^2 - 4ac = D \Longrightarrow c = \frac{(-D) + b^2}{4a}$$

De esta manera se deduce que dado un discriminante $D < 0$ se tiene que hay finitas formas reducidas con discriminante D y por lo tanto el número de clases propiamente equivalentes es también finito y se dice que dos formas están en la misma clase si son propiamente equivalentes, de esta manera denotamos $h(D)$ como el número de clases de formas primitivas definidas positivas de discriminante D.

Teorema 3.2: Sea $D < 0$, entonces el número $h(D)$ de clases de formas primitivas definidas positivas de discriminante D es finito.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 27 (Teorema 2,13).

Ahora con todos estos ingredientes podemos generalizar el paso de descenso con la siguiente proposición y los siguientes teoremas.

Proposición 3.1: Sea n un entero positivo y p un primo impar que no divide a n, entonces $(-n/p) = 1$ si y sólo si p es representado por una de las $h(-4n)$ formas reducidas de discriminante $-4n$.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 28 (Proposición 2,15).

Teorema 3.3: Sea $D \equiv 0, 1\ mod(4)$ negativo y sea $\mathcal{X} : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ el homomorfismo del lema 2.2, entonces para un primo impar p que no divide a D, $[p] \in ker(\mathcal{X})$ si y sólo si p es representado por una de las $h(D)$ formas reducidas de discriminante D.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 28 (Teorema 2,16).

Nótese que para el caso $h(D) = 1$ el teorema 3.3 resuelve el paso de descenso ya que todos los primos impares p, tal que $[p] \in ker(\mathcal{X})$, son representados por una única forma reducida, así que no necesitamos clasificar de alguna manera los primos p.

Teorema 3.4: Sea n un entero positivo, entonces

$$h(-4n) = 1 \Longleftrightarrow n = 1, 2, 3, 4, 7$$

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 29 (Teorema 2,18).

Este último teorema 3.4 muestra porque el paso de descenso funcionó tan bien para $n = 1, 2, 3$ pero no para $n = 5$.

4. Teoría elemental de género

Ahora que se ha descubierto que $h(D) = 1$ se cumple para casos finitos, queremos saber como clasificar a los números primos representados por $x^2 + ny^2$ cuando $h(-4n) > 1$, o sea queremos saber como separar formas reducidas con mismo discriminante, para ello usaremos las ideas de Legendre. Se dice que dos formas cuadráticas están en el mismo género si representan a los mismos valores de $(\mathbb{Z}/D\mathbb{Z})^*$ sobre $(\mathbb{Z}/D\mathbb{Z})$, entonces cada género consiste de finitas clases de formas reducidas. El impacto de esta idealización se hace cuando se usa el teorema 3.3 y la definición de forma principal, el cual se define como

$$\begin{array}{rl} x^2 - \frac{D}{4}y^2 & D \equiv 0\ mod(4) \\ x^2 + xy + \frac{1-D}{4}y^2 & D \equiv 1\ mod(4) \end{array}$$

donde $D < 0$. Nótese que en el caso $D \equiv 0\ mod(4)$ en la forma principal tenemos a $x^2 + ny^2$. Ahora definiremos la clase lateral, el cual es un concepto que se usará en los siguientes resultados.

Definición de clase lateral izquierda: Sean H y G grupos y $H \le G$, entonces una clase lateral izquierda xH en G se define como $xH = \{xH : x \in G\}$ (en este caso xH no representa una acción de grupo).

Proposición 4.1: Dado un entero negativo $D \equiv 0, 1\ mod(4)$, sea $ker(\mathcal{X}) \subset (\mathbb{Z}/D\mathbb{Z})^*$ como en el teorema 3.3, y sea $f(x, y)$ una forma con discriminante D, entonces se tiene que

i. Los valores en $(\mathbb{Z}/D\mathbb{Z})^*$ representados por la forma principal de discriminante D forma un subgrupo $H \subset ker(\mathcal{X})$.

ii. Los valores en $(\mathbb{Z}/D\mathbb{Z})^*$ representados por una forma $f(x,y)$ forman una clase lateral izquierda de H en $ker(\mathcal{X})$.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, páginas $31, 32$ (Lema 2.24).

Teorema 4.1: Sea $D \equiv 0, 1 \ mod(4)$ negativo, y sea $H \subset ker(\mathcal{X})$ como en la proposición 4.1, si H' es una clase lateral izquierda de H en $ker(\mathbb{Z})$ y p es un primo impar que no divide a D, entonces $[p] \in H'$ si y sólo si p es representado por una forma reducida de discriminante D en el genero de H'.

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 32 (Teorema 2,26).

Corolario 4.1: Sea n un entero positivo y p un primo impar que no divide a n. Entonces p es representado por una forma de discriminante $-4n$ en el género principal si y sólo si para algún entero β se cumple que

$$p \equiv \beta^2, \beta^2 + n \ mod(4n)$$

Demostración: Ver prueba en [1]. Capítulo 1, sección 2, página 33 (Corolario 2,27).

5. Ejemplos

Muestre que

$$p = x^2 + 6y^2 \Longleftrightarrow p \equiv 1, 7 \ mod(24)$$
$$p = 2x^2 + 3y^2 \Longleftrightarrow p = 5, 11 \ mod(24)$$

Notese que ambas formas tienen discriminante $D = -24$, de esta manera hallaremos las formas reducidas con discriminante $D = -24$.

$$a \leq \sqrt{\frac{24}{3}} = \sqrt{8} \approx 2$$

Entonces tenemos las siguientes opciones

$$\begin{array}{ccc} a = 2 & a = 2 & a = 2 \\ b = 0 & b = \pm 1 & b = 2 \\ c = \frac{24}{8} = 3 & c = \frac{25}{8} & c = \frac{28}{8} \end{array}$$

$$\begin{array}{cc} a = 1 & a = 1 \\ b = 0 & b = 1 \\ c = \frac{24}{4} = 6 & c = \frac{25}{4} \end{array}$$

Entonces hay dos formas reducidas las cuales son $2x^2 + 3y^2$ y $x^2 + 6y^2$.
Ahora debemos hallar el kernel de $\mathcal{X} : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$, donde

$$(\mathbb{Z}/24\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}$$

Donde 1 es siempre residuo cuádratico de cualquier módulo, entonces

$$\left(\frac{-24}{5}\right) = \left(\frac{1}{5}\right) = 1$$
$$\left(\frac{-24}{7}\right) = \left(\frac{4}{7}\right) = 1$$
$$\left(\frac{-24}{11}\right) = \left(\frac{9}{11}\right) = 1$$

$$\left(\frac{-24}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{168/8} = -1$$
$$\left(\frac{-24}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right)(-1)^{186/4} = \left(\frac{2}{5}\right) = -1$$
$$\left(\frac{-24}{19}\right) = \left(\frac{14}{19}\right) = \left(\frac{7}{19}\right)\left(\frac{2}{19}\right) = \left(\frac{19}{7}\right)(-1)^{(18\cdot 6/4)+1} = \left(\frac{5}{7}\right) = \left(\frac{2}{5}\right)(-1)^{6\cdot 4/4} = -1$$
$$\left(\frac{-24}{23}\right) = \left(\frac{22}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{11}{23}\right) = \left(\frac{23}{11}\right)(-1)^{22\cdot 10/4} = -\left(\frac{1}{23}\right) = -1$$

Una vez ya hallamos el kernel de $\mathcal{X}$, ahora usando el corolario 4.1 tenemos que de $1, 5, 7, 11$ el que cumple con las condiciones son $1, 7$, ya que

$$p \equiv 1^2 \ mod(24)$$
$$p \equiv 1^2 + 6 \ mod(24)$$

Por lo tanto

$$p = x^2 + 6y^2 \iff p \equiv 1, 7 \ mod(24)$$

y usando el teorema 3.3 se tiene que las representaciones restantes van a la otra clase, o sea

$$p = 2x^2 + 3y^2 \iff p = 5, 11 \ mod(24)$$

Muestre que

$$p = x^2 + xy + 4y^2 \iff p \equiv 1, 4 \ mod(15)$$
$$p = 2x^2 + xy + 2y^2 \iff p = 2, 8 \ mod(15)$$

Notese que ambas formas tienen discriminante $D = -15$, de esta manera hallaremos las formas reducidas con discriminante $D = -15$.

$$a \leq \sqrt{\frac{15}{3}} = \sqrt{5} \approx 2$$

Entonces tenemos las siguientes opciones

$$\begin{array}{ccc} a = 2 & a = 2 & a = 2 \\ b = 0 & b = \pm 1 & b = 2 \\ c = \frac{15}{8} = 3 & c = \frac{16}{8} = 2 & c = \frac{19}{8} \end{array}$$

$$\begin{array}{cc} a = 1 & a = 1 \\ b = 0 & b = 1 \\ c = \frac{15}{4} = 6 & c = \frac{16}{4} = 4 \end{array}$$

Entonces hay dos formas reducidas las cuales son $2x^2 + xy + 2y^2$ y $x^2 + xy + 4y^2$.
Ahora debemos hallar el kernel de $\mathcal{X} : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$, donde

$$(\mathbb{Z}/15\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

Donde 1 es siempre residuo cuádratico de cualquier módulo, entonces

$$\left(\frac{-15}{17}\right) = \left(\frac{2}{17}\right) = (-1)^{288/8} = 1$$
$$\left(\frac{-15}{19}\right) = \left(\frac{4}{19}\right) = 1$$
$$\left(\frac{-15}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{7-1/2} = -1$$
$$\left(\frac{-15}{23}\right) = \left(\frac{8}{23}\right) = (-1)^{176\cdot 3} = 1$$

$$\left(\frac{-15}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{11}{7}\right)(-1)^{10\cdot 6/4} = -\left(\frac{4}{7}\right) = -1$$
$$\left(\frac{-15}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)(-1)^{12\cdot 10/4} = \left(\frac{2}{11}\right) = (-1)^{120/8} = -1$$
$$\left(\frac{-15}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right)(-1)^{28\cdot 6/4} = -\left(\frac{1}{7}\right) = -1$$

Una vez ya hallamos el kernel de $\mathcal{X}$, vemos de manera inmediata que la forma principal $x^2 + xy + 4y^2$ representa al 4 y al 1, entonces

$$p = x^2 + xy + 4y^2 \iff p \equiv 1, 4 \; mod(15)$$

Por otro lado se tiene que $2x^2 + xy + 2y^2$ representa al 2 y al 8, entonces

$$p = 2x^2 + xy + 2y^2 \iff p = 2, 8 \; mod(15)$$

Referencias

[1] David A. Cox, *Primes of the form x^2+ny^2—Fermat, class field theory, and complex multiplication*, AMS Chelsea Publishing, Providence, RI, [2022] ©2022. Third edition [of 1028322] with solutions; With contributions by Roger Lipsett. MR4502401