IDEALES COPRIMOS AL CONDUCTOR Y EL NÚMERO DE CLASES

SEBASTIÁN RAHAUSEN

Introducción

Sea $\mathcal{O} = [1, fw_K]$ un orden de conductor f en un cuerpo cuadrático imaginario K. En la Sección 1 describiremos el grupo de clases de ideales $C(\mathcal{O})$ en términos del orden maximal $\mathcal{O}_K$ (ver Proposición 1.6). Para esto, necesitaremos encontrar una relación entre $\mathcal{O}$-ideales propios y $\mathcal{O}_K$-ideales. Esto lo haremos estudiando *$\mathcal{O}$-ideales coprimos al conductor f*. En la Sección 2 aplicaremos la Proposición 1.6 para obtener una fórmula para el *número de clases* $h(\mathcal{O})$ en términos del conductor f y el número de clases $h(\mathcal{O}_K)$ (ver Teorema 2.1). Luego, usaremos el Teorema 2.1 para hallar una fórmula que relaciona los números de clases de dos ordenes arbitrarios $\mathcal{O}' \subseteq \mathcal{O}$ en K (ver Corolario 2.2), y para probar el Teorema de Baker, Heegner y Stark (Teorema 4.1 de Charla 1-2) asumiendo verdadero el caso de discriminantes d_K de ordenes maximales (ver Teorema 2.3).

1. Ideales coprimos al conductor

Esta sección está basada en la parte C de la sección 7 del Capítulo 2 de [Cox13].

Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K. Comenzamos con la siguiente definición

Definición 1.1. Diremos que un $\mathcal{O}$-ideal $\mathfrak{a} \neq 0$ es *coprimo a f* si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

Los $\mathcal{O}$-ideales coprimos al conductor satisfacen las siguientes propiedades básicas

Lema 1.2. *Sea $\mathcal{O}$ un orden de conductor f.*

(1) *Un $\mathcal{O}$-ideal $\mathfrak{a}$ es coprimo a f si y sólo si* $\mathrm{mcd}(N(\mathfrak{a}), f) = 1$.
(2) *Todo $\mathcal{O}$-ideal coprimo a f es propio.*

Demostración. (1): Sea $m_f : \mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ la función multiplicación por f. Notar que m_f es un homomorfismo de grupos abelianos finitos de orden $N(\mathfrak{a})$. Es sencillo verificar que

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \Leftrightarrow m_f \text{ es sobreyectiva } \Leftrightarrow m_f \text{ es isomorfismo de grupos.}$$

Por el teorema fundamental de grupos abelianos finitos (ver [DF04, I.5.2 Theorem 3]), se tiene que m_f es un isomorfismo de grupos si y sólo si $\mathrm{mcd}(N(\mathfrak{a}), f) = 1$. Esto muestra (1).

(2): Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. Mostraremos que $\mathfrak{a}$ es un $\mathcal{O}$-ideal propio, i.e.,

$$\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}.$$

Como $\mathfrak{a}$ es un $\mathcal{O}$-ideal, la inclusión $\supset$ es directa. Para probar la otra, sea $\beta \in K$ tal que $\beta\mathfrak{a} \subset \mathfrak{a}$. Afirmamos que $\beta \in \mathcal{O}_K$. En efecto, multiplicando por $\mathcal{O}_K$ se obtiene una inclusión de $\mathcal{O}_K$-ideales $\beta\mathfrak{a}\mathcal{O}_K \subset \mathfrak{a}\mathcal{O}_K$. Cada ideal del orden maximal $\mathcal{O}_K$ es propio (Observación 2.12, Charla 3), luego invertible en $I_K := I(\mathcal{O}_K)$. Multiplicando por $(\mathfrak{a}\mathcal{O}_K)^{-1}$ obtenemos $\beta\mathcal{O}_K \subset \mathcal{O}_K$, lo que prueba $\beta \in \mathcal{O}_K$. Luego

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K.$$

Además, $f\mathcal{O}_K \subset \mathbb{Z} + f\mathcal{O}_K = \mathcal{O}$, lo que junto con la inclusión anterior prueba $\beta\mathcal{O} \subset \mathcal{O}$. Por tanto $\beta = \beta \cdot 1 \in \beta\mathcal{O} \subset \mathcal{O}$. Esto muestra que $\mathfrak{a}$ es propio. □

Del Lema 1.2 se sigue que los $\mathcal{O}$-ideales coprimos a f están en $I(\mathcal{O})$ y son cerrados bajo multiplicación (pues si $\mathfrak{a}, \mathfrak{b}$ son coprimos a f, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ muestra que $\mathfrak{ab}$ también será coprimo a f). Por tanto, ellos generan un subgrupo de $I(\mathcal{O})$ que denotamos $I(\mathcal{O}, f)$. Dentro de $I(\mathcal{O}, f)$ tenemos el subgrupo $P(\mathcal{O}, f)$ generado por los ideales pricipales $\alpha\mathcal{O}$ donde $\alpha \in \mathcal{O}$ satisface $\mathrm{mcd}(N(\alpha), f) = 1$. Así, podemos describir $C(\mathcal{O})$ en términos de $I(\mathcal{O}, f)$ y $P(\mathcal{O}, f)$ como sigue:

Proposición 1.3. *Se tiene un isomorfismo de grupos de clases de ideales*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq C(\mathcal{O})$$

Demostración. Por Corolario 0.1 de Charla 4, cada clase de ideales en $C(\mathcal{O})$ contiene un $\mathcal{O}$-ideal coprimo a f. Así, el morfismo natural $I(\mathcal{O}, f) \to C(\mathcal{O})$ es sobreyectivo, y es claro que su núcleo es $I(\mathcal{O}, f) \cap P(\mathcal{O})$. Entonces basta probar

$$P(\mathcal{O}, f) = I(\mathcal{O}, f) \cap P(\mathcal{O}).$$

La inclusión $P(\mathcal{O}, f) \subset I(\mathcal{O}, f) \cap P(\mathcal{O})$ es obvia. Para probar la otra inclusión, notar que un elemento arbitrario de $I(\mathcal{O}, f) \cap P(\mathcal{O})$ es de la forma $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$, donde $\alpha \in K$ y $\mathfrak{a}, \mathfrak{b}$ son $\mathcal{O}$-ideales coprimos a f, pues $I(\mathcal{O}, f)$ es (por definición) generado por $\mathcal{O}$-ideales coprimos a f. Escribiendo $m = N(\mathfrak{b})$, afirmamos que $m\alpha \in \mathcal{O}$. En efecto, $\overline{\mathfrak{b}} = m\mathfrak{b}^{-1}$ es un $\mathcal{O}$-ideal, luego

$$m\alpha\mathcal{O} = \mathfrak{a}m\mathfrak{b}^{-1} = \mathfrak{a}\overline{\mathfrak{b}} \subset \mathcal{O} \Rightarrow m\alpha \in \mathcal{O}.$$

Como $N(m\alpha\mathcal{O}) = N(\mathfrak{a})N(\mathfrak{b})$ es coprimo a f, se tiene $m\alpha\mathcal{O} \in P(\mathcal{O}, f)$. También $m\mathcal{O} \in P(\mathcal{O}, f)$, pues su norma $N(\mathfrak{b})^2$ es coprimo a f. Por tanto $\alpha\mathcal{O} = m\alpha\mathcal{O} \cdot (m\mathcal{O})^{-1} \in P(\mathcal{O}, f)$. □

Para cada orden $\mathcal{O}$ de conductor f, los $\mathcal{O}$-ideales coprimos f se relacionan bien con ciertos ideales del orden maximal $\mathcal{O}_K$ que ahora definimos

Definición 1.4. Dado un entero positivo m, un $\mathcal{O}_K$-ideal $\mathfrak{a}$ es *coprimo a* m si $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.

Igual como en el Lema 1.2, se prueba que esto es equivalente a $\mathrm{mcd}(N(\mathfrak{a}), m) = 1$. Por tanto, los $\mathcal{O}_K$-ideales coprimos a m generan un subgrupo de I_K, que denotamos $I_K(m) \subset I_K$. Ahora veremos la relación que dijimos antes

Proposición 1.5. *Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K.*

1. *Si $\mathfrak{a}$ es un $\mathcal{O}_K$-ideal coprimo a f, entonces $\mathfrak{a} \cap \mathcal{O}$ es un $\mathcal{O}$-ideal coprimo a f de la misma norma.*
2. *Si $\mathfrak{a}$ es un $\mathcal{O}$-ideal coprimo a f, entonces $\mathfrak{a}\mathcal{O}_K$ es un $\mathcal{O}_K$-ideal coprimo a f de la misma norma.*
3. *La función $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induce un isomorfimo de grupos $I_K(f) \xrightarrow{\sim} I(\mathcal{O}, f)$, y la inversa de esta función es dada por $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.*

Demostración. (1): Sea $\mathfrak{a}$ un $\mathcal{O}_K$-ideal coprimo a f. El morfismo natural

$$\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$$

es inyectivo, así que $N(\mathfrak{a} \cap \mathcal{O})$ divide a $N(\mathfrak{a})$. Luego, como $N(\mathfrak{a})$ es coprimo a f, entonces $N(\mathfrak{a} \cap \mathcal{O})$ también lo es, lo que prueba que $\mathfrak{a} \cap \mathcal{O}$ es coprimo a f. Para demostrar la igualdad de normas, basta ver que el morfismo anterior es sobreyectivo. Como $N(\mathfrak{a})$ es coprimo a f, multiplicación por f induce un isomorfismo (de grupos) de $\mathcal{O}_K/\mathfrak{a}$. Pero además $f\mathcal{O}_K \subset \mathcal{O}$, entonces se obtiene la sobreyectividad. Esto muestra (1).

Antes de mostrar (2) y (3), probaremos las siguientes dos igualdades de ideales:

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= \mathfrak{a} \quad \text{si } \mathfrak{a} \text{ es un } \mathcal{O}\text{-ideal coprimo a } f \\ (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K &= \mathfrak{a} \quad \text{si } \mathfrak{a} \text{ es un } \mathcal{O}_K\text{-ideal coprimo a } f. \end{aligned} \tag{1.1}$$

Para probar la primera, sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f, luego

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} \\ &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O}) \\ &\subset \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \subset \mathfrak{a} + \mathfrak{a} \cdot f\mathcal{O}_K. \end{aligned}$$

Como $f\mathcal{O}_K \subset \mathcal{O}$, esto prueba $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} \subset \mathfrak{a}$. La otra inclusión es directa, por tanto se verifica la primera igualdad. Para probar la segunda igualdad, sea $\mathfrak{a}$ un $\mathcal{O}_K$-ideal coprimo a f. Primero note que $\mathfrak{a} = \mathfrak{a}\mathcal{O}$, pues $\mathfrak{a}\mathcal{O} \subset \mathfrak{a}\mathcal{O}_K = \mathfrak{a}$ y $\mathfrak{a} = \mathfrak{a}\{1\} \subset \mathfrak{a}\mathcal{O}$. Luego

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a}.$$

Además, $f\mathfrak{a} \subset f\mathcal{O}_K \subset \mathcal{O}$, de modo que $f\mathfrak{a} \subset \mathfrak{a} \cap \mathcal{O} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$, lo que junto con la inclusión anterior, prueba que $\mathfrak{a} \subset (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$. La otra inclusión es directa, por tanto se cumple la segunda igualdad.

(2): Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. La igualdad

$$\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a} + f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K,$$

muestra que $\mathfrak{a}\mathcal{O}_K$ también es coprimo a f. Ahora, usando (1) y la primera igualdad de (1.1), se obtiene directamente

$$N(\mathfrak{a}\mathcal{O}_K) = N(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) = N(\mathfrak{a}),$$

lo que completa la demostración de (2).

(3): Usando las igualdades de (1.1), se obtiene directamente una biyección entre los monoides de $\mathcal{O}$- y $\mathcal{O}_K$-ideales coprimos a f, vía $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Además, la igualdad

$$(\mathfrak{ab})\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K \cdot \mathfrak{b}\mathcal{O}_K,$$

muestra que esta función es multiplicativa. Es sencillo verificar que esta biyección de monoides se extiende a un isomorfismo de grupos $I(\mathcal{O}, f) \simeq I_K(f)$, $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_K]$, y su inversa es dada por $[\mathfrak{a}] \mapsto [\mathfrak{a} \cap \mathcal{O}]$. Esto muestra (3). □

Usando la Proposición 1.5 se puede probar un resultado sobre factorización única de ideales coprimos al conductor (ver Apéndice A, Corolario 3.2). El resultado principal de esta sección describe $C(\mathcal{O})$ en términos del orden maximal.

Proposición 1.6. *Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K. Entonces hay isomorfismos naturales*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f),$$

donde $P_{K,\mathbb{Z}}(f)$ es el subgrupo de $I_K(f)$ generado por los ideales principales de la forma $\alpha\mathcal{O}_K$, donde $\alpha \in \mathcal{O}_K$ satisface $\alpha \equiv a \mod f\mathcal{O}_K$ para algún entero a coprimo a f.

Observación 1.7. Para no confundirse, recordamos que el subíndice K lo ocupamos para el orden maximal $\mathcal{O}_K$ (como en $I_K, I_K(f)$, etc.), mientras que no ponemos subíndices para el orden $\mathcal{O}$ (como en $I(\mathcal{O}), I(\mathcal{O}, f)$, etc.).

Demostración. El isomorfismo $C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f)$ fue demostrado en la Proposición 1.3. Para demostrar el otro isomorfismo, consideremos el isomorfismo $I(\mathcal{O}, f) \xrightarrow{\sim} I_K(f)$, $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_K]$ obtenido en la Proposición 1.5. Bajo este isomorfismo, el subgrupo $P(\mathcal{O}, f)$ de $I(\mathcal{O}, f)$ es enviado a un subgrupo $\tilde{P}$ de $I_K(f)$, de modo que

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/\tilde{P}.$$

Así, basta probar que $\tilde{P} = P_{K,\mathbb{Z}}(f)$. Para esto, primero mostraremos que para $\alpha \in \mathcal{O}_K$ se cumple

$$\begin{aligned} \alpha \equiv a \mod f\mathcal{O}_K,\ a \in \mathbb{Z},\ \gcd(a, f) = 1 \\ \iff \alpha \in \mathcal{O},\ \gcd(N(\alpha), f) = 1. \end{aligned} \tag{1.2}$$

Para la implicancia directa, asumamos que $\alpha \equiv a \mod f\mathcal{O}_K$, donde $a \in \mathbb{Z}$ es coprimo a f. Notar que $N(\alpha) \equiv a^2 \mod f$. En efecto, tenemos que $\alpha = a + f\beta$ para cierto $\beta \in \mathcal{O}_K$, y un cálculo directo muestra que

$$N(\alpha) = a^2 + f\underbrace{(aTr(\beta) + fN(\beta))}_{\in\mathbb{Z}}.$$

Luego, $\gcd(N(\alpha), f) = \gcd(a^2, f) = \gcd(a, f) = 1$, y como $f\mathcal{O}_K \subset \mathcal{O}$ y $\alpha \equiv a \mod f\mathcal{O}_K$, vemos que $\alpha \in \mathcal{O}$.

Conversamente, sea $\alpha \in \mathcal{O} = [1, fw_K]$ tal que $\gcd(N(\alpha), f) = 1$. Escribiendo $\alpha = a + bfw_K$ $(a, b \in \mathbb{Z})$, se ve que $\alpha \equiv a \mod f\mathcal{O}_K$. Como $\gcd(N(\alpha), f) = 1$ y $N(\alpha) \equiv a^2 \mod f$, se tiene que $\gcd(a, f) = 1$. Esto muestra (1.2).

Ahora probaremos $\tilde{P} = P_{K,\mathbb{Z}}(f)$. Por definición, $P(\mathcal{O}, f)$ es generado por los ideales $\alpha\mathcal{O}$, donde $\alpha \in \mathcal{O}$ y $\gcd(N(\alpha), f) = 1$. Entonces $\tilde{P}$ es generado por los ideales $\alpha\mathcal{O}_K$ correspondientes, y por la equivalencia (1.2), esto implica que $\tilde{P} = P_{K,\mathbb{Z}}(\mathcal{O}, f)$. □

2. El número de clases

Esta sección esta basada en la parte D de la sección 7 del Capítulo 2 de [Cox13].

En esta sección aplicaremos la Proposición 1.6 para obtener una fórmula para el *número de clases* $h(\mathcal{O}) := |C(\mathcal{O})|$ en términos de su conductor y el número de clases $h(\mathcal{O}_K)$ del orden maximal. Antes de enunciar la fórmula, necesitamos recordar algunas notaciones:

Dado un entero D y un primo impar p, definimos el *símbolo de Legendre*

$$\left(\frac{D}{p}\right) = \begin{cases} 0 & \text{si } p \mid D \\ 1 & \text{si } p \nmid D \text{ y } D \text{ es residuo cuadrático módulo } p \\ -1 & \text{si } p \nmid D \text{ y } D \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Recordamos que se llama *residuo cuadrático* módulo m a cualquier entero r coprimo con m para el que tenga solución la congruencia

$$x^2 \equiv r \mod m$$

es decir, cuando r tiene una raíz cuadrada módulo m.

Dado un entero D, para $p = 2$ definimos el *símbolo de Kronecker*

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & \text{si } 2 \mid D \\ 1 & \text{si } D \equiv \pm 1 \mod 8 \\ -1 & \text{si } D \equiv \pm 3 \mod 8. \end{cases}$$

Notar que para el caso particular que $D = d_K$ es el discriminante de un cuerpo cuadrático imaginario K, el símbolo de Kronecker se calcula como

$$\left(\frac{d_K}{2}\right) = \begin{cases} 0 & \text{si } 2 \mid d_K \\ 1 & \text{si } d_K \equiv 1 \mod 8 \\ -1 & \text{si } d_K \equiv 5 \mod 8, \end{cases}$$

(recordar que $d_K \equiv 1 \mod 4$ si d_K es impar). Ahora enunciamos la fórmula para $h(\mathcal{O})$:

Teorema 2.1. *Sea $\mathcal{O}$ un orden de conductor $f > 1$ en un cuerpo cuadrático imaginario K. Entonces*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right). \tag{2.3}$$

Además, $h(\mathcal{O})$ es siempre un múltiplo entero de $h(\mathcal{O}_K)$.

(Para ejemplos de cálculos de números de clases usando el Teorema 2.1 ver Apéndice B.)

Demostración. Como $I_K(f) \subset I_K$ y $P_{K,\mathbb{Z}}(f) \subset I_K(f) \cap P_K$, obtenemos directamente una sucesión exacta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K(f)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K/P_K & \longrightarrow & 0 \\ & & & & \downarrow \wr & & \| & & \\ & & & & C(\mathcal{O}) & \longrightarrow & C(\mathcal{O}_K) & & \end{array} \tag{2.4}$$

donde el isomorfismo $C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$ se obtiene de la Proposición 1.6. Por Corolario 0.1 de Charla 4, cada clase en $C(\mathcal{O}_K)$ contiene un $\mathcal{O}_K$-ideal que es coprimo a f. Esto implica que $C(\mathcal{O}) \to C(\mathcal{O}_K)$ es sobreyectiva, lo que prueba que $h(\mathcal{O}_K)$ divide a $h(\mathcal{O})$. Más aún, la exactitud de (2.4) implica que

$$h(\mathcal{O}) = h(\mathcal{O}_K)|(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)|, \tag{2.5}$$

así que $h(\mathcal{O})$ es un múltiplo entero de $h(\mathcal{O}_K)$. Solo falta calcular $|(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)|$. La idea clave es relacionar este cuociente al grupo de unidades $(\mathcal{O}_K/f\mathcal{O}_K)^*$.

Definimos un morfismo $\phi : (\mathcal{O}_K/f\mathcal{O}_K)^* \to (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)$ por $\phi([\alpha]) = [\alpha\mathcal{O}_K]$. Veremos que ϕ está bien definido. Si $[\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^*$, el $\mathcal{O}_K$-ideal $\alpha\mathcal{O}_K$ es coprimo a f y por tanto pertenece a $I_K(f) \cap P_K$. Más aún, si $\alpha \equiv \beta \mod f\mathcal{O}_K$, podemos tomar $[u] \in (\mathcal{O}_K/f\mathcal{O}_K)^*$ con $u\alpha \equiv u\beta \equiv 1 \mod f\mathcal{O}_K$. Entonces $u\alpha\mathcal{O}_K, u\beta\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$, y así

$$(\alpha\mathcal{O}_K)(\beta\mathcal{O}_K)^{-1} = (u\alpha\mathcal{O}_K)(u\beta\mathcal{O}_K)^{-1} \in P_{K,\mathbb{Z}}(f),$$

lo que demuestra que ϕ está bien definido.

Ahora mostraremos que ϕ es sobreyectivo. Un elemento arbitrario de $I_K(f) \cap P_K$ se puede escribir como $\alpha\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$, donde $\alpha \in K$ y $\mathfrak{a}, \mathfrak{b}$ son $\mathcal{O}_K$-ideales coprimos a f. Escribiendo $m = N(\mathfrak{b})$, hemos visto que $m\alpha \in \mathcal{O}_K$ y que $m\alpha\mathcal{O}_K$ es coprimo a f (ver demostración de Proposición 1.3). Como $m\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$, se sigue que $[\alpha\mathcal{O}_K] = [m\alpha\mathcal{O}_K] = \phi([m\alpha])$, lo que prueba que ϕ es sobreyectivo.

Determinaremos el núcleo de ϕ a través de una sucesión exacta de grupos que construiremos usando los siguientes morfismos de grupos

$$\varphi : \{\pm 1\} \to (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^*, \ \pm 1 \mapsto ([\pm 1], \pm 1)$$

$$\psi : (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^* \to (\mathcal{O}_K/f\mathcal{O}_K)^*,\ ([a],\alpha) \mapsto [a\alpha].$$

Mostraremos que la siguiente sucesión de grupos

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\varphi} (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^* \xrightarrow{\psi} (\mathcal{O}_K/f\mathcal{O}_K)^* \xrightarrow{\phi} (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f) \longrightarrow 1, \tag{2.6}$$

es exacta. Como ϕ es sobreyectivo y claramente φ es inyectivo, solo falta verificar que $\ker(\psi) = \mathrm{im}(\varphi)$ y $\ker(\phi) = \mathrm{im}(\psi)$.

En primer lugar, es obvio que $\mathrm{im}(\varphi) \subset \ker(\psi)$. Para verificar la inclusión recíproca sea $([a],\alpha) \in \ker(\psi)$, es decir, $[a] \in (\mathbb{Z}/f\mathbb{Z})^*$ y $\alpha \in \mathcal{O}_K^*$ satisfacen $[a\alpha] = [1]$ en $(\mathcal{O}_K/f\mathcal{O}_K)^*$. Mostraremos que $([a],\alpha) \in \mathrm{im}(\varphi) = \{([\pm 1], \pm 1)\}$. Tenemos dos casos

(i) $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$,
(ii) $K = \mathbb{Q}(\sqrt{-1})$ o $K = \mathbb{Q}(\sqrt{-3})$.

En el caso (i) se tiene $\mathcal{O}_K^* = \{\pm 1\}$, de modo que $\alpha = \pm 1$, lo que implica $[a] = [\pm 1]$.

En el caso (ii), se tiene $\mathcal{O}_K^* = \{\pm 1, \pm w_K, \pm w_K^2\}$, donde $w_K \in \{i, e^{2\pi i/6}\}$. Así que tenemos tres subcasos

- $\alpha = \pm 1$,
- $\alpha = \pm w_K$,
- $\alpha = \pm w_K^2$ si $w_K = e^{2\pi i/6} =: \zeta$.

Si $\alpha = \pm 1$, se tiene $[a] = [\pm 1]$.

Ahora notar que la condición $[a\alpha] = [1]$ en $(\mathcal{O}_K/f\mathcal{O}_K)^*$ implica que

$$a\alpha = 1 + f(m + nw_K) = (1 + fm) + fnw_K$$

para ciertos $m, n \in \mathbb{Z}$.

Probaremos por contradicción que los otros dos subcasos no pueden ocurrir.

Si $\alpha = \pm w_K$, tenemos que

$$\pm a w_K = (1 + fm) + fnw_K \Rightarrow 0 = (1 + fm)1 + (fn \mp a)w_K.$$

Luego, como $\{1, w_K\}$ es $\mathbb{Z}$-linealmente independiente, en particular se tiene $1 + fm = 0$, es decir, $fm = -1$. Como $f, m \in \mathbb{Z}$, esto implica que $f \in \{\pm 1\}$, lo que contradice $f > 1$.

Si $\alpha = \pm\zeta^2 = \pm(\zeta - 1)$, tenemos que

$$\pm a(\zeta - 1) = (1 + fm) + fn\zeta \Rightarrow 0 = (1 + fm \pm a) + (fn \mp a)\zeta.$$

Como $\{1, w_K\}$ es $\mathbb{Z}$-linealmente independiente, se tiene

$$1 + fm \pm a = 0 \tag{2.7}$$

$$fn \mp a = 0.$$

Reemplazando $a = \pm fn$ en la ecuación (2.7) se obtiene $f(m+n) = -1$. Como $f, m, n \in \mathbb{Z}$, esto implica $f \in \{\pm 1\}$, lo que contradice $f > 1$.

Esto muestra que $\ker(\psi) \subset \mathrm{im}(\varphi)$. Por tanto $\ker(\psi) = \mathrm{im}(\varphi)$.

Ahora mostraremos que $\ker(\phi) = \mathrm{im}(\psi)$. Primero, si $[a\alpha] \in \mathrm{im}(\psi)$, entonces $\phi([a\alpha]) = [a\alpha\mathcal{O}_K] = [a\mathcal{O}_K] = P_{K,\mathbb{Z}}(f)$, pues a es coprimo a f. Así $[a\alpha] \in \ker(\phi)$. Conversamente, sea $[\alpha] \in \ker(\phi)$, i.e., $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. Por definición de $P_{K,\mathbb{Z}}(f)$, $\alpha\mathcal{O}_K = (\beta\mathcal{O}_K)(\gamma\mathcal{O}_K)^{-1}$, donde $\beta, \gamma \in \mathcal{O}_K$ satisfacen $[\beta] = [b], [\gamma] = [c]$ en $(\mathcal{O}_K/f\mathcal{O}_K)^*$ para ciertos $b, c \in \mathbb{Z}$ coprimos a f. Como $\alpha\mathcal{O}_K = (\beta\gamma^{-1})\mathcal{O}_K$, se sigue que $\alpha = u\beta\gamma^{-1}$ para algún $u \in \mathcal{O}_K^*$. Luego

$$\psi(([bc^{-1}], u)) = [bc^{-1}u] = [u][b][c]^{-1} = [u][\beta][\gamma]^{-1} = [u\beta\gamma^{-1}] = [\alpha].$$

Por tanto $[\alpha] \in \mathrm{im}(\psi)$. Esto muestra la exactitud de (2.6).

De la exactitud de (2.6) se deduce que

$$|(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)| = \frac{|(\mathcal{O}_K/f\mathcal{O}_K)^*|}{\frac{|(\mathbb{Z}/f\mathbb{Z})^*||\mathcal{O}_K^*|}{2}} = \frac{|(\mathcal{O}_K/f\mathcal{O}_K)^*|}{|(\mathbb{Z}/f\mathbb{Z})^*|[\mathcal{O}_K^* : \mathcal{O}^*]}, \tag{2.8}$$

la última igualdad es porque para todo orden $\mathcal{O}$ de conductor $f > 1$ se cumple que $\mathcal{O}^* = \{\pm 1\}$ y por tanto $|\mathcal{O}_K^*|/2 = [\mathcal{O}_K^* : \mathcal{O}^*]$.

Es bien conocido que (ver [Apostol76, 2.5 Theorem 2.4])

$$|(\mathbb{Z}/f\mathbb{Z})^*| = f \prod_{p|f} \left(1 - \frac{1}{p}\right),$$

y después mostraremos que (ver Proposición 5.1 en Apéndice C)

$$|(\mathcal{O}_K/f\mathcal{O}_K)^*| = f^2 \prod_{p|f} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Usando estas dos fórmulas y las ecuaciones (2.5), (2.8), obtenemos

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right),$$

lo que demuestra la fórmula (2.3). □

Usando el Teorema 2.1, podemos relacionar los números de clases $h(m^2D)$ y $h(D)$ como sigue

Corolario 2.2. *Sea $D \equiv 0, 1 \mod 4$ negativo, y sea m un entero positivo. Entonces*

$$h(m^2D) = \frac{h(D)m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right),$$

donde $\mathcal{O}$ y $\mathcal{O}'$ son los ordenes de discriminante D y m^2D respectivamente (y $\mathcal{O}'$ tiene índice m en $\mathcal{O}$).

Demostración. Supongamos que el orden $\mathcal{O}$ en el cuerpo cuadrático imaginario K tiene discriminante D y conductor f. Entonces el orden $\mathcal{O}' \subset \mathcal{O}$ de índice m tiene discriminante m^2D y conductor mf. Para ambos ordenes usamos el Teorema 2.1

$$h(m^2D) = h(\mathcal{O}') = \frac{h(\mathcal{O}_K)mf}{[\mathcal{O}_K^* : \mathcal{O}'^*]} \prod_{p|mf} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

$$h(D) = h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Dividiendo estas dos expresiones y multiplicando por $h(D)$, se obtiene

$$h(m^2D) = \frac{h(D)m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{\substack{p|m \\ p\nmid f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right). \tag{2.9}$$

Usando la multiplicatividad del símbolo de Legendre y/o del símbolo de Kronecker, se tiene

$$\begin{aligned}\prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right) &= \prod_{\substack{p|m \\ p\nmid f}} \left(1 - \underbrace{\left(\frac{f}{p}\right)^2}_{1}\left(\frac{d_K}{p}\right)\frac{1}{p}\right) \prod_{p|f} \left(1 - \underbrace{\left(\frac{f}{p}\right)^2}_{0}\left(\frac{d_K}{p}\right)\frac{1}{p}\right) \\ &= \prod_{\substack{p|m \\ p\nmid f}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).\end{aligned}$$

Reemplazando esta igualdad en la ecuación (2.9) se obtiene la fórmula deseada. □

Este corolario fue probado primero por Gauss, y su demostración se puede encontrar en *Disquisitiones Arithmeticae* [Gauss, §§254-256].

El único método que aprendimos en la Charla 1-2 para calcular números de clases $h(D)$ para $D < 0$ fue contar formas reducidas. Esto se vuelve tedioso cuando $|D|$ es grande, pero hay otros metodos disponibles. Para usar el Teorema 2.1, es necesario calcular $h(d_K)$, y se tiene una fórmula clásica

$$h(d_K) = -\frac{|\mathcal{O}_K^*|}{2|d_K|} \sum_{n=1}^{|d_K|-1} \left(\frac{d_K}{n}\right) n, \tag{2.10}$$

donde $\left(\frac{d_K}{n}\right)$ es definido para $n = p_1 \cdots p_r$, p_i primo, por $\left(\frac{d_K}{n}\right) := \prod_{i=1}^r \left(\frac{d_K}{p_i}\right)$. Esta fórmula se puede probar a través de métodos analíticos (ver [BS66, Chapter 5, Section 4]).

La fórmula (2.10) permite calcular $h(d_K)$ para cualquier cuerpo cuadrático imaginario K, pero no describe la forma como crece $h(d_K)$ cuando $|d_K|$ crece. Gauss estudió este crecimiento de

forma experimental en *Disquisitiones* [Gauss, 41, §302], pero no hubo demostraciones rigurosas hasta los 1930s. El mejor resultado se debe a Siegel, quien en 1935 probó que

$$\lim_{d_K\to-\infty}\frac{\log h(d_K)}{\log|d_K|}=\frac{1}{2}.$$

Se deduce que para cada $\epsilon>0$, existe C_ϵ tal que

$$h(d_K)>C_\epsilon|d_K|^{(1/2)-\epsilon}$$

para todo cuerpo de discriminante $d_K<0$. Esto implica que $h(d_K)\to+\infty$ si $|d_K|\to+\infty$. Lamentablemente, la constante C_ϵ en la demostración de Siegel no es calculable efectivamente (por dificultades relacionadas con la Hipótesis de Riemann). Sin embargo, gracias a trabajos de Goldfield, Gross, Zagier y Oesterlé en los 1980s, se obtuvo una cota inferior más débil, pero explícita

$$h(d_K)>\frac{\log|d_K|}{55}\prod_{p|d_K,\ p<d_K}\left(1-\frac{[2\sqrt{p}]}{p+1}\right),$$

donde $[\,\cdot\,]$ es la función parte entera y log está en base e.

Usando esta cota, teoría de género de formas cuadráticas y el Teorema 2.1 se puede probar que solo hay un número finito de órdenes con un número de clases h dado (ver Apendice D). Pero, cuando h es pequeño, determinar todos los órdenes que tienen número de clases h sigue siendo un problema difícil. La respuesta para el caso $h=1$ es dada en el siguiente teorema que también fue enunciado en el Teorema 4.1 de las charlas 1-2.

Teorema 2.3 (Baker, Heegner, Stark)**.**

(i) *Si K es un cuerpo cuadrático imaginario de discriminante d_K, entonces*

$$h(d_K)=1\Leftrightarrow d_K\in\{-3,-4,-7,-8,-11,-19,-43,-67,-163\}.$$

(ii) *Si $D\equiv 0,1 \mod 4$ es negativo, entonces*

$$h(D)=1\Leftrightarrow D\in\{-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163\}.$$

No veremos una demostración completa de este teorema. Solo demostraremos que (i) implica (ii). Notar que es obvio que (ii) implica (i). La demostración de (i) es una materia diferente. En el Teorema 4.2 de las charla 1-2, fue probado el caso cuando el discriminante es par, usando un método elemental debido a Landau. La demostración del caso cuando el discriminante es impar requiere el uso de funciones modulares y de la teoría CM.

Demostración. Probaremos (i)⇒(ii) del Teorema 2.3. Asumamos (i). Entonces para probar la implicancia recíproca de (ii), basta verificar que $h(-12)=h(-16)=h(-27)=h(-28)=1$. Lo haremos usando el Teorema 2.1.

En el caso $D=-12=2^2(-3)$ se tiene $d_K=-3$ (e.d., $K=\mathbb{Q}(\sqrt{-3})$), $f=2$, $h(-3)=1$, $\mathcal{O}_K^*=\{\pm1,\pm e^{\pi i/3},\pm e^{2\pi i/3}\}$. Además $-3\equiv 5 \mod 8$, lo que implica $\left(\frac{-3}{2}\right)=-1$, así tenemos

$$h(-12)=\frac{2}{3}\left(1-\left(\frac{-3}{2}\right)\frac{1}{2}\right)=\frac{2}{3}\cdot\frac{3}{2}=1.$$

Si $D=-16=2^2(-4)$, se tiene $d_K=-4$ (e.d., $K=\mathbb{Q}(\sqrt{-1})$), $f=2$, $h(-4)=1$, $\mathcal{O}_K^*=\{\pm1,\pm i\}$ y $\left(\frac{-4}{2}\right)=0$ (pues $2|-4$). Luego

$$h(-16)=\frac{2}{2}\left(1-\left(\frac{-4}{2}\right)\frac{1}{2}\right)=1.$$

Si $D=-27=3^2(-3)$, se tiene $d_K=-3$ (e.d., $K=\mathbb{Q}(\sqrt{-3})$), $f=3$, $h(-3)=1$, $|\mathcal{O}_K^*|=6$ y $\left(\frac{-3}{3}\right)=0$ (pues $3|-3$). Entonces

$$h(-27)=\frac{3}{3}\left(1-\left(\frac{-3}{3}\right)\frac{1}{3}\right)=1.$$

Por último, si $D=-28=2^2(-7)$, se tiene $d_K=-7$ (e.d. $K=\mathbb{Q}(\sqrt{-7})$), $f=2$, $h(-7)=1$, $\mathcal{O}_K^*=\{\pm1\}$ y $\left(\frac{-7}{2}\right)=1$ (pues $-7\equiv 1 \mod 8$), así obtenemos

$$h(-28)=2\left(1-\left(\frac{-7}{2}\right)\frac{1}{2}\right)=2\cdot\frac{1}{2}=1.$$

Esto muestra la implicancia recíproca.

Para probar la implicancia directa, asumamos que $h(D)=1$ y anotemos $D=f^2d_K$. Por el Teorema 2.1 tenemos que $h(d_K)|h(D)$, lo que implica $h(d_K)=1$. Por (i) esto determina las

posibilidades para d_K. Solo falta ver cuales conductores $f > 1$ pueden ocurrir. Consideremos primero el caso $\mathcal{O}_K^* = \{\pm 1\}$. Si $f > 2$, es sencillo verificar que

$$1 = h(D) = f \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) > 1,$$

así que este caso se excluye. Si $f = 2$, tenemos que

$$\begin{aligned} 1 = h(D) = 2\left(1 - \left(\frac{d_K}{2}\right)\frac{1}{2}\right) &\Leftrightarrow \left(\frac{d_K}{2}\right) = 1 \\ &\Leftrightarrow d_K \equiv 1 \mod 8 \\ &\Leftrightarrow d_K = -7 \\ &\Leftrightarrow D = -28. \end{aligned}$$

Ahora consideramos el caso $\mathcal{O}_K^* \neq \{\pm 1\}$, e.d., $K = \mathbb{Q}(\sqrt{-1})$ o $K = \mathbb{Q}(\sqrt{-3})$.
Si $K = \mathbb{Q}(\sqrt{-1})$, entonces $\mathcal{O}_K^* = \{\pm 1, \pm i\}$ y $d_K = -4$. Es sencillo verificar que

$$h(D) = \frac{f}{2} \prod_{p|f} \left(1 - \left(\frac{-4}{p}\right)\frac{1}{p}\right) > 1 \quad \text{si} \quad f > 2,$$

por tanto se excluye este caso. Por ejemplo, si $f = 3$, se tiene $\left(\frac{-4}{3}\right) = -1$, pues $-4 = 2$ y $1^2 = 2^2 = 1$ en $\mathbb{Z}/3\mathbb{Z}$, por tanto

$$h(-36) = \frac{3}{2}\left(1 - \left(\frac{-4}{3}\right)\frac{1}{3}\right) = \frac{3}{2} \cdot \frac{4}{3} = 2.$$

Si $f = 2$, se tiene $\left(\frac{-4}{2}\right) = 0$ (pues $2|-4$) y

$$h(-16) = 1 \cdot \left(1 - \left(\frac{-4}{2}\right)\frac{1}{2}\right) = 1 \cdot 1 = 1.$$

Para el caso $K = \mathbb{Q}(\sqrt{-3})$ se tiene $|\mathcal{O}_K^*| = 6$ y $d_K = -3$. Es sencillo verificar que

$$h(D) = \frac{f}{3} \prod_{p|f} \left(1 - \left(\frac{-3}{p}\right)\frac{1}{p}\right) > 1 \quad \text{si} \quad f > 3,$$

por tanto se excluye este caso. Por ejemplo, si $f = 4$, se tiene $\left(\frac{-3}{2}\right) = -1$ (pues $-3 \equiv 5 \mod 8$), luego

$$h(-48) = 2 \cdot \left(1 - \left(\frac{-3}{2}\right)\frac{1}{2}\right) = 2 \cdot \frac{3}{2} = 3.$$

Si $f = 3$, se tiene $\left(\frac{-3}{3}\right) = 0$ (pues $3|-3$) y

$$h(-27) = 1 \cdot \left(1 - \left(\frac{-3}{3}\right)\frac{1}{3}\right) = 1 \cdot 1 = 1.$$

Si $f = 2$, se tiene

$$h(-12) = \frac{2}{3}\left(1 - \left(\frac{-3}{2}\right)\frac{1}{2}\right) = \frac{2}{3} \cdot \frac{3}{2} = 1.$$

Esto muestra la implicancia directa. □

3. Apéndice A. Factorización de ideales coprimos al conductor

En este apéndice usaremos la Proposición 1.5 para obtener un resultado (ver Corolario 3.2) sobre factorización única de $\mathcal{O}$-ideales coprimos a f en productos de $\mathcal{O}$-ideales primos que también son coprimos a f. Para eso, primero veremos que la biyección entre $\mathcal{O}$- y $\mathcal{O}_K$-ideales coprimos a f obtenida en la Proposición 1.5, lleva $\mathcal{O}$-ideales primos en $\mathcal{O}_K$-ideales primos.

Corolario 3.1. *Sea $\mathcal{O}$ un orden de conductor f, y sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. Entonces*

$$\mathfrak{a} \text{ es un } \mathcal{O}\text{-ideal primo} \Leftrightarrow \mathfrak{a}\mathcal{O}_K \text{ es un } \mathcal{O}_K\text{-ideal primo.}$$

Demostración. El morfismo natural $\phi : \mathcal{O}/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ está bien definido, pues $\mathfrak{a} \subset \mathfrak{a}\mathcal{O}_K$. Es sencillo ver que ϕ es un homomorfimo de anillos. Probaremos que ϕ es un isomorfismo de anillos. Para ver su inyectividad, sea $\alpha + \mathfrak{a} \in \ker \phi$, e.d., $\alpha \in \mathcal{O} \cap \mathfrak{a}\mathcal{O}_K$. Por la primera igualdad de (1.1) tenemos que $\mathcal{O} \cap \mathfrak{a}\mathcal{O}_K = \mathfrak{a}$, luego $\alpha \in \mathfrak{a}$, lo que prueba la inyectividad de ϕ. La sobreyectividad se deduce de $N(\mathfrak{a}) = N(\mathfrak{a}\mathcal{O}_K)$ (ver Proposición 1.5), pues un monomorfismo de anillos finitos del mismo orden es automáticamente sobreyectivo. Por tanto ϕ es isomorfismo.

Como ϕ es un isomorfismo de anillos, entonces $\mathcal{O}/\mathfrak{a}$ es dominio de integridad si y sólo si $\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ lo es. Esto muestra el resultado. □

Usando la factorización única de ideales en $\mathcal{O}_K$ y la Proposición 1.5 probaremos que

Corolario 3.2. *Todo $\mathcal{O}$-ideal coprimo a f se factoriza de manera única como producto de $\mathcal{O}$-ideales primos que también son coprimos a f.*

Demostración. Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. Por factorización única de ideales en el orden maximal $\mathcal{O}_K$, podemos escribir de manera única

$$\mathfrak{a}\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}, \tag{3.11}$$

donde los $\mathfrak{p}_i$ son $\mathcal{O}_K$-ideales primos distintos, n_i son enteros positivos. Como $\mathfrak{a}\mathcal{O}_K$ es coprimo a f (por Proposición 1.5) y la norma es multiplicativa, cada $\mathfrak{p}_i$ es coprimo a f. Luego, por (1) de Proposición 1.5, cada $\mathfrak{p}_i \cap \mathcal{O}$ es un $\mathcal{O}$-ideal coprimo a f. Por Corolario 3.1, cada $\mathfrak{p}_i \cap \mathcal{O}$ es un $\mathcal{O}$-ideal primo, pues los $(\mathfrak{p}_i \cap \mathcal{O})\mathcal{O}_K = \mathfrak{p}_i$ (por (1.1)) son $\mathcal{O}_K$-ideales primos. Así

$$\begin{aligned}
\mathfrak{a} &= \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} && \text{por (1,1)} \\
&= \left(\prod_{i=1}^{r} \mathfrak{p}_i^{n_i}\right) \cap \mathcal{O} && \text{por (3,11)} \\
&= \prod_{i=1}^{r} (\mathfrak{p}_i \cap \mathcal{O})^{n_i} && \text{(ejercicio sencillo),}
\end{aligned}$$

obtenemos una descomposición de $\mathfrak{a}$ en un producto de $\mathcal{O}$-ideales primos que son coprimos a f. La unicidad de esta factorización se deduce de la unicidad de la factorización (3.11) de $\mathfrak{a}\mathcal{O}_K$ y de la biyección entre $\mathcal{O}$- y $\mathcal{O}_K$-ideales coprimos a f dada por la Proposición 1.5. □

Un contraejemplo para el corolario anterior cuando se elimina la hipótesis "coprimo a f"

Ejemplo 3.3. Sea K un cuerpo cuadrático imaginario, sea p un número primo y sea $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_K$ un orden de conductor p en K. Afirmamos que el $\mathcal{O}$-ideal $\mathfrak{b} = p\mathcal{O} = p\mathbb{Z} + p^2\mathcal{O}_K$ no es un producto de $\mathcal{O}$-ideales primos. Note que $\mathfrak{b}$ no es coprimo a p.

Sea $\mathfrak{p} = p\mathcal{O}_K \subset \mathcal{O}$. Para demostrar la afirmación, primero probaremos que

(1) $\mathfrak{p}$ es un $\mathcal{O}$-ideal primo en $\mathcal{O}$,
(2) $\mathfrak{p}^2 \subsetneq \mathfrak{b} \subsetneq \mathfrak{p}$.

(1): Usando el segundo teorema del isomorfismo se obtiene

$$\mathcal{O}/\mathfrak{p} = (\mathbb{Z} + p\mathcal{O}_K)/p\mathcal{O}_K \simeq \mathbb{Z}/(p\mathcal{O}_K \cap \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z},$$

de modo que $\mathfrak{p}$ es un $\mathcal{O}$-ideal maximal en $\mathcal{O}$.

(2): Escribamos $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}w_K$, de modo que $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(pw_K)$. Luego

$$\begin{aligned}
\mathfrak{p} &= p\mathcal{O}_K = \mathbb{Z}p + \mathbb{Z}(pw_K), \\
\mathfrak{b} &= p\mathcal{O} = \mathbb{Z}p + \mathbb{Z}(p^2w_K), \\
\mathfrak{p}^2 &= p^2\mathcal{O}_K = \mathbb{Z}p^2 + \mathbb{Z}(p^2w_K),
\end{aligned}$$

lo que muestra $\mathfrak{p}^2 \subsetneq \mathfrak{b} \subsetneq \mathfrak{p}$. (Notar que esto sería imposible en un dominio de Dedekind.)

Ahora demostraremos que $\mathfrak{b}$ no es un producto de $\mathcal{O}$-ideales primos. Por absurdo, asumamos que $\mathfrak{b}$ es un producto de $\mathcal{O}$-ideales primos. Si $\mathfrak{q}$ es un $\mathcal{O}$-ideal primo que divide a $\mathfrak{b}$, entonces se tiene $\mathfrak{q} \supset \mathfrak{b} \supset \mathfrak{p}^2$, lo que implica $\mathfrak{q} \supset \mathfrak{p}$. Luego $\mathfrak{q} = \mathfrak{p}$, pues $\mathfrak{p}$ es un $\mathcal{O}$-ideal maximal. Como $\mathfrak{q}$ fue tomado arbitrariamente, tenemos que $\mathfrak{b}$ debe ser una potencia de $\mathfrak{p}$. Pero esto es imposible, ya que por (2) sabemos que $\mathfrak{p}^2 \subsetneq \mathfrak{b} \subsetneq \mathfrak{p}$, y $\mathfrak{p}^n \subset \mathfrak{p}^2$ para todo $n \geq 3$. Esto muestra la afirmación.

Finalmente observamos que, si K es cualquier cuerpo de números de grado $n > 1$, de manera análoga se puede probar que el $\mathcal{O}$-ideal $\mathfrak{b} = p\mathcal{O} = p\mathbb{Z} + p^2\mathcal{O}_K$ no es un producto de $\mathcal{O}$-ideales primos. (ver [Conrad, Example 8.2].)

4. Apéndice B. Cálculos de números de clases

Usando el Teorema 2.1 calcularemos algunos números de clases. Veremos dos ejemplos.

Ejemplo 4.1. El cuerpo $K = \mathbb{Q}(\sqrt{-1})$ tiene discriminante $d_K = -4$. Su orden maximal $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ tiene número de clases $h(\mathcal{O}_K) = 1$ (ver Ejemplo 3.7 (2) de Charla 3) y grupo de unidades es $\mathcal{O}_K^* = \{\pm 1, \pm i\}$. Para cada entero $f > 1$ consideremos el orden $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\sqrt{-1}$ de conductor f en K. Se tiene $[\mathcal{O}_K^* : \mathcal{O}_f^*] = 4/2 = 2$. Usando la fórmula (2.3) obtenemos

$$h(\mathcal{O}_f) = \frac{f}{2} \prod_{p|f} \left(1 - \left(\frac{-4}{p}\right) \frac{1}{p}\right).$$

Calcularemos $h(\mathcal{O}_f)$ para algunos valores de f. El símbolo de Kronecker $\left(\frac{-4}{2}\right) = 0$, pues $2|-4$. Ahora calculamos algunos símbolos de Legendre. En $\mathbb{Z}/3\mathbb{Z}$ se tiene $-4 = 2$ y $1^2 = 2^2 = 1$, luego -4 no es residuo cuadrático módulo 3, por tanto $\left(\frac{-4}{3}\right) = -1$. En $\mathbb{Z}/5\mathbb{Z}$ se tiene $-4 = 1$ y $1^2 = 1$, de modo que -4 es residuo cuadrático módulo 5, luego $\left(\frac{-4}{5}\right) = 1$. En $\mathbb{Z}/7\mathbb{Z}$ se tiene que $-4 = 3$, y $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ son congruentes a $1, 4, 2, 2, 4, 1$ respectivamente. Por tanto -4 no es residuo cuadrático módulo 7 y $\left(\frac{-4}{7}\right) = -1$. De la misma forma se verifica que $\left(\frac{-4}{11}\right) = -1$. Usando estos valores obtenemos

p	2	3	5	7	11
$1 - \left(\frac{-4}{p}\right)\frac{1}{p}$	1	$\frac{4}{3}$	$\frac{4}{5}$	$\frac{8}{7}$	$\frac{12}{11}$

Con estos datos calculamos

$h(\mathcal{O}_2) = \frac{2}{2} \cdot 1 = 1$

$h(\mathcal{O}_3) = \frac{3}{2} \cdot \frac{4}{3} = 2$

$h(\mathcal{O}_4) = \frac{4}{2} \cdot 1 = 2$

$h(\mathcal{O}_5) = \frac{5}{2} \cdot \frac{4}{5} = 2$

$h(\mathcal{O}_6) = \frac{6}{2} \cdot 1 \cdot \frac{4}{3} = 4$

$h(\mathcal{O}_7) = \frac{7}{2} \cdot \frac{8}{7} = 4$

$h(\mathcal{O}_8) = \frac{8}{2} \cdot 1 = 4$

$h(\mathcal{O}_9) = \frac{9}{2} \cdot \frac{4}{3} = 6$

$h(\mathcal{O}_{10}) = \frac{10}{2} \cdot 1 \cdot \frac{4}{5} = 4$

$h(\mathcal{O}_{11}) = \frac{11}{2} \cdot \frac{12}{11} = 6$

$h(\mathcal{O}_{12}) = \frac{12}{2} \cdot 1 \cdot \frac{4}{3} = 8$

$h(\mathcal{O}_{30}) = \frac{30}{2} \cdot 1 \cdot \frac{4}{3} \cdot \frac{4}{5} = 16$

$h(\mathcal{O}_{210}) = \frac{210}{2} \cdot 1 \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{8}{7} = 128$

$h(\mathcal{O}_{462}) = \frac{462}{2} \cdot 1 \cdot \frac{4}{3} \cdot \frac{8}{7} \cdot \frac{12}{11} = 384$

$h(\mathcal{O}_{3465}) = \frac{3465}{2} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{8}{7} \cdot \frac{12}{11} = 2304.$

Ejemplo 4.2. (Análogo al ejemplo anterior) El cuerpo $K = \mathbb{Q}(\sqrt{-14})$ tiene discriminante $d_K = -56$. Su orden maximal $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-14}$ tiene número de clases $h(\mathcal{O}_K) = h(-56) = 4$ (ver Ejemplo (5) de Charla 1-2) y grupo de unidades $\mathcal{O}_K^* = \{\pm 1\}$. Para cada entero $f > 1$ consideremos el orden $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\sqrt{-14}$ de conductor f en K. Se tiene $[\mathcal{O}_K^* : \mathcal{O}_f^*] = 2/2 = 1$. Usando la fórmula (2.3) obtenemos

$$h(\mathcal{O}_f) = 4f \prod_{p|f} \left(1 - \left(\frac{-56}{p}\right) \frac{1}{p}\right).$$

Calculemos $h(\mathcal{O}_f)$ para algunos valores de f. El símbolo de Kronecker $\left(\frac{-56}{2}\right) = 0$, pues $2|-56$. Ahora calculamos algunos símbolos de Legendre. En $\mathbb{Z}/3\mathbb{Z}$ se tiene $-56 = 1$ y $1^2 = 1$, así vemos que -56 es residuo cuadrático módulo 3, por tanto $\left(\frac{-56}{3}\right) = 1$. Para $p = 7$, se tiene $\left(\frac{-56}{7}\right) = 0$, pues $7|-56$. En $\mathbb{Z}/11\mathbb{Z}$ se tiene que $-56 = 10$, y $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2$ son congruentes a $1, 4, 9, 5, 3, 3, 5, 9, 4, 1$ respectivamente. Entonces -56 no es residuo cuadrático módulo 11 y $\left(\frac{-56}{11}\right) = -1$. Con estos valores se obtiene

p	2	3	5	7	11
$1-\left(\frac{-56}{p}\right)\frac{1}{p}$	1	$\frac{2}{3}$	$\frac{4}{5}$	1	$\frac{12}{11}$

Con esta información calculamos

$h(\mathcal{O}_2) = 4 \cdot 2 \cdot 1 = 4$

$h(\mathcal{O}_3) = 4 \cdot 3 \cdot \frac{2}{3} = 8$

$h(\mathcal{O}_4) = 4 \cdot 4 \cdot 1 = 16$

$h(\mathcal{O}_5) = 4 \cdot 5 \cdot \frac{4}{5} = 16$

$h(\mathcal{O}_6) = 4 \cdot 6 \cdot 1 \cdot \frac{2}{3} = 16$

$h(\mathcal{O}_7) = 4 \cdot 7 \cdot 1 = 28$

$h(\mathcal{O}_8) = 4 \cdot 8 \cdot 1 = 32$

$h(\mathcal{O}_9) = 4 \cdot 9 \cdot \frac{2}{3} = 24$

$h(\mathcal{O}_{10}) = 4 \cdot 10 \cdot 1 \cdot \frac{4}{5} = 32$

$h(\mathcal{O}_{11}) = 4 \cdot 11 \cdot \frac{12}{11} = 48$

$h(\mathcal{O}_{12}) = 4 \cdot 12 \cdot 1 \cdot \frac{2}{3} = 32$

$h(\mathcal{O}_{30}) = 4 \cdot 30 \cdot 1 \cdot \frac{2}{3} \cdot \frac{4}{5} = 64$

$h(\mathcal{O}_{210}) = 4 \cdot 210 \cdot 1 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 1 = 448$

$h(\mathcal{O}_{462}) = 4 \cdot 462 \cdot 1 \cdot \frac{2}{3} \cdot 1 \cdot \frac{12}{11} = 1344$

$h(\mathcal{O}_{3465}) = 4 \cdot 3465 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 1 \cdot \frac{12}{11} = 8064.$

5. Apéndice C. Fórmula para el orden de $(\mathcal{O}_K/\mathfrak{a})^*$

En este apéndice probaremos la siguiente fórmula

Proposición 5.1. *Sea K un cuerpo cuadrático imaginario. Para cada ideal $\mathfrak{a}$ de $\mathcal{O}_K$ se tiene la fórmula*

$$|(\mathcal{O}_K/\mathfrak{a})^*| = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right). \tag{5.12}$$

En particular, si f es un entero positivo, la fórmula anterior toma la forma

$$|(\mathcal{O}_K/f\mathcal{O}_K)^*| = f^2 \prod_{p|f} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right). \tag{5.13}$$

Demostración. Primero demostraremos la fórmula en el caso que $\mathfrak{a} = \mathfrak{p}^n$ es potencia de un primo de $\mathcal{O}_K$. Lo haremos por inducción en n. Si $n = 1$, $\mathcal{O}_K/\mathfrak{p}$ es cuerpo, luego $(\mathcal{O}_K/\mathfrak{p})^* = (\mathcal{O}_K/\mathfrak{p})\backslash\{\mathfrak{p}\}$. Así

$$|(\mathcal{O}_K/\mathfrak{p})^*| = N(\mathfrak{p}) - 1 = N(\mathfrak{p})\left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

se cumple la fórmula para $n = 1$. Ahora asumamos que la fórmula vale para $n - 1 \geq 1$, i.e.,

$$|(\mathcal{O}_K/\mathfrak{p}^{n-1})^*| = N(\mathfrak{p})^{n-1}\left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

Demostraremos la fórmula para n a través de una sucesión exacta de grupos. Para eso definiremos dos morfismos de grupos.

Consideremos primero el homomorfismo de grupos

$$\psi : (\mathcal{O}_K/\mathfrak{p}^n)^* \to (\mathcal{O}_K/\mathfrak{p}^{n-1})^*,\ \psi([\alpha]) = [\alpha].$$

Afirmamos que ψ es sobreyectivo. Tomemos un elemento $[\alpha] \in (\mathcal{O}_K/\mathfrak{p}^{n-1})^*$, esto significa que existen $[\beta] \in (\mathcal{O}_K/\mathfrak{p}^{n-1})^*$ y $\gamma \in \mathfrak{p}^{n-1}$ tal que $\alpha\beta - 1 = \gamma$. Notar que $\mathfrak{p}^{2n-2} \subseteq \mathfrak{p}^n$, pues $n \geq 2$

implica $2n-2 \geq n$. Luego, como

$$\begin{aligned}\alpha\beta(1-\gamma)-1 &= (\alpha\beta-1)-\alpha\beta\gamma \\ &= \gamma-\alpha\beta\gamma \\ &= \gamma(1-\alpha\beta) \\ &= -\gamma^2 \in \mathfrak{p}^{2n-2} \subseteq \mathfrak{p}^n,\end{aligned}$$

se tiene que $[\alpha] \in (\mathcal{O}_K/\mathfrak{p}^n)^*$, lo que demuestra la sobreyectividad de ψ.

Ahora definimos una función

$$\phi : \mathcal{O}_K/\mathfrak{p} \to (\mathcal{O}_K/\mathfrak{p}^n)^*.$$

Por unicidad de factorización de ideales en $\mathcal{O}_K$, sabemos que $\mathfrak{p}^n \subsetneq \mathfrak{p}^{n-1}$. Entonces, podemos tomar $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$. Definimos

$$\phi([\alpha]) := [1+\alpha u].$$

Veremos que ϕ está bien definida. Sea $[\alpha] \in \mathcal{O}_K/\mathfrak{p}$. Como u está en el $\mathcal{O}_K$-ideal $\mathfrak{p}^{n-1}$, tenemos $\alpha u \in \mathfrak{p}^{n-1}$. Luego $[\alpha u] = [0]$ en $\mathcal{O}_K/\mathfrak{p}^{n-1}$, y así $[\alpha u + 1] = [1] \in (\mathcal{O}_K/\mathfrak{p}^{n-1})^*$. Usando la sobreyectividad de ψ se obtiene $[1+\alpha u] \in (\mathcal{O}_K/\mathfrak{p}^n)^*$. Además, si $\alpha \equiv \beta \mod \mathfrak{p}$, entonces $(1+\alpha u) \equiv (1+\beta u) \mod \mathfrak{p}^n$, pues $u \in \mathfrak{p}^{n-1}$. Por tanto ϕ está bien definido.

Afirmamos que ϕ es homomorfismo de grupos. En efecto, si $[\alpha], [\beta] \in (\mathcal{O}_K/\mathfrak{p})$, se tiene

$$\begin{aligned}\phi([\alpha])\phi([\beta]) &= [1+\alpha u][1+\beta u] \\ &= [(1+\alpha u)(1+\beta u)] \\ &= [1+(\alpha+\beta)u+\alpha\beta u^2] \\ &= \underbrace{[1+(\alpha+\beta)u]}_{\phi([\alpha+\beta])} + [\alpha\beta]\underbrace{[u^2]}_{0} \\ &= \phi([\alpha]+[\beta]).\end{aligned}$$

Esto muestra que ϕ es homomorfismo de grupos.

Obtendremos directamente la fórmula para n si probamos que la sucesión de grupos

$$1 \longrightarrow \mathcal{O}_K/\mathfrak{p} \xrightarrow{\phi} (\mathcal{O}_K/\mathfrak{p}^n)^* \xrightarrow{\psi} (\mathcal{O}_K/\mathfrak{p}^{n-1})^* \longrightarrow 1, \tag{5.14}$$

es exacta, pues en tal caso

$$\begin{aligned}|(\mathcal{O}_K/\mathfrak{p}^n)^*| &= |\ker(\psi)||\mathrm{im}(\phi)| \\ &= |\mathcal{O}_K/\mathfrak{p}||(\mathcal{O}_K/\mathfrak{p}^{n-1})^*| \\ &= N(\mathfrak{p})N(\mathfrak{p})^{n-1}\left(1-\frac{1}{N(\mathfrak{p})}\right) \\ &= N(\mathfrak{p})^n\left(1-\frac{1}{N(\mathfrak{p})}\right).\end{aligned} \tag{5.15}$$

Como ψ es sobreyectiva, para probar la exactitud de (5.14), solo falta verificar que ϕ es inyectiva. Para eso, asumamos que $[1+\alpha u] = [1]$ en $(\mathcal{O}_K/\mathfrak{p}^n)^*$, luego $[\alpha u] = [0]$ en $\mathcal{O}_K/\mathfrak{p}^n$. Queremos ver que $\alpha \in \mathfrak{p}$. Por absurdo, asumamos $\alpha \notin \mathfrak{p}$. Entonces $[\alpha] \in (\mathcal{O}_K/\mathfrak{p})^*$. Como la sobreyectividad de ψ fue probada para $n \geq 2$ arbitrario, tenemos que $[\alpha] \in (\mathcal{O}_K/\mathfrak{p}^n)^*$, es decir, existe $\beta \in \mathcal{O}_K$ tal que $[\beta][\alpha] = [1]$ en $(\mathcal{O}_K/\mathfrak{p}^n)^*$. Luego en $\mathcal{O}_K/\mathfrak{p}^n$ se tiene

$$[u] = [1][u] = [\beta][\alpha][u] = [\beta][\alpha u] = [\beta][0] = [0],$$

es decir, $u \in \mathfrak{p}^n$ (contradicción). Por tanto ϕ es inyectivo y la sucesión (5.14) es exacta. Esto muestra la fórmula para el caso que $\mathfrak{a} = \mathfrak{p}^n$ es potencia de un primo de $\mathcal{O}_K$.

En general, si $\mathfrak{a}$ es un $\mathcal{O}_K$-ideal arbitrario, consideremos su factorización en potencias de $\mathcal{O}_K$-ideales primos distintos

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}.$$

Por el teorema chino del resto, tenemos un isomorfismo de anillos

$$\mathcal{O}_K/\mathfrak{a} \simeq \prod_{i=1}^{r} (\mathcal{O}_K/\mathfrak{p}_i^{n_i}),$$

que induce un isomorfismo entre sus grupos de unidades

$$(\mathcal{O}_K/\mathfrak{a})^* \simeq \prod_{i=1}^{r} (\mathcal{O}_K/\mathfrak{p}_i^{n_i})^*.$$

Así, la fórmula (5.12) para $\mathfrak{a}$ se obtiene directamente usando la fórmula para potencias de primos (5.15) y la multiplicatividad de la norma.

Finalmente, si f es un entero positivo, usando la fórmula (5.12) con $\mathfrak{a} = f\mathcal{O}_K$ y el resultado [Cox13, Proposition 5.16] para los primos que aparecen en la factorización única de f en potencias de primos enteros, se obtiene directamente la fórmula (5.13). □

6. Apéndice D. Finitud de la cantidad de órdenes con un número de clases dado

En este apéndice usaremos la desigualdad

$$h(d_K) > \frac{\log |d_K|}{55} \prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right), \tag{6.16}$$

el Teorema 2.1 y teoría de género de formas cuadráticas para demostrar que solo hay un número finito de órdenes con un número de clases h dado (ver Teorema 6.3 y Corolario 6.4). Para eso necesitamos algunos resultados previos.

Lema 6.1. *Para todo primo $p \geq 11$ se cumple*

$$1 - \frac{[2\sqrt{p}]}{p+1} \geq \frac{1}{2}. \tag{6.17}$$

Demostración. Para $p = 11$, se tiene

$$1 - \frac{[2\sqrt{11}]}{11+1} = 1 - \frac{[6,63324...]}{12} = 1 - \frac{6}{12} = \frac{1}{2}.$$

Para $p = 13$, tenemos que

$$1 - \frac{[2\sqrt{13}]}{13+1} = 1 - \frac{[7,21110...]}{14} = 1 - \frac{7}{14} = \frac{1}{2}.$$

Supongamos entonces que $p \geq 17$. Notar que la desigualdad (6.17) es equivalente a

$$\frac{[2\sqrt{p}]}{p+1} \leq \frac{1}{2}.$$

Luego, como $[2\sqrt{p}] \leq 2\sqrt{p}$, basta probar

$$\frac{2\sqrt{p}}{p+1} \leq \frac{1}{2},$$

que es equivalente a

$$p^2 - 14p + 1 \geq 0,$$

esto es,

$$(p - (7 + 4\sqrt{3}))(p - (7 - 4\sqrt{3})) \geq 0.$$

Esta desigualdad se satisface, pues $p \geq 17 > 7 + 4\sqrt{3}, 7 - 4\sqrt{3}$. Esto muestra el lema. □

Usando el Lema 6.1, hallaremos una cota inferior para $\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)$.

Lema 6.2. *Sea h entero positivo y asumamos $h(d_K) = h$. Entonces, se cumple*

$$\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \geq \frac{1}{3 \cdot 2^{\nu_2(h)+2}}, \tag{6.18}$$

donde ν_2 es la valuación 2-ádica.

Demostración. Sea μ el número de primos que divide a d_K, y sean $p_1, \ldots, p_r$ los primos impares que dividen a d_K (de modo que $\mu = r + 1$ o r dependiendo si $d_K \equiv 0$ o $1 \mod 4$). Por [Cox13, Theorem 6.1(iii)] y [Cox13, Corollary 3.14(i)] se tiene que $2^{\mu-1} \mid h$, lo que implica $\mu \leq \nu_2(h)+1$. Usando el Lema 6.1, demostraremos la desigualdad (6.18) para los distintos casos posibles.

Supongamos $d_K \equiv 1 \mod 4$. Luego $\mu = r$.

Si $p_i \geq 11$ para todo i, se tiene

$$\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \geq \frac{1}{2^r} \geq \frac{1}{2^{\nu_2(h)+1}} > \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.$$

Si $p_1 = 3$ y $p_i \geq 11$ para todo $i = 2, \ldots, r$, se tiene

$$\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \geq \left(1 - \frac{[2\sqrt{3}]}{4}\right) \frac{1}{2^{r-1}} \geq \frac{1}{4} \cdot \frac{1}{2^{\nu_2(h)}} > \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.$$

Si $p_1 = 3$, $p_2 = 5$ y $p_i \geq 11$ para todo $i = 3, \ldots, r$, se tiene

$$\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \geq \left(1 - \frac{[2\sqrt{3}]}{4}\right)\left(1 - \frac{[2\sqrt{5}]}{6}\right) \frac{1}{2^{r-2}} \geq \frac{1}{4} \cdot \frac{1}{3} \cdot \frac{1}{2^{\nu_2(h)}} = \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.$$

Los demás casos se demuestran de forma análoga.

Ahora supongamos $d_K \equiv 0 \mod 4$. Luego $\mu = r + 1$.
Si $p_i \geq 11$ para todo i, se tiene

$$\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) \geq \left(1 - \frac{[2\sqrt{2}]}{3}\right) \frac{1}{2^r} \geq \frac{1}{3} \cdot \frac{1}{2^{\nu_2(h)}} > \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.$$

Si $p_1 = 3$, $p_2 = 5$ y $p_3 = 7$, se tiene

$$\begin{aligned}\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) &\geq \left(1 - \frac{[2\sqrt{2}]}{3}\right)\left(1 - \frac{[2\sqrt{3}]}{4}\right)\left(1 - \frac{[2\sqrt{5}]}{6}\right)\left(1 - \frac{[2\sqrt{7}]}{8}\right) \frac{1}{2^{r-3}} \\ &\geq \frac{1}{3} \cdot \frac{1}{4} \cdot \frac{1}{3} \cdot \frac{3}{8} \cdot \frac{1}{2^{\nu_2(h)-3}} = \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.\end{aligned}$$

Si $p_1 = 5$, $p_2 = 7$, se tiene

$$\begin{aligned}\prod_{p|d_K,\ p<d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right) &\geq \left(1 - \frac{[2\sqrt{2}]}{3}\right)\left(1 - \frac{[2\sqrt{5}]}{6}\right)\left(1 - \frac{[2\sqrt{7}]}{8}\right) \frac{1}{2^{r-2}} \\ &\geq \frac{1}{3} \cdot \frac{1}{3} \cdot \frac{3}{8} \cdot \frac{1}{2^{\nu_2(h)-2}} = \frac{1}{3 \cdot 2^{\nu_2(h)+1}} > \frac{1}{3 \cdot 2^{\nu_2(h)+2}}.\end{aligned}$$

De forma análoga se demuestran los demás casos. □

Sea h un entero positivo fijo y asumamos $h(d_K) = h$. Usando la desigualdad (6.16) y el Lema (6.2) se obtiene directamente

$$h \geq \frac{\log |d_K|}{165 \cdot 2^{\nu_2(h)+2}}.$$

Despejando $|d_K|$ de esta desigualdad obtenemos

$$|d_K| \leq e^{165 \cdot 2^{\nu_2(h)+2} h}, \tag{6.19}$$

lo que demuestra que hay una cantidad finita de discriminantes negativos d_K con número de clases h.

Ahora demostraremos el resultado principal de este apéndice.

Teorema 6.3. *Sea h entero positivo. Entonces, la ecuación*

$$h(D) = h,$$

donde $D \equiv 0, 1 \mod 4$ es negativo, tiene una cantidad finita de soluciones.

Demostración. Sea $D \equiv 0, 1 \mod 4$ entero negativo tal que $h(D) = h$. Por [Cox13, Exercise 7.3(d)] existe un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario K que tiene discriminante D. Sea f el conductor de $\mathcal{O}$. Luego $D = f^2 d_K$, donde d_K es el discriminante del orden maximal $\mathcal{O}_K$.

Por el Teorema 2.1, tenemos que $h(d_K) \mid h$, luego $\nu_2(h(d_K)) \leq \nu_2(h)$. Luego, usando la cota (6.19) obtenemos

$$|d_K| \leq e^{165 \cdot 2^{\nu_2(h(d_K))+2} h(d_K)} \leq e^{165 \cdot 2^{\nu_2(h)+2} h}.$$

Multiplicando esta cota por f^2 se obtiene

$$|D| \leq e^{165 \cdot 2^{\nu_2(h)+2} h} f^2.$$

Solo falta acotar f en función de h.

Sea μ el número de primos que divide a D, y sean $p_1, \dots, p_r$ los primos impares que dividen a D (de modo que $\mu = r+1$ o r dependiendo si $d_K \equiv 0$ o $1 \mod 4$). Por [Cox13, Theorem 3.15(i)] y [Cox13, Corollary 3.14(i)] se tiene que $2^{\mu-1} \mid h$, lo que implica $\mu \leq \nu_2(h)+1$. Recordar que, por el Teorema 0.1 de la charla 4, tenemos $h(\mathcal{O}) = h(D)$, $h(\mathcal{O}_K) = h(d_K)$. Luego, por el Teorema 2.1, tenemos

$$\begin{aligned} h &= \frac{h(d_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right) \frac{1}{p}\right) \\ &\geq \frac{f}{3} \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &\geq \frac{f}{3 \cdot 2^{r+1}} \\ &\geq \frac{f}{3 \cdot 2^{\nu_2(h)+2}}. \end{aligned}$$

Por tanto

$$|D| \leq e^{165 \cdot 2^{\nu_2(h)+2} h} \cdot 3^2 \cdot 2^{2\nu_2(h)+4} h^2,$$

lo que demuestra que hay una cantidad finita de posibilidades para D. □

Como para cada entero negativo $D \equiv 0, 1 \mod 4$ existe un único orden en un cuerpo cuadrático imaginario, usando el Teorema 6.3 se obtiene directamente el siguiente resultado.

Corolario 6.4. *Sea h entero positivo. Entonces existe una cantidad finita de órdenes $\mathcal{O}$ en cuerpos cuadráticos imaginarios tales que $h(\mathcal{O}) = h$.*

Referencias

[Apostol76] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, New York, Inc, 1976. 2

[BS66] Z. I. Borevich, I. R. Shafarevich. *Number Theory.* Adacemic Press, New York, 1966. 2

[Conrad] K. Conrad. *Ideal Factorization.* Algebraic number theory, Unique factorization of ideals: https://kconrad.math.uconn.edu/blurbs/ 3.3

[Cox13] D. A. Cox. *Primes of the form $x^2 + ny^2$.* Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. 1, 2, 5, 6, 6

[DF04] D. S. Dummit, R. M. Foote. *Abstract Algebra.* Third Edition. University of Vermont. John Wiley & Sons, Inc, 2004. 1

[Gauss] C. F. Gauss. *Disquisitiones Arithmeticae*, Leipzig, 1801. Republished in 1863 as Volume I of *Werke*. French translation, *Reserches Arithmétiques*, Paris, 1807. (Reprint by Hermann, Paris, 1910.) German translation, *Untersuchungen über Höhere Arithmetik*, Berlin, 1889. (Reprint by Chelsea, New York, 1965.) English Translation, Yale, New Haven, 1966. (Reprint by Springer-Verlag, Berlin, Heidelberg, and New York, 1986.) 2, 2

E-mail address: srahausen@gmail.com