Cubo
A Mathematical Journal

CUBO, A Mathematical Journal
Vol. 27, no. 2, pp. 191–207, Agosto 2025
DOI: 10.56754/0719-0646.2702.191

Algunas extensiones infinitas de $\mathbb{Q}$ con la propiedad de Bogomolov

Benjamín Castillo[1,✉]

[1] *Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Macul, Santiago, Chile.*
brcastillo@uc.cl✉

RESUMEN

Sea ℓ un número primo y $K_\ell = \mathbb{Q}(\zeta_\ell)$ el cuerpo ciclotómico donde ζ_ℓ es una raíz primitiva ℓ-ésima de la unidad. Eligiendo un ideal primo $\mathfrak{p} \subseteq \mathcal{O}_{K_\ell}$ en el anillo de enteros algebraicos de K_ℓ, denotamos por $S_{\mathfrak{p},\ell}$ todas las extensiones de Galois de K_ℓ de grado ℓ donde $\mathfrak{p}$ no se escinde. Sea $L_{\mathfrak{p},\ell}$ el *compositum* de los cuerpos de clases de Hilbert de los cuerpos de $S_{\mathfrak{p},\ell}$. En este trabajo mostramos que $L_{\mathfrak{p},\ell}$ satisface la propiedad de Bogomolov analizando ciertos grados locales sobre K_ℓ. También estudiamos la relación de $L_{\mathfrak{p},\ell}$ con otras familias existentes en la literatura que satisfacen la propiedad de Bogomolov en el caso $\ell = 2$.

Palabras clave: Alturas, propiedad de Bogomolov, grados locales.

2020 AMS Mathematics Subject Classification: 11G50, 11S15.

Publicado: 15 de agosto de 2025
Aceptado: 28 de marzo de 2025
Recibido: 29 de julio de 2024

Cubo
A Mathematical Journal

CUBO, A Mathematical Journal
Vol. 27, no. 2, pp. 191–207, August 2025
DOI: 10.56754/0719-0646.2702.191

Some infinite extensions of $\mathbb{Q}$ satisfying Bogomolov's property

Benjamín Castillo[1,✉]

[1] *Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Macul, Santiago, Chile.*
brcastillo@uc.cl✉

ABSTRACT

Let ℓ be a prime number and $K_\ell = \mathbb{Q}(\zeta_\ell)$ the cyclotomic field, where ζ_ℓ is a primitive ℓ-root of unity. Choosing a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{K_\ell}$ in the ring of algebraic integers of K_ℓ, we denote by $S_{\mathfrak{p},\ell}$ all the Galois extensions of K_ℓ of degree ℓ where $\mathfrak{p}$ does not split. Let $L_{\mathfrak{p},\ell}$ be the *compositum* of Hilbert class fields of the fields of $S_{\mathfrak{p},\ell}$. In this work, we show that $L_{\mathfrak{p},\ell}$ satisfies Bogomolov's property by analyzing certain local degrees over K_ℓ. We also study the relation between $L_{\mathfrak{p},\ell}$ and other families present in the literature satisfying Bogomolov's property in the case $\ell = 2$.

Keywords and Phrases: Heights, Bogomolov property, local degrees.

2020 AMS Mathematics Subject Classification: 11G50, 11S15.

Published: 15 August, 2025
Accepted: 28 March, 2025
Received: 29 July, 2024

1. Introducción

Sea $\alpha \in \overline{\mathbb{Q}}$ un número algebraico y $h(\alpha)$ la altura logarítmica absoluta de Weil. Por un teorema de Kronecker, $h(\alpha) = 0$ si y solo si α es cero o una raíz de la unidad. Fuera de estos casos, D. H. Lehmer preguntó si $[\mathbb{Q}(\alpha) : \mathbb{Q}]h(\alpha)$ se puede acotar inferiormente de manera uniforme en α (ver [12, §13, página 476]). De manera más precisa:

Problema de Lehmer. *Existe un número real positivo c tal que para todo $\alpha \in \overline{\mathbb{Q}}^{\times}$ que no sea raíz de la unidad*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

Algunos de los resultados más cercanos al respecto se deben a Dobrowolski en [7] y a Smyth en [20]. Sin embargo, una posible solución parece estar fuera de alcance en estos momentos, por lo que se estudian variantes más débiles del problema. Siguiendo [4], decimos que un conjunto $\mathcal{A}$ de números algebraicos tiene la *propiedad de Bogomolov* (B) si existe un número real positivo T tal que el conjunto

$$\mathcal{A}(T) = \{\alpha \in \mathcal{A} \setminus \{0\} : h(\alpha) < T\}$$

consiste de todas las raíces de la unidad en $\mathcal{A}$. En otras palabras, los conjuntos con la propiedad (B) cumplen que el cero está aislado de los valores de $h(\alpha)$ y existe una cota inferior para la altura.

Todo cuerpo de números cumple la propiedad (B), así que para encontrar ejemplos no triviales debemos ver extensiones algebraicas infinitas de $\mathbb{Q}$. También es fácil encontrar cuerpos que no tengan la propiedad (B), por ejemplo el cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ no tiene (B) pues $h(2^{1/n}) = h(2)/n$. Al día de hoy se conocen ejemplos y criterios de cuerpos con la propiedad (B). Daremos un breve resumen de los resultados más generales.

1973: En [17], A. Schinzel demostró que el cuerpo de números algebraicos totalmente reales $\mathbb{Q}^{\mathrm{tr}}$ tiene la propiedad (B).

2000: En [2], F. Amoroso y U. Zannier mostraron que la máxima extensión abeliana K^{ab} de un cuerpo de números K satisface (B). En particular, cada extensión abeliana de K satisface (B).

2001: En [4, Theorem 2], E. Bombieri y U. Zannier probaron que cada extensión de Galois infinita $L/\mathbb{Q}$ con grado local acotado en algún primo racional (ver definición 2.1) tiene la propiedad (B).

2011: En [9], P. Habegger introdujo una familia de extensiones de Galois infinitas no abelianas sobre $\mathbb{Q}$ que no tienen grado local acotado sobre algún primo racional y que satisfacen (B). Más concretamente, sea E una curva elíptica definida sobre $\mathbb{Q}$ y E_{tors} el grupo de puntos de torsión en E definido en alguna clausura algebraica de $\mathbb{Q}$. Habegger consideró el cuerpo

$\mathbb{Q}(E_{\text{tors}})$ generado por el conjunto de coordenadas de los puntos en E_{tors} respecto a un modelo de Weierstrass de E con coeficientes racionales.

En [1], F. Amoroso, S. David y U. Zannier generalizaron el resultado sobre cuerpos con grado local acotado ([4, Theorem 2]) y extensiones abelianas ([2]).

Teorema 1.1 (Amoroso, David, Zannier)**.** *Sea K un cuerpo de números y L/K una extensión de Galois infinita con grupo de Galois G. Si $E \subseteq L$ es el cuerpo fijo por el centro $\mathrm{Z}(G)$ y E/K tiene grado local acotado en algún lugar no arquimedeano v en K acotado por d_0, entonces L tiene la propiedad* (B)*, con cota inferior uniforme en v, d_0 y $[K:\mathbb{Q}]$.*

Sumado a un resultado de S. Checcoli ([5, Theorem 1]), obtuvieron el siguiente corolario:

Corolario 1.2. *Si K es un cuerpo de números y L/K una extensión de Galois infinita con grupo de Galois G tal que $G/\mathrm{Z}(G)$ tiene exponente finito b, entonces L tiene la propiedad* (B)*, de manera uniforme en b y $[K:\mathbb{Q}]$.*

En este trabajo exhibiremos una familia de extensiones algebraicas infinitas de $\mathbb{Q}$ que satisfacen (B) como consecuencia del Teorema 1.1. Además, en algunos casos particulares mostraremos que las extensiones no satisfacen la hipótesis del Corolario 1.2 (lo que se interpreta como estar «lejos del caso abeliano») y que no pertenecen a la familia expuesta por P. Habegger en [9].

Nuestra construcción es la siguiente. Sea ℓ un número primo, $K_\ell = \mathbb{Q}(\zeta_\ell)$ el cuerpo ciclotómico donde ζ_ℓ es una raíz ℓ-ésima de la unidad primitiva, y sea $\mathfrak{p} \subseteq \mathcal{O}_{K_\ell}$ un ideal primo en el anillo de enteros algebraicos de K_ℓ. Definimos

$$S_{\mathfrak{p},\ell} = \{L/K_\ell \mid \text{una extensión de Galois con } [L:K_\ell] = \ell \text{ y tal que } \mathfrak{p} \text{ no se escinde en } L\}.$$

Para cada $L \in S_{\mathfrak{p},\ell}$, sea H_L el cuerpo de clases de Hilbert de L (es decir, la máxima extensión abeliana no ramificada de L). Finalmente, sea $L_{\mathfrak{p},\ell}$ el *compositum* de todos los H_L para $L \in S_{\mathfrak{p},\ell}$.

Teorema 1.3. *$L_{\mathfrak{p},\ell}$ satisface* (B).

Si $\ell = 2$ entonces K_ℓ es simplemente $\mathbb{Q}$, así que escribimos p en vez de $\mathfrak{p}$ y $S_{p,2}$ es el conjunto de cuerpos cuadráticos donde p no se escinde. En este caso obtenemos los siguientes resultados.

Teorema 1.4. *Sea p un número primo impar y E un cuerpo de números contenido en $L_{p,2}$ tal que $L_{p,2}/E$ es una extensión de Galois infinita. Entonces,*

$$\mathrm{Gal}(L_{p,2}/E)/\mathrm{Z}(\mathrm{Gal}(L_{p,2}/E))$$

tiene exponente infinito.

Teorema 1.5. *Sea p un primo impar. Si E es una curva elíptica definida sobre un cuerpo de números K, entonces $L_{p,2} \not\subset K(E_{\text{tors}})$.*

El Teorema 1.3 se sigue de que $L_{\mathfrak{p},\ell}/K_\ell$ es una extensión de Galois que tiene grado local acotado en el valor absoluto inducido por $\mathfrak{p}$. Los Teoremas 1.4 y 1.5 esencialmente extienden lo que ya se sabía del trabajo de A. Galateau en [8], donde se demuestran resultados similares para un cuerpo contenido estrictamente en $L_{p,2}$ cuya construcción es muy parecida (la diferencia es que Galateau impone más restricciones al conjunto $S_{p,2}$).

La demostración del Teorema 1.4 usa la misma idea de [8, Proposition 3.2], la cual es que el exponente del grupo de clases de cuerpos cuadráticos imaginarios crece a medida que su discriminante (en valor absoluto) lo hace (ver por ejemplo [16]). Para demostrar el Teorema 1.5 replicaremos exactamente la prueba de [8, Proposition 3.3]; si bien podríamos limitarnos a citarla, probablemente para el lector será más cómodo leerla aquí.

Para concluir la introducción deberíamos justificar que $L_{\mathfrak{p},\ell}$ en la mayoría de los casos es una extensión interesante, o sea que es una extensión infinita de $\mathbb{Q}$. Basta mostrar que el conjunto $S_{\mathfrak{p},\ell}$ no es finito, lo cual demostramos al final de la sección 4.

2. Grado local acotado

Manteniendo la notación usada en la introducción, en esta sección demostraremos que $L_{\mathfrak{p},\ell}/K_\ell$ es una extensión de Galois que tiene grado local acotado en el valor absoluto inducido por $\mathfrak{p}$, lo que nos permite mostrar la propiedad (B) para $L_{\mathfrak{p},\ell}$ (ver Teorema 1.3). Empecemos con una definición.

Definición 2.1. *Sea K un cuerpo de números, v un lugar no arquimedeano en K y L/K una extensión algebraica. Decimos que L/K tiene* grado local acotado *en v si existe un entero n tal que para cada extensión w de v en L se tiene que $[L_w : K_v] \leq n$, donde L_w y K_v son las completaciones correspondientes a w y v.*

Lema 2.2. *Sea K un cuerpo de números y fijemos un valor absoluto no arquimedeano v en K. Sea $\mathcal{F}$ una familia infinita de extensiones finitas de K. Supongamos que existe un entero d tal que para todo H en $\mathcal{F}$ y para toda extensión l a H de v se tiene que $[H_l : K_v] \leq d$. Si L es el compositum de las extensiones en $\mathcal{F}$, entonces L tiene grado local acotado en v.*

Demostración. Básicamente replicamos la demostración de [4, Proposition 1].

K_v tiene una cantidad finita de extensiones de grado m (ver por ejemplo [14, Corollary 2, página 226]), lo cual aplica para todo $m \in \mathbb{N}$. Luego, la colección $\mathcal{C}$ de extensiones de K_v de grado a lo más d es finita. En particular, si M es el *compositum* de los cuerpos en $\mathcal{C}$, entonces la extensión M/K_v es finita. Por hipótesis, para cada $H \in \mathcal{F}$ su completación en cualquier valor absoluto $l|v$

está contenido en $\mathcal{C}$, entonces, si w es cualquier valor absoluto en L sobre v, podemos incrustar $L_w \hookrightarrow M$ ya que L es el *compositum* de las extensiones en $\mathcal{F}$. Así, $[L_w : K_v] \leq [M : K_v]$ donde el último sólo depende de v y d. Por lo tanto, L tiene grado local acotado en v. □

Ahora mostremos que podemos aplicar este lema a nuestra construcción.

Proposición 2.3. *Sea $L \in S_{\mathfrak{p},\ell}$ y H su cuerpo de clases de Hilbert. Si l es un valor absoluto en H sobre $\mathfrak{p}$, entonces*

$$[H_l : (K_\ell)_\mathfrak{p}] \leq \ell^2 \cdot (\textit{orden de } \mathfrak{p} \textit{ en el grupo de clases de } K_\ell)$$

donde $(K_\ell)_\mathfrak{p}$ es la completación de K_ℓ respecto a $\mathfrak{p}$.

Demostración. Por definición de $S_{\mathfrak{p},\ell}$ se tiene que $\mathfrak{p}$ no se escinde en L y L/K_ℓ es una extensión de Galois de grado ℓ, así, w denotará a un representante del único lugar en L bajo l; además, $\mathfrak{P} \subseteq \mathcal{O}_H$ y $\mathfrak{g} \subseteq \mathcal{O}_L$ denotarán a los primos correspondientes a cada valor absoluto.

Primero es claro que $[L_w : (K_\ell)_\mathfrak{p}] = \ell$. Por otro lado, sabemos que $[H_l : L_w] = e_{H/L}(\mathfrak{P}) f_{H/L}(\mathfrak{P})$, donde $e_{H/L}$ y $f_{H/L}$ son el índice de ramificación y grado de inercia de $\mathfrak{P}$, así que basta calcular estos invariantes. H/L es una extensión abeliana no ramificada, por lo que $e_{H/L}(\mathfrak{P}) = 1$ y $f_{H/L}(\mathfrak{P}) = \operatorname{ord}(\sigma_\mathfrak{g}) = \operatorname{ord}([\mathfrak{g}])$, donde $\sigma_\mathfrak{g}$ es el elemento de Frobenius. La última igualdad viene del isomorfismo de *Reciprocidad de Artin* $C(\mathcal{O}_L) \simeq \operatorname{Gal}(H/L)$ dado por $[\mathfrak{g}] \mapsto \sigma_\mathfrak{g}$, donde $C(\mathcal{O}_L)$ es el grupo de clases de $\mathcal{O}_L$ (ver [11, Chapter V, Theorem 5.7] para una demostración).

Si $\mathfrak{p}$ es inerte en L entonces $\mathfrak{g} = \mathfrak{p}\mathcal{O}_L$. En el otro caso, si $\mathfrak{p}$ se ramifica en L entonces $\mathfrak{g}^\ell = \mathfrak{p}\mathcal{O}_L$. Luego, si n es el orden de $\mathfrak{p}$ en el grupo de clases de K_ℓ tenemos que

$$[H_l : L_w] = \operatorname{ord}([\mathfrak{g}]) \leq \begin{cases} \ell \cdot n & \text{si } \mathfrak{p} \text{ se ramifica en } L \\ n & \text{si } \mathfrak{p} \text{ es inerte en } L \end{cases}$$

con lo cual el resultado sigue de la ley de las torres. □

El último ingrediente que falta para probar que $L_{\mathfrak{p},\ell}/K_\ell$ satisface (B) es mostrar que $L_{\mathfrak{p},\ell}/K_\ell$ es una extensión de Galois. Para esto es suficiente la siguiente buena propiedad que tienen los cuerpos de clases de Hilbert.

Lema 2.4. *Sea k un cuerpo de números, F/k una extensión de Galois finita y H_F el cuerpo de clases de Hilbert de F. La extensión H_F/k es de Galois.*

Demostración. Sea L/H_F una extensión de cuerpos y $\sigma : H_F \to L$ un morfismo de k-álgebras. Notemos que $\sigma(H_F)$ es una extensión abeliana no ramificada de $\sigma(F) = F$, con lo cual $\sigma(H_F) \subseteq H_F$ y por tanto $\sigma(H_F) = H_F$. Luego, la extensión H_F/k es de Galois. □

Ahora demostrar que $L_{\mathfrak{p},\ell}$ tiene la propiedad (B) es sencillo.

Demostración del Teorema 1.3. Primero la extensión $L_{\mathfrak{p},\ell}/K_\ell$ es de Galois por el Lema 2.4. Por la Proposición 2.3 tenemos que $L_{\mathfrak{p},\ell}$ es el *compositum* de cuerpos de números tal que, para cada valor absoluto en ellos sobre $\mathfrak{p}$, el grado de su completación sobre $(K_\ell)_\mathfrak{p}$ está acotado por $\ell^2 \cdot \mathrm{ord}([\mathfrak{p}])$, donde $[\mathfrak{p}]$ es la clase de $\mathfrak{p}$ en el grupo de clases de K_ℓ. Luego, $L_{\mathfrak{p},\ell}$ tiene grado local acotado en $\mathfrak{p}$ por el Lema 2.2. Por lo tanto, $L_{\mathfrak{p},\ell}$ satisface (B) por el Teorema 1.1. □

3. El caso $\ell = 2$

En esta sección realizaremos un análisis más explícito de qué cuerpo aparece al completar $L_{\mathfrak{p},2}$, obteniendo la extensión bi-cuadrática de $\mathbb{Q}_p$, en el sentido de que es la extensión de $\mathbb{Q}_p$ de grado 4 cuyo índice de ramificación y grado residual es 2. Esto nos va permitir dar una cota inferior para el límite inferior de la altura en $L_{\mathfrak{p},2}$ gracias a [4, Theorem 2].

Recordemos que en el caso $\ell = 2$ se tiene que $K_\ell = \mathbb{Q}$, por lo que simplificaremos la notación cambiando $\mathfrak{p}$ por p un número primo impar (en lo que sigue es relevante que el primo p sea impar), $S_{\mathfrak{p},2}$ por S_p y $L_{\mathfrak{p},2}$ por L_p. En resumen, nuestro cuerpo base es $\mathbb{Q}$, S_p son los cuerpos cuadráticos donde p no se escinde y L_p es el *compositum* de los cuerpos de clases de Hilbert H_K para $K \in S_p$.

Fijando notación, dado K en S_p sea H_K su cuerpo de clases de Hilbert, $\mathfrak{p} \subseteq \mathcal{O}_K$ el ideal primo sobre p, $\mathfrak{P} \subseteq \mathcal{O}_{H_K}$ cualquier ideal primo sobre $\mathfrak{p}$ y $K_\mathfrak{p}$, $H_\mathfrak{P}$ los cuerpos completados de K y H_K respecto a estos primos. El siguiente resultado es claro.

Lema 3.1. *Para $K_\mathfrak{p}$ tenemos las siguientes posibilidades:*

- *Si p es inerte en K: $K_\mathfrak{p}$ es la extensión cuadrática no ramificada de $\mathbb{Q}_p$.*
- *Si p se ramifica en K: $K_\mathfrak{p}$ es una extensión cuadrática ramificada de $\mathbb{Q}_p$.*

Por otro lado, siguiendo la demostración de la Proposición 2.3 obtenemos lo siguiente.

Proposición 3.2. *Para $H_\mathfrak{P}$ tenemos las siguientes posibilidades:*

- *Si p es inerte en K: $H_\mathfrak{P}$ es la extensión cuadrática no ramificada de $\mathbb{Q}_p$.*
- *Si p se ramifica en K y $\mathfrak{p}$ es principal: $H_\mathfrak{P}$ es una extensión cuadrática ramificada de $\mathbb{Q}_p$.*
- *Si p se ramifica en K y $\mathfrak{p}$ no es principal: $H_\mathfrak{P}$ es una extensión de $\mathbb{Q}_p$ de grado 4 moderadamente ramificada, es decir, $e(H_\mathfrak{P}/\mathbb{Q}_p) = f(H_\mathfrak{P}/\mathbb{Q}_p) = 2$.*

Demostración. Ver la demostración de la Proposición 2.3 y tener en mente que "$\mathfrak{g}$" y "$\mathfrak{p}$" en esa proposición son, en este caso, $\mathfrak{p}$ y p respectivamente. □

Ahora somos capaces de especificar quienes son los cuerpos $H_{\mathfrak{P}}$.

Proposición 3.3. *Sea p un primo impar y $K \in S_p$. Los cuerpos p-ádicos que pueden aparecer al completar H_K respecto a un valor absoluto sobre p son $\mathbb{Q}_p(\sqrt{\zeta})$, $\mathbb{Q}_p(\sqrt{\zeta\pi})$, $\mathbb{Q}_p(\sqrt{\pi})$ y $\mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$, donde π es un primo fijo en $\mathbb{Z}_p$ y ζ es una raíz primitiva de la unidad de orden $p-1$.*

En particular, el compositum de todos ellos es $\mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$.

Demostración. La herramienta clave de la demostración es [14, Proposition 5.31].

El primer y segundo punto de la Proposición 3.2 recaen en las opciones $\mathbb{Q}_p(\sqrt{\zeta})$, $\mathbb{Q}_p(\sqrt{\zeta\pi})$, $\mathbb{Q}_p(\sqrt{\pi})$, donde π es un primo fijo en $\mathbb{Z}_p$ y ζ es una raíz primitiva de la unidad de orden $p-1$.

Para el tercer punto de la Proposición 3.2, notemos que $H_{\mathfrak{P}}$ es la extensión cuadrática no ramificada de $K_{\mathfrak{p}}$ (ver Proposición 2.3), así que por [14, Proposition 5.31]

$$H_{\mathfrak{P}} = K_{\mathfrak{p}}(\sqrt{\zeta}),$$

donde ζ se puede escoger igual que antes pues estamos en el caso en que p se ramifica en K. Por el Lema 3.1 tenemos que $K_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{\pi})$ ó $K_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{\zeta\pi})$. En cualquier caso,

$$H_{\mathfrak{P}} = \mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$$

que es la extensión bi-cuadrática de $\mathbb{Q}_p$ por [14, Proposition 5.32]. □

Proposición 3.4. *L_p satisface que*

$$\liminf_{\alpha\in L_p} h(\alpha) \geq \frac{\log p}{4(p^2+1)}.$$

Demostración. Sea $M = \mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$ la extensión bi-cuadrática de $\mathbb{Q}_p$ donde π es un primo fijo en $\mathbb{Z}_p$ y ζ una raíz de la unidad de orden $p-1$. En particular, $e(M/\mathbb{Q}_p) = f(M/\mathbb{Q}_p) = 2$.

Si $v|p$ es un valor absoluto en L_p, por la Proposición 3.2 podemos tomar un H_K tal que $(H_K)_v \simeq \mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$. Luego, por la Proposición 3.3 tenemos la incrustación

$$H_K \hookrightarrow L_p \hookrightarrow \mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$$

con lo cual $(L_p)_v \simeq \mathbb{Q}_p(\sqrt{\pi},\sqrt{\zeta})$.

Con esto, $p \in S(L_p)$ donde $S(L_p)$ es el conjunto de números primos q tal que L_p se puede incrustar en una extensión finita L de $\mathbb{Q}_q$. Como $L_p/\mathbb{Q}$ es una extensión normal (ver Lema 2.4) podemos usar la cota inferior de [4, Theorem 2], la cual es

$$\liminf_{\alpha\in L_p} h(\alpha) \geq \frac{1}{2}\sum_{q\in S(L_p)} \frac{\log q}{e_q(q^{f_q}+1)} \geq \frac{\log p}{4(p^2+1)}. \qquad \square$$

4. Resultados auxiliares

En esta sección demostraremos los resultados necesarios para la demostración del Teorema 1.4. Esta sección se inspira en precisar la idea utilizada en [8, Proposition 3.2]. Como la demostración del Teorema 1.4 es sencilla, para el lector probablemente sea más eficiente pasar directamente a la siguiente sección y volver en caso de querer verificar los detalles. Al final también mostraremos que $S_{\mathfrak{p},\ell}$ no es finito. Empecemos con la noción de grupo dihedral generalizado.

Definición 4.1. *Sea N un grupo abeliano no trivial. El grupo dihedral generalizado de N es el producto semidirecto*

$$N \rtimes \mathbb{Z}/2\mathbb{Z}$$

donde $\mathbb{Z}/2\mathbb{Z}$ actúa en N invirtiendo elementos, así que la operación de grupo viene dada por

$$(n_1,0)\cdot(n_2,a) = (n_1n_2,a)$$
$$(n_1,1)\cdot(n_2,a) = (n_1n_2^{-1},1+a)$$

Lo denotamos por Dih(N).

El siguiente resultado elemental nos será bastante útil.

Lema 4.2. *Si N es un grupo abeliano no trivial entonces* $\mathrm{Z}(\mathrm{Dih}(N))$ *es un grupo de exponente 2.*

Demostración. Sea $n \in N$. Si $(n,0) \in \mathrm{Z}(\mathrm{Dih}(N))$, operando $(n,0)$ con $(n,1)$ vemos que

$$(n,0)\cdot(n,1) = (n^2,1) = (e_N,1) = (n,1)\cdot(n,0)$$

con lo cual $n^2 = e_N$ y $(n,0)$ tiene orden 2.

Por otro lado, es claro que todo elemento en $\mathrm{Dih}(N)$ de la forma $(n,1)$ tiene orden 2. $\square$

Lema 4.3. *Si K es un cuerpo cuadrático imaginario y H_K su cuerpo de clases de Hilbert, el grupo de Galois de $H_K/\mathbb{Q}$ es un grupo dihedral generalizado*

$$\mathrm{Gal}(H_K/\mathbb{Q}) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Demostración. La extensión $H_K/\mathbb{Q}$ es de Galois por el Lema 2.4. Fijemos una incrustación $H_K \subset \mathbb{C}$

y sea $\tau : \mathbb{C} \to \mathbb{C}$ la conjugación compleja. Notemos que tenemos la secuencia exacta

$$0 \to \mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_K/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 0$$

la cual se escinde pues $\tau \in \mathrm{Gal}(H_K/\mathbb{Q})$ (ver Lema 2.4) y tenemos la sección $\tau_{|K} \mapsto \tau_{|H_K}$. Entonces,

$$\mathrm{Gal}(H_K/\mathbb{Q}) \simeq \mathrm{Gal}(H_K/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$$

donde τ actúa en $\mathrm{Gal}(H_K/K)$ conjugando elementos.

Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ y $\sigma_{\mathfrak{p}}$ el elemento de Frobenius, es sabido que $\sigma_{\tau(\mathfrak{p})} = \tau \circ \sigma_{\mathfrak{p}} \circ \tau^{-1}$, así que en vista del isomorfismo de *Reciprocidad de Artin* $C(\mathcal{O}_K) \simeq \mathrm{Gal}(H/K)$ dado por $[\mathfrak{p}] \mapsto \sigma_{\mathfrak{p}}$ (ver [11, Chapter V, Theorem 5.7] para una demostración), $\mathrm{Gal}(K/\mathbb{Q})$ actúa en el grupo de clases $C(\mathcal{O}_K)$ mandando a un primo a su conjugado, que es su inverso pues estamos en una extensión cuadrática. Por lo tanto,

$$\mathrm{Gal}(H_K/\mathbb{Q}) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}$$

donde $\mathbb{Z}/2\mathbb{Z}$ actúa en $C(\mathcal{O}_K)$ invirtiendo elementos. □

El lema anterior es lo que nos va a permitir hablar sobre el exponente del grupo de clases $C(\mathcal{O}_K)$ de un cuerpo cuadrático imaginario K (recordamos que el exponente de un grupo es el mínimo común múltiplo de los ordenes de los elementos del grupo). Ahora precisaremos la idea de que este exponente va creciendo a medida que el discriminante de K lo hace. Primero necesitamos un resultado de densidad.

Lema 4.4. *Sea p un número primo impar. Si $\mathcal{A}$ es el conjunto de primos que son residuos cuadráticos módulo p y que además son congruentes a 3 módulo 4, entonces $d(\mathcal{A}) = 1/4$ donde $d(\mathcal{A})$ es la densidad de Dirichlet.*

Demostración. Sean $a, m \in \mathbb{Z}$ con $(a, m) = 1$, sea $\mathcal{P}(a; m)$ el conjunto de primos q tal que $q \equiv a$ mód m.

Si r es un residuo cuadrático módulo p y $r \equiv 3 \mod 4$, por el teorema chino del resto existe una única clase s en $\mathbb{Z}/4p\mathbb{Z}$ tal que $r \equiv s \mod 4p$. Por el teorema de Dirichlet sobre primos en progresión aritmética $d(\mathcal{P}(s; 4p)) = 1/(2(p-1))$ (ver [10, Theorem 1, página 251]). Además, es sabido que la cantidad de residuos cuadráticos módulo p es $(p-1)/2$, así que por la aditividad de la densidad $d(\mathcal{A}) = 1/4$. □

El siguiente teorema se debe a F. Pappalardi.

Teorema 4.5. *Si d es un entero positivo y $m(d)$ es el exponente del grupo de clases de $\mathbb{Q}(\sqrt{-d})$, para todos los $d < x$ tales que $-d$ es un discriminante se tiene que*

$$m(d) > \frac{\log d/4}{\log\log d},$$

salvo a lo más $O\left(x^{1-A(\log\log x)^{-1}}\right)$ excepciones. Más precisamente, para cada $A \leq \frac{1}{2}\log 2$ se tiene que

$$\#\left\{d \leq x : m(d) \leq \frac{\log d/4}{\log\log d}\right\} \ll_A x^{1-A(\log\log x)^{-1}}.$$

Demostración. Ver [16, Theorem 1.2]. □

Observación 4.6. *En particular, el conjunto de excepciones tiene densidad natural cero y por ende también tiene densidad de Dirichlet cero.*

Nos interesa que el exponente vaya creciendo en un grupo específico de cuerpos cuadráticos imaginarios.

Proposición 4.7. *Sea p un número primo impar. Si $\mathcal{C}$ es la colección de cuerpos cuadráticos $\mathbb{Q}(\sqrt{-q})$ donde q es un primo congruente a 3 módulo 4 que es residuo cuadrático módulo p, entonces, para todo $n \in \mathbb{N}$ existe $\mathbb{Q}(\sqrt{-q_n}) \in \mathcal{C}$ tal que*

$$m(q_n) > n$$

donde $m(q_n)$ es el exponente del grupo de clases de $\mathbb{Q}(\sqrt{-q_n})$.

Demostración. La condición $q \equiv 3 \mod 4$ ciertamente hace que $-q$ sea un discriminante. Notemos que si A es un número real positivo, se tiene que

$$\lim_{x\to+\infty} \frac{x^{A(\log\log x)^{-1}}}{\log x} = +\infty.$$

Por el teorema de los números primos, $\pi(x) \sim \frac{x}{\log x}$, luego, el cálculo anterior nos muestra que la cantidad de primos menores o iguales a x sobrepasa al conjunto de excepciones del Teorema 4.5 a medida que x crece, y por ende podemos encontrar un primo q suficientemente grande tal que $m(q) > n$. Como esta condición depende del tamaño de q, podemos tomar un q_n tal que $\mathbb{Q}(\sqrt{-q_n}) \in \mathcal{C}$ y $m(q_n) > n$. Notemos que si esto último no fuera posible, quiere decir que los números mayores que q del conjunto $\mathcal{A}$ del Lema 4.4 están todos contenidos en el conjunto de excepciones del Teorema 4.5. Sin embargo, esto implicaría que $\mathcal{A}$ tiene densidad de Dirichlet cero, lo cual no es cierto. □

Observación 4.8. *Lo mismo aplica si consideramos q que no es residuo cuadrático módulo p, lo cual será necesario en la demostración del Teorema 1.4.*

Los siguientes resultados son para justificar que $L_{\mathfrak{p},\ell}$ en general es una extensión infinita de $\mathbb{Q}$. Recordemos que la notación utilizada se encuentra en la introducción.

Lema 4.9. *Para cada clase $\overline{\alpha} \in \mathcal{O}_{K_\ell}/\mathfrak{p}$, existen infinitos $\beta \equiv \alpha \mod \mathfrak{p}$ tal que $x^\ell - \beta$ es irreducible en K_ℓ.*

Demostración. Sea α representante de alguna clase en $\mathcal{O}_{K_\ell}/\mathfrak{p}$ y supongamos que α es una potencia ℓ-ésima en K_ℓ, es decir, existe $a \in K_\ell$ tal que $\alpha = a^\ell$. En particular, $a \in \mathcal{O}_{K_\ell}$.

Si $p \in \mathfrak{p}$ tenemos que $\alpha \equiv \alpha + (p^\ell)^n \mod \mathfrak{p}$ para todo $n \in \mathbb{N}$. Si $\alpha + (p^\ell)^n$ es una potencia ℓ-ésima, digamos, $\alpha + (p^\ell)^n = c_n^\ell$ con $c_n \in \mathcal{O}_{K_\ell}$, entonces $a^\ell + (p^n)^\ell = c_n^\ell$ y $(a, p^n, c_n) \in (\mathcal{O}_{K_\ell})^3$ serían soluciones de la ecuación

$$x^\ell + y^\ell = z^\ell$$

en $\mathcal{O}_{K_\ell} = \mathbb{Z}[\zeta_\ell]$.

Si $\ell > 3$, el Teorema de Faltings (*cf.* [3, página 352]) asegura que la curva $X^\ell + Y^\ell = 1$ tiene una cantidad finita de puntos racionales en K_ℓ. Si $\ell = 3$, la ecuación no tiene soluciones por el teorema de Kummer sobre la ecuación de Fermat para primos regulares (*cf.* [15, pp. 37-38]). Luego, en ambos casos existen infinitos $\beta_n = \alpha + (p^\ell)^n$ tal que $x^\ell - \beta_n$ es irreducible.

Si $\ell = 2$, el argumento anterior no funciona. Sin embargo, en ese caso $\mathcal{O}_{K_\ell} = \mathbb{Z}$ por lo que el resultado es claro. □

Proposición 4.10. *$S_{\mathfrak{p},\ell}$ no es finito cuando $\mathfrak{p} \nmid \ell$.*

Demostración. Si L es una extensión de Galois de K_ℓ de grado ℓ podemos asumir que $L = K_\ell(\sqrt[\ell]{\alpha})$ para algún $\alpha \in \mathcal{O}_{K_\ell}$, *i.e.*, cuyo generador tiene polinomio minimal $x^\ell - \alpha \in \mathcal{O}_{K_\ell}[x]$. Nos limitaremos a analizar bajo que condiciones $\mathfrak{p}$ es inerte en L.

Si $\alpha \not\equiv 0 \mod \mathfrak{p}$ entonces $x^\ell - \alpha$ es separable módulo $\mathfrak{p}$ y por ende $\mathfrak{p}$ no se ramifica en L. Además, $\mathfrak{p}$ se escinde en L si y solo si $x^\ell \equiv \alpha \mod \mathfrak{p}$ tiene solución en $\mathcal{O}_{K_\ell}$ (ver por ejemplo [6, Proposition 5.11]). Tomando un generador de $(\mathcal{O}_{K_\ell}/\mathfrak{p})^\times$ es un simple ejercicio ver que esto último es equivalente a que

$$\alpha^{\frac{N(\mathfrak{p})-1}{(\ell, N(\mathfrak{p})-1)}} \equiv 1 \mod \mathfrak{p}.$$

Sea s la característica de $\mathcal{O}_{K_\ell}/\mathfrak{p}$. Notemos que $N(\mathfrak{p})-1 = s^{f_\mathfrak{p}}-1$ donde $f_\mathfrak{p}$ es el grado de inercia de $\mathfrak{p}$. Por otro lado, recordemos que $K_\ell = \mathbb{Q}(\zeta_\ell)$ es un cuerpo ciclotómico, con lo cual $f_\mathfrak{p} = \mathrm{ord}_{\mathbb{F}_\ell^\times}(s)$ y por ende $(\ell, N(\mathfrak{p})-1) = \ell$. En resumen,

$$\mathfrak{p} \text{ se escinde en } L \iff \alpha^{\frac{N(\mathfrak{p})-1}{\ell}} \equiv 1 \mod \mathfrak{p}.$$

Luego, en el caso de que α no sea raíz del polinomio $x\cdot(x^{\frac{N(\mathfrak{p})-1}{\ell}}-1)$ módulo $\mathfrak{p}$ se tendrá que $\mathfrak{p}$ es inerte en L. El lema anterior muestra que podemos encontrar una cantidad infinita de extensiones L/K_ℓ de este tipo, lo cual concluye la demostración. □

5. Relación de $L_{\mathfrak{p},2}$ con otras familias

En esta última sección vamos a probar el Teorema 1.4 y Teorema 1.5. También recordamos que la demostración del Teorema 1.5 se puede encontrar en [8, Proposition 3.3] y aquí simplemente la vamos a reescribir.

Al igual que en la sección 3, simplificamos la notación cambiando $\mathfrak{p}$ por p un número primo impar, $S_{\mathfrak{p},2}$ por S_p y $L_{\mathfrak{p},2}$ por L_p. En resumen, nuestro cuerpo base es $\mathbb{Q}$, S_p son los cuerpos cuadráticos donde p no se escinde y L_p es el *compositum* de los cuerpos de clases de Hilbert H_K para $K \in S_p$.

Consideremos la colección

$$R_p = \left\{\mathbb{Q}(\sqrt{-q}) : q \text{ es primo, } q \equiv 3 \mod 4 \text{ y } \left(\frac{-q}{p}\right) = -1\right\}$$

donde $\left(\text{-}\right)$ es el símbolo de Legendre (de hecho, esta es la colección utilizada por A. Galateau en [8]). Con estas condiciones $-q$ es un discriminante y p es inerte en $\mathbb{Q}(\sqrt{-q})$, por lo que $R_p \subset S_p$. La ventaja de trabajar con los cuerpos de clases de Hilbert de estos cuerpos cuadráticos es que su intersección a pares es trivial.

Lema 5.1. *Sean K y K' cuerpos cuadráticos distintos contenidos en R_p y H_K, $H_{K'}$ los cuerpos de clases de Hilbert respectivos. Se tiene que $H_K \cap H_{K'} = \mathbb{Q}$.*

Demostración. Sea q un número primo. Notemos que $H_{\mathbb{Q}(\sqrt{-q})}/\mathbb{Q}$ se ramifica solo en q, ya que $\mathbb{Q}(\sqrt{-q})/\mathbb{Q}$ se ramifica solo en q y $H_{\mathbb{Q}(\sqrt{-q})}/\mathbb{Q}(\sqrt{-q})$ no se ramifica.

Si q y s son primos distintos, la intersección de $H_{\mathbb{Q}(\sqrt{-q})}$ y $H_{\mathbb{Q}(\sqrt{-s})}$ es trivial, pues en caso contrario tendría ramificación por el teorema de Minkowski (*cf.* [15, Chapter III, (2.17)]) la cual se extendería sobre estos dos cuerpos. □

Ahora estamos listos para probar el Teorema 1.4.

Demostración del Teorema 1.4. La demostración será por contradicción, asumamos que este exponente es finito y llamémoslo I.

Al existir una cantidad finita de cuerpos intermedios $E/M/\mathbb{Q}$ solo puede haber una cantidad finita de $K \in R_p$ tal que $H_K \cap E \neq \mathbb{Q}$, ya que por el Lema 5.1 estos cuerpos no pueden repetirse cuando variamos K. Entonces, por la Proposición 4.7 podemos fijar un $K \in R_p$ tal que $C(\mathcal{O}_K)$ tiene exponente mayor que $2I$ y $H_K \cap E = \mathbb{Q}$. Con esto, siendo $H_K E$ el *compositum* de H_K y E, tenemos que

$$\mathrm{Gal}(H_K E/E) \simeq \mathrm{Gal}(H_K/\mathbb{Q})$$

y por el Lema 4.3

$$\mathrm{Gal}(H_K E/E) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}. \tag{5.1}$$

Tenemos las extensiones $L_p/H_K E/E$ y además la extensión $H_K E/E$ es de Galois, por lo que $\mathrm{Gal}(H_K E/E)$ es isomorfo a un cociente de $\mathrm{Gal}(L_p/E)$ que llamaremos C. Notemos que la proyección $\pi : \mathrm{Gal}(L_p/E) \twoheadrightarrow C$ induce un homomorfismo sobreyectivo

$$\mathrm{Gal}(L_p/E)/\mathrm{Z}(\mathrm{Gal}(L_p/E)) \twoheadrightarrow C/\mathrm{Z}(C),$$

con lo cual $\mathrm{Gal}(H_K E/E)/\mathrm{Z}(\mathrm{Gal}(H_K E/E))$ tiene exponente menor o igual que I. Luego, el isomorfismo (5.1) y Lema 4.2 nos dice que $C(\mathcal{O}_K)$ tiene exponente menor o igual que $2I$, lo cual es una contradicción. Por lo tanto, I no puede ser finito. □

Por último, veamos que L_p no pertenece a la familia establecida por Habegger ([9]).

Demostración del Teorema 1.5. Por contradicción supongamos que $L_p \subset K(E_{\mathrm{tors}})$.

Si E tiene multiplicación compleja, $K(E_{\mathrm{tors}}) \subset K^{\mathrm{ab}}$ (ver por ejemplo [19, página 428]) con lo cual $\mathrm{Gal}(L_p/L_p \cap K) \simeq \mathrm{Gal}(L_p K/K)$ sería abeliano, lo que contradice el Teorema 1.4.

Si E no tiene multiplicación compleja, sea q un número primo que satisface las condiciones de R_p y es suficientemente grande de tal forma que q no ramifica en K, la curva elíptica E tiene buena reducción en todos los primos de K sobre q y es posible ocupar el teorema de imagen abierta de Serre ([18]):

$$\mathrm{Gal}(K(E[q])/K) \simeq \mathrm{GL}_2(\mathsf{F}_q)$$

donde $E[q]$ son los puntos de q-torsión de E.

Si $M_q = \mathbb{Q}(\sqrt{-q})$ y H_{M_q} su cuerpo de clases de Hilbert, la extensión $H_{M_q}/\mathbb{Q}$ ramifica moderadamente en q y no ramifica en otros primos por lo que $H_{M_q} \subseteq K(E[q])$. Además, podemos escoger q tal que

$$\mathrm{Gal}(H_{M_q}/\mathbb{Q}) \simeq C(\mathcal{O}_{M_q}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

(donde $\mathbb{Z}/2\mathbb{Z}$ actúa invirtiendo elementos) no sea abeliano, para esto basta que $C(\mathcal{O}_{M_q})$ no tenga exponente 2 (ver Lema 4.2 y Lema 4.3).

Es posible incrustar este grupo de Galois como un subgrupo normal de $\mathrm{GL}_2(\mathsf{F}_q)$ que no está contenido en su centro. Al ser $\mathrm{PSL}_2(\mathsf{F}_q)$ un grupo simple, se tiene que $|\mathrm{Gal}(H_{M_q}/\mathbb{Q})| \geq q(q^2-1)$ y por ende

$$|C(\mathcal{O}_{M_q})| \geq \frac{q(q^2-1)}{2}.$$

Siguiendo [13], por la fórmula analítica del número de clases tenemos que

$$|C(\mathcal{O}_{M_q})| = \frac{\omega(M_q)\sqrt{q}}{2\pi} L(1,\chi),$$

donde $\omega(M_q)$ es el número de raíces de la unidad en M_q y χ el caracter asociado a M_q. Sabemos que $\omega(M_q) \leq 6$ y $L(1,\chi) \leq \log(\sqrt{q}) + 1$, como se observa en [13, página 214]. Luego,

$$|C(\mathcal{O}_{M_q})| \leq \frac{3}{\pi}\sqrt{q}(\log(\sqrt{q}) + 1)$$

llegando a una contradicción. □

Agradecimientos

Este trabajo fue principalmente el resultado de mi tesis de Magíster; agradezco al profesor Ricardo Menares quien me enseñó sus ideas y guió durante ese proceso. También agradezco a los evaluadores anónimos por sus valiosos comentarios y correcciones que mejoraron la calidad de este manuscrito.

Referencias

[1] F. Amoroso, S. David, y U. Zannier, "On fields with property (B)," *Proceedings of the American Mathematical Society*, vol. 142, no. 6, pp. 1893–1910, 2014, doi:10.1090/S0002-9939-2014-11925-3.

[2] F. Amoroso y U. Zannier, "A relative Dobrowolski lower bound over abelian extensions," *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze*, vol. 29, no. 3, pp. 711–727, 2000.

[3] E. Bombieri y W. Gubler, *Heights in Diophantine geometry.* Cambridge university press, 2006.

[4] E. Bombieri y U. Zannier, "A note on heights in certain infinite extensions of $\mathbb{Q}$," *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni*, vol. 12, no. 1, pp. 5–14, 2001.

[5] S. Checcoli, "Fields of algebraic numbers with bounded local degrees and their properties," *Transactions of the American Mathematical Society*, vol. 365, no. 4, pp. 2223–2240, 2013, doi:10.1090/S0002-9947-2012-05712-6.

[6] D. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed., ser. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2014.

[7] E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial," *Acta Arithmetica*, vol. 34, no. 4, pp. 391–401, 1979.

[8] A. Galateau, "Small height in fields generated by singular moduli," *Proceedings of the American Mathematical Society*, vol. 144, no. 7, pp. 2771–2786, 2016, doi:10.1090/proc/13058.

[9] P. Habegger, "Small height and infinite nonabelian extensions," *Duke Mathematical Journal*, vol. 162, no. 11, pp. 2027 – 2076, 2013, doi:10.1215/00127094-2331342.

[10] K. Ireland y M. Rosen, *A classical introduction to modern number theory.* Springer New York, NY, 1982, vol. 84 (First edition), doi:10.1007/978-1-4757-1779-2.

[11] G. J. Janusz, *Algebraic number fields.* American Mathematical Society, 1996, vol. 7 (Second edition).

[12] D. H. Lehmer, "Factorization of certain cyclotomic functions," *Annals of Mathematics*, vol. 34, no. 3, pp. 461–479, 1933, doi:10.2307/1968172.

[13] S. Louboutin, "L-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field," *Mathematics of Computation*, vol. 59, no. 199, pp. 213–230, 1992, doi:10.2307/2152992.

[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., ser. Springer Monographs in Mathematics. Springer Berlin, Heidelberg, 2004, doi:10.1007/978-3-662-07001-7.

[15] J. Neukirch, *Algebraic number theory*. Springer Berlin, Heidelberg, 1999, vol. 322.

[16] F. Pappalardi, "On the exponent of the ideal class group of $\mathbb{Q}(\sqrt{-d})$," *Proceedings of the American Mathematical Society*, vol. 123, no. 3, pp. 663–671, 1995, doi:10.2307/2160784.

[17] A. Schinzel, "On the product of the conjugates outside the unit circle of an algebraic number," *Acta Arithmetica*, vol. 24, no. 4, pp. 385–399, 1973.

[18] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," *Inventiones mathematicae*, vol. 15, pp. 259–331, 1971, doi:10.1007/BF01405086.

[19] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed. Springer New York, NY, 2009, doi: 10.1007/978-0-387-09494-6.

[20] C. Smyth, "The Mahler measure of algebraic numbers: a survey," in *Number theory and polynomials. Proceedings of the workshop, Bristol, UK, April 3–7, 2006*. Cambridge: Cambridge University Press, 2008, pp. 322–349, doi: 10.1017/CBO9780511721274.021.