$\mathbb{Q}$-CURVAS Y CARACTERES DE HECKE EN EL MÉTODO MODULAR

LUCAS VILLAGRA TORCOMIAN

Presentado ante la Facultad de Matemática, Astronomía, Física y Computación como parte de los requerimientos para la obtención del grado de Doctor en Matemática de la

UNIVERSIDAD NACIONAL DE CÓRDOBA

22 de febrero de 2023

Director: Dr. ARIEL PACETTI

Tribunal Especial:

Titulares:
Dr. Luis Víctor Dieulefait (UB)
Dr. Juan Pablo Rossetti (UNC)
Dr. Iván Angiono (UNC)

Suplentes:
Dr. Gonzalo Tornaría (Udelar)
Dr. Diego Armando Sulca (UNC)

A mis padres.

Agradecimientos

Son muchas las personas que, por distintos motivos, me gustaría nombrar en esta oportunidad. Es para mí sumamente difícil seleccionar un criterio para escribir los nombres, pero después de meditarlo, decidí quedarme con dos grupos: aquellas personas que tuvieron una incidencia directa en esta tesis, y aquellas que tuvieron una incidencia directa en mí durante el doctorado (o quizá antes) y que por ende se pueden interpretar también como las que afectaron al trabajo indirectamente, a través de mí.

Comenzando con los del primer grupo, me gustaría agradecerles a Iván y Ariel, por las correcciones que me mandaron, que seguramente ayudaron a que mejore la calidad del escrito. Quiero destacar en este punto también a Ale, que sin ningún tipo de obligación (moral ni de ninguna otra índole) leyó la tesis "de pe a pa", marcándome errores en prácticamente todas las páginas.

Muchos de mis amigos surgieron de la FAMAF. De mi último período, quiero rescatar a algunos compañeros de doctorado, que son Vale, Lu y Ale. A ellos les agradezco por escuchar mis quejas sobre la vida matemática infinidad de veces, y por abrirse conmigo para poder compartir distintas visiones y percepciones de la misma. Su amistad fue muy importante para no sentirme solo, especialmente en la última parte de este trayecto.

A Ale le quiero agradecer particularmente por darme la posibilidad de ser por momentos una fuente de inspiración. Lo conocí a los once años, y el hecho de haber sido compañeros desde el entrenamiento para las olimpíadas, hasta ser compañeros de docencia y de oficina me permitió haber vivido de cerca su amor por la matemática, que seguramente algo me habrá contagiado.

A Guille, por tener la condición, peculiar, de hacerme sentir entendido. Por abrirse conmigo a su manera y por mostrarme que puedo contar con él; en particular, por invitarme a comer lasaña cuando lo necesitaba.

A Agus, por ser una amiga especial. Por haberme visto crecer (por momentos más de cerca y otros más de lejos) desde que entré a la facultad. Amén del placer de haber hecho la carrera a su lado (¡hecho que se aprecia y se extraña ahora mucho más!), quiero reconocer lo lindo de poder seguir compartiendo a la distancia, y de saber que siempre está dispuesta a escucharme.

A Estefi en esta oportunidad le agradezco por dos cosas. Primero, simplemente por ayudarme a crecer como persona. Segundo, por su amabilidad y su empatía para acompañarme durante el comienzo de mi doctorado, con todo lo que eso implicó para mí. Imposible saber qué hubiera sido de esta tesis sin ella.

A Joaco y a Pipi, por ser unos lindos amigos. Por ser incondicionales y por compartir conmigo su alegría.

A Romi, por ser mi mayor sostén y por acompañarme durante la escritura de esta tesis prácticamente todo el tiempo, sentada a mi lado. Por ser una de las personas más dulces que conozco y por darme el privilegio de ser su compañero. Sin dudas, su cariño y su apoyo son dos grandes pilares que sostienen esta tesis.

A Ariel, mi padre matemático, por ser el director que siempre quise. Con su pasión me enseñó cómo hacer matemática con diversión y alegría, al mismo tiempo que con seriedad y oficio. Por ser un ejemplo de lo que (no) quiero ser como matemático. Por darme el espacio para generar una intimidad, por jugar al rol de psicólogo en innumerable ocasiones y por transmitirme siempre una

absoluta confianza en mí.

A mi familia, porque sin ellos no estaría escribiendo estas palabras. El apoyo y acompañamiento que siempre recibí desde chico hicieron que pueda embarcar hacia mis objetivos, hasta poder cumplirlos. Quiero destacar a mi papá, por ser mi primer referente académico. Por generar en mí el deseo del conocimiento desde muy pequeño y la admiración por la lógica. Y a mi mamá, claro, por ser un ejemplo de superación diario. Por incentivarme desde chico y mostrarme sus valores, que hoy admiro. Por, además, ser una gran referente académica. Pero, por sobre todo, por ser la persona en este mundo que más amor me ha dado.

Finalmente, agredezco a las siguiente entidades:

A la Universidad Nacional de Córdoba por brindarme el espacio para que continuara formándome como profesional, y más importante aún, como persona, de manera gratuita.

A CONICET por el apoyo económico otorgado durante el doctorado.

Al Club Atlético Belgrano, por ofrecerme durante tantos años el mayor cable a tierra que tengo. Sin este club hermoso la saturación de las responsabilidades me ganaría. En especial, quiero agradecer al plantel del 2022, por brindarme un año fantástico; la felicidad que me aportaron fue fundamental para poder seguir trabajando. Nombrar a todos en este momentoresultaría tedioso, pero sí me gustaría destacar a Guillermo.

Estas páginas, en las que voy haciendo anotaciones
con una claridad que para ellas perdura,
las acabo de releer y me interrogo.
¿Qué es esto, para qué todo esto? [...]
Releo, sí, estas páginas que representan horas pobres,
pequeños sosiegos o ilusiones,
grandes esperanzas desviadas hacia el paisaje,
penas como cuartos donde no se entra,
ciertas voces,
un gran cansancio,
el evangelio por escribir.
Cada uno tiene su vanidad,
y la vanidad de cada uno
es su olvido de que hay otros con un alma igual.
Mi vanidad son algunas páginas,
unos fragmentos,
ciertas dudas...

F. Pessoa, Libro del desasosiego.

Resumen

Esta tesis tiene como foco de estudio la resolución de cierto tipo de ecuaciones diofánticas, conocidas como "Ecuaciones de Fermat Generalizadas".

Recordemos que el Último Teorema de Fermat (UTF) establece que las únicas soluciones enteras de la ecuación $x^n + y^n = z^n$ con $n \geq 3$ son aquellas que satisfacen que $xyz = 0$. La demostración de dicha afirmación fue finalmente probada por Andrew Wiles. Desde entonces, hubo un incremento en el interés del estudio de las Ecuaciones de Fermat Generalizadas, o ecuaciones de tipo Fermat, que son aquellas de la forma $Ax^q + By^r = Cz^p$.

En este trabajo estudiaremos las soluciones primitivas de las ecuaciones $x^4 - dy^2 = z^p$ y $x^2 - dy^6 = z^p$, donde d es un número entero y p es un número primo. Dichas ecuaciones han sido estudiadas y completamente resueltas para unos pocos valores particulares de d, pero en esta oportunidad daremos una receta para estudiar las ecuaciones para un valor de d arbitrario.

La estrategia que utilizaremos para lograr nuestro objetivo será la misma que la utilizada para el UTF, usualmente denominada como el método modular. En ella, se involucran diversos objetos, como las curvas elípticas, las representaciones de Galois y las formas modulares. Gran parte de la complejidad del estudio de las ecuaciones mencionadas, es que las curvas elípticas naturalmente asociadas a sus soluciones no están definidas sobre cuerpos totalmente reales cuando d no es un cuadrado perfecto y es un entero negativo, sino que están definidas sobre $\mathbb{Q}(\sqrt{d})$, y por lo tanto no existen resultados de modularidad para tales curvas. Entonces, la estrategia consiste en explotar el hecho de que las curvas elípticas resultarán ser $\mathbb{Q}$-curvas. Gran parte de la novedad del trabajo consiste en definir explícitamente un caracter de Hecke χ por el cual se pueda twistear la representación de Galois asociada a una $\mathbb{Q}$-curva definida sobre $\mathbb{Q}(\sqrt{d})$ de manera que la representación de Galois twisteada por χ se extienda al grupo de Galois absoluto de $\mathbb{Q}$. Entonces, conociendo explícitamente el twist y usando las conjeturas de Serre (ya demostradas) podremos garantizar (basándonos en resultados de imagen grande de Ellenberg y de bajada de nivel de Ribet) la existencia de formas modulares concretas que son calculables. Luego profundizamos en distintos tipos de herramientas que permiten analizar las formas modulares obtenidas, de manera tal de probar la no existencia de soluciones primitivas no triviales de nuestras ecuaciones, al menos para valores de p suficientemente grandes.

Palabras clave: Ecuaciones de Fermat Generalizadas, método modular, $\mathbb{Q}$-curvas, caracteres de Hecke, formas modulares, representaciones de Galois.

2020 Mathematics subject classification: 11D41, 11F80.

Abstract

This thesis focuses on the resolution of a certain type of Diophantine equations, known as "Generalized Fermat Equations".

Recall that Fermat's Last Theorem (FLT) states that the only integer solutions of the equation $x^n + y^n = z^n$ with $n \geq 3$ are those that satisfy $xyz = 0$. That statement was finally proved by Andrew Wiles. Since then, there has been an increased interest in the study of Generalized Fermat Equations, or Fermat-type equations, which are those of the form $Ax^q + By^r = Cz^p$.

In this work we will study the primitive solutions of the equations $x^4 - dy^2 = z^p$ and $x^2 - dy^6 = z^p$, where d is an integer and p is a prime number. These equations have been studied and completely solved for a few particular values of d, but in this opportunity we will give a recipe to study the equations for an arbitrary value of d.

The strategy we will use to achieve our goal will be the same as the one used for FLT, commonly known as the modular method. Several objects are involved, such as elliptic curves, Galois representations and modular forms. The complexity of studying the mentioned equations lies in the fact that the elliptic curves naturally associated with their solutions are not defined over totally real fields when d is not a perfect square and is a negative integer. Instead, they are defined over $\mathbb{Q}(\sqrt{d})$, so in particular there are no modularity results for such curves. Therefore, the strategy focus on the fact that the elliptic curves will turn out to be $\mathbb{Q}$-curves. A significant novelty of this work consists in explicitly defining a Hecke character χ by which we can twist the Galois representation associated to a $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{d})$ such that the twisted Galois representation by χ extends to the absolute Galois group of $\mathbb{Q}$. Then, explicitly knowing the twist and using Serre's conjectures (already proven) we can guarantee (based on large image results due to Ellenberg's and Ribet's level lowering theorem) the existence of modular forms that are computable. We then delve into different types of tools that allow us to analyze the obtained modular forms, in order to prove the non-existence of non-trivial primitive solutions of our equations, at least for sufficiently large values of p.

Key words: Generalized Fermat Equations, modular method, $\mathbb{Q}$-curves, Hecke characters, modular forms, Galois representations.

2020 Mathematics subject classification: 11D41, 11F80.

Índice

Notación

- $\overline{\mathbb{Q}}$, $\overline{\mathbb{Q}}_p$: fijamos clausuras algebraicas para $\mathbb{Q}$ y $\mathbb{Q}_p$, para todo primo p, junto con sus inyecciones en $\mathbb{C}$.
- $\mathbb{F}_{p^r}$: el único cuerpo finito (salvo isomorfismo) de p^r elementos.
- $\overline{\mathbb{F}}_p$: una clausura algebraica fija de $\mathbb{F}_p$.
- K : en general denotará un cuerpo, y más aún un cuerpo de números (una extensión finita de $\mathbb{Q}$) a partir del Capítulo 2. En este caso, fijamos una inyección en $\overline{\mathbb{Q}}$.
- $\mathbb{I}_K$: el anillo de los idèles de K.
- $\mathrm{Cl}(K)$: el grupo de clases de K.
- G_K : el grupo de Galois absoluto de K, $\mathrm{Gal}(\overline{K}/K)$. Cuando K sea un cuerpo de números escribiremos $\overline{\mathbb{Q}}$ en vez de $\overline{K}$.
- $\mathscr{O}_K$: el anillo de enteros de K.
- $\mathfrak{p}$, $\mathfrak{p}_q$: ideales primos de $\mathscr{O}_K$ sobre p y q, respectivamente. También utilizamos la notación $\mathfrak{p} \mid p$.
- $K_\mathfrak{p}$: la completación de K en $\mathfrak{p}$.
- χ_K : cuando K es cuerpo de números, el caracter asociado a la extensión $K/\mathbb{Q}$.
- $v_\mathfrak{p}$: la valuación $\mathfrak{p}$-ádica normalizada en $K_\mathfrak{p}$
- E/K : curva elíptica definida sobre K. Muchas veces omitiremos la notación del cuerpo si se sobreentiende.
- $E(L)$: puntos de una curva elíptica E que estén en L.
- $E[m]$: puntos de m-torsión de E.
- $\Delta, \Delta(E)$: discriminante de una curva elíptica.
- $N(E)$: conductor de una curva E. A veces podemos denotarlo simplemente como N.
- $\mathbb{Z}/m$: el anillo de los enteros cocientado por el subgrupo $m\mathbb{Z}$.
- $\mathrm{rad}(n)$: el producto de todos los primos que dividen a n.
- $\mathscr{N}$: la función norma (de los espacios correspondientes).
- ψ_d : caracter cuadrático asociado a la extensión $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.
- χ_{cyc}, χ_p: caracter ciclotómico de módulo p.

Introducción

Breve contexto histórico

Las ecuaciones diofánticas son ecuaciones polinomiales, usualmente definidas con coeficientes enteros. Su nombre se deriva de *Dióphantos*, un matemático griego nacido en Alejandría. Dióphantos, cuyo nacimiento se estima en algún momento entre los años 200 y 214, es considerado para muchos como el "padre del álgebra", por ser uno de los primeros en introducir un simbolismo y operar sin ninguna representación geométrica. Su renombre se debe principalmente por ser el autor de una serie de libros llamada *Arithmetica*.

Junto con Dióphantos, demás matemáticos babilonios, chinos, egipcios y griegos se concentraron en estudiar las soluciones enteras o racionales de algunas ecuaciones diofánticas, dando así origen a una de las ramas más antiguas de la matemática, ubicada dentro de la teoría de números. Probablemente una de las características más atractivas de esta rama es que usualmente los enunciados son fáciles de comprender, y sin embargo pueden resultar muy complejos de resolver. A menudo ocurre que, con la intención de resolver un problema en particular, los matemáticos desarrollan nuevas técnicas y teorías que dan lugar a nuevos campos de estudio.

Pierre de Fermat (1601–1665) fue abogado y matemático francés que estudió de una de las copias al latín de Arithmetica. Se caracterizó por realizar distintas observaciones y afirmaciones en los márgenes de estos libros, aunque muchas de ellas sin ofrecer demostración alguna. Leonhard Euler (1707–1783) fue un matemático suizo, considerado como uno de los más importantes de la historia, que con el tiempo se interesó en las conjeturas propuestas por Fermat y probó muchas de ellas. En particular, Euler no pudo dar con la solución de lo que hoy se conoce como "El Último Teorema de Fermat". Según la historia lo marca, su nombre se debe en parte por ser uno de los últimos resultados de Fermat en ser probado o refutado, y llevó el nombre de "Teorema" porque Fermat afirmó tener una prueba para el mismo, sólo que a ésta, como era usual en él, nunca la escribió. Enunciaremos y discutiremos con más profundidad del teorema en la Sección 1.6, pero parece oportuno finalizar diciendo que el Último Teorema de Fermat fue completamente resuelto en 1995 (ver [80, 87]) y su demostración se le atribuye a Andrew Wiles.

Estado del arte

La prueba de Wiles del Último Teorema de Fermat, generó un fuerte impacto en el estudio de las ecuaciones diofánticas. Se comenzó a prestar un interés especial a las llamadas Ecuaciones de Fermat Generalizadas, que son aquellas de la forma

$$Ax^q + By^r = Cz^p, \tag{1.8}$$

donde A, B y C son enteros no nulos fijos coprimos entre sí. En general, hallar todas las soluciones de una ecuación diofántica puede resultar un problema extremadamente difícil, ya que no existe un algoritmo que lo lleve a cabo. Por otro lado, la estrategia utilizada por Wiles en su prueba del

Último Teorema de Fermat, conocida como el *método modular*, se puede aplicar a otras ecuaciones diofánticas para probar la no existencia de (cierto tipo de) soluciones.

Decimos que una solución $(a, b, c) \in \mathbb{Z}^3$ de (1.8) es *primitiva* si $\text{mcd}(a, b, c) = 1$ y decimos que es *trivial* si $abc = 0$. En [31], Darmon y Granville prueban que para cada tripla (q, r, p) tal que $1/q + 1/r + 1/p < 1$, la ecuación (1.8) tiene finitas soluciones primitivas. Cuando (q, r, p) no está fija, la finitud de soluciones primitivas resulta una consecuencia de la conjetura ABC (ver la Sección 5.4 de [31] y sus referencias). Luego, se espera que valga la siguiente conjetura.

Conjetura 1. Sean A, B, C enteros no nulos coprimos entre sí fijos. Entonces existe sólo una cantidad finita de triplas (a^q, b^r, c^p) con $(a, b, c) \in \mathbb{Z}^3$, $abc \neq 0$ y p, q, r primos tales que:

- $1/q + 1/r + 1/p < 1$,
- $\text{mcd}(a, b, c) = 1$,
- $Aa^q + Bb^r = Cc^p$.

El método modular, es una especie de "guía" que se puede utilizar para estudiar las soluciones de algunas Ecuaciones de Fermat Generalizadas. Una condición necesaria para aplicar el método modular pareciera ser que el conjunto de exponentes $\{q, r, p\}$ tenga sólo un elemento que varíe, mientras que el resto esté fijo. Una versión simplificada del procedimiento (más detalles serán dados en la Subsección 1.7.1) es la siguiente: digamos que p es el exponente que permitimos que recorra distintos valores libremente. Primero, a partir de una solución primitiva de la ecuación, uno debe definir una curva elíptica E con propiedades muy especiales, como por ejemplo que su discriminante sea "casi" una potencia p-ésima. Luego, al analizar la representación de Galois módulo p asociada a E (ver Subsección 1.2.1) se debe probar la modularidad de dicha representación, es decir, mostrar que tal representación coincide con la de una forma modular nueva con nivel y Nebentypus "conocidos" e independientes de la solución con la que comenzamos (en general esto último se logra con los resultados de baja de nivel de Ribet; ver Sección 1.5). Por último, uno calcula los espacios particulares de formas modulares y utiliza diferentes técnicas de eliminación (como en las que profundizaremos en la Sección 2.4.1), apuntando a probar que ("casi") ninguna de las formas nuevas de dicho espacio está relacionada con soluciones primitivas de la ecuación; por ende tales soluciones no pueden existir.

Nuestro aporte

Esta tesis doctoral tuvo su origen al intentar estudiar casos particulares de la ecuación (1.8). Nos centramos en dos tipos distintos de familias de ecuaciones, a saber la ecuación

$$x^4 - dy^2 = z^p, \tag{1}$$

y la ecuación

$$x^2 - dy^6 = z^p, \tag{2}$$

para valores enteros de d libres de cuadrados y donde p es un número primo. Más adelante veremos por qué es suficiente con asumir dichas hipótesis sobre d (ver Observaciones 17 y 32) y sobre p (ver Observación 6).

La primera ecuación fue estudiada en [38] para $d = -1$ y en [37] para $d = -2, -3$. Los artículos [38] y [37] probaron lo que se considera un "resultado asintótico", es decir que prueba la existencia de una constante N_d tal que todas las soluciones primitivas no triviales de la ecuación (1) tienen exponente $p \leq N_d$. Explícitamente, las constantes son $N_d = 211, 349, 131$ para $d = -1, -2, -3$ respectivamente. La mayor contribución de [4] fue extender el resultado para valores pequeños de

p, probando la no existencia de soluciones primitivas no triviales para exponentes $n \geq 4$ (no necesariamente primo) cuando $d = -1$ y la existencia de una única solución primitiva no trivial para exponentes $n \geq 4$ cuando $d = -2$.

La ecuación (2) fue estudiada en [3] para $d = -1$ y en [51] para $d = -3$, donde la no existencia de soluciones primitivas no triviales fue probada para todos los exponentes $n \geq 3$ cuando $d = -1$, mientras que existe una única solución primitiva no trivial para exponentes $n \geq 4$ cuando $d = -3$. La conexión crucial entre las ecuaciones (1) y (2) es que en ambos casos, a una hipotética solución primitiva no trivial (a, b, c) uno puede asociarle una curva elíptica sobre la extensión cuadrática $K = \mathbb{Q}(\sqrt{d})$, completando así el primer paso de la estrategia general descripta anteriormente. Dicha curva tiene la propiedad de ser una $\mathbb{Q}$-curva (i.e. una curva elíptica isógena a todos sus conjugados de Galois; ver Definición 1.1.7). En el caso de la ecuación (1), la curva elíptica fue propuesta en [37], y está dada por la ecuación

$$E_{(a,b,c)} : y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{-d}b)x. \tag{3}$$

En el caso de la ecuación (2), en [3] y en [51] los autores le adjuntan a una solución (a, b, c) una $\mathbb{Q}$-curva con un punto de 3-torsión. Generalizando sus ideas (y utilizando la descripción de curvas elípticas con un punto de 3-torsión dada por Kubert [54]), definimos a partir de una solución (a, b, c) de (2) la $\mathbb{Q}$-curva

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3, \tag{4}$$

donde $(0, 0)$ es un punto racional de orden 3. Parte de nuestra contribución al estudio de (2) reside en el hecho de que tal curva elíptica cumple con los requerimientos de la estrategia general (como lo veremos en la Sección 4).

Una propiedad clave de las $\mathbb{Q}$-curvas es que sus representaciones de Galois se pueden "extender" a todo el grupo de Galois, probando así el segundo paso de la estrategia mencionada. Más concretamente, un resultado de Ribet (Teorema 1.5.9) implica que si E/K es una $\mathbb{Q}$-curva entonces existe un caracter χ tal que la representación de Galois twisteada $\rho_{E,p} \otimes \chi$ se extiende al grupo de Galois absoluto $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (aquí $\rho_{E,p}$ denota la representación de Galois de la curva E inducida al mirar la acción del grupo de Galois en el módulo de Tate $T_p(E)$; ver Sección 1.2.1). El resultado de Ribet no es explícito, pues depende de trivializar un cociclo naturalmente asociado a la $\mathbb{Q}$-curva E. En los artículos anteriormente mencionados, la manera en la que el cociclo fue trivializado fue utilizando un algoritmo de Quer [68] que encuentra un elemento ad-hoc (vía el Teorema 90 de Hilbert) luego de una búsqueda tediosa. La desventaja de tal dirección es que a priori no hay ningún control de la ramificación del caracter ni una descripción clara del caracter en sí.

Una de las mayores contribuciones del presente trabajo es proveer una alternativa al aporte de Ribet. A saber, damos una descripción explícita de un caracter de Hecke χ tal que las representaciones de Galois $\rho_{E_{(a,b,c)},p} \otimes \chi$ se extienden a todo el grupo de Galois $G_{\mathbb{Q}}$ (y su respectivo resultado para la representación $\rho_{\widetilde{E}_{(a,b,c)},p}$). Para explicar nuestro aporte, introduciremos a continuación un poco de notación que utilizaremos (y recordaremos) a lo largo del trabajo.

Si t es un entero, denotemos por ψ_t al caracter cuadrático correspondiente a la extensión $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$ vía teoría de cuerpos de clases. Dada $L/\mathbb{Q}$ una extensión de Galois, denotamos por $G_L := \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ al grupo de Galois absoluto de L. Sea $\rho : G_L \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ una representación de Galois y sea $\tau \in G_{\mathbb{Q}}$. Denotamos por ${}^{\tau}\rho$ a la representación de Galois de G_L dada por ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$.

Una propiedad muy importante que satisface la curva $E_{(a,b,c)}$ es que si τ denota cualquier elemento de $G_{\mathbb{Q}}$ no trivial en K, entonces ${}^{\tau}\rho_{E_{(a,b,c)},p} \sim \rho_{E,p} \otimes \psi_{-2}$ (ver Proposición 3.1.1). Análogamente, bajo ciertas hipótesis, ${}^{\tau}\rho_{\widetilde{E}_{(a,b,c)},p} \sim \rho_{\widetilde{E}_{(a,b,c)},p} \otimes \psi_{-3}$ (ver Proposición 4.1.1). Recordar que una representación de G_K se extiende a $G_{\mathbb{Q}}$ si y sólo si ${}^{\tau}\rho \sim \rho$, para τ como antes. Aunque éste es un resultado bien sabido por los expertos, daremos una prueba de este hecho en los Teoremas 3.2.9 y 4.2.4, ya que necesitamos tener control del conductor de la representación. Notar que si construimos

un caracter de Hecke de orden finito $\chi_t : G_K \to \overline{\mathbb{Q}}^\times$ satisfaciendo

$$^\tau\chi_t = \chi_t \cdot \psi_{-t},$$

para $t = 2, 3$, entonces la representación twisteada $\rho_{E_{(a,b,c)},p} \otimes \chi_2$ (respectivamente $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3$) se extiende a $G_{\mathbb{Q}}$. Una de las mayores contribuciones de este trabajo es dar una estrategia general para la construcción del caracter de Hecke χ_t (ver Sección 1.7.1). Más precisamente, damos una construcción explícita de tal caracter para los casos $t = 2$ y t un primo congruente a 3 módulo 4. Este resultado tiene interés en sí mismo, ya que podría ser aplicado para otros problemas diofánticos que involucren $\mathbb{Q}$-curvas.

Por construcción, el caracter de Hecke χ_t ramifica sólo en primos que ramifican en $K/\mathbb{Q}$ y en los que dividen a $2t$. Retomando al problema de extender las representaciones $\rho_{E_{(a,b,c)},p}$ y $\rho_{\widetilde{E}_{(a,b,c)},p}$, este hecho permite probar que la reducción de la representación extendida tiene conductor divisible sólo por primos que dividen a $6d$. En particular, construimos una representación (cuya modularidad se sigue de las conjeturas de Serre; ver Teorema 1.5.3) con conductor "pequeño", completando los primeros pasos de la estrategia. Más aún, en los Corolarios 3.3.1 y 4.3.1 exponemos una descripción explícita del conductor y el Nebentypus de tales representaciones residuales.

Para aplicar los últimos pasos del método, se precisa un resultado sobre la imagen de la representación de Galois residual (para luego aplicar los resultados de bajada de nivel de Ribet) y un procedimiento para la eliminación de formas modulares. Para nuestros propósitos, los principales resultados acerca de imágenes de representaciones de Galois residuales asociadas a $\mathbb{Q}$-curvas están dados por Ellenberg (Proposiciones 2.4.6 y 2.4.7). Para el caso en que el cuerpo es cuadrático imaginario ($d < 0$), el Teorema 2.4.8 establece que si E es una $\mathbb{Q}$-curva sobre un cuerpo cuadrático imaginario K de manera que existe un primo $\mathfrak{q} \nmid 6$ en donde E tiene reducción multiplicativa, entonces para todo primo p suficientemente grande (digamos $p > N_K$), la imagen residual es "grande" (i.e. su imagen proyectiva es todo $\mathrm{PGL}_2(\mathbb{F}_p)$). Más aún, el artículo de Ellenberg contiene cotas que permiten calcular explícitamente la constante N_K, que depende sólo del cuerpo base K y (a priori) del grado de la $\mathbb{Q}$-curva. Incluimos algunas mejoras que se encuentran en la literatura sobre el resultado original de Ellenberg, y escribimos un código en `PARI/GP` para calcular las cotas necesarias en cada uno de los ejemplos. Además, probamos cómo el Teorema 2.4.8 puede ser "adaptado" (bajo ciertas hipótesis) a cuerpos cuadráticos reales.

Finalmente, además de explicar cómo los resultados de Ellenberg permiten eliminar formas con multiplicación compleja, veremos distintas herramientas para descartar formas que no provienen de soluciones de las ecuaciones (1) y (2) (para p suficientemente grade). Todos los resultados finales sobre las ecuaciones (1) y (2) son de la siguiente forma:

La ecuación (1) (respectivamente (2)) para $d = (\dagger)$ no tiene ninguna solución primitiva no trivial si p satisface la condición $(\star)$.

La Tabla 3.4.1 (respectivamente 4.4.1) resume para cada valor de $(\dagger)$ la condición $(\star)$. La elección de los valores de $(\dagger)$ es arbitraria, ya que en principio nuestro método podría aplicar a cualquier valor de $(\dagger)$, teniendo en cuenta las limitaciones computacionales de los algoritmos utilizados para construir los espacios de formas modulares.

Cada capítulo o sección, referenciará con precisión los artículos en los cuales está basado, pero parece oportuno aclarar que todo este trabajo se desprende de la serie de artículos [64, 65], en colaboración con Ariel Pacetti, y de [46], junto con Franco Golfieri y Ariel Pacetti. A su vez, una continuación natural de los mencionados trabajos se puede encontrar en [82] y en [47]. En [82] el autor de esta tesis profundiza en el estudio de las soluciones primitivas de la ecuación (1) pero en esta ocasión sobre cuerpos de números distintos de $\mathbb{Q}$. En [47], junto con Franco Golfieri y Ariel Pacetti se obtienen resultados asintóticos para (1) y (2) para infinitos valores de d.

Los cálculos computacionales del presente trabajo fueron realizados utilizando `PARI/GP` [67], `Magma` [7] y `Sage` [81]. Tanto los códigos utilizados como los resultados obtenidos de los mismos se encuentran disponibles en [83].

Contenidos

Este trabajo está organizado de la siguiente forma: en el Capítulo 1 están contenidos todos los preliminares necesarios. En él se encuentran las nociones básicas para los demás capítulos. Éstas incluyen los conceptos de curvas elípticas, $\mathbb{Q}$-curvas, representaciones de Galois, caracteres de Hecke, formas modulares y resultados clásicos, como por ejemplo el de modularidad y de bajada de nivel. Al final de este capítulo se reúnen todos los ingredientes para dar con la prueba del Último Teorema de Fermat, con la intención de reforzar la idea del esquema de su demostración. En esa dirección, se concluye con las Ecuaciones de Fermat Generalizadas y con una descripción más abstracta acerca del método modular.

El Capítulo 2 tiene como objetivo exponer la estrategia que utilizaremos para resolver las ecuaciones (1) y (2), la cual, basada en el método modular, consta de cuatro pasos. Por ende, este capítulo posee cuatro secciones, cada una destinada a mostrar con generalidad los resultados y las herramientas que se utilizarán para atacar cada una de las ecuaciones. En la Sección 1.7.1 simplemente se exponen algunas propiedades básicas de las soluciones de las ecuaciones y de sus curvas asociadas. En la Sección 1.7.1 se muestra la filosofía general que se seguirá para definir el caracter de Hecke por el cual se deberá twistear, y luego cómo se deriva de ello la extensión de la representación y la modularidad. En la Sección 2.4 se analizan los distintos métodos para descartar formas modulares, tanto para el caso de un cuerpo cuadrático real como imaginario. En particular, en la Subsección 2.4.5 se analizan en detalles los resultados de Ellenberg y se trabaja en cómo extenderlos y/o complementarlos.

El Capítulo 3 está completamente destinado a la resolución de la ecuación (1). En él veremos cómo proceder con cada uno de los cuatro pasos establecidos en el Capítulo 2. Al final, en la Sección 3.2.2 se encuentra la Tabla 3.4.1 con los valores de d con los que se trabajó, junto con el enunciado y demostración de cada uno de éstos.

Finalmente, el Capítulo 4 está dirigido al estudio de la ecuación (2). En la Sección 4.3.1 también se puede encontrar la Tabla 4.4.1 con los valores d que fueron estudiados.

Un resumen más detallado de lo que se realiza en cada uno de los últimos tres capítulos se puede encontrar al comienzo de los mismos.

Capítulo 1

Preliminares

Let us assume we know nothing,
which is a reasonable approximation.

D. Kazhdan.

1.1 Curvas elípticas

Las curvas elípticas son un objeto de amplio interés en la teoría de números, como también en otras ramas de la matemática. Se pueden estudiar desde distintos puntos de vista, y hay basta bibliografía para consultar. Las principales referencias que tendremos en cuenta son [78] y [77].

La forma más sencilla de dar su definición es decir que llamaremos por *curva elíptica* a una curva algebraica proyectiva de género 1, con un punto marcado. Si bien es una manera rápida de definir curva elíptica, no es quizá muy concreta para nuestros propósitos. Por eso, cabe destacar que en general, toda curva elíptica sobre un cuerpo K se puede describir como una curva algebraica plana no singular de la forma

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

donde $a_i \in K$. La ecuación de la cúbica E es lo que denominamos como *ecuación de Weierstrass*. En caso de que E sea no singular (y por lo tanto una curva elíptica) es común considerar como "punto marcado" al punto del infinito $O = [0, 1, 0]$ que obtenemos al proyectivizar la curva con una variable z. Algunos de los invariantes más importantes de las curvas elípticas son los siguientes:

$$\begin{aligned}
&b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6\\
&b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
&c_4 = b_2^2 - 24b_4,\\
&c_6 = -b_3^2 + 36b_2b_4 - 216b_6,\\
&\Delta = -b_2^2b_8 - 8b_3^4 - 27b_2^6 + 9b_2b_4b_6,\\
&j = c_4^3/\Delta.
\end{aligned}$$

Diremos que Δ es el *discriminante* de E y que j es su *j-invariante*. No hemos dicho aún el significado de que una cúbica como E sea no singular. Una curva en general es no singular si no posee singularidades. No nos detendremos a definir qué es punto singular, debido a que en esta oportunidad esta información se puede leer fácilmente del discriminante de la curva. Más concretamente, E es no singular si y sólo si $\Delta \neq 0$. La información que provee el j-invariante de la curva está íntimamente relacionada con la siguiente pregunta:

¿Es única la ecuación de Weierstrass para una curva elíptica dada?

Suponiendo que la recta en el infinito, es decir la recta $z = 0$ en $\mathbb{P}^2$, debe intersecar a E únicamente en O, entonces el único cambio de variables que fija a O y preserva la forma de Weierstrass de la ecuación es de la forma

$$x = u^2x' + r \quad \text{y} \quad y = u^3y' + u^2sx' + t, \tag{1.2}$$

donde $u, r, s, t \in \overline{K}$ y $u \neq 0$ (ver [78, III.3.1b]). Diremos que dos ecuaciones de Weierstrass definidas sobre K son *isomorfas* sobre un cuerpo $L \supseteq K$ si difieren de un cambio de de variables como en (1.2), donde $u, r, s, t \in L$.

Lema 1.1.1. *Sean E y E' dos curvas elípticas sobre K dadas en su ecuación de Weierstrass, con j-invariantes j y j' respectivamente. Entonces E y E' son isomorfas sobre $\overline{K}$ si y sólo si $j = j'$.*

De ahora en adelante, cuando hablemos de curvas elípticas, asumiremos que están dadas en su forma de Weiestrass. El Lema 1.1.1 nos dice que el j-invariante de una curva elíptica no se modifica al hacer un cambio de variables como en (1.2). Veamos cómo afecta esto al discriminante de la curva.

Lema 1.1.2. *Sea E una curva elíptica con discriminante Δ. Sea E' la curva elíptica obtenida por el cambio de variables en (1.2) y sea Δ' su discriminante. Entonces $\Delta' = \Delta u^{-12}$.*

Sea K un cuerpo de números y sea $\mathscr{O}_K$ su anillo de enteros. Si E es una curva elíptica sobre K (E/K de ahora en adelante) entonces existe un cambio de variables como en (1.2) tal que los coeficientes a_i de la ecuación isomorfa resultan estar todos en $\mathscr{O}_K$. Dado un primo $\mathfrak{p}$ en $\mathscr{O}_K$, diremos que E tiene un *modelo minimal respecto de* $\mathfrak{p}$ si existe un modelo de E que cumple que la valuación de su discriminante en el primo $\mathfrak{p}$ es menor o igual a la valuación del discriminante de cualquier curva isomorfa. Más aún, diremos que E/K tiene un *modelo minimal* si E tiene un modelo minimal respecto de todo ideal primo $\mathfrak{p}$. Si K tiene número de clases 1, entonces toda curva elíptica E/K tiene un modelo minimal, que lo denotaremos por Δ_{min}. En el caso en que el número de clases de K no sea trivial, no necesariamente existe un modelo minimal, pero fijado un ideal primo $\mathfrak{p}$ en $\mathscr{O}_K$ sí existe un modelo minimal con respecto a $\mathfrak{p}$. Dicho modelo es único salvo unidades.

Sea K un cuerpo de números y sea E/K una curva elíptica tal que sus coeficientes están en el anillo de enteros $\mathscr{O}_K$. Si $\mathfrak{p}$ es un ideal primo en $\mathscr{O}_K$, entonces podemos reducir los coeficientes de la curva módulo $\mathfrak{p}$. La ecuación ahora define una curva sobre un cuerpo finito $\mathbb{F}_{p^r}$, donde p es el único primo racional que pertenece a $\mathfrak{p}$. Cabe preguntarse si la curva reducida es singular o no, lo cual es equivalente a que la reducción de su discriminante minimal módulo $\mathfrak{p}$ sea trivial o no.

Definición 1.1.3. Sea E una curva elíptica sobre un cuerpo de números K, sea $\mathfrak{p}$ un ideal primo de $\mathscr{O}_K$ y sea Δ_{min} el discriminante de un modelo minimal de E en $\mathfrak{p}$. Entonces decimos que E tiene

- *Buena reducción* en $\mathfrak{p}$ si $\mathfrak{p} \nmid \Delta_{\text{min}}$ y *mala reducción* en $\mathfrak{p}$ si $\mathfrak{p} \mid \Delta_{\text{min}}$.
- *Reducción multiplicativa* en $\mathfrak{p}$ si la reducción es mala y además $\mathfrak{p} \nmid c_4$.
- *Reducción aditiva* en $\mathfrak{p}$ si la reducción es mala y además $\mathfrak{p} \mid c_4$.

Aquí, c_4 hace referencia al invariante del modelo minimal de E en $\mathfrak{p}$.

Si $\mathfrak{p}$ es un primo de buena reducción para E/K, denotamos por $\tilde{E}$ a la reducción de la curva módulo $\mathfrak{p}$. Sea p^r el número de elementos del cuerpo residual de K en $\mathfrak{p}$. Definimos entonces

$$a_{\mathfrak{p}}(E) := p^r + 1 - \#\tilde{E}(\mathbb{F}_{p^r}). \tag{1.3}$$

Proposición 1.1.4 (Hasse). *Si E es una curva elíptica sobre un cuerpo de números K y $\mathfrak{p}$ es un primo de buena reducción entonces $|a_{\mathfrak{p}}(E)| \leq 2\sqrt{\mathcal{N}(\mathfrak{p})}$, donde $\mathcal{N}$ es la función norma.*

Sea E/K una curva elíptica y $\mathfrak{p}$ un primo en $\mathscr{O}_K$. Sabemos que los primos que tienen mala reducción son aquellos que dividen a Δ_{min}, donde Δ_{min} es el discriminante de un modelo minimal de E en $\mathfrak{p}$. Existe otro elemento asociado a la curva E que encubre sus primos de mala reducción. Lo llamaremos el *conductor* de la curva, y lo denotaremos por N. El conductor de E está dado por la siguiente fórmula:

$$N = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}},$$

donde el producto corre sobre los ideales primos $\mathfrak{p}$ de $\mathscr{O}_K$ y $f_{\mathfrak{p}}$ está definido de la siguiente forma:

$$f_{\mathfrak{p}} = \begin{cases} 0 & \text{si } E \text{ tiene buena reducción en } \mathfrak{p}, \\ 1 & \text{si } E \text{ tiene reducción multiplicativa en } \mathfrak{p}, \\ 2+\delta_{\mathfrak{p}} & \text{si } E \text{ tiene reducción aditiva en } \mathfrak{p}. \end{cases}$$

Más aún, $\delta_{\mathfrak{p}} = 0$ si $\mathfrak{p} \nmid 2, 3$. Para los primos $\mathfrak{p}$ arriba de 2 y 3 la fórmula es más compleja, pero no será necesaria por el momento (los interesados pueden ver [77, IV §10]). Cabe aclarar que $\delta_{\mathfrak{p}}$ está acotado por un número que sólo depende del cuerpo K y de $\mathfrak{p}$. Decimos que E es *semiestable* si $f_{\mathfrak{p}} \leq 1$ para todo $\mathfrak{p}$.

Dada una curva elíptica E/K, lo más natural que uno querría entender es el conjunto de puntos de la curva sobre K, o sobre alguna otra extensión de K. Denotaremos por $E(L)$ al conjunto de puntos de E sobre el cuerpo $L \supseteq K$. Recordemos que una curva elíptica en particular es una curva proyectiva, que puede ser vista con un modelo afín como el de (1.1) junto con un punto O en el infinito. La ventaja de trabajar con el plano proyectivo es que en él, toda recta corta a una curva elíptica E en tres puntos (contados con multiplicidad). Luego, a partir de dos puntos $P, Q \in E(L)$, podemos construir un tercero en $E(L)$, que denotaremos por $P * Q$, tomando como $P * Q$ el tercer punto de intersección entre E y la recta proyectiva que une a P y Q. Hemos definido entonces una operación en $E(L)$, de la que a partir de dos puntos podemos generar otro. Sin embargo, dicha operación no define en $E(L)$ una estructura de grupo. Pero, si ahora denotamos por $P + Q$ al tercer punto en $E(L)$ que resulta de la intersección entre E y la recta que une $P * Q$ con O, obtenemos una nueva operación $(P, Q) \mapsto P + Q$ que sí define una estructura de grupo, en la que es fácil ver que O es el elemento neutro. También es inmediato ver que dicha operación es conmutativa (es decir que $E(L)$ tiene estructura de grupo abeliano). Lo realmente complicado es ver que dicha operación es asociativa. De ahora en adelante, cuando hablemos de $E(L)$ como un grupo, ésta es la única operación que consideraremos. Uno de los resultados más importantes sobre la estructura del grupo $E(L)$ es el siguiente.

Teorema 1.1.5 (Mordell-Weil). *Sea E una curva elíptica sobre un cuerpo de números K. Entonces $E(K)$ tiene estructura de grupo abeliano finitamente generado.*

Si E/K es una curva elíptica entonces lo usual es que $\text{End}_{\overline{K}}(E) \simeq \mathbb{Z}$. Los casos especiales son aquellos en donde $\mathbb{Z}$ está estrictamente metido en $\text{End}_{\overline{K}}(E)$. En esos casos $\text{End}_{\overline{K}}(E)$ es isomorfo a un orden $\mathscr{O}$ de un cuerpo cuadrático imaginario L. Bajo esas circunstancias diremos entonces que E tiene *multiplicación compleja* por $\mathscr{O}$.

Si E/K tiene multiplicación compleja por L, es sencillo ver que $a_{\mathfrak{p}}(E) = 0$ para todo primo $\mathfrak{p}$ de K inerte en la extensión LK/K.

1.1.1 $\mathbb{Q}$-curvas

Como el título de esta tesis lo indica, las $\mathbb{Q}$-curvas serán uno de nuestros principales objetos de estudio, y aparecerán a lo largo del trabajo. Son una clase particular de curvas elípticas, y para

definirlas introduciremos brevemente algunos conceptos. De ahora en adelante, en este sección K es un cuerpo de característica 0.

Definición 1.1.6. Dos curvas elípticas E_1/K y E_2/K se dicen *isógenas* sobre K si existe un morfismo de curvas algebraicas $\varphi : E_1 \to E_2$ no trivial sobre K (es decir con coeficientes en K) que a la vez es homomorfismo de grupos. En este caso decimos que φ es una *isogenía*.

Si φ es una isogenía entre curvas elípticas, entonces φ tiene núcleo finito. Se dice que el *grado* de φ es $|\ker(\varphi)|$. Para hablar de $\mathbb{Q}$-curvas, trabajaremos sobre cuerpos de números K en donde la extensión $K/\mathbb{Q}$ sea Galois. Entonces, si

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

es una curva elíptica sobre K (i.e. $a_i \in K$) y σ es un elemento de $\mathrm{Gal}(K/\mathbb{Q})$, denotamos por E^σ o por $\sigma(E)$ a la curva elíptica *conjugada*

$$E^\sigma : y^2 + \sigma(a_1)xy + \sigma(a_3)y = x^3 + \sigma(a_2)x^2 + \sigma(a_4)x + \sigma(a_6).$$

Definición 1.1.7. Sea K un cuerpo de números tal que la extensión $K/\mathbb{Q}$ es Galois y sea E/K una curva elíptica. Decimos que E es una $\mathbb{Q}$-*curva* si E es $\overline{K}$-isógena a E^σ para todo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Notemos entonces que si E/K es una $\mathbb{Q}$-curva, para todo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ existe una isogenía $\varphi_\sigma : E \to E^\sigma$ definida sobre $\overline{K}$. Sea L la menor subextensión de $\overline{K}/K$ sobre la cual están definidas todas las isogenías φ_σ. Diremos entonces que E está *totalmente definida* en L, o que L es el *cuerpo de definición total* de E. Más aún, si el grado de las isogenías φ_σ es siempre n, decimos que E es una $\mathbb{Q}$-curva de *grado* n.

Claramente, toda curva elíptica *racional* (es decir definida sobre $\mathbb{Q}$) es trivialmente una $\mathbb{Q}$-curva. Es posible pensar que las $\mathbb{Q}$-curvas son las generalizaciones naturales de las curvas elípticas racionales. Esto se puede visualizar mejor con la siguiente idea. Sea $K/\mathbb{Q}$ una extensión de Galois con grupo de Galois $\{1, \sigma_2, \cdots, \sigma_r\}$. Sea E una curva elíptica racional y sea p un número primo que se parte completamente en K, es decir $p = \mathfrak{p}\mathfrak{p}^{\sigma_2} \cdots \mathfrak{p}^{\sigma_r}$. Si miramos a E como curva definida sobre K, es claro que $a_\mathfrak{p}(E) = a_\mathfrak{p}(E^{\sigma_i})$, para cualquier σ_i. Ahora supongamos que tenemos una curva elíptica E que no es racional pero sí es una $\mathbb{Q}$-curva totalmente definida sobre K. En este caso, si p es como antes, obtendremos nuevamente que $a_\mathfrak{p}(E) = a_\mathfrak{p}(E^{\sigma_i})$. Más aún, esto caracteriza completamente a las $\mathbb{Q}$-curvas, es decir, son las únicas curvas que cumplen con lo anterior para todo primo p que se parta completamente.

1.1.2 Weil pairing e isomorfismos (anti) simplécticos

Sea E/K una curva elíptica y fijemos un entero $m \geq 2$. Asumamos también que m es coprimo con la característica de K, si esta fuera positiva. Denotemos por $E[m]$ al núcleo de la función

$$\begin{aligned}[m] : E(\overline{K}) &\to E(\overline{K}) \\ P &\mapsto mP\end{aligned}$$

Es decir, que

$$E[m] = \ker([m]) = \{P \in E(\overline{K}) : mP = O\}. \tag{1.4}$$

Llamamos a dicho conjunto la m-torsión de E. Como grupo abstracto, $E[m]$ tiene la forma $E[m] \simeq \mathbb{Z}/m \times \mathbb{Z}/m$ (ver [78, III Corolario 6.4b]). En [78, III §8] se puede encontrar la construcción de una función, llamada *Weil pairing*, de la forma $e_m : E[m] \times E[m] \to \mu_m$, donde μ_m es el conjunto de las raíces m-ésimas de la unidad. Sus propiedades más importantes se engloban en el siguiente resultado.

Proposición 1.1.8. *El Weil pairing e_m es:*

- *Bilineal:*

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2);$$

- *Alternante: $e_m(T, T) = 1$, y en particular $e_m(T, S) = e_m(S, T)^{-1}$;*
- *No degenerada: si $e_m(S, T) = 1$ para todo $S \in E[m]$ entonces $T = O$;*
- *Invariante por la acción de Galois: para todo $\sigma \in G_K$,*

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma);$$

- *Compatible: si $S \in E[mm']$ y $T \in E[m]$, entonces*

$$e_{mm'}(S, T) = e_m([m']S, T).$$

Demostración. Ver [78, III Proposición 8.1]. □

Si $\phi : E_1 \to E_2$ es una isogenía entre curvas elípticas, denotamos por $\hat{\phi} : E_2 \to E_1$ a la isogenía dual de ϕ (ver [78, III §6]).

Proposición 1.1.9. *Sea $S \in E_1[m]$, $T \in E_2[m]$ y $\phi : E_1 \to E_2$ una isogenía. Entonces*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

Demostración. Ver [78, III Proposición 8.2]. □

Sean E y E' curvas elípticas sobre un cuerpo de números K y $\phi : E \to E'$ una isogenía definida sobre K. Sea p un número primo coprimo con grado(ϕ). La isogenía ϕ induce un isomorfismo $\phi : E[p] \to E'[p]$ de G_K-módulos. Aplicando las Proposiciones 1.1.8 y 1.1.9 tenemos que

$$e_{E'}(\phi(P), \phi(Q)) = e_E(P, \hat{\phi}\phi(Q)) = e_E(P, Q)^{d_\phi},$$

donde $d_\phi \in \mathbb{F}_p^\times$ es el grado de la isogenía (en la última igualdad también usamos que $[d_\phi] = \hat{\phi}\phi$; ver [78, III Teorema 6.1]).

Decimos que ϕ es un *isomorfismo simpléctico* o un *isomorfismo antisimpléctico* si $d(\phi)$ es un cuadrado o no cuadrado módulo p, respectivamente. También decimos que $E[p]$ y $E'[p]$ son *(anti) simplécticamente isomorfos* si existe un (anti) isomorfismo.

Observación 1. A priori $E[p]$ y $E'[p]$ podrian ser simplécticamente y anti simplécticamente isomorfos.

Ahora si ℓ es un primo distinto de p y $\mathfrak{l}$ es un primo de K arriba de ℓ, podemos considerar el isomorfismo $\phi_\mathfrak{l} : E[p] \to E'[p]$ de $G_{K_\mathfrak{l}}$-módulos, que se obtiene de mirar las curvas E y E' sobre $K_\mathfrak{l}$. Entonces el tipo simpléctico de $\phi_\mathfrak{l}$ es igual al tipo simpléctico de ϕ.

1.2 Representaciones de Galois

De ahora en adelante p es un número primo, K es un cuerpo de números y G_K denota el grupo de Galois absoluto de K, $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Recordemos que G_K resulta un grupo topológico con la topología de Krull. Denotamos por $\mathbb{F}_{p^r}$ el único cuerpo (salvo isomorfismos) de p^r elementos. También denotamos por $\mathscr{O}_K$ al anillo de enteros de K. Para esta sección se puede consultar [36] y también (para una lectura en español) [61].

Definición 1.2.1. Sea L una extensión finita de $\mathbb{Q}_p$. Una *representación de Galois p-ádica de dimensión n* es un homomorfismo de grupos continuo

$$\rho : G_K \to \mathrm{GL}_n(L).$$

Si $\rho' : G_K \to \mathrm{GL}_n(L)$ es otra representación de Galois p-ádica de dimensión n entonces decimos que ρ y ρ' son *equivalentes (o isomorfas)* si existe una matriz $M \in \mathrm{GL}_n(\overline{L})$ tal que $\rho'(\sigma) = M\rho(\sigma)M^{-1}$ para todo $\sigma \in G_K$. En este caso utilizaremos la notación $\rho \sim \rho'$.

Proposición 1.2.2. *Sea $\rho : G_K \to \mathrm{GL}_n(L)$ una representación de Galois p-ádica. Entonces ρ es equivalente a una representación $\rho' : G_K \to \mathrm{GL}_n(\mathscr{O}_L)$.*

Demostración. Ver [36, Proposición 9.3.5] para el caso $K = \mathbb{Q}$. El caso K general resulta igual, ya que sólo se utiliza que $G_{\mathbb{Q}}$ es compacto, lo cual vale también para G_K. □

Definición 1.2.3. Una *representación de Galois módulo p de dimensión n* es un homomorfismo de grupos continuo $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Dos representaciones de Galois mod p de dimensión n ρ y ρ' se dicen equivalentes ($\rho \sim \rho'$) si existe un elemento $M \in \mathrm{GL}_n(\overline{\mathbb{F}}_{p^r})$ tal que $\rho'(\sigma) = M\rho(\sigma)M^{-1}$ para todo $\sigma \in G_K$.

Notar que dada una representación p-ádica ρ de G_K podemos suponer, por Proposición 1.2.2, que ρ toma valores en $\mathrm{GL}_n(\mathscr{O}_L)$. Luego, reduciendo módulo el ideal maximal de $\mathscr{O}_L$ obtenemos una representación mod p, $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F}_{p^r})$, donde $\mathbb{F}_{p^r}$ es el cuerpo residual de $\mathscr{O}_L$.

Definición 1.2.4. Una representación $\rho : G_K \to \mathrm{GL}_n(L)$ se dice *irreducible* si no existe un L-subespacio vectorial propio $L' \subset L^n$ tal que $\rho(\sigma)L' \subseteq L'$ para todo $\sigma \in G_K$.

Definición 1.2.5. Decimos que una representación $\rho : G_K \to \mathrm{GL}_n(L)$ es *absolutamente irreducible* si la representación $G_K \to \mathrm{GL}_n(L) \hookrightarrow \mathrm{GL}_n(\overline{L})$ es irreducible.

La definición de ser absolutamente irreducible es equivalente a decir que la representación es irreducible sobre cualquier extensión algebraica de L.

Como veremos más adelante, las representaciones de dimensión 2 serán de mayor interés, puesto que son las obtenidas al mirar representaciones asociadas a curvas elípticas. Veamos a continuación una definición y un resultado para esta dimensión particular.

Definición 1.2.6. Sea K un cuerpo totalmente real. Una representación de Galois ρ de G_K de dimensión 2 se dice *impar* si $\det(\rho(c)) = -1$ para c cualquier conjugación compleja.

Proposición 1.2.7. *Sea p un primo impar. Sea K un cuerpo totalmente real y $\overline{\rho}$ una representación de Galois mod p de dimensión 2. Entonces $\overline{\rho}$ es irreducible si y sólo si es absolutamente irreducible.*

Demostración. Ver por ejemplo la observación luego del Teorema 1.1 de [63]. □

Definición 1.2.8. Sean $\rho : G_K \to \mathrm{GL}_n(L)$, $\rho' : G_K \to \mathrm{GL}_m(L)$ dos representaciones de Galois. La *suma directa* de ρ y ρ' es la representación de dimensión $n+m$ dada por

$$\begin{aligned} \rho \oplus \rho' : G_K &\to \mathrm{GL}_{n+m}(L). \\ \sigma &\mapsto \begin{pmatrix} \rho(\sigma) & 0 \\ 0 & \rho'(\sigma) \end{pmatrix} \end{aligned}$$

El *producto tensorial de* ρ y ρ' es la representación dada por

$$\begin{aligned} \rho \otimes \rho' : G_K &\to \mathrm{GL}_{n+m}(L). \\ \sigma &\mapsto \rho(\sigma) \otimes \rho'(\sigma) \end{aligned}$$

El morfismo de Frobenius

Veamos a continuación un breve repaso de algunas nociones básicas de la teoría de cuerpos de clases. Sea p un número primo y sea $\mathfrak{p}$ un ideal maximal de $\overline{\mathbb{Z}}$ sobre p (es decir que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$). Se define el *grupo de descomposición* de $\mathfrak{p}$ como

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

A su vez, llamamos *grupo de inercia* de $\mathfrak{p}$ al subgrupo

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ para todo } x \in \overline{\mathbb{Z}}\}.$$

Notar que la acción de $D_{\mathfrak{p}}$ en $\overline{\mathbb{Z}}/\mathfrak{p}$ dada por $\sigma(x+\mathfrak{p}) = \sigma(x) + \mathfrak{p}$ induce un morfismo φ de $D_{\mathfrak{p}}$ en $\mathrm{Gal}(\overline{\mathbb{Z}}/\mathfrak{p}/\mathbb{F}_p) = G_{\mathbb{F}_p}$. A su vez, sabemos que $G_{\mathbb{F}_p}$ es un grupo cíclico generado por $\sigma_p : x \mapsto x^p$. Un *morfismo de Frobenius* sobre p es un elemento $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ tal que $\varphi(\mathrm{Frob}_{\mathfrak{p}}) = \sigma_p$.

Lema 1.2.9. *Sea p un primo racional y $\mathfrak{p} \in \overline{\mathbb{Z}}$ ideal maximal sobre p. Sea $\varphi : D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$ definida como arriba. Entonces φ es suryectiva y $\ker(\varphi) = I_{\mathfrak{p}}$.*

En particular el Lema 1.2.9 implica que $D_{\mathfrak{p}}/I_{\mathfrak{p}} \simeq G_{\mathbb{F}_p}$ y que $\mathrm{Frob}_{\mathfrak{p}}$ está bien definido módulo el subgrupo de inercia. Más aún, se tiene que

$$\mathrm{Frob}_{\sigma(\mathfrak{p})} = \sigma^{-1} \mathrm{Frob}_{\mathfrak{p}}\, \sigma. \tag{1.5}$$

Definición 1.2.10. Sea $\rho : G_K \to \mathrm{GL}_n(L)$ una representación de Galois. Dado un número primo p, decimos que ρ es *no ramificada* en p si $\rho(I_{\mathfrak{p}}) = \{1\}$ para cualquier primo $\mathfrak{p} \subset \overline{\mathbb{Z}}$ sobre p.

Notar que la definición anterior no depende del primo $\mathfrak{p}$ ya que cualesquiera dos primos $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ que contengan a p satisfacen que sus grupos de inercia son conjugados, con lo cual ρ es trivial en uno si y sólo si es trivial en el otro. Por otro lado, diremos que ρ es *ramificada* en p si $\rho(I_{\mathfrak{p}}) \neq \{1\}$ para algún (todo) primo $\mathfrak{p}$ sobre p.

Luego, por lo dicho anteriormente, si ρ es no ramificada en p, entonces $\rho(\mathrm{Frob}_{\mathfrak{p}})$ está bien definido. Además, continuando con la notación anterior, si $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son dos primos arriba de p, entonces existe un $\sigma \in G_{\mathbb{Q}}$ tal que $\sigma(\mathfrak{p}) = \overline{\mathfrak{p}}$. Luego, del hecho de que ρ sea un morfismo y de (1.5) se deduce que $\rho(\mathrm{Frob}_{\mathfrak{p}})$ y $\rho(\mathrm{Frob}_{\overline{\mathfrak{p}}})$ son matrices conjugadas, y por lo tanto sus polinomios característicos coinciden. Entonces, si $\mathrm{car}(M) = \det(xI - M)$ denota el polinomio característico de la matriz M, podemos definir

$$\mathrm{car}(\mathrm{Frob}_p) := \mathrm{car}(\mathrm{Frob}_{\mathfrak{p}}),$$

para cualquier $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ ideal maximal tal que $p \in \mathfrak{p}$.

Teorema 1.2.11 (Chebotarev)**.** *Para todo primo p, salvo finitos, tomemos para cada ideal maximal $\mathfrak{p}$ de $\overline{\mathbb{Z}}$ que divide a p, un elemento de Frobenius* $\mathrm{Frob}_{\mathfrak{p}}$*. El conjunto de tales elementos forman una base densa de $G_{\mathbb{Q}}$.*

Proposición 1.2.12. *Sean ρ_1, ρ_2 dos representaciones de Galois. Si para todo número primo p, salvo finitos, y para cada ideal primo $\mathfrak{p}$ sobre p vale que $\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \rho_2(\mathrm{Frob}_{\mathfrak{p}})$ entonces $\rho_1 = \rho_2$.*

Demostración. Se sigue del hecho de que las representaciones de Galois son funciones continuas y de que, por Teorema 1.2.11 el conjunto $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p}}$ es denso en $G_{\mathbb{Q}}$. □

Más aún, si relajamos la hipótesis de que las representaciones coincidan en $\mathrm{Frob}_{\mathfrak{p}}$ y nos restringimos a analizar sus polinomios característicos obtenemos un resultado similar, como el siguiente.

Teorema 1.2.13. *Sean ρ y ρ' dos representaciones de Galois irreducibles (p-ádica o de módulo p) ramificadas sólo en una cantidad finita de primos. Si para casi todo primo q (es decir para todos salvo una cantidad finita) en donde las dos representaciones son no ramificadas se satisface que*

$$\mathrm{car}(\rho(\mathrm{Frob}_q)) = \mathrm{car}(\rho'(\mathrm{Frob}_q)),$$

entonces ρ y ρ' son isomorfas.

1.2.1 Representaciones de Galois de curvas elípticas

Sea E una curva elíptica sobre un cuerpo de números K. Sea m un entero positivo y consideremos la m-torsión de la curva, es decir el conjunto $E[m]$ definido como en (1.4). Es fácil ver que G_K actúa sobre $E[m]$ coordenada a coordenada, es decir, si $P = (x, y)$ es un punto en $E[m]$, entonces $\sigma(P) := (\sigma(x), \sigma(y)) \in E[m]$.

Como $E[m] \simeq \mathbb{Z}/m \times \mathbb{Z}/m$ es un $\mathbb{Z}/m$-módulo de dimensión 2, entonces podemos fijar una base $\{P, Q\}$ de $E[m]$. Entonces, para cada elemento $\sigma \in G_K$ existen $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in \mathbb{Z}/m$ tales que

$$\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix}.$$

Esta acción induce entonces una función $\sigma \mapsto \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$.

Teorema 1.2.14. *Sean K un cuerpo de números, E/K una curva elíptica y $m \geq 1$ un entero. La acción de G_K en $E[m]$ define una representación de Galois módulo m de dimensión 2*

$$\overline{\rho}_{E,m} : G_K \to \mathrm{GL}_2(\mathbb{Z}/m).$$

Cabe destacar que al cambiar la base de $E[m]$ por otra, la representación obtenida será isomorfa a la anterior.

Proposición 1.2.15. *Sea p un número primo. La representación $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ obtenida a partir de la acción de G_K en los puntos de p-torsión de una curva elíptica resulta ser una representación impar.*

Sea $\overline{\rho}_{E,p}$ como en la proposición anterior. Como consecuencia de la Proposición 1.2.7, si K es totalmente real, entonces $\overline{\rho}_{E,p}$ es absolutamente irreducible si y sólo si es irreducible. Como veremos más adelante, asegurar la irreducibilidad absoluta de $\overline{\rho}_{E,p}$ es uno de los pasos importantes que se tienen a la hora de aplicar el método modular. Con respecto a la ramificación de representaciones de Galois asociadas a curvas elípticas, el resultado más importante es el de Néron-Ogg-Shafarevich. Sin embargo, al estar dicho criterio enunciado para representaciones globales, primero analizaremos las propiedades de la representación $\overline{\rho}_{E,p}$.

Teorema 1.2.16 (Hellegouarch)**.** *Sea E/K una curva elíptica, $q \neq p$ un primo impar que no ramifica en K y $\mathfrak{q}$ en K sobre q. Sea Δ_{min} el discriminante de un modelo minimal de E con respecto a $\mathfrak{q}$. Si $\mathfrak{q}$ es un primo de reducción multiplicativa y $p \mid v_{\mathfrak{q}}(\Delta_{min})$ entonces $\overline{\rho}_{E,p}$ es no ramificada en $\mathfrak{q}$.*

A continuación nos concentraremos en las posibles imágenes de una representación $\overline{\rho}_{E,p}$. Sea $M_2(\mathbb{F}_p)$ el anillo de matrices de 2×2 con coeficientes en $\mathbb{F}_p$.

Definición 1.2.17. Sea R un subanillo de $M_2(\mathbb{F}_p)$ tal que y sea G un subgrupo de $\mathrm{GL}_2(\mathbb{F}_p)$ tal que $G \simeq R^\times$. Entonces decimos que

- G es un *subgrupo de Borel*, si R es el anillo de las matrices triangulares superiores,
- G es un *subgrupo de Cartan split* si $R \simeq \mathbb{F}_p \times \mathbb{F}_p$ (matrices diagonales),
- G es un *subgrupo de Cartan non-split* si $R \simeq \mathbb{F}_{p^2}$.

Sea $\mathrm{PGL}_2(\mathbb{F}_p) := \mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$. Una representación de Galois $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ induce una *representación proyectiva*

$$\mathbb{P}\overline{\rho} : G_K \to \mathrm{PGL}_2(\mathbb{F}_p).$$

Existe una clasificación sobre los posibles subgrupos de $\mathrm{PGL}_2(\mathbb{F}_p)$. Si $\mathrm{PSL}_2(\mathbb{F}_p) := \mathrm{SL}_2(\mathbb{F}_p)/\{\pm 1\}$ entonces todo subgrupo distinto de $\mathrm{PSL}_2(\mathbb{F}_p)$ debe estar contenido en un subgrupo maximal de $\mathrm{PGL}_2(\mathbb{F}_p)$. Más concretamente, tenemos el siguiente resultado.

Teorema 1.2.18 (Dickson)**.** *Sea H un subgrupo de $\mathrm{PGL}_2(\mathbb{F}_p)$. Entonces se cumple alguna de las siguientes:*

- *$H = \mathrm{PSL}_2(\mathbb{F}_p)$, o*
- *$H = \mathrm{PGL}_2(\mathbb{F}_p)$, o*
- *H está contenido en un subgrupo de Borel, o*
- *H está contenido en el normalizador de un subgrupo de Cartan, o*
- *excepcionalmente se satisface alguno de los siguientes isomorfismos: $H \simeq A_4, S_4$ ó A_5.*

A partir del teorema de Dickson, se deriva uno de los resultados más importantes acerca de una representación de Galois definida a partir de una curva elíptica, a saber:

Teorema 1.2.19 (Serre)**.** *Sea E/K una curva elíptica sin multiplicación compleja. Entonces $\overline{\rho}_{E,p}$ es suryectiva para casi todo p.*

En particular, si E es una curva elíptica sin multiplicación compleja, sabemos que $\overline{\rho}_{E,p}$ es suryectiva para p suficientemente grande. Una pregunta natural es qué ocurre en el caso de multiplicación compleja.

Proposición 1.2.20. *Sea E una curva elíptica con multiplicación compleja por un orden $\mathcal{O}$ de L. Sea p que no divida al discriminante de $\mathcal{O}$. Entonces $\mathrm{Im}(\overline{\rho}_{E,p})$ está contenida en el normalizador de un subgrupo de Cartan. Más aún, se cumple lo siguiente:*

- *Si p se parte en L, entonces $\mathrm{Im}(\overline{\rho}_{E,p})$ está contenida en el normalizador de un subgrupo de Cartan split.*
- *Si p es inerte en L, entonces $\mathrm{Im}(\overline{\rho}_{E,p})$ está contenida en el normalizador de un subgrupo de Cartan non-split.*

Demostración. Aunque el resultado es bien conocido por los expertos, se puede ver en [60, Lema 6.2]. □

Hemos mostrado cómo construir una representación de Galois módulo p a partir de una curva elíptica. Veamos a continuación cómo se construye una representación p-ádica. Así como las primeras fueron definidas a partir de la acción de un grupo de Galois sobre los puntos de p-torsión de la curva, ahora deberemos mirar la acción del grupo de Galois sobre un $\mathbb{Z}_p$-módulo, donde $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ en el primo p.

Sea E/K una curva elíptica. Notemos que la función $[p]$ definida en Sección 1.1.2 induce la siguiente sucesión

$$\{O\} \xleftarrow{[p]} E[p] \xleftarrow{[p]} E[p^2] \xleftarrow{[p]} E[p^3] \xleftarrow{[p]} \cdots$$

Se define entonces como *módulo de Tate* p-ádico al límite inverso

$$T_p(E) := \lim_{\leftarrow p} E[p].$$

Del hecho de que $E[p]$ sea un $\mathbb{Z}/p$-módulo libre de rango 2 se deduce fácilmente que $T_p(E) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Es fácil notar que la acción del grupo de Galois G_K sobre los $\mathbb{Z}/p^n$-módulos $E[p^n]$ conmuta con la isogenía $[p]$. Esto induce una acción de G_K en $T_p(E)$, un $\mathbb{Z}_p$-módulo libre de rango 2. Luego, existe una representación de Galois p-ádica de dimensión 2

$$\rho_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p) \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$$

adjuntada a la curva E/K.

Teorema 1.2.21 (Néron-Ogg-Shafarevich)**.** *Sea E/K una curva elíptica y $\mathfrak{q}$ un primo de K. Las siguientes afirmaciones son equivalentes:*

- *E tiene buena reducción en $\mathfrak{q}$.*
- *$\rho_{E,p}$ es no ramificada en $\mathfrak{q}$ para algún primo p tal que $\mathfrak{q} \nmid p$.*
- *$\rho_{E,p}$ es no ramificada en $\mathfrak{q}$ para todo primo p tal que $\mathfrak{q} \nmid p$.*

Aplicando el Teorema de Néron-Ogg-Shafarevich se puede deducir el siguiente resultado.

Teorema 1.2.22. *Sea p un primo y E/K una curva elíptica de conductor N. La representación de Galois $\rho_{E,p}$ es no ramificada en todo $\mathfrak{q} \nmid pN$. Sea $\mathfrak{P}$ un ideal en $\overline{\mathbb{Z}}$ sobre $\mathfrak{q}$. Entonces*

$$\mathrm{car}(\rho_{E,p}(\mathrm{Frob}_{\mathfrak{P}})) = x^2 - a_{\mathfrak{q}}(E)x + \mathscr{N}(\mathfrak{q}),$$

donde $a_{\mathfrak{q}}(E)$ está definido como en (1.3). Además, la representación $\rho_{E,p}$ es irreducible.

A continuación enunciaremos un resultado de Mazur que no será de gran utilidad para nosotros, ya que sólo aplica a curvas racionales. Sin embargo, creemos que puede ser provechosa su postulación, por completitud a la sección, y porque veremos luego cómo se aplica en la prueba del Último Teorema de Fermat, quedando así establecido el rol que este tipo de resultado juega en el método modular.

Teorema 1.2.23 (Mazur)**.** *Sea $E/\mathbb{Q}$ una curva elíptica y p un número primo. Supongamos que vale una de las siguientes condiciones.*

- *$p \geq 11$ y E es semiestable,*
- *$p \geq 5$, E es semiestable y el conjunto de 2-torsión es racional (i.e. $E[2] \subseteq \mathbb{Q}^2 \cup \{O\}$).*

Entonces $\overline{\rho}_{E,p}$ es irreducible.

1.3 Caracteres

El principal objetivo de esta sección es introducir el concepto de caracter de Hecke. Para ello definimos primero la noción de caracter, presentamos los caracteres de Dirichlet, definimos los idèles y finalmente los caracteres de Hecke. Esta sección está basada en [84].

Definición 1.3.1. Dado un grupo G, un *caracter* de G es un homomorfismo de grupos $\chi : G \to \overline{\mathbb{Q}}^{\times}$.

Definición 1.3.2. Un *caracter de Dirichlet* de módulo n es un caracter del grupo $(\mathbb{Z}/n)^{\times}$.

Observación 2. Para todo $a \in (\mathbb{Z}/n)^{\times}$ se cumple que $\chi(a)$ es una raíz $\varphi(n)$-ésima de la unidad, donde φ es la función de Euler. En efecto, por el Pequeño Teorema de Fermat tenemos que

$$\chi(a)^{\varphi(n)} = \chi(a^{\varphi(n)}) = \chi(1) = 1.$$

Definición 1.3.3. Un caracter de Dirichlet se dice *primitivo* si no es inducido por otro caracter de módulo más chico.

1.3.1 Adèles e idèles

Los adèles fueron definidos en primera instancia por el francés Chevalley con el fin de describir la teoría global de clases para extensiones infinitas. Años después operó con los idèles para dar una conexión entre la teoría de clases global y la local. El objetivo de esta corta subsección es simplemente introducir el concepto de idèles. Referimos a [16] para una lectura profunda sobre los adèles e idèles.

Sea K un cuerpo de números. Denotamos por M_K al conjunto de todos los lugares de K y por S_∞ al conjunto de todos los lugares arquimedianos. Consideremos primero un subconjunto finito S de M_K tal que $S_\infty \subseteq S$. Podemos definir entonces al conjunto de *S-adèles* como

$$\mathbb{A}_K^S := \prod_{v \notin S} \mathscr{O}_v \times \prod_{v \in S} K_v.$$

Lema 1.3.4. *Si $S_\infty \subseteq S \subseteq M_K$ entonces $\mathbb{A}_K^S$ dotado de la topología producto resulta un anillo topológico (con la suma y el producto punto a punto) localmente compacto.*

Definimos así el *anillo de adèles* como la unión de todos los S-adèles. Es decir,

$$\mathbb{A}_K := \bigcup_{\substack{S_\infty \subseteq S, \\ S \subseteq M_K}} \mathbb{A}_K^S.$$

Notemos que resulta así $\mathbb{A}_K = \{(x_v)_v : x_v \in \mathscr{O}_v \text{ para todo } v \in M_K \text{ salvo una cantidad finita}\}$. Esto es claramente un subconjunto del producto de los K_v y se llama el *producto directo restringido* de los K_v respecto de los $\mathscr{O}_v$. Las operaciones que le dan a $\mathbb{A}_K$ la estructura de anillo son el producto y la suma lugar a lugar. A su vez, también se puede dotar a este anillo con una topología no trivial, definida a través de los elementos de su base, que serán los entornos básicos de $\mathbb{A}_K^S$ para cada S finito que contiene a S_∞. Finalmente resulta así $\mathbb{A}_K$ un anillo topológico.

Teorema 1.3.5 (Fórmula del producto)**.** *Si K es un cuerpo de números y $x \in K^{\times}$ entonces*

$$\prod_{v \in M_K} |x|_v = 1.$$

El conjunto de los *idèles* es por definición $\mathbb{I}_K := \mathbb{A}_K^\times$. Esto nos dice que

$$\begin{aligned}\mathbb{I}_K := \mathbb{A}_K^\times =&\{(x_v) \in \mathbb{A}_K : \text{ existe } (y_v) \in \mathbb{A}_K \text{ tal que } (x_v)(y_v) = 1\}\\ =&\{(x_v) \in \mathbb{A}_K : \text{ existe } (y_v) \in \mathbb{A}_K \text{ tal que } x_v y_v = 1 \quad \forall v \in M_K\}\\ =&\{(x_v) \in \mathbb{A}_K : x_v \in K_v^\times \text{ para todo } v \text{ y } x_v \in \mathscr{O}_v^\times \text{ para casi todo } v\}.\end{aligned}$$

Por lo tanto $\mathbb{I}_K$ coincide con el producto directo restringido de los $K_v^\times$ respecto de los $\mathscr{O}_v^\times$. La razón por la cual lo denotamos $\mathbb{I}_K$ y no simplemente $\mathbb{A}_K^\times$ es la topología. Vamos a considerar en $\mathbb{I}_K$ la topología producto, que no coincide con la heredada por la de los adèles.

Lema 1.3.6. *La topología producto en $\mathbb{I}_K$ es estrictamente más fina que la inducida por $\mathbb{A}_K$.*

Demostración. Ver [84, Lema 4.2.1]. □

1.3.2 Caracteres de Hecke

Consideremos en $\overline{\mathbb{Q}}^\times$ la topología inducida de $\mathbb{C}$.

Definición 1.3.7. Un **caracter de Hecke** de K es un caracter continuo $\chi : \mathbb{I}_K \to \overline{\mathbb{Q}}^\times$ que es trivial en $K^\times$, es decir, $\chi(K^\times) = 1$.

Para cada lugar v, definimos $i_v : K_v^\times \to \mathbb{I}_K$ dado por

$$(i_v(x))_w = \begin{cases} x & \text{si } v = w,\\ 1 & \text{si } v \neq w.\end{cases}$$

y la función $\chi_v : K_v^\times \to \overline{\mathbb{Q}}^\times$ dada por $x \mapsto \chi(i_v(x))$.

Lema 1.3.8. *Para cada lugar v de K, i_v es continua y por lo tanto χ_v es continuo.*

Demostración. Ver [84, Lema 5.4.2]. □

Proposición 1.3.9. $\chi(x) = \prod_v \chi_v(x_v)$, *donde* $x = (x_v)$.

Demostración. Ver [84, Proposición 5.4.5]. □

Teorema 1.3.10. *Sea v un lugar finito y $\chi_v : K_v^\times \to \overline{\mathbb{Q}}^\times$ un caracter de orden finito. Entonces χ_v es continuo.*

Demostración. Ver [84, Teorema 5.4.6]. □

Utilizando resultados de la teoría de cuerpos de clases se puede ver que existe una correspondencia entre los caracteres de Hecke de K de orden finito y las representaciones de Galois de dimensión 1, $\rho : G_K \to \overline{\mathbb{Q}}^\times$. A la hora de construir el caracter de Hecke mencionado en la introducción, utilizaremos constantemente esta correspondencia (ver Sección 1.7.1).

1.4 Formas modulares

Las formas modulares conforman una gran área de estudio dentro de la teoría de números. Su análisis ha desarrollado un gran crecimiento en el campo, y por ello mucho se podría abarcar en esta sección. Sin embargo, nos remitiremos a las definiciones y a los resultados necesarios para esta tesis. Para mayor información, recomendamos [36], una de las principales referencias en el tema.

Definición 1.4.1. Dado N un número natural, definimos el *subgrupo de congruencia principal* de nivel N como

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

(aquí la congruencia se interpreta entrada a entrada).

En general, diremos que un subgrupo Γ es un *subgrupo de congruencia* de nivel N si Γ es un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ tal que $\Gamma(N) \subseteq \Gamma$. En este trabajo nos será de mayor interés el siguiente subgrupo de congruencia de nivel N

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Denotemos por $\mathcal{H}$ al semiplano complejo $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ (también conocido como plano de Poincaré). Notemos que $\mathrm{SL}_2(\mathbb{Z})$ actúa en $\mathcal{H}$ como

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

Notemos que la matriz $T := \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ pertenece a $\Gamma(N)$ y que $Tz = z + N$.

Sea $f : \mathcal{H} \to \mathbb{C}$ una función holomorfa tal que $f(Tz) = f(z)$. Entonces f es periódica con período N. Luego, existe una función $g : D' \to \mathbb{C}$ de manera que $f(z) = g(q)$, donde $q = e^{2\pi iz/N}$ y D' es el disco pinchado de centro 0 y radio 1. Como g es holomorfa, podemos analizar su serie de Laurent en 0. Diremos que f es *holomorfa en* ∞ si g se extiende analíticamente a $q = 0$. En este caso,

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad \text{donde } q = e^{2\pi iz/N}.$$

Llamamos *coeficientes de Fourier* a los coeficientes $a_n(f)$ de la serie. Si g es otra función con las mismas propiedades, decimos que $f \equiv g \pmod{p}$ si $a_n(f) \equiv a_n(g) \pmod{p}$ para casi todo $n \geq 0$.

Dado $k \in \mathbb{Z}$ y $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ utilizaremos la siguiente notación:

$$f[\gamma]_k(z) := (cz+d)^{-k} f(\gamma z).$$

Definición 1.4.2. Sea k un número entero y Γ un subgrupo de congruencia de nivel N. Una *forma modular de peso k respecto de* Γ es una función $f : \mathcal{H} \to \mathbb{C}$ que satisface lo siguiente:

- f es holomorfa.
- $f = f[\gamma]_k$ para todo $\gamma \in \Gamma$.
- $f[\gamma]_k$ es holomorfa en ∞ para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Más aún, se dice que f es *cuspidal* si $a_0(f[\gamma]_k) = 0$ para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Denotamos por $M_k(\Gamma)$ al conjunto de todas las formas modulares de peso k respecto de Γ y por $S_k(\Gamma)$ al subconjunto de formas cuspidales de $M_k(\Gamma)$.

Lema 1.4.3. *$M_k(\Gamma)$ y $S_k(\Gamma)$ son $\mathbb{C}$- espacios vectoriales.*

Otro subgrupo de congruencia importante es

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Notemos que si M es un natural tal que $M \mid N$, entonces $\Gamma_1(N) \subseteq \Gamma_1(M)$ y por lo tanto $S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$. Esta es una de las tantas formas de incrustar $S_k(\Gamma_1(M))$ en $S_k(\Gamma_1(N))$ ver [36, § 5.6]. Llamaremos *espacio de formas modulares (cuspidales) viejas* al espacio de todas las formas que provienen de un nivel menor, y lo denotaremos por $S_k(\Gamma_1(N))^{\text{old}}$. Luego, el *espacio de formas modulares (cuspidales) nuevas*, denotado por $S_k(\Gamma_1(N))^{\text{new}}$, es el complemento ortogonal de $S_k(\Gamma_1(N))^{\text{old}}$ en $S_k(\Gamma_1(N))$ respecto del producto interno de Petersson (ver [36, Definición 5.4.1]).

Diremos que una forma cuspidal nueva es *normalizada* cuando $a_1(f) = 1$. Los *operadores de Hecke* son una familia de operadores $\{T_n\}_{n\in\mathbb{N}}$ que actúa en el espacio $S_k(\Gamma_1(N))$. No definiremos estos operadores (ver [36, § 6.3]) pero es importante saber que $S_k(\Gamma_1(N))^{\text{new}}$ admite una base de autovectores simultáneos para todos los operadores T_n. Llamamos *autoformas* a las formas cuspidales nuevas que son autovectores y que son normalizadas.

Proposición 1.4.4. *Sea $f = \sum_{n=1}^{\infty} a_n(f) q^n$ una autoforma de nivel N. Entonces $T_n f = a_n(f) f$ para todo $n \in \mathbb{N}$ tal que $(n, N) = 1$.*

Demostración. Ver [36, pág. 195]. □

Definición 1.4.5. Si $f = \sum_{n=1}^{\infty} a_n(f) q^n$ es una autoforma, definimos como *cuerpo de coeficientes* de f al cuerpo $\mathbb{Q}(\{a_n(f)\}_n)$, y lo denotamos por K_f.

Proposición 1.4.6. *Si f es una autoforma entonces K_f es un cuerpo de números. Más aún, los coeficientes de Fourier de f son enteros algebraicos.*

Demostración. Ver el Teorema 6.5.1 y su discusión posterior en [36]. □

A continuación veremos cómo se pueden partir los espacios $M_k(\Gamma_1(N))$ y $S_k(\Gamma_1(N))$ como suma de espacios más pequeños. Sea N un número natural y sea $\varepsilon : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ un caracter de Dirichlet de módulo N. Se define

$$M_k(\Gamma_0(N), \varepsilon) := \left\{ f \in M_k(\Gamma_1(N)) : f[\gamma]_k = \varepsilon(d) f \text{ para todo } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}.$$

Análogamente se define $S_k(\Gamma_0(N), \varepsilon)$. Si $f \in M_k(\Gamma_0(N), \varepsilon)$ diremos que es una *forma modular de peso k, nivel N y Nebentypus ε*. De su definición, es directo que tomando el caracter trivial $\varepsilon = 1$ obtenemos $M_k(\Gamma_0(N), 1) = M_k(\Gamma_0(N))$. Al igual que antes, es fácil extender el concepto de autoforma para formas que pertenecen a los espacios $S_k(\Gamma_0(N), \varepsilon)$.

Observación 3. $M_k(\Gamma_0(N), \varepsilon) = \{0\}$ salvo que $\varepsilon(-1) = (-1)^k$ (ver [36, Ejercicio 4.3.3]).

Lema 1.4.7. *Los espacios $M_k(\Gamma_1(N))$ y $S_k(\Gamma_1(N))$ se descomponen como*

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} M_k(\Gamma_0(N), \varepsilon), \quad S_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} S_k(\Gamma_0(N), \varepsilon),$$

donde la suma recorre todos los caracteres de Dirichlet ε de nivel N.

Vía la construcción de Eichler-Shimura, a partir de una autoforma $f \in S_2(\Gamma_0(N), \varepsilon)$ es posible definir una variedad abeliana A_f de dimensión $\dim(A_f) = [K_f : \mathbb{Q}]$. No definiremos el concepto de variedad abeliana, pero cabe la aclaración de que las curvas elípticas son todas las variedades abelianas de dimensión 1. Luego, mirando nuevamente la acción de un grupo de Galois sobre los

puntos de m-torsión de A_f se puede definir, análogamente al caso de curvas elípticas, una representación de Galois. Para el caso en que el peso k no sea igual a 2, Deligne construyó no variedades abelianas, sino otros objetos geométricos que también inducen representaciones de Galois. Luego, en general tenemos el siguiente resultado

Teorema 1.4.8 (Eichler-Shimura, Deligne, Deligne-Serre)**.** *Sea $f \in S_k(\Gamma_0(N), \varepsilon)$ una autoforma y sea p un número primo. Para cada primo $\mathfrak{p}$ de $\mathscr{O}_{K_f}$ sobre p existe una representación de Galois de dimensión 2 irreducible*

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\mathfrak{p}}),$$

donde $K_{f,\mathfrak{p}}$ es la completación de K_f en $\mathfrak{p}$. Además, esta representación es no ramificada en todo primo $q \nmid pN$. Para cada tal q, sea $\mathfrak{q} \subseteq \overline{\mathbb{Z}}$ un ideal maximal sobre q. Entonces

$$\mathrm{car}(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}})) = x^2 - a_q(f)x + \varepsilon(q)q^{k-1}.$$

Notar la similitud del Teorema 1.4.8 con el Teorema 1.2.22 cuando $k = 2$ y $\varepsilon = 1$. En este caso $f \in S_2(\Gamma_0(N))$ y el polinomio característico nos dice que $\det(\rho_{f,\mathfrak{p}}) = \varepsilon\chi_p$, donde χ_p es el caracter ciclotómico (ver [36, pág. 379] para su definición) y el caracter ε está siendo identificado con su representación de Galois asociada (ver [36, pág. 378]). Si c es una conjugación compleja entonces $\chi_p(c) = -1$. Por otro lado, por Observación 3, $\varepsilon(c) = \varepsilon(-1) = 1$ cuando $k = 2$. Esto implica que la representación $\rho_{f,\mathfrak{p}}$ es impar.

Al igual que para curvas elípticas, también es posible generar representaciones de Galois de dimensión 2 módulo p asociadas a una autoforma $f \in S_2(\Gamma_0(N), \varepsilon)$. Esto resulta de que, salvo isomorfismo, podemos asumir que la imagen de $\rho_{f,\mathfrak{p}}$ cae en $\mathrm{GL}_2(\mathscr{O}_{K_{f,\mathfrak{p}}})$ (por Proposición 1.2.2), y por lo tanto reduciendo módulo el ideal maximal de $\mathscr{O}_{K_{f,\mathfrak{p}}}$ obtenemos

$$\overline{\rho}_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r}),$$

para algún $r \in \mathbb{N}$. Más generalmente, consideraremos representaciones $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. Inspirados en las propiedades que cumplen las curvas elípticas con multiplicación compleja damos la siguiente definición.

Definición 1.4.9. Decimos que una forma nueva $f = \sum_{n=1}^{\infty} a_n(f)q^n$ tiene *multiplicación compleja* si existe un cuerpo cuadrático imaginario K tal que $a_p(f) = 0$ para todo primo p inerte en K. En dicho caso K es el único con dicha propiedad (si el peso de la forma es ≥ 2) y decimos que f tiene *multiplicación compleja por K*.

1.4.1 Atkin-Lehner y L-series

A continuación introduciremos algunos conceptos junto con su notación, que serán utilizados luego, principalmente en la Sección 2.4.5. Por eso, es posible que sea preferible omitir su lectura hasta llegar a dicha sección.

Sea N un entero positivo. Si q es un divisor (positivo) de N tal que $\mathrm{mcd}(q, N/q) = 1$ entonces existen $a, b, c, d \in \mathbb{Z}$ tales que la matriz

$$W_q = \begin{pmatrix} qa & b \\ Nc & qd \end{pmatrix}$$

tiene determinante q. La matriz W_q normaliza $\Gamma_0(N)$ e induce un operador w_q en el espacio de formas cuspidales $S_k(\Gamma_0(N))$ que conmutan con los operadores de Hecke T_p para todo primo $p \nmid q$.

El operador lineal w_q no depende de la elección de a, b, c, d y se llama la *involución de Atkin-Lehner* de $S_k(\Gamma_0(N))$. Cualquier forma cuspidal $f \in S_k(\Gamma_0(N))$ que es un autovector para todo T_p con $p \nmid N$ es también autovector de w_q, con autovalor ± 1.

Sea $f \in S_2(\Gamma_0(N))$ con q-expansión $f(z) = \sum_{n\geq 1} a_n(f)q^n$. Si χ es un caracter de Dirichlet, se define el twist $f \otimes \chi$ como la serie

$$(f \otimes \chi)(z) = \sum_{n\geq 1} a_n(f)\chi(n)q^n.$$

Además, el twist tiene asociado una función holomorfa sobre $\{\mathrm{Re}(s) > 2\}$, dada por

$$L(f \otimes \chi, s) = \sum_{n\geq 1} \frac{a_n(f)\chi(n)}{n^s},$$

que se puede extender analíticamente a todo $\mathbb{C}$ (ver [55, Lema 3.1 (ii)]). Luego, cada caracter χ define la función $L_\chi : f \to L_\chi(f \otimes \chi, 1)$ que aparece en (2.6).

1.5 Modularidad de representaciones y de curvas elípticas

Definición 1.5.1. Una representación de Galois p-ádica irreducible impar

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(L)$$

tal que $\det(\rho) = \chi_p^{k-1}\varepsilon$, donde ε tiene imagen finita y χ_p es el caracter ciclotómico en p, es *modular* si existe una forma nueva $f \in S_k(\Gamma_0(N), \varepsilon)$ tal que $K_{f,\mathfrak{p}}$ se incrusta en L para algún ideal maximal $\mathfrak{p}$ de $\mathscr{O}_{K_f}$ sobre p y tal que $\rho_{f,\mathfrak{p}} \sim \rho$.

Definición 1.5.2. Una representación irreducible impar $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ es *modular de tipo* (N, k, ε) si existe una forma nueva $f \in S_k(\Gamma_0(N), \varepsilon)$ y un ideal maximal $\mathfrak{p}$ de $\mathscr{O}_{K_f}$ sobre p tal que $\overline{\rho}_{f,\mathfrak{p}} \sim \overline{\rho}$.

Dada una representación de Galois $\overline{\rho}$ mod p , Serre definió en [74] el *nivel de Serre* $N(\overline{\rho})$, el *peso de Serre* $k(\overline{\rho})$ y el *Nebentypus de Serre* $\varepsilon(\overline{\rho})$ asociado a $\overline{\rho}$. No daremos estas definiciones, pues pueden resultar un poco técnicas, pero cabe mencionar que de la definición del nivel, se deduce la siguiente observación.

Observación 4. Sea $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ una representación de Galois. Por un lado, $p \nmid N(\overline{\rho})$. Por otro lado, un primo $q \neq p$ divide a $N(\overline{\rho})$ si y sólo si $\overline{\rho}$ ramifica en q.

Además, en el mismo artículo Serre conjeturó el siguiente resultado, probado por Khare y Wintenberger en [49, 50].

Teorema 1.5.3 (Conjetura de Serre)**.** *Sea $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ una representación impar irreducible. Entonces $\overline{\rho}$ es modular de tipo $(N(\overline{\rho}), k(\overline{\rho}), \varepsilon(\overline{\rho}))$.*

El concepto de que $\overline{\rho}$ sea *finita en p* tampoco lo daremos (ver [74, pág 189]). Sin embargo, al ser de suma importancia a la hora de aplicar el método modular, enunciaremos el resultado que en la práctica utilizaremos. Al trabajar con representaciones anexadas a curvas elípticas, nos remitiremos a ese caso (ver similitud con Teorema 1.2.16).

Proposición 1.5.4. *Sea E/K una curva elíptica y $\overline{\rho}_{E,p}$ su representación de Galois mód p asociada. Sea Δ_{min} el discriminante de un modelo minimal de E en $\mathfrak{p}$. Si E tiene reducción multiplicativa en $\mathfrak{p}$ y $p \mid v_{\mathfrak{p}}(\Delta_{min})$ entonces $\overline{\rho}_{E,p}$ es finita en $\mathfrak{p}$.*

El siguiente teorema será fundamental a la hora de "remover" primos del nivel y poder dar el resultado más importante de "bajada de nivel", que es el Teorema 1.5.6.

Teorema 1.5.5 (Bajada de nivel de Ribet). *Sea $f \in S_2(\Gamma_1(qN))$, donde q es un número primo tal que $q \nmid N$. Sea p un número primo tal que $p \nmid qN$ y sea $\mathfrak{p}$ un primo en $\mathcal{O}_{K_f}$ arriba de p. Supongamos que $\overline{\rho}_{f,\mathfrak{p}}$ es absolutamente irreducible y que es finita en $\mathfrak{q}$ (primo en $\mathcal{O}_{K_f}$ arriba de q). Entonces $\overline{\rho}_{f,\mathfrak{p}}$ es modular de tipo $(N, 2, 1)$.*

Demostración. Ver [70]. □

Notemos que una condición importante para el Teorema 1.5.5 es que p no divida al nivel de la forma modular. Para lidiar con p cuando está en el nivel es que precisaremos la hipótesis de que la representación sea finita en p. Bajo esta condición, tenemos el siguiente resultado.

Teorema 1.5.6 (Mazur-Ribet). *Sea $p \geq 3$ un número primo. Sea $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{p^r})$ una representación absolutamente irreducible y modular de tipo $(N, 2, \varepsilon)$, donde ε es no ramificado en p. Si $\overline{\rho}$ es finita en p entonces $\overline{\rho}$ es modular de tipo $(N(\overline{\rho}), 2, \varepsilon(\overline{\rho}))$.*

En la siguiente sección veremos cómo se demuestra la prueba del Último Teorema de Fermat. Para ello, es necesario (al menos para casos particulares) el siguiente teorema.

Teorema 1.5.7 (Teorema de Modularidad). *Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N. Entonces existe una forma nueva $f \in S_2(\Gamma_0(N))$ con cuerpo de coeficientes $K_f = \mathbb{Q}$ tal que $\rho_{f,p} \sim \rho_{E,p}$ para todo p.*

A veces abusamos de la notación diciendo que E es una curva elíptica *modular*, haciendo referencia a que la representación $\rho_{E,p}$ es modular para todo p. De hecho, una equivalencia al Teorema 1.5.7 que no involucra representaciones de Galois en su enunciado es el siguiente.

Teorema 1.5.8 (Teorema de Modularidad). *Sea E una curva elíptica sobre $\mathbb{Q}$ con conductor N. Entonces existe una forma nueva $f \in S_2(\Gamma_0(N))$ con cuerpo de coeficientes $K_f = \mathbb{Q}$ tal que $a_p(E) = a_p(f)$ para todo primo $p \nmid N$.*

1.5.1 Representaciones de $\mathbb{Q}$-curvas

En la Sección 1.1.1 motivamos la definición de una $\mathbb{Q}$-curva, mostrando que podía ser vista como una generalización de una curva elíptica racional. En el Teorema 1.5.7 vimos que las representaciones de curvas elípticas racionales son modulares. Luego, tiene sentido preguntarse si las representaciones de $\mathbb{Q}$-curvas son modulares o no. El siguiente resultado nos muestra que la representación a priori no tiene por qué ser modular, pero que al twistearla por un caracter (ver Definición 1.2.8) podremos extenderla a una representación de $G_{\mathbb{Q}}$.

Teorema 1.5.9 (Ribet). *Sea E/K una $\mathbb{Q}$-curva y sea $\rho_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p) \subseteq \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ la representación de Galois p-ádica asociada a la curva E. Existe un caracter de Hecke $\chi : G_K \to \overline{\mathbb{Q}}^{\times}$ tal que $\rho_{E,p} \otimes \chi$ se extiende a una representación de Galois $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$, es decir, $\rho|_{G_K} = \rho_{E,p} \otimes \chi$.*

Demostración. Ver [71]. □

Notar que si la representación reducida $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ es irreducible e impar entonces por Teorema 1.5.3 la representación es modular. Si bien el Teorema 1.5.9 tiene una importancia teórica muy grande, en parte porque induce la idea de que las $\mathbb{Q}$-curvas pueden ser buenas candidatas a tener en cuenta en el método modular, no es tan útil en la práctica. El hecho de que la prueba del teorema no sea constructiva, no nos provee información sobre el caracter χ por el cual se twistea, y por lo tanto poco podremos decir del nivel y del Nebentypus de la forma asociada a la representación $\overline{\rho}$.

Como se mencionó en la introducción, en este trabajo nos encargaremos de construir explícitamente un caracter con las propiedades de χ.

1.6 El Último Teorema de Fermat

El Último Teorema de Fermat es sin duda uno de los resultados más famosos en la matemática, no sólo por su elegante y sencillo enunciado, sino también por el pasar del tiempo hasta dar con su prueba. Vasta información sobre la historia detrás de dicho teorema puede ser encontrada en la literatura (ver por ejemplo [30], o [45] para una versión en español). Cabe destacar que fue postulado por Pierre de Fermat alrededor de 1630, en el margen de una hoja de una copia del libro *Arithmetica*, y que más de 300 años pasaron hasta dar con la ansiada demostración, siendo esto último considerado con caracter positivo para muchos expertos, ya que con su búsqueda varias ramas de la teoría de números moderna tuvieron su origen. Finalmente, la prueba completa se le acredita a Andrew Wiles, culminada con los trabajos [80, 87] en 1995. Sin más preámbulos, a continuación enunciamos el teorema.

Teorema (Fermat-Wiles)**.** *Toda solución entera* (a, b, c) *de la ecuación*

$$x^n + y^n = z^n, \tag{1.6}$$

para un número natural $n \geq 3$ *satisface* $abc = 0$.

Cabe destacar que, si bien Wiles fue el último en dar con la clave a la prueba, la demostración puede ser vista como un trabajo colaborativo en donde varios matemáticos tuvieron su aporte. Esto provocó que la demostración naturalmente se partiera en varios pasos, probando así Wiles el último. Dicha serie de pasos, hoy en día es bien conocida como el *método modular* o *método de modularidad*. El nombre surge como necesidad, puesto que era notorio que dicho esquema de demostración podía ser repetido para probar la no existencia de soluciones de diversas ecuaciones diofánticas. Lógicamente, a lo largo de los años el método fue perfeccionándose, y es por eso que en la Sección 1.7.1 será expuesto con cierto grado de generalidad. Sin embargo, consideramos oportuno tratar de entender su idea principal mediante su primer uso [1], es decir, con la demostración del Último Teorema de Fermat.

Observación 5. Usualmente, uno de los primeros hechos a destacar es que la ecuación (1.6) es homogénea. Es simple notar que esto nos permite enfocarnos sólo en la soluciones (a, b, c) en donde a, b y c no tengan factores en común, ya que si $q \mid a, b, c$ entonces $\left(\frac{a}{q}, \frac{b}{q}, \frac{c}{q}\right)$ también es solución de (1.6). Repitiendo este proceso podemos eliminar todos los factores en común.

Observación 6. Notar que basta probar el enunciado para $n = 4$ y luego para $n = p \geq 3$ un número primo. Para ilustrar esta idea, tomemos a modo de ejemplo un número compuesto n divisible por un primo p y asumamos que el teorema vale para p, es decir que toda solución en $\mathbb{Z}^3$ de la ecuación $x^p + y^p = z^p$ tiene alguna coordenada nula. Entonces, el teorema debe ser cierto para n, pues si suponemos que $n = pm$ y (a, b, c) es solución de la ecuación $x^n + y^n = z^n$ entonces (a^m, b^m, c^m) es solución de $x^p + y^p = z^p$, por lo que $abc = 0$.

Demostración. El caso $n = 4$ fue probado por el mismo Fermat, y el caso $n = 3$ por Euler. Luego, por Observación 6, suponemos que $n = p \geq 5$ es un número primo. La afirmación se demuestra por el absurdo.

Supongamos que (a, b, c) es una solución con $abc \neq 0$. Por Observación 5 podemos asumir, sin pérdida de generalidad, que a, b y c no tienen factores en común. Más aún, intercalando los valores de $\{a, b, c\}$ podemos suponer que a y c son impares, mientras que b es par. También podemos asumir que $a \equiv -1 \pmod 4$, pues si $a \equiv 1 \pmod 4$ entonces $(-a, -b, -c)$ resulta ser una solución como la que buscamos. Entonces se realizan los siguientes pasos:

[1] Para ser más precisos, la conexión entre curvas elípticas, representaciones de Galois y ecuaciones diofánticas se remota a los trabajos de Serre [74] y Darmon [27, 28], pero siempre asumiendo conjeturas de modularidad.

Paso 1. Se define la curva elíptica

$$E_{(a,b,c)} : y^2 = x(x - a^p)(x + b^p), \tag{1.7}$$

cuyo discriminante es $\Delta(E_{(a,b,c)}) = 2^{-8}(ab)^{2p}(a^p + b^p)^2 = 2^{-8}(abc)^{2p}$. El conductor de la curva es $N(E_{(a,b,c)}) = rad(abc)$ (donde el radical de un número es el producto de los primos que lo dividen). Esto, además de implicar que $E_{(a,b,c)}$ es semiestable, nos dice que $E_{(a,b,c)}$ es minimal. Notar también que $E_{(a,b,c)}[2] = \{O, (0,0), (a^p, 0), (-b^p, 0)\} \subseteq \mathbb{Q}^2 \cup \{O\}$.

Paso 2. Como $E_{(a,b,c)}$ es racional, por Teorema 1.5.7 sabemos que $\rho := \rho_{E_{(a,b,c)},p}$ es modular de nivel $N(a,b,c)$ y entonces $\overline{\rho}$ es modular de tipo $(N(a,b,c), 2, 1)$.

Paso 3. Como $p \mid v_q(N(E_{(a,b,c)}))$ para todo q impar entonces por Teorema 1.2.16 y por Observación 4 tenemos que $N(\overline{\rho}) = 2$. Por otro lado, por Teorema 1.2.23, la representación $\overline{\rho}$ resulta irreducible, y además $\overline{\rho}$ es finita en p, por Proposición 1.5.4. Luego, aplicando el Teorema 1.5.6 tenemos que existe una forma nueva $f \in S_2(\Gamma_0(2))$ tal que $\overline{\rho} \sim \overline{\rho}_{f,p}$.

Paso 4. Como $S_2(\Gamma_0(2)) = \{0\}$ entonces tenemos una contradicción.

□

Observación 7. Las soluciones triviales (es decir aquellas soluciones (a,b,c) tales que $abc = 0$) dan lugar a curvas singulares, y por lo tanto no modulares (ver la fórmula de $\Delta(E_{(a,b,c)})$). Es por eso que la prueba tiene éxito. Esto es parte de las posibles obstrucciones del método, que veremos en la Sección 1.7.1.

Observación 8. Notar que en el Paso 2 se tiene asociada una forma $f_{(a,b,c)}$ cuyo nivel depende de la solución, mientras que en el Paso 3, obtenemos una forma modular f cuyo peso y nivel es independiente de (a,b,c) y de p. Esto hace posible luego calcular un espacio particular (en este caso $S_2(\Gamma_0(2))$).

Históricamente, el Paso 2 fue el último en probarse. Más concretamente, Wiles prueba que toda curva elíptica racional semiestable es modular, lo cual era suficiente pues $E_{(a,b,c)}$ es semiestable. Como vimos en el Teorema 1.5.7, este hecho luego se generaliza a todas las curvas racionales.

1.7 Ecuaciones de Fermat Generalizadas

Si bien las ecuaciones diofánticas siempre fueron de gran interés, la demostración del Último Teorema de Fermat, junto con el método modular impulsaron su estudio dando lugar a la resolución de nuevos problemas. En esa dirección, uno de los trabajos más influyentes de la época es el artículo de Darmon y Granville [31]. Allí, los autores exploran sobre diversas ecuaciones, prestándole especial énfasis a las llamadas *Ecuaciones de Fermat Generalizadas* o *Ecuaciones de tipo Fermat*. Dichas ecuaciones son aquellas de la forma

$$Ax^q + By^r = Cz^p, \tag{1.8}$$

con A, B, C números enteros coprimos no nulos. Al igual que para la ecuación (1.6), siempre estamos interesados en las soluciones enteras.

Definición 1.7.1. Una solución (a,b,c) de (1.8) se dice que es *trivial* si $abc = 0$.

Es decir, que si $n \geq 3$, entonces la ecuación (1.6) del Último Teorema de Fermat no tiene soluciones no triviales. En la Observación 5 notamos que podíamos suponer que las coordenadas de las soluciones de (1.6) no tuvieran factores en común, debido a que la ecuación es homogénea. La diferencia más importante a notar entre la ecuación (1.6) y la ecuación (1.8) es que la segunda deja de ser homogénea (y por lo tanto no es una curva plana en $\mathbb{Q}$). Aún así, como más adelante veremos, es

necesario mantener la misma condición entre las coordenadas de las soluciones. Esto da lugar a la siguiente definición.

Definición 1.7.2. Una solución (a, b, c) de (1.8) se dice que es *primitiva* si $\text{mcd}(a, b, c) = 1$.

Una de las conjeturas más importantes acerca de las ecuaciones del tipo (1.8) es la siguiente, que resulta como consecuencia de la conjetura ABC (ver [31]).

Conjetura 1. *Sean A, B, C enteros coprimos dos a dos. Entonces existen finitas ternas (a^q, b^r, c^p) con $abc \neq 0$ y p, q, r primos tales que:*

- $\frac{1}{q} + \frac{1}{r} + \frac{1}{p} < 1$,
- $mcd(a, b, c) = 1$,
- $Aa^q + Bb^r = Cc^p$.

Cabe aclarar, que para la conjetura anterior, contamos a las soluciones del tipo $1^q + 2^3 = 3^2$ sólo una vez. En dirección a la Conjetura 1, fijando también los exponentes de la ecuación (1.8), tenemos el siguiente resultado de vital importancia (ver [31, Teorema 2]).

Teorema 1.7.3 (Darmon-Granville)**.** *Sean A, B, C enteros no nulos y q, r, p enteros tales que $\frac{1}{q} + \frac{1}{r} + \frac{1}{p} < 1$. Entonces la ecuación (1.8) tiene finitas soluciones primitivas.*

La idea de la prueba del teorema anterior consiste en ver que las soluciones primitivas de (1.8) se pueden mapear a puntos de una curva de género $\chi(q, r, p)$, con $\chi(q, r, p)^{-1} = \frac{1}{q} + \frac{1}{r} + \frac{1}{p}$. Luego, si $\chi(q, r, p) > 1$ entonces por el teorema de Faltings (ver [40]) existen finitos puntos en la curva, y por ende finitas soluciones de (1.8). Notar que esto implica que la demostración no es constructiva. Es decir, que no se tiene una cota de la cantidad de soluciones de la ecuación. Con respecto a la Conjetura 1, se han probado algunas versiones para casos particulares, por ejemplo si $A = B = C = 1$ se tienen los siguientes resultados para las infinitas familias de exponentes (q, r, p): Wiles y Taylor-Wiles para el Último Teorema de Fermat (p, p, p) [80, 87], Darmon-Merel para $(p, p, 2)$ y $(p, p, 3)$ [32], Ellenberg y Bennet-Ellenberg-Ng para $(2, 4, p)$ [4, 38], Bennet-Chen para $(2, 6, p)$ [3], etc.

1.7.1 El método modular

Así como la ecuación (1.6) del Último Teorema de Fermat tuvo una generalización natural a la ecuación (1.8), parece apropiado intentar dar con un esquema de receta general para atacar alguna ecuación de tipo Fermat en la cual uno espera que no haya (muchas) soluciones primitivas no triviales.

La estrategia del método modular explicada probablemente con mayor generalidad se puede encontrar en [29]. La idea central es la siguiente: primero, a partir de una solución de la ecuación, construir una representación de Galois dimensión 2 con valores en $\text{GL}_2(\mathbb{F}_p)$ y conductor acotado. Segundo, mostrar que las representaciones construidas provienen de un objeto analítico. Más precisamente, de una forma modular de peso 2 y nivel N igual al nivel de Serre, que debería ser independiente de la solución con la que se comenzó. Finalmente, si uno pudiera probar que todas las representaciones módulo p provenientes de todas las formas modulares de peso 2 y nivel N no son isomorfas a las representaciones construidas a partir de soluciones no triviales, entonces uno podría resolver la ecuación.

En la práctica, la forma en la que se suele asociar una representación residual a una solución de una ecuación diofántica es a partir de las curvas elípticas (como vimos en la prueba del Último Teorema de Fermat. Muchas veces, a tales curvas las llamamos *curvas de Frey*, dado que en el caso

del Último Teorema de Fermat, la curva elíptica $E_{(a,b,c)}$ definida en (1.7) fue estudiada por Frey). Es por esto que a continuación daremos una idea más básica de los pasos a seguir, en la que nos basaremos en el Capítulo 2 para dar una estrategia para atacar las ecuaciones (1) y (2).

Paso 1. A una hipotética solución primitiva adjuntar una curva elíptica (de Frey) E.

Paso 2. Probar que E es modular, es decir, que existe una forma modular (ya sea clásica, de Hilbert, o de Bianchi) natural asociada a E.

Paso 3. Probar que cierta representación residual $\bar{\rho}_E$ adjuntada a E es absolutamente irreducible para concluir (vía resultados de bajada de nivel vistos en la Sección 1.5) que $\bar{\rho}_E$ corresponde a una forma en algún espacio (casi) independiente de la solución con la que comenzamos.

Paso 4. En este paso debemos obtener una contradicción, que provenga de suponer que existe una solución primitiva no trivial. Para eso, debemos probar que ninguna de las formas que se encuentran en los espacios del punto anterior puede estar relacionada con una solución primitiva no trivial.

Cabe destacar que en la prueba del Último Teorema de Fermat, el Paso 4 era directo, pues no había formas para descartar. En general la dimensión del espacio no será cero y por lo tanto habrá que aplicar nuevas estrategias (ver Sección 2.4) para poder dar con el Paso 4.

Observación 9. Sea K el cuerpo de definición de la curva E del Paso 1. Si $K = \mathbb{Q}$, el Paso 2 es directo, por Teorema 1.5.7. En el caso K cuadrático o cúbico totalmente real también está probada la modularidad (ver [34,42]); esto es, que existe una forma modular de Hilbert asociada a nuestra curva. Esto también fue probado recientemente para cuerpos cuárticos totalmente reales que no contengan a $\sqrt{5}$ (ver [8]). En general, se conjetura que toda curva elíptica sobre un cuerpo de números K sea modular. La prueba de dicha conjetura parece aún muy lejana, especialmente para cuerpos imaginarios. Para estos últimos aún no hay nada totalmente demostrado aún para los casos cuadráticos, en donde se espera que toda curva tenga asociada una forma modular de Bianchi. Sin embargo, muy recientemente se logró probar modularidad de curvas elípticas sobre infinitos cuerpos cuadráticos imaginarios (ver [14]).

Como fue mencionado en la Observación 8, la bajada de nivel es un paso fundamental para poder dar luego con la contradicción, y como se pudo ver en la demostración del Último Teorema de Fermat, para ello precisamos (entre otras cosas), que el discriminante de la curva sea de la forma $\Delta(E) = \Delta_1 \Delta_2^p$, donde Δ_1 es algo que no depende de la solución, sino de la ecuación (1.8), mientras que Δ_2 sí depende de la solución y satisface que todo primo que divide a Δ_2 y no a Δ_1 es de reducción multiplicativa para E (ver Teorema 1.2.16 y Proposición 1.5.4). Precisamente esta condición que debe cumplir el discriminante, es la que da una pequeña referencia al modelo de curva que hay que tomar en el Paso 1.

Obstrucciones del método: El primer obstáculo con el que uno se encuentra a la hora de intentar seguir los pasos del método, es que no existe un algoritmo que permita lidiar con el Paso 1. En [29], fantásticamente Darmon explica cómo asociar una curva a cada solución de una ecuación de tipo Fermat para dos familias grandes de exponentes: (p, p, r) y (r, r, p) (aquí p es la variable que se mueve, mientras que r está fijo). Sin embargo, las curvas construidas por Darmon son, en general, superelípticas (curvas que son de género mayor a 1). Recientemente ha habido algunos avances en esta dirección (ver [5, 6, 18]).

Por otro lado, asumiendo que uno es capaz de llevar adelante el Paso 1, probar resultados de modularidad y de "imagen grande" de representaciones no siempre es sencillo. Parte de este trabajo está dedicada a extender representaciones para así poder asegurar su modularidad. Por último, el Paso 4 presenta dos dificultades de carácter muy distinto. Por un lado, calcular el espacio de formas modulares de peso 2 y cierto nivel no siempre es realizable, ya que computacionalmente esto puede

ser muy costoso. En segundo lugar cabe mencionar que (suponiendo que el espacio en cuestión fue calculado) si bien hay distintas técnicas que nos permitirán llevar a cabo el proceso de eliminación de formas (ver Sección 2.4), no siempre serán suficientes para lograr una contradicción (como es el caso de dos importantes ecuaciones (ecuaciones (1.9) y (1.10)) que veremos más abajo). Para ilustrar este último impedimento en el método, analicemos uno de los fenómenos más frecuentes:

Asumamos que queremos estudiar todas las soluciones primitivas de una ecuación de la forma de (1.8), y que el objeto asociado a una solución primitiva (a, b, c) en el Paso 1 es una curva elíptica $E_{(a,b,c)}$. Es claro que existen soluciones triviales, como por ejemplo, la solución $(a, b, c) = (0, 0, 0)$. Cabe preguntarse entonces cómo es posible llegar a una contradicción siendo que sí existen soluciones.

Si bien no hay una receta para encontrar nuestra curva $E_{(a,b,c)}$, en la práctica la construcción de la curva implicará que $E_{(0,0,0)}$ sea singular (como en el caso del Último Teorema de Fermat) y por lo tanto no le corresponderá una forma modular en el espacio en el que estamos buscando. Esto resuelve el problema de la solución $(0, 0, 0)$, pero es común que existan otras soluciones triviales, como es el caso de las ecuaciones que estudiaremos en esta tesis (ecuaciones (1) y (2)), que tienen las soluciones $(a, b, c) = (\pm 1, 0, 1)$ y sin embargo no definen una curva singular (ver Sección 3.1 y 4 respectivamente). Por el contrario, en este caso obtenemos una curva elíptica con multiplicación compleja. La ventaja que tienen nuestras ecuaciones es que, salvo pocas excepciones (ver Lemas 3.1.8 y 4.1.9 respectivamente), las curvas elípticas (no singulares) $E_{(a,b,c)}$ van a tener multiplicación compleja si y sólo sí (a, b, c) es trivial (distinta de $(0, 0, 0)$) ¡Esto nos da una nueva forma de distinguir las soluciones triviales de las demás!

Luego, esto delata aún más la complejidad del Paso 1, pues no sólo precisamos que el objeto asociado sea lo suficientemente adecuado, como para luego poder aplicar bajada de nivel en el Paso 3, sino que además necesitamos que distinga las soluciones triviales de las no triviales[2].

En los Capítulos 3 y 4 veremos que un fenómeno similar ocurrirá con las ecuaciones (1) y (2). Sin embargo, cabe destacar que este no es siempre el caso; es decir que existen ecuaciones diofánticas que a priori se muestran aptas para ser tratadas con el método descripto anteriormente, pero que a posteriori resultan ser de mayor complejidad. A modo de ejemplo: se espera que si $n > 2$ es un número entero, la única solución primitiva no trivial de la ecuación

$$x^2 + y^3 = z^n \tag{1.9}$$

sea la solución de Catalán, $(x, y, z) = (\pm 3, -2, 1)$.

Otro problema aún abierto es probar que si $n > 2$ es un número entero, entonces la única solución primitiva no trivial de la ecuación

$$x^2 - 2 = y^n \tag{1.10}$$

es la solución $(x, y) = (\pm 1, -1)$, cuando n es impar.

Observación 10. En ambos casos, las soluciones *excepcionales* son las problemáticas, ya que la solución $(\pm 3, -2, 1)$ de la ecuación (1.9) define una curva elíptica sin multiplicación compleja (y por lo tanto indistinguible de las otras hipotéticas soluciones) y la solución $(\pm 1, -1)$ de la ecuación (1.10) define una curva elíptica con multiplicación compleja pero sobre un cuerpo cuadrático real, con lo cual sólo la podremos distinguir de otras soluciones para algunos valores primos de n, usando el mismo argumento que veremos en la Observación 16. Más concretamente, el verdadero inconveniente es que ambas soluciones son soluciones para infinitos valores de n, y por lo tanto no es posible, en principio, dar una respuesta afirmativa a las conjeturas para n suficientemente grande[3].

[2] Para ser más precisos, uno espera poder distinguir aquellas soluciones que satisfacen la ecuación para toda variable en el exponente (como las triviales en el caso del Último Teorema de Fermat) de las demás.

[3] En el caso de la ecuación (1.10) sí está probado para n suficientemente grande, pero no vía el método modular, sino utilizando argumentos analíticos.

Capítulo 2

Estrategia general para las ecuaciones (1) y (2)

Comienzo a creer que nunca se puede probar nada.
Estas son hipótesis juiciosas que explican los hechos;
pero veo tan bien que proceden de mí,
que son simplemente una manera de unificar mis conocimientos [...].
Lentos, perezosos, fastidiados,
los hechos se acomodan en rigor al orden que yo quiero darles;
pero éste sigue siendo exterior a ellos.
Tengo la impresión de hacer un trabajo puramente imaginativo.

J.P. Sartre, La Náusea.

El objetivo del presente capítulo es exponer en términos globales las distintas herramientas, junto con una estrategia, que se utilizarán para estudiar las soluciones de las ecuaciones (1) y (2). Como ambas ecuaciones son de tipo Fermat, la política que utilizaremos está basada en el método modular (ver Sección 1.7.1). A continuación exponemos la metodología. El resto del capítulo se dividirá en cuatro secciones, cada una correspondiente a uno de los siguientes pasos.

Cabe aclarar que este capítulo está basado en los artículos [64] y [65], junto con Ariel Pacetti. A su vez, la Sección 2.4 se basa en el artículo en conjunto con Ariel Pacetti y Franco Golfieri [46].

Paso 1 (Construcción). A una supuesta solución primitiva (a, b, c) de la ecuación (1) (respectivamente (2)), le adjuntaremos una curva elíptica, denotada por $E_{(a,b,c)}$ (respectivamente $\widetilde{E}_{(a,b,c)}$) que estará definida sobre el cuerpo cuadrático $K = \mathbb{Q}(\sqrt{d})$. Más aún, $E_{(a,b,c)}$ y $\widetilde{E}_{(a,b,c)}$ resultarán ser una $\mathbb{Q}$-curva de grado 2 y 3 respectivamente (ver Definición 1.1.7) totalmente definida sobre una extensión cuadrática de K.

Paso 2 (Twist, extensión y modularidad). Supongamos por un momento que K es un cuerpo cuadrático imaginario (es decir $d < 0$). Por lo dicho en la Observación 9, no es claro cómo asociar un objeto analítico a nuestra curva $E_{(a,b,c)}$. Dado p un primo, consideramos la representación de Galois p-ádica $\rho_{E_{(a,b,c)},p} : G_K \to \mathrm{GL}_2(\mathbb{Q}_p)$ adjuntada a E. Uno de los resultados principales del presente trabajo consiste en construir de manera explícita un caracter de Hecke $\chi : G_K \to \overline{\mathbb{Q}}^{\times}$ tal que $\rho_{E_{(a,b,c)},p} \otimes \chi$ se extiende a una representación de $G_{\mathbb{Q}}$; es decir, que existe una representación $\tilde{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p)$ tal que $\tilde{\rho}_p|_{G_K} = \rho_{E_{(a,b,c)},p} \otimes \chi$. El mismo razonamiento aplica para la curva $\widetilde{E}_{(a,b,c)}$. Luego, por Teorema 1.5.3, ahora sí tenemos asegurada la existencia de una forma modular clásica, digamos $f_{(a,b,c)}$, cuya representación es isomorfa a la reducción (módulo p) de $\tilde{\rho}_p$. Dicha

forma es entonces el objeto analítico que buscábamos. En particular, presentaremos una fórmula para para el nivel y el Nebentypus de $f_{(a,b,c)}$.

Si K es real, en principio no es necesario utilizar dicha estrategia, ya que la curva estaría definida sobre un cuerpo cuadrático real, y por ende tendría automáticamente una forma modular de Hilbert asociada (ver Observación 9). Sin embargo, como veremos en la Sección 3.4.2, esta estrategia falla computacionalmente, ya que resultan incalculables los espacios de formas modulares de Hilbert del nivel correspondiente (ver Tabla 4.4.1). Por lo tanto, para el caso $d > 0$ también necesitaremos la construcción del caracter χ.

Paso 3 (Bajada de nivel). : Veremos que el discriminante de la curva $E_{(a,b,c)}$ (respectivamente $\widetilde{E}_{(a,b,c)}$) es "casi" una potencia p-ésima, con lo cual, luego de aplicar los teoremas de bajada de nivel, obtendremos una congruencia entre $f_{(a,b,c)}$ y otra forma nueva cuyo nivel sea divisible sólo por $2d$ (respectivamente $6d$). Notar que para aplicar el Teorema 1.5.6 se precisa que la representación residual tenga imagen absolutamente irreducible. Luego, asumiendo dicha hipótesis tendríamos garantizada la existencia de una forma modular nueva f en $S_2(\Gamma_0(N), \varepsilon)$, donde N es un nivel concreto que no depende ni de p ni de (a, b, c), tal que $f_{(a,b,c)} \equiv f \pmod{p}$. Queda así establecido entonces el problema de probar que la reducción módulo p de $\tilde{\rho}_p$ es absolutamente irreducible.

Paso 4 (Contradicción). Este último paso consiste en probar que ninguna de las formas f obtenidas en el paso anterior puede estar relacionada con una solución primitiva no trivial. Para ello deberemos calcular computacionalmente los espacios $S_2(\Gamma_0(N), \varepsilon)$.

2.1 Paso 1: Construcción de la curva elíptica

Como se mencionó en la introducción, para estudiar las soluciones primitivas de (1), en [37] los autores adjuntan a una hipotética solución la curva

$$E_{(a,b,c)} : y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{d}b)x,$$

definida sobre el cuerpo $K = \mathbb{Q}(\sqrt{d})$. Para estudiar la ecuación (2), en [64] proponemos como objeto natural asociado a una solución primitiva (a, b, c) la curva

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{d}xy - 4d(a + b^3\sqrt{d})y = x^3,$$

definida nuevamente sobre $K = \mathbb{Q}(\sqrt{d})$ (generalizando la construcción de [3]).

Sea $\tau \in G_{\mathbb{Q}}$ un elemento cuya restricción a K no coincide con la identidad, y denotemos por ψ_t al caracter cuadrático correspondiente a la extensión cuadrática $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$ vía teoría de cuerpos de clases. Una de las propiedades más importantes que probaremos para las cuevas $E_{(a,b,c)}$ y $\widetilde{E}_{(a,b,c)}$ es que son $\mathbb{Q}$-curvas. Más concretamente, veremos lo siguiente.

Proposición 3.1.1. La curva elíptica $E_{(a,b,c)}$ es una $\mathbb{Q}$-curva totalmente definida sobre el cuerpo $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$. Más aún, $\tau(E_{(a,b,c)})$ es isógena al twist cuadrático $E_{(a,b,c)} \otimes \psi_{-2}$.

Proposición 4.1.1. La curva elíptica $\widetilde{E}_{(a,b,c)}$ es una $\mathbb{Q}$-curva totalmente definida sobre el cuerpo $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$. Más aún, $\tau(\widetilde{E}_{(a,b,c)})$ es isógena al twist cuadrático $\widetilde{E}_{(a,b,c)} \otimes \psi_{-3}$.

El siguiente resultado será de gran utilidad luego. Su demostración se desprende fácilmente de la hipótesis de primitividad de la solución.

Lema 2.1.1. *Sea (a, b, c) una solución primitiva de la ecuación (1) o (2) con $p > 3$. Entonces*

- *$mcd(ac, d) = 1$.*

- *Si* $d \equiv 3, 5, 7 \pmod 8$ *entonces uno de* $\{a, b\}$ *es par y el otro impar.*
- *Si* 2 *no se parte en* K *(i.e.* $d \not\equiv 1 \pmod 8$*), entonces* c *es impar.*
- *Si* 3 *no se parte en* K *(i.e.* $d \not\equiv 1 \pmod 3$*), entonces* c *no es divisible por* 3*.*

2.2 Paso 2: Construcción del caracter de Hecke (twist), extensión y modularidad

Recordemos que este es el paso encargado de trasladar la información de la curva $E_{(a,b,c)}$ (o $\widetilde{E}_{(a,b,c)}$) hacia una forma modular $f_{(a,b,c)}$.

Como se mencionó en el Paso 2 de nuestra estrategia general, precisamos la construcción de un caracter de Hecke χ por el cual luego twistearemos para extender la representación. A continuación veremos el procedimiento con el cual se definirá dicho caracter.

Dado un cuerpo de números L, denotemos por $\mathbb{I}_L$ a su grupo de idèles y por $\mathrm{Cl}(L)$ a su grupo de clases. La teoría de cuerpos de clases relaciona caracteres finitos de G_L con caracteres finitos del grupo de idèles $\mathbb{I}_L$. Haremos uso constante de dicha relación, denotando con la misma letra ambas encarnaciones del mismo objeto (y esperando no generar confusión por ello).

Sea $\tau \in G_{\mathbb{Q}}$ y $\chi : \mathbb{I}_L \to \overline{\mathbb{Q}}^{\times}$ un caracter de Hecke de orden finito. Denotamos por ${}^{\tau}\chi$ al caracter de Hecke dado en un elemento $\alpha \in \mathbb{I}_L$ por

$$ {}^{\tau}\chi(\alpha) = \chi(\tau(\alpha)). \tag{2.1}$$

Vía teoría de cuerpos de clases, el caracter ${}^{\tau}\chi$ corresponde al caracter en G_L dado por ${}^{\tau}\chi(\sigma) = \chi(\tau\sigma\tau^{-1})$. En general, si $\rho : G_L \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ es una representación de Galois, y $\tau \in G_{\mathbb{Q}}$, denotamos por ${}^{\tau}\rho$ a la representación de Galois cuyo valor en $\sigma \in G_L$ está dado por ${}^{\tau}\rho(\sigma) = \rho(\tau\sigma\tau^{-1})$.

Si K es una extensión cuadrática de $\mathbb{Q}$, una representación $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ se extiende a una representación de dimensión 2 de $G_{\mathbb{Q}}$ si y sólo si ${}^{\tau}\rho \sim \rho$, donde $\tau \in G_{\mathbb{Q}}$ es cualquier elemento cuya restricción a G_K no es la identidad (aunque este resultado es bien conocido por los expertos, una prueba será dada en el Teorema 3.2.9).

Sea t un entero, y sea ψ_t el caracter de $G_{\mathbb{Q}}$ correspondiente a la extensión cuadrática $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. La Proposición 3.1.1 implica que para cualquier primo p, ${}^{\tau}\rho_{E_{(a,b,c)},p}$ es isomorfa a $\rho_{E_{(a,b,c)},p} \otimes \psi_{-2}$, mientras que la Proposición 4.1.1 implica que para cualquier primo p, ${}^{\tau}\rho_{\widetilde{E}_{(a,b,c)},p}$ es isomorfa a $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \psi_{-3}$. Si construimos un caracter de Hecke $\chi_t : G_K \to \overline{\mathbb{Q}}^{\times}$ que satisfaga que

$$ {}^{\tau}\chi_t = \chi_t \cdot \psi_{-t}$$

(como caracteres de G_K) entonces la representación twisteada $\rho_{E_{(a,b,c)},p} \otimes \chi_2$ (respectivamente la representación $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3$) es isomorfa a ${}^{\tau}(\rho_{E_{(a,b,c)},p} \otimes \chi_2)$ (respectivamente a ${}^{\tau}(\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi_3)$) y luego ésta se extiende a una representación de dimensión 2 de $G_{\mathbb{Q}}$ (ver Teorema 3.2.9 y 4.2.4). Más aún, una descripción explícita de χ y de su conductor permite dar una fórmula para el nivel y el Nebentypus de la representación extendida. Esto da lugar al siguiente problema.

Problema: Sea ψ_t el caracter cuadrático de $G_{\mathbb{Q}}$ correspondiente a la extensión $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$. Encontrar un caracter de Hecke χ_t de G_K tal que ${}^{\tau}\chi_t = \chi_t \cdot \psi_{-t}$.

Uno de los resultados principales es dar una solución al problema planteado para $t = 2$ (correspondiente a la ecuación (1)) y para t un primo congruente a 3 módulo 4 (correspondiente a la

ecuación (2)). Para explicar cómo funciona nuestra construcción, consideremos la siguiente sucesión exacta corta

$$0 \longrightarrow L^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times (L \otimes \mathbb{R})^\times) \longrightarrow \mathbb{I}_L \xrightarrow{\mathrm{Id}} \mathrm{Cl}(L) \longrightarrow 0. \tag{2.2}$$

Comenzamos definiendo el caracter de Hecke χ_t en elementos del primer término de la sucesión y luego lo extendemos a elementos de $\mathbb{I}_L$ tales que vía el mapa Id son representantes del grupo de clases. En esta instancia nos gustaría hacer una observación importante, pues la imagen puede ser un poco engañosa: nuestro caracter χ_t no será trivial en las unidades (el primer término de la secuencia), ¡Con lo cual no definirá un caracter de todo el grupo de clases! Será en cambio un caracter del grupo de clases de rayos.

Recordar que los caracteres de Hecke son triviales en los elementos de $L^\times$, con lo cual sólo resta definir nuestro caracter en unidades locales (que determinan el comportamiento de la ramificación de la extensión abeliana dada por el núcleo del caracter χ_t). Notar que $(\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times (L \otimes \mathbb{R})^\times) \cap L^\times = \mathscr{O}_L^\times$, con lo cual hay una condición de compatibilidad que deberá ser comprobada.

Condición de compatibilidad: el producto de las componentes locales evaluadas en una unidad es igual a 1, i.e.

$$\prod_v \chi_{t,v}(\epsilon) = 1 \tag{2.3}$$

para todo $\epsilon \in \mathscr{O}_L^\times$. Verificar esta propiedad es lo que hace a la construcción de los caracteres de Hecke complicada en general.

En nuestro caso, el cuerpo L es el cuerpo cuadrático K, por lo que su conjunto de unidades es bien conocido en el caso de ser imaginario. Nuestro caracter χ_t ramificará a lo sumo en los primos impares que ramifiquen en $K/\mathbb{Q}$ (con exponentes 1 en el conductor), en los primos que dividen a 2 y en los primos que dividen a t.

Sea $\mathscr{N} : \mathbb{I}_K \to \mathbb{I}_\mathbb{Q}$ la función norma. La manera de verificar la condición de compatibilidad de nuestro caracter (y otras propiedades que satisface) es vía la construcción de un caracter de Hecke racional auxiliar ε_t (que resultará ser el Nebentypus de nuestra representación extendida) no ramificado fuera de $2td$, con las siguientes propiedades que relacionan ε_t con χ_t:

1. El caracter local $\chi_{t,\mathfrak{p}}$ satisface que ${}^\tau\chi_{t,\mathfrak{p}} = \chi_{t,\mathfrak{p}} \cdot ((\psi_{-t})_p \circ \mathscr{N})$.

2. Sea p un primo impar ramificado en $K/\mathbb{Q}$ y sea $\mathfrak{p}$ el único primo de $\mathscr{O}_K$ que lo divide. Luego, bajo el isomorfismo de cuerpos $\mathscr{O}_K/\mathfrak{p} \to \mathbb{Z}/p$, el caracter local $\chi_{t,\mathfrak{p}}$ es $\varepsilon_{t,p}\delta_p$, donde δ_p es el caracter cuadrático de $(\mathbb{Z}/p)^\times$.

3. Una condición extra en primos que dividen a 2, de manera que la condición de compatibilidad valga (una condición similar a (2.3) para las unidades de K).

4. Para todo $\sigma \in G_K$, $\chi_t(\sigma)^2 = \varepsilon_t(\sigma)$ (o en términos de idèles, $\chi_t^2 = \varepsilon_t \circ \mathscr{N}$).

Veamos el rol que juega cada propiedad impuesta. La primera condición es necesaria para que χ_t resuelva localmente el problema. La segunda condición juega un rol crucial a la hora de probar la condición de compatibilidad (vía reciprocidad cuadrática). Es una versión local de la última.

Lema 2.2.1. *Sea $p \nmid t$ un primo impar racional y $\mathfrak{p}$ un primo de $\mathscr{O}_K$ que lo divide. Entonces la segunda condición implica que la cuarta condición se satisfaga localmente, a saber, $\chi_{t,\mathfrak{p}}^2 = \varepsilon_{t,p} \circ \mathscr{N}$.*

Demostración. Para primos $\mathfrak{p} \nmid 2td$, ambos caracteres son triviales, con lo cual el enunciado se satisface trivialmente. Para primos impares $\mathfrak{p}$ (de norma p) tales que $\mathfrak{p} \nmid t$ y $\mathfrak{p} \mid d$, recordar que la restricción de $\varepsilon_{t,p}$ a $G_{K_\mathfrak{p}}$ es igual a (como caracteres de Hecke) $\varepsilon_{t,p} \circ \mathscr{N}$, donde $\mathscr{N} : K_\mathfrak{p} \to \mathbb{Q}_p$ es la

norma. Como p ramifica en $K/\mathbb{Q}$, la norma local (módulo $\mathfrak{p}$) está dada por $x \mapsto x^2$, con lo cual vale la igualdad

$$\chi^2_{t,\mathfrak{p}}(x) = \varepsilon^2_{t,p}(x) = \varepsilon_{t,p}(x^2) = \varepsilon_{t,p} \circ \mathscr{N}(x).$$

□

La tercera condición es necesaria para probar la condición de compatibilidad. Las primeras tres condiciones son necesarias para definir el caracter χ_t en elementos del primer término de (2.2). La última condición será utilizada para extender el caracter a los idèles que son representantes del grupo de clases de K (vía Id).

La estrategia general para probar la existencia de los caracteres ε_t y χ_t con las propiedades anteriores es partir el conjunto de los primos impares $\{p : p \text{ primo impar que ramifica en } K/\mathbb{Q}\}$ en cuatro conjuntos. Más concretamente, para $t = 2$ serán divididos dependiendo de su congruencia módulo 8, mientras que para t primo impar, serán divididos dependiendo de cuándo p es un cuadrado módulo t o no y si p es un cuadrado módulo 4 o no. Luego, para los primos p en cada conjunto daremos una definición explícita del caracter local $\varepsilon_{t,p}$ y $\chi_{t,\mathfrak{p}}$, satisfaciendo las anteriores cuatro propiedades. La descripción (y la prueba) dependen de si $t = 2$ o t es un primo impar congruente a 3 módulo 4, con lo cual cada caso será considerado en su capítulo correspondiente. Para alivianar la notación, en cada capítulo eliminaremos a t de la notación como subíndice de los caracteres.

2.3 Paso 3: Bajada de nivel de Ribet

En esta sección se exponen los resultados que se utilizarán para ver que la reducción de la representación extendida $\tilde{\rho}_p$ es absolutamente irreducible. Para ver que $\overline{\tilde{\rho}_p}$ es absolutamente irreducible en particular, es suficiente probar que $\rho_{E_{(a,b,c)},p}$ (respectivamente $\rho_{\widetilde{E}_{(a,b,c)},p}$) es absolutamente irreducible. Para ello, un importante resultado es el siguiente.

Proposición 2.3.1 (Ellenberg)**.** *Sea K cuerpo cuadrático y E/K una $\mathbb{Q}$-curva. Supongamos que E tiene reducción multiplicativa en un primo $\mathfrak{q} \nmid 6$. Entonces si $p > 7$ y $p \neq 13$, $\rho_{E,p}$ es absolutamente irreducible.*

Demostración. Ver [38, Proposición 3.2]. □

Luego, para garantizar imagen absolutamente irreducible, resta considerar el caso en donde las curvas $E_{(a,b,c)}$ y $\widetilde{E}_{(a,b,c)}$ no tengan un primo $\mathfrak{q} \nmid 6$ de reducción multiplicativa. Como veremos en los Lemas 3.1.3 y 4.1.2, estos casos se corresponden exactamente con las soluciones (a, b, c) en donde c está soportado en $\{2, 3\}$ (es decir que los únicos primos que pueden dividir a c son 2 y 3). Para el caso de la ecuación (2) veremos que esto no puede ocurrir si p es suficientemente grande (ver Proposición 4.3.4). Para el caso de la ecuación (1) tenemos el siguiente resultado, cuya prueba será expuesta en la Sección 3.2.2.

Proposición 3.3.3. Sea $K = \mathbb{Q}(\sqrt{d})$. Si (a, b, c) es una solución no primitiva de (1) tal que c está soportado en $\{2, 3\}$ entonces existe una cota N_K tal que si $p > N_K$ la representación $\rho_{E_{(a,b,c)},p}$ tiene imagen absolutamente irreducible.

A veces la constante N_K de la proposición anterior puede resultar un poco grande. En el caso en que K sea cuadrático real el siguiente resultado será de gran utilidad para bajar el valor de la cota.

Teorema 2.3.2 (Freitas-Siksek)**.** *Sea K real cuadrático, ϵ una unidad fundamental de K y sea*

$$B = \mathscr{N}(mcm((\mathscr{N}(\epsilon^{12}) - 1), (\mathscr{N}(\bar{\epsilon}^{12}) - 1))).$$

Sea $p \nmid B$ un primo no ramificado en $K/\mathbb{Q}$ tal que $p \geq 17$ o $p = 11$. Sea E/K una curva elíptica y $\mathfrak{q} \nmid p$ un primo de buena reducción para E. Sea

$$P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}(E)X + \mathscr{N}(\mathfrak{q})$$

el polinomio característico del Frobenius para E en $\mathfrak{q}$. Sea $r \geq 1$ un entero tal que $\mathfrak{q}^r$ es principal. Si E es semiestable en todos los primos $\mathfrak{p}$ que dividen a p y

$$p > Res(P_{\mathfrak{q}}(X), X^{12r} - 1),$$

entonces $\bar{\rho}_{E,p}$ es irreducible.

Demostración. Ver [43, Teorema 1]. □

Observación 11. Notar que el resultado anterior utiliza un primo de buena reducción para la curva. Para usar más de un primo (por ejemplo, si se quiere refinar aún más la cota) se razona de la siguiente forma: tomamos $q > 5$ inerte en K y supongamos que $p > 71$. Si q es de buena reducción entonces utilizamos el teorema anterior. Caso contrario, q será de reducción multiplicativa (ver Lema 3.1.3, respectivamente Lema 4.1.2). Por lo tanto, por [63, Teorema 1.2] la representación es irreducible.

2.4 Paso 4: Test para descartar formas

Recordemos que en el Paso 1 se comienza suponiendo que existe una solución primitiva. Luego, si queremos probar la no existencia de soluciones primitivas y no triviales entonces suponiendo esta última condición, debemos llegar, como bien lo indica el nombre del Paso 4, a una contradicción. Para obtener dicho absurdo, deberemos eliminar la posible existencia de una forma $f \in S_2(\Gamma_0(N), \varepsilon)$ que proviene de tal solución (a, b, c). Con lo cual, lo que se expondrá en la presente sección serán algunos métodos para descartar posibles formas f.

2.4.1 Truco de Mazur

Sea f en un espacio $S_2(\Gamma_0(N), \varepsilon)$ como el que se obtiene en el Paso 3 de la estrategia general, luego de haber aplicado la bajada de nivel a una representación proveniente de una solución (a, b, c). Por simplicidad de notación asumiremos que (a, b, c) es solución de (1), por lo que utilizaremos sólo la curva $E_{(a,b,c)}$; el mismo análisis funciona para la ecuación (2), reemplazando en todos lados $E_{(a,b,c)}$ por $\widetilde{E}_{(a,b,c)}$.

Sean p y q números primos distintos tales que q no ramifica en $K/\mathbb{Q}$. Sea $\mathfrak{q}$ un primo en K que divide a q. Denotemos por f^{BC} el cambio de base de f a K. Recordemos que la q-expansión de f^{BC} está dada por la siguiente regla (ver por ejemplo [22, pág. 413] y sus referencias):

$$a_{\mathfrak{q}}(f^{\mathrm{BC}}) = \begin{cases} a_q(f) & \text{si } \mathscr{N}(\mathfrak{q}) = q, \\ a_q(f)^2 - 2q\varepsilon(q) & \text{si } \mathscr{N}(\mathfrak{q}) = q^2, \end{cases} \tag{2.4}$$

donde $\mathscr{N}$ es la función norma. La idea detrás del truco de Mazur es estudiar la ecuación en cuestión módulo q, para obtener información de $a_{\mathfrak{q}}(E_{(a,b,c)})$. Para cada punto $(\tilde{a}, \tilde{b}, \tilde{c}) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\}$, consideramos la curva $E_{(\tilde{a},\tilde{b},\tilde{c})}$ sobre $\mathbb{F}_q$. Entonces, algunas de las siguientes dos opciones ocurre:

- La curva $E_{(\tilde{a},\tilde{b},\tilde{c})}$ es no singular, en cuyo caso si (a, b, c) es una solución entera que se reduce a $(\tilde{a}, \tilde{b}, \tilde{c})$, debe valer que $a_{\mathfrak{q}}(E_{(a,b,c)}) = a_{\mathfrak{q}}(E_{(\tilde{a},\tilde{b},\tilde{c})})$ y más aún,

$$\chi(\mathfrak{q})a_{\mathfrak{q}}(E_{(\tilde{a},\tilde{b},\tilde{c})}) \equiv a_{\mathfrak{q}}(f^{\mathrm{BC}}) \pmod{p},$$

o

- La curva $E_{(a,b,c)}$ tiene mala reducción en $\mathfrak{q}$, en cuyo caso estamos justamente en las hipótesis de bajada de nivel y
$$a_q(f)^2 \equiv \varepsilon^{-1}(q)(q+1)^2 \pmod{p}.$$

La prueba de este último hecho (bien conocida por los expertos) se puede encontrar en [3, Lema 24]. En ambos casos, cada lado de la congruencia puede ser computado, y si resultan ser diferentes, obtenemos una lista finita de candidatos para el primo p, que debe dividir a su diferencia. Este método es muy poderoso, y corriéndolo para unos pocos valores de q nos permite descartar (para p más grande que la diferencia) todas las formas cuyo cuerpo de coeficientes no contenga a $\mathbb{Q}(\chi)$. Con el fin de facilitar futuras referencias, enunciamos a continuación lo anteriormente explicado en la siguiente proposición.

Proposición 2.4.1 (Truco de Mazur)**.** *Sea (a,b,c) una solución primitiva y $f \in S_2(\Gamma_0(N),\varepsilon)$ tal que $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi} \sim \overline{\rho}_{f,K,p}$, donde $\rho_{f,K,p} = \rho_{f,p}|_{G_K}$. Sea q un primo racional tal que $q \nmid pN$. Sea $\mathfrak{q}$ un primo de $\mathscr{O}_K$ que divide a q y definimos*

$$B(q,f;a,b,c) := \begin{cases} \mathscr{N}(a_{\mathfrak{q}}(E_{(a,b,c)})\chi(\mathfrak{q}) - a_q(f)) & \text{si } q \nmid c \text{ y } q \text{ se parte en } K, \\ \mathscr{N}(a_q(f)^2 - a_q(E_{(a,b,c)})\chi(q) - 2q\varepsilon(q)) & \text{si } q \nmid c \text{ y } q \text{ es inerte } K, \\ \mathscr{N}(\varepsilon^{-1}(q)(q+1)^2 - a_q(f)^2) & \text{si } q \mid c. \end{cases}$$

Entonces $p \mid B(q,g;a,b,c)$.

La manera de aplicar la proposición anterior es la siguiente: dado un primo q que no divida a $2d$ (respectivamente $6d$ si trabajamos con la ecuación (2)), se define

$$C(q,f) = \prod_{(a,b,c)\in\mathbb{F}_q^3\setminus\{(0,0,0)\}} B(q,f;a,b,c).$$

Entonces p divide a $C(q,f)$, que ya no depende de (a,b,c). Luego, calculando algunos valores de $C(q.f)$ para distintos primos q y tomando el máximo común divisor obtenemos en algunos casos una cota para p (más precisamente, un conjunto finito de valores que puede tomar p). Sin embargo, en algunas situaciones sucede que $C(q,f)$ es siempre igual a cero, en cuyo caso no podemos descartar la forma f para ningún primo p. Como se mencionó al comienzo de la sección, la misma estrategia se utiliza para estudiar las soluciones de (2), utilizando la curva $\widetilde{E}_{(a,b,c)}$.

Recordar que las soluciones triviales $(\pm 1, 0, 1)$ se corresponderán con formas $f_\pm$ con multiplicación compleja (Corolarios 3.3.2, 4.3.2). Como son soluciones para todos los valores de p, la Proposición 2.4.1 implica que $p \mid C(q,f_\pm)$ para todos los primos p, con lo cual $C(q,f_\pm) = 0$ para todo q. En particular, el método de Mazur fallará a la hora de intentar descartar dichas formas con multiplicación compleja.

Sin embargo, las formas modulares con multiplicación compleja tienen la propiedad de que la imagen de su representación de Galois no es tan grande como se espera (su imagen vive en el normalizador de un grupo de Cartan, por Proposición 1.2.20). En particular, si podemos probar que dada una solución primitiva no trivial (a,b,c) existe un primo $q > 3$ que divide a c entonces un resultado de Ellenberg (Teorema 2.4.8) implicará que nuestra representación $\tilde{\rho}_p$ tiene imagen proyectiva residual suryectiva para p suficientemente grande, y por lo tanto no puede ser congruente a una forma con multiplicación compleja. Luego, será factible probar la no existencia de soluciones primitivas no triviales (para p suficientemente grande). Esto da lugar al siguiente problema.

Problema : ¿Cómo podemos descartar las formas con multiplicación compleja cuando c está soportado en $\{2,3\}$?

Como fue mencionado en la sección anterior, este problema es de fácil solución en el caso de la ecuación (2), pues para p suficientemente grande c nunca estará soportado en $\{2,3\}$. Para el

caso de la ecuación (1) este es un problema muy delicado, que por el momento no tenemos una respuesta general. Sin embargo, para los ejemplos de esta tesis, veamos que algunas ideas sencillas son suficientes para obtener resultados.

Supongamos que (a, b, c) es una solución primitiva no trivial de (1) con c divisible por 3 (sólo posible si $d \equiv 1 \pmod 3$, por Lema 2.1.1). Entonces la forma modular $f_{(a,b,c)}$ (adjuntada a la extensión de $\rho_{E_{(a,b,c)},p} \otimes \chi$) tiene nivel divisible por 3 (ver Teorema 3.2.9) y es congruente a una forma modular f cuyo nivel no es divisible por 3 (ver Corolario 3.3.1). En particular, estamos en las hipótesis de "bajada de nivel" en 3, con lo cual, por Proposición 2.4.1,

$$\mathscr{N}(\varepsilon^{-1}(3)(3+1)^2 - a_3(f)^2) \equiv 0 \pmod p. \tag{2.5}$$

En la práctica, esto nos dará una cota para los posibles exponentes p. Luego, resta analizar el caso en donde c sea una potencia de 2. Por Lema 2.1.1, si $d \not\equiv 1 \pmod 8$ entonces c no puede ser par. Si $d \equiv 1 \pmod 8$ entonces $2 \mid ab$, en cuyo caso c es impar, o $2 \nmid ab$, en cuyo caso c es par. Más adelante veremos que cuando $d \equiv 1 \pmod 8$, hay dos posibles exponentes para los primos que dividen a 2 en el conductor de $E_{(a,b,c)}$ (dependiendo de la paridad de ab; ver Lema 3.1.5 y su prueba). Entonces, en el espacio correspondiente a las soluciones en donde $2 \mid ab$ (donde residen las formas $f_\pm$), sabemos que c es impar, con lo cual no estamos en el caso en que c sea una potencia de 2 (c no puede ser 1, pues buscamos soluciones no triviales). Luego, en dicho espacio podremos utilizar el resultado de Ellenberg. Finalmente, en el espacio en donde viven las soluciones con c una potencia de 2 no se encuentran las soluciones triviales, con lo cual no hay una razón obvia por la cual el truco de Mazur no funcione allí. Aún así, ocasionalmente habrá formas provenientes de soluciones no triviales que pasen sistemáticamente el truco de Mazur. Es por eso que a continuación expondremos otros métodos que serán útiles a la hora de descartar formas modulares.

2.4.2 El tipo local

Sea K_λ una extensión finita de $\mathbb{Q}_\ell$. La correspondencia local de Langlands da una biyección entre el conjunto de representaciones automorfas de $\mathrm{GL}_2(K_\lambda)$ y el conjunto de representaciones del grupo de Weil-Deligne de K_λ (seguiremos la normalización de Carayol de [15]). Recordemos que una representación de Weil-Deligne consiste de una representación compleja ρ de dimensión 2 del grupo de Weil $W(K_\lambda)$, junto con un operador de monodromía N. Sea $\omega_1 : W(\mathbb{Q}_\ell) \to \mathbb{C}^\times$ el caracter no ramificado que manda el Frobenius a $\|\ell\|_\ell$ (y usamos la misma notación para su restricción a $W(K_\lambda)$). Para $\ell \neq 2$, hay tres tipos locales para una representación de Weil-Deligne ρ con Nebentypus trivial:

1. **Serie Principal**: El endomorfismo es $N = 0$ y $\rho = \chi \oplus \chi^{-1}\omega_1^{1-k}$ para algún casi caracter $\chi : W(K_\lambda)^{\mathrm{ab}} \to \mathbb{C}^\times$.

2. **Steinberg o Representación especial**: El endomorfismo N está dado por la matriz $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ y la representación ρ es $\omega_1^r \left(\begin{smallmatrix} \chi\omega_1 & 0 \\ 0 & \chi \end{smallmatrix}\right)$ para algún casi caracter $\chi : W(K_\lambda) \to \mathbb{C}^\times$.

3. **Representación Supercuspidal**: El endomorfismo es $N = 0$ y $\rho = \mathrm{Ind}_{W(E)}^{W(K_\lambda)} \varkappa$, donde E es una extensión cuadrática de K_λ y $\varkappa : W(E)^{\mathrm{ab}} \to \mathbb{C}^\times$ es un casi caracter que no factoriza por el mapa norma con un casi caracter de $W(K_\lambda)^{\mathrm{ab}}$.

Observación 12. Hay una gran diferencia entre una representación serie principal y una supercuspidal, ya que la primera es reducible (y descomponible) mientras que la segunda no.

El tipo de inercia local de una representación automorfa de $\mathrm{GL}_2(\mathbb{Q}_p)$ es la clase de isomorfismo de su restricción al subgrupo de inercia (que está relacionado con la restricción de su contraparte de Weil-Deligne).

Proposición 2.4.2. *Sea $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ una representación de Galois modular, y sea λ un primo de K cuya característica residual es coprima con p. Si el tipo local de ρ en λ es una serie principal (respectivamente supercuspidal) dada por un caracter χ (respectivamente $\varkappa$) de orden n coprimo con p entonces su reducción también es de tipo serie principal (respectivamente supercuspidal) dada por un caracter de orden n.*

Demostración. Denotemos por K_λ la completación de K en el ideal λ. Por teoría local de cuerpos de clases, el caracter χ que aparece en la restricción $\rho|D_\lambda$ a un grupo de descomposición en λ proviene de un caracter de Hecke $\chi : W(K_\lambda) \to \overline{\mathbb{Q}}_p$. El núcleo del mapa reducción $\overline{\mathbb{Z}}_p \to \overline{\mathbb{F}}_p$ es un pro-p-grupo. Como el orden de χ es coprimo con p, el caracter reducido $\tilde{\chi}$ tiene el mismo orden que χ, probando así la primera afirmación del enunciado. En el caso supercuspidal, el caracter residual $\tilde{\varkappa}$ tiene el mismo orden que $\varkappa$, lo cual nos conduce a probar que no factoriza por el mapa norma (por lo que la representación residual también sería irreducible). Si $\tilde{\varkappa} = \tilde{\theta} \circ \mathscr{N}$, para algún caracter $\tilde{\theta} : W(E) \to \overline{\mathbb{F}}_p$, sea $\theta : W(E) \to \overline{\mathbb{Q}}_p$ el levantado del Teichmuller de $\tilde{\theta}$. Entonces $\kappa = \theta \circ \mathscr{N}$ (pues ambos caracteres tienen orden coprimo con p y sus reducciones coinciden). □

Observación 13. Las representaciones ρ que aparecen durante este trabajo provienen de $\mathbb{Q}$-curvas (cuya modularidad será probada vía el Teorema 1.5.3). Como el cuerpo de coeficientes de una curva elíptica es el de los racionales, cualquier caracter (tanto en el tipo serie principal o el tipo supercuspidal) que aparecen en un primo de mala reducción tiene orden n con $\varphi(n) \leq 2$. En particular, $n \in \{1, 2, 3, 4, 6\}$. Luego para $p > 3$, el tipo local se preserva por congruencias.

El tipo de ℓ-inercia de la representación p-ádica ρ es la clase de isomorfismo de la restricción de ρ al grupo de descomposición de ℓ. Existe un algoritmo (basado en [59]) que está implementado en `Sage` y `Magma`, que dada una forma nueva racional y un primo que divide al nivel calcula su tipo local. El problema es que con frecuencia el espacio $S_2(\Gamma_0(N), \varepsilon)$ tiene dimensión muy grande, haciendo que los cálculos sean irrealizables (desde un punto de vista computacional).

2.4.3 El argumento simpléctico

El argumento simpléctico es una herramienta poderosa para estudiar congruencias entre curvas elípticas. La idea es considerar no sólo cuándo dos curvas tienen representaciones residuales isomorfas, sino añadir también información en cómo el isomorfismo relaciona sus Weil pairings. Su primera versión (y aplicación) aparece en [52] (ver [41] para las distintas aplicaciones históricas y los últimos resultados). A continuación enunciaremos dos instancias del argumento simpléctico que serán utilizadas luego en la Sección 4.3.1 (ver la Sección 1.1.2 para la definición de (anti) simplécticamente isomorfo).

Teorema 2.4.3. *Sean $\ell \neq p$ primos con $p \geq 3$. Sean E, E' curvas elípticas sobre $\mathbb{Q}_\ell$ con reducción multiplicativa. Supongamos que $E[p] \simeq E'[p]$ como $G_{\mathbb{Q}_\ell}$-módulos. Más aún, asumamos que $p \nmid v_\ell(\Delta(E))$. Entonces $p \nmid v_\ell(\Delta(E'))$ y además, $E[p]$ y $E'[p]$ son simplécticamente isomorfos si y sólo si $\left(\frac{v_\ell(\Delta(E))/v_\ell(\Delta(E'))}{p}\right) = 1$.*

Más aún, $E[p]$ y $E'[p]$ no pueden ser simultáneamente simplécticamente isomorfas y anti simplécticamente isomorfas.

Demostración. Ver [52] (y [41, Teorema 13]). □

Además precisamos una versión para extensiones ramificadas. Resultados en esta dirección se pueden ver en [48]. Recordemos que si K es un cuerpo local y E/K es una curva elíptica con reducción potencialmente buena, el *defecto* de E es el grado de la extensión mínima de K^{ur} donde E tiene buena reducción.

Teorema 2.4.4. *Sea $\ell \equiv 2 \pmod 3$ un número primo, K una extensión ramificada de $\mathbb{Q}_\ell$ y sea $p \neq \ell$ un primo, con $p \geq 5$. Sean E, E' dos curvas elípticas sobre K con un punto de orden 3 en $K_\mathfrak{l}$ (donde $\mathfrak{l}$ es un primo en K que divide a ℓ), con reducción potencialmente buena y defecto 3. Sea $r = 0$ si $v(\Delta(E)) \equiv v(\Delta(E')) \pmod 3$ y $r = 1$ en caso contrario. Supongamos que $E[p]$ y $E'[p]$ son isomorfos como G_K-módulos. Entonces $E[p]$ y $E'[p]$ son simplécticamente isomorfos si y sólo si $\left(\frac{\ell}{p}\right)^r = 1$.*

Más aún, $E[p]$ y $E'[p]$ no pueden ser simultáneamente simplécticamente isomorfas y anti simplécticamente isomorfas.

Demostración. La prueba es una mímica del Caso 1 de la página 79 de [41]. Una propiedad importante de nuestras hipótesis es que el hecho de que $\ell \equiv 2 \pmod 3$ y que $K/\mathbb{Q}_\ell$ es ramificado, implica que no hay raíces cúbicas de la unidad en K (además de la trivial), con lo cual la extensión de K obtenida de añadir los puntos de p-torsión es no abeliana (por [41, Corolario 5]).

El hecho de que no haya raíces cúbicas de la unidad en K, implica que elevar al cubo es una biyección en los cuerpos residuales, con lo cual el Lema 15 de loc.cit. se sigue sin ningún cambio. En particular, la misma matriz de representación del Frobenius y la inercia del Lema 25 se cumplen. Con estos ingredientes en las manos, es claro que la prueba del Caso 1 de la página 79 de [41] se sigue mutatis mutandis. □

2.4.4 Usando la información de la 3-torsión

Consideremos la siguiente situación general: Sean E y E' curvas elípticas racionales. Sea N un número entero. Supongamos que E tiene un punto de N-torsión y que para un primo grande p existe un isomorfismo de módulos de Galois $E[p] \simeq E'[p]$ ¿Cómo afecta el punto de N-torsión de E a la curva E'?

Teorema 2.4.5. *Sea K un cuerpo de números, E/K y E'/K curvas elípticas. Supongamos que E tiene un punto K-racional de orden N y que existe un ideal primo $\mathfrak{q}$ de buena reducción para E' tal que $a_\mathfrak{q}(E') \not\equiv \mathcal{N}(\mathfrak{q}) + 1 \pmod N$. Entonces si $p > \max\{\mathcal{N}(\mathfrak{q}) + 1 + 2\sqrt{\mathcal{N}(\mathfrak{q})}, 4\sqrt{\mathcal{N}(\mathfrak{q})}\}$, los G_K-módulos $E[p]$ y $E'[p]$ no son isomorfos.*

Demostración. Supongamos que $E[p]$ y $E'[p]$ son isomorfos como G_K-módulos para algún primo $p > 4\sqrt{\mathcal{N}(\mathfrak{q})}$. Como $p > 3$, la Proposición 2.4.2 y la Observación 13 implican que la curva E tiene buena reducción o reducción multiplicativa en el primo $\mathfrak{q}$ (porque una curva con reducción aditiva o potencialmente multiplicativa no puede tener buena reducción módulo un primo impar). Si E tiene reducción multiplicativa en $\mathfrak{q}$, entonces el hecho de que $\rho_{E',p}$ sea no ramificada en $\mathfrak{q}$ implica que estamos en el caso de "bajada de nivel". Luego, $a_\mathfrak{q}(E) \equiv \pm(\mathcal{N}(\mathfrak{q}) + 1) \pmod p$. Por la cota de Hasse (Proposición 1.1.4), $|a_\mathfrak{q}(E)| \leq 2\sqrt{\mathcal{N}(\mathfrak{q})}$. Si $p > \mathcal{N}(\mathfrak{q}) + 1 + 2\sqrt{\mathcal{N}(\mathfrak{q})}$ tal congruencia no se puede satisfacer, por lo que E debe tener buena reducción en q. Luego, como las representaciones de Galois de dimensión dos son congruentes módulo p, $a_\mathfrak{q}(E) \equiv a_\mathfrak{q}(E') \pmod p$. Nuevamente, por la cota de Hasse, ambos valores $|a_\mathfrak{q}(E)|, |a_\mathfrak{q}(E')| \leq 2\sqrt{\mathcal{N}(\mathfrak{q})}$, por lo que si $p > 4\sqrt{\mathcal{N}(\mathfrak{q})}$, $a_\mathfrak{q}(E) = a_\mathfrak{q}(E')$. Pero como E tiene un punto K-racional de orden N, $a_\mathfrak{q}(E') \equiv 1 + \mathcal{N}(\mathfrak{q}) \pmod N$, dando una contradicción. □

2.4.5 Eliminando formas con multiplicación compleja: el aporte de Ellenberg.

En la Sección 2.4.1 vimos la importancia de poder descartar formas con multiplicación compleja, puesto que en particular las formas $f_\pm$ asociadas a las soluciones triviales $(\pm 1, 0, 1)$ tienen multiplicación compleja, y no podrán ser eliminadas por ninguno de los métodos anteriores.

En esta sección nos centraremos en mostrar cómo utilizaremos algunos resultados obtenidos por Ellenberg en [38,39] y dividiremos en casos, según si el cuerpo de números K es real o imaginario, en

caso de ser necesario. Recordemos que las formas con multiplicación compleja tienen la particularidad de que la imagen de su representación residual está contenida en el normalizador de un subgrupo de Cartan (Proposición 1.2.20). Este puede ser split o no split. Respecto al primer caso, siguiendo las ideas de Darmon-Merel, Ellenberg probó lo siguiente.

Proposición 2.4.6. *Sea $K/\mathbb{Q}$ una extensión cuadrática, E/K una $\mathbb{Q}$-curva de grado n libre de cuadrados y sea p primo tal que $p = 11$ o $p > 13$ con mcd$(p, n) = 1$. Supongamos que existe un primo $\mathfrak{q} \nmid 6$ en donde E tiene reducción multiplicativa. Entonces la imagen proyectiva residual módulo p de $\rho_{E,p}$ no está contenida en el normalizador de un subgrupo de Cartan split.*

Demostración. Ver [38, Proposición 3.4]. □

La principal ventaja de la Proposición 2.4.6 es que no impone condición alguna acerca de si $K/\mathbb{Q}$ es real o imaginaria. Notemos también que no será suficiente para descartar formas con multiplicación compleja, ya que no menciona nada acerca de si la imagen residual de la representación está contenida o no en el normalizador de un subgrupo de Cartan no split. Para el caso en el que $K/\mathbb{Q}$ sea imaginaria, utilizaremos resultados más fuertes probados por Ellenberg que trabajarán también con el caso Cartan no split. En el caso real, la falta de resultados sobre el caso no split impondrá alguna condición de congruencia para el exponente p de la ecuación a la hora de poder asegurar la no existencia de soluciones. Esto será explicado en la Observación 16. Cabe destacar que bajo ciertas condiciones, extenderemos también algunos resultados de Ellenberg para el caso real. Para ello, debemos mencionar también que Ellenberg probó lo siguiente:

Proposición 2.4.7. *Sea $K/\mathbb{Q}$ una extensión cuadrática,χ_K el caracter de Dirichlet asociado y E/K una $\mathbb{Q}$-curva de grado n con un primo de reducción potencialmente multiplicativa $\mathfrak{q} \nmid 6$. Además, supongamos que se satisface una de las siguientes:*

(i) existe $f \in S_2(\Gamma_0(p^2))$ tal que $w_p f = f$, o

(ii) existe $f \in S_2(\Gamma_0(np^2))$ tal que $w_p f = f$ y $w_n f = -f$,

con $L(f \otimes \chi_K, 1) \neq 0$. Entonces existe una constante $N_{K,n}$ tal que si $p > N_{K,n}$, la representación proyectiva residual módulo p de E es suryectiva.

Demostración. Ver Proposiciones 3.2, 3.4, Teorema 3.14 y Sección 4 de [38]. □

Por Proposición 3.1.1 (respectivamente 4.1.1), la curva $E_{(a,b,c)}$ (respectivamente $\widetilde{E}_{(a,b,c)}$) es una $\mathbb{Q}$-curva de grado 2 (respectivamente 3). Introduciremos a continuación las nociones necesarias que fueron utilizadas para encontrar formas que satisfagan las condiciones (i) o (ii).

Seguiremos con la notación utilizada en la Subsección 1.4.1. Sean χ_K el caracter correspondiente a $K/\mathbb{Q}$, N un entero positivo, y $\mathfrak{f}$ el conductor de χ_K. Sea $\mathcal{F}$ una base ortogonal del producto de Petersson para $S_2(\Gamma_0(N))$. Dada $f \in S_2(\Gamma_0(N))$, cuya q-expansión es de la forma $f(z) = \sum_{n\geq 0} a_m(f) e^{2i\pi nz}$ y χ un caracter de Dirichlet, recordar que tenemos definida la función L_χ. Definimos entonces

$$(a_m, L_\chi)_N = \sum_{f\in\mathcal{F}} a_m(f) L(f \otimes \chi, 1). \tag{2.6}$$

Si $M \mid N$, se denota por $(a_m, L_\chi)_N^M$ a la contribución a $(a_m, L_\chi)_N$ de la formas que provienen del nivel M. Para probar la existencia de una forma nueva que cumpla las hipótesis de la Proposición 2.4.7, basta ver que $(a_1, L_{\chi_K})_N^{p-\text{new}}$ no se anula, donde $N = p^2$ o $N = np^2$.

El caso K imaginario

Bajo la hipótesis de que K es imaginario, Ellenberg prueba que existe una forma modular que satisface (i) de la Proposición 2.4.7 para p suficientemente grande (ver [38, Proposición 3.9]). Más concretamente, muestra que

$$(a_1, L_{\chi_K})_{p^2}^{p-\text{new}} = (a_1, L_{\chi_K})_{p^2} - p(p^2-1)^{-1}(a_1 - p^{-1}\chi_K(p)a_p, L_{\chi_K})_p \tag{2.7}$$

no se anula. En particular, tenemos lo siguiente.

Teorema 2.4.8 (Ellenberg). *Sea $d < 0$ y $E/\mathbb{Q}(\sqrt{d})$ una $\mathbb{Q}$-curva de grado n libre de cuadrados que satisface que existe un primo $\mathfrak{q} \nmid 6$ de reducción multiplicativa para E. Entonces existe un entero N_d tal que la representación proyectiva residual de E en p es suryectiva para todos los primos $\mathfrak{p}$ de norma mayor a N_d. Más aún, en la Tabla 2.4.1 están presentadas algunas de las cotas que pueden ser tomadas.*

d	N_d	d	N_d	d	N_d
-2	257	-6	599	-13	1627
-3	7	-7	283	-15	457
-5	547	-11	409	-19	683

Tabla 2.4.1: Cotas de Ellenberg.

Observación 14. A priori la constante N_d del teorema anterior depende también del grado n de la $\mathbb{Q}$-curva, pues el resultado es una consecuencia de la Proposición 2.4.7. Sin embargo, como sólo nos concentraremos en la condición (i) de dicha proposición (que no depende de n), entonces las cotas son independientes de n.

Demostración. Como mencionamos anteriormente, este resultado fue probado en [38], donde se mostró un método para encontrar la cota N_d. El valor explícito de N_d fue dado en: [4] para $d = -1$ y $d = -2$ y en [37] para todos los valores de d cuyo conductor del cuerpo $\mathbb{Q}(\sqrt{d})$ sea como mucho 8 (junto con un refinamiento de la cota vía un cálculo computacional finito en [51] para $d = -3$). Además, en el artículo anteriormente mencionado, se presentaron cotas inferiores para $(a_1, L_{\chi_K})_{p^2}^{p-\text{new}}$, donde la mayor contribución proviene del primer término. En [39, Teorema 1] se probó la siguiente fórmula:

$$(a_m, L_{\chi_K})_{p^2} = 4\pi\chi_K(m)e^{-2\pi m/\sigma N log(N)} - E^{(3)} + E_3 - E_2 - E_1 + (a_m, B(\sigma N\log(N))), \tag{2.8}$$

donde σ se toma de la forma $\frac{q^2}{2\pi}$ y $N = p^2$. El Teorema 1 de [39] provee las siguientes cotas (notar que la primera cota no es la dada en el artículo de Ellenberg, dado que tenía un error, cuya errata está dada en el Apéndice de [64]):

- $|(a_m, B(\sigma N\log(N)))| \leq 2(4\pi\zeta^2(3/2)+1)(400/399)^3 exp(2\pi)q^2 m^{3/2}N^{-1/2}d(N)N^{-2\pi\sigma/q^2}$, donde $d(N)$ denota el número de divisores de N.
- $|E_1| \leq (16/3)\pi^3 m^{3/2}\sigma\log(N)\exp(-N/2\pi m\sigma\log(N))$.
- $|E_3| \leq (8/3)\zeta(3/2)^2\pi^3\sigma m^{3/2}N^{-1/2}\log(N)d(N)\exp(-N/2\pi m\sigma\log(N))$.
- $|E^{(3)}| \leq 16\pi^3 m\sum_{c>0,N|c}\min\{\frac{2}{\pi}\phi(q)c^{-1}\log(c), \frac{1}{6}\sigma N\log(N)m^{1/2}c^{-3/2}d(c)\}$, donde ϕ es la función de Euler.

Además, vale la siguiente cota:

- Si el discriminante del cuerpo es par, entonces por [4, Proposición 10]

$$|E_2| \leq 64q\phi(q)\pi^5 m^2 \left(\frac{\zeta(2)}{6}/N^2 + \frac{1}{\pi}\left(\zeta(3)log\left(\frac{eN}{2}\right)\right) - \zeta'(3)N^{-3}\right)$$
$$+32\pi^5\zeta(7/2)^2 m^{5/2} d(N) N^{-7/2}\left(\left(\frac{N^2}{4\pi^2 m}+1\right)(1-\theta)^{-1} + (1-\theta)^{-2}\right)\exp\left(-\frac{N}{2\pi\sigma m\log(N)}\right)$$
$$+\frac{512}{3}\zeta(11/2)^2\pi^7 m^{7/2} d(N) N^{-11/2}(1-\theta^2)^{-3},$$

  donde $x = \sigma N\log(N)$ y $\theta = \exp(-2\pi/x)$. Caso contrario, por [39, Teorema 1],

$$|E_2| \leq \frac{8}{9}\pi^5\zeta(7/2)^2 m^{5/2}\sigma^2 N^{-3/2}\log^2(N).$$

- Por [38, Lema 3.13], para $t = 1$ o $t = p$ tenemos

$$(a_{mt}, L_{\chi_K})_p \leq 2\sqrt{3}m^{1/2}d(m)(1-\exp(-2\pi/q\sqrt{p}))^{-1}(4\pi + 16\zeta^2(3/2)\pi^2 p^{-3/2}).$$

Denotamos por $E_1(p,q)$, $E_2(p,q)$, $E_3(p,q)$, $E_4(p,q,t)$ y bound1(p,q) a las cotas de E_1, E_2, E_3, $E^{(3)}$ y $(a_1, B(\sigma N\log(N)))$ respectivamente. La variable t está en la cota de $E^{(3)}$ porque para obtener una cota más simple (siguiendo la notación de Ellenberg) se parte la suma dependiendo si $c \leq t$ ó $c > t$, para t un número natural. Sea $F(p,q,t) := 4\pi e^{-2\pi^2/p^2 q\log(p)} - E_4(p,q,t) - E_3(p,q) - E_2(p,q) - E_1(p,q) - \text{bound1}(p,q)$. Entonces por las ecuaciones (2.7) y (2.8) tenemos:

$$(a_1, L_{\chi_K})_{p^2}^{p-\text{new}} \geq F(p,q,t) - \frac{1}{p^2-1}(a_p, L_{\chi_K})_p - \frac{p}{p^2-1}(a_1, L_{\chi_K})_p. \tag{2.9}$$

Para acotar $(a_p, L_{\chi_K})_p$ y $(a_1, L_{\chi_K})_p$ usamos la cota de Ellenberg [38, Teorema 3.13], obteniendo una función $F_2(p,q,m)$ tal que $(a_m, L_{\chi_K})_p \leq F_2(p,q,m)$. Por lo tanto, usando dicha cota y la desigualdad (2.9) obtenemos que:

$$(a_1, L_{\chi_K})_{p^2}^{p-\text{new}} \geq F(p,q,t) - \frac{1}{p^2-1}F_2(p,q,p) - \frac{p}{p^2-1}F_2(p,q,1). \tag{2.10}$$

Notemos que, como las funciones $4\pi e^{-2\pi^2/p^2 q\log(p)}$, $-E_4(p,q,t)$, $-E_3(p,q)$, $-E_2(p,q)$, $-E_1(p,q)$ y $-\text{bound1}(p,q)$ son funciones crecientes (en p), la función $F(p,q,t)$ es creciente. Además se puede deducir que $-\frac{1}{p^2-1}F_2(p,q,p)$ y $-\frac{p}{p^2-1}F_2(p,q,1)$ son también funciones crecientes, con lo cual $(a_1, L_{\chi_K})_{p^2}^{p-\text{new}}$ es creciente. Entonces, para asegurar que $(a_1, L_{\chi_K})_{p^2}^{p-\text{new}}$ es no nulo, es suficiente con encontrar el primer primo p en donde el lado derecho de (2.10) sea positivo. Implementamos este código siguiendo la notación anterior en `PARI/GP`.

Queremos remarcar que la cota citada para $d = -3$ depende de la cota de Ellenberg, con lo cual a priori necesita ser modificada para incluir la cota correcta de $|(a_m, B(\sigma N\log(N)))|$. A continuación un ejemplo de cómo corrimos el código con la función `EllenbergBound(p,q,t)` para $d = -2$:

```
? EllenbergBound(263,8,263^2*100)
% 1 = 0.35180253548860681202421271666168865921
```

□

Observación 15. Por [38, Proposición 3.9], uno puede mejorar las cotas anteriores buscando para cada primo p menor a la cota N_d una forma nueva f de peso 2 que satisfaga las condiciones de la Proposición 2.4.7. En algunas ocasiones (como en [51]) uno puede comprobar esto numéricamente para todos los primos $p < N_d$ para así obtener una cota muy chica que reemplace a N_d. Esto es útil

para primos chicos (digamos menores que 150), pero para primos más grandes, los espacios a calcular tienen una dimensión muy grande y los cálculos computacionales se tornan irrealizables. Uno se puede restringir a las formas modulares con coeficientes racionales (porque se corresponden a curvas elípticas racionales, y existen tablas de curvas elípticas de conductor hasta $500,000$), pero en general esto no es suficiente para descartar todos los casos. Por ejemplo, si aplicamos este razonamiento en el caso $d = -5$, obtenemos que para 63 de los 97 primos entre 11 y 547 el resultado de Ellenberg se aplica. Sin embargo, existen primos muy grandes (como por ejemplo 541) que no pueden ser descartados utilizando sólo curvas elípticas y para los cuales el espacio $S_2(\Gamma_0(p^2))$ tiene dimensión muy grande.

El caso K real

El caso K real no fue tratado por Ellenberg. Nos concentraremos en cómo extender los resultados a este caso cuando el grado de la $\mathbb{Q}$-curva sea $n = 2$ (el caso $n = 3$ debería ser similar). Incluso en el caso $n = 2$, deja de ser cierto que siempre va a existir una forma que cumpla con las hipótesis de la Proposición 2.4.7, a saber.

Proposición 2.4.9. *Sea $K/\mathbb{Q}$ es una extensión cuadrática real en la que p no ramifica y 2 no se parte. Entonces no existe una forma nueva que satisfaga alguna de las condiciones (i) o (ii) de la Proposición 2.4.7.*

Demostración. Para una forma nueva f, denotamos por $\epsilon(f)$ al signo de su ecuación funcional (recordar que el signo de la ecuación funcional es el signo opuesto de la involución canónica). Recordemos de [13, §I.5] que si $f \in S_2(\Gamma_0(N))$ es una forma nueva y ψ es un caracter de Dirichlet cuyo conductor es coprimo con N entonces $\epsilon(f \otimes \psi) = \epsilon(f)\psi(-N)$. Supongamos que $f \in S_2(p^2)$ satisface que $w_p(f) = f$, con lo cual el signo de la ecuación funcional es igual a -1. Luego, si p no ramifica en $K/\mathbb{Q}$, el twist $f \otimes \chi_K$ también tiene signo de la ecuación funcional igual a -1 (ya que $\chi_K(-p^2) = 1$ cuando K es cuadrático real), con lo cual $L(f \otimes \chi_K, 1) = 0$.

Supongamos que f es una forma nueva de nivel $2p^2$. Las hipótesis en los autovalores de Atkin-Lehner implican que $\epsilon(f) = 1$. Supongamos que 2 es no ramificado en $K/\mathbb{Q}$. Entonces $\epsilon(f \otimes \chi_K) = \chi_K(-2p^2) = \chi_K(2) = 1$ si y sólo si 2 se parte en $K/\mathbb{Q}$. Cuando 2 ramifica en $K/\mathbb{Q}$, podemos escribir $d_K = d_1 \cdot d_2$, donde $d_1 \in \{-4, \pm 8\}$ y d_2 es un discriminante fundamental impar. Supongamos $d_1 = -4$; escribiendo $f \otimes \chi_K = (f \otimes \chi_{d_1}) \otimes \chi_{d_2}$, es suficiente entender el cambio de signo para el primer twist (la forma $f \otimes \chi_{-4}$ siendo una forma de nivel $16p^2$). Por un resultado de Atkin-Lehner (ver [2, Teorema 7]) $w_2(f \otimes \chi_{-4}) = -1$ mientras que $w_p(f \otimes \chi_{-4}) = w_p(f)$. Luego, $\epsilon(f \otimes \chi_{-4}) = \epsilon(f) = 1$ y como d_2 es negativo (y por lo tanto $\chi_{d_2}(-1) = -1$), $\epsilon(f \otimes \chi_K) = -1$. Un cálculo similar (usando que $w_2(f \otimes \chi_8) = 1$ y $w_2(f \otimes \chi_{-8}) = -1$) prueba el resto de los casos. □

El primo 2 se parte en $K/\mathbb{Q}$

La Proposición 2.4.9 nos asegura que cuando 2 es inerte o ramifica en $K/\mathbb{Q}$, no hay posibilidad de extender el resultado de Ellenberg obtenido para el caso imaginario. Supongamos entonces que 2 se parte en $K/\mathbb{Q}$. Como se puede ver en la fórmula (2.6), la prueba de Ellenberg de la existencia de una forma nueva con las propiedades dichas consiste en acotar un promedio de los valores centrales twisteados en todo el espacio de formas modulares de nivel p^2 (ya que las formas con el signo incorrecto de la involución de Atkin-Lehner en tal espacio tienen valor central cero). La idea para el caso real consiste en focalizarse en el nivel $2p^2$; es decir que allí buscaremos una forma que satisfaga (ii) de la Proposición 2.4.7. Mientras que considerando el espacio $S_2(\Gamma_0(2p^2))^{\text{new}}$ los cálculos son dificultosos, calcularemos un promedio no sobre todo el espacio, sino sobre el subespacio con un signo de Atkin-Lehner en p fijo (por lo tanto imponiendo también una condición al signo de Atkin-Lehner

en 2). Tales cálculos fueron llevados a cabo en [55] (ver la prueba del Corolario 4). Desafortunadamente, las constantes en el artículo de Le Fourn no son explícitas, por lo que debemos añadir algunos detalles extras a su prueba (sugerimos al lector tener una copia de tal artículo a mano para el resto de sección, ya que seguiremos su notación y sus definiciones, especialmente la Sección 6).

La desigualdad $J_1(x) \leq \frac{|x|}{2}$ y $|S(1,n;c)| < \sqrt{c}\tau(c)$ (usada en el artículo de Ellenberg) transforma la desigualdad (6.3) de [55] en

$$|A_{N,Q,c}(x)| \leq \frac{\pi}{3} \cdot \frac{xe^{-2\pi/x}\tau(c)}{Qc^{3/2}}, \tag{2.11}$$

para $x \geq 71$ (usando que $(1-e^{-2\pi/x})^{-1} \leq \frac{x}{6}$ cuando $x \geq 71$). La misma cota para J_1 da la desigualdad explícita para la ecuación (6.4)

$$|A_{N,Q,c}(x)| \leq \frac{12}{\pi} \frac{(\log(Dc)+1)\sqrt{D}}{cQ} e^{-2\pi/x}. \tag{2.12}$$

Para obtener una cota para $A_{N,Q}(x) = 2\pi \sum_{c>0,(N/Q)|c,(c,Q)=1} A_{N,Q,c}(x)$ partimos la suma como en [55]. Supongamos que $N \neq Q$, con lo que en la siguiente suma no hay término para $c = D$:

$$|A_{N,Q}(x)| \leq \frac{12}{\pi} \frac{\sqrt{D}e^{-2\pi/x}}{Q} \sum_{\substack{c<x^2 \\ (N/Q)|c}} \frac{(\log(Dc)+1)}{c} + \frac{\pi}{3} \sum_{\substack{c>x^2 \\ (N/Q)|c}} \frac{xe^{-2\pi/x}\tau(c)}{Qc^{3/2}}.$$

Para la primera suma interna, escribiendo $c = (N/Q)b$, obtenemos la siguiente desigualdad

$$\sum_{\substack{c<x^2 \\ (N/Q)|c}} \frac{(\log(Dc)+1)}{c} = \frac{Q}{N}\left(\left(1+\log(\frac{DN}{Q})\right)\sum_{b=1}^{\frac{x^2Q}{N}} \frac{1}{b} + \sum_{b=1}^{\frac{x^2Q}{N}} \frac{\log(b)}{b}\right) \leq$$
$$\frac{Q}{N}\left(\left(1+\log(\frac{DN}{Q})\right)\left(1+\log(\frac{x^2N}{Q})\right) + \frac{\log^2(\frac{x^2N}{Q})}{2}\right), \tag{2.13}$$

donde la última desigualdad proviene de la comparación usual entre la serie y la integral. Para acotar la suma $\sum_{c>X^2} \frac{\tau(c)}{c^{3/2}}$, recordar las siguientes desigualdades:

1. Para todo real $s > 1$, $\sum_{n\geq X} \frac{1}{n^s} \leq -\frac{X^{1-s}}{1-s} + \frac{X^{-s}}{2}$ (ver por ejemplo [1, Lema 3.1]),
2. Para $X > 1$ un número real, $\sum_{d\leq X} \frac{1}{d} \leq \log(X) + \gamma + \frac{7}{12X}$ donde γ es la constante de Euler-Mascheroni, $\gamma \leq 0.58$ (ver ecuación (3.1) de [35]).

Luego, si $s > 1$,

$$\sum_{n\geq X} \frac{\tau(n)}{n^s} = \sum_{n\geq X}\left(\sum_{d|n} \frac{1}{n^s}\right) = \sum_d \frac{1}{d^s} \sum_{m\geq X/d} \frac{1}{m^s} \leq \zeta(s) \sum_{d>X} \frac{1}{d^s} + \sum_{d\leq X} \frac{1}{d^s}\left(-\frac{(X/d)^{1-s}}{(1-s)} + \frac{(X/d)^{-s}}{2}\right) \leq$$
$$\zeta(s)\left(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2}\right) - \frac{X^{1-s}}{(1-s)} \sum_{d\leq X} \frac{1}{d} + \frac{X^{1-s}}{2} \leq$$
$$\zeta(s)\left(-\frac{X^{1-s}}{(1-s)} + \frac{X^{-s}}{2}\right) - \frac{X^{1-s}}{(1-s)}(\log(X) + \gamma + \frac{7}{12X}) + \frac{X^{1-s}}{2}.$$

Substituyendo en $s = 3/2$, X por X^2 y asumiendo $X \geq 32$, obtenemos

$$\sum_{n \geq X^2} \frac{\tau(n)}{n^{3/2}} \leq \frac{6\log(X)}{X}. \tag{2.14}$$

Usando ambas desigualdades, obtenemos (para $N \neq Q$)

$$|A_{N,Q}(x)| \leq \frac{12\sqrt{D}e^{-2\pi/x}}{N\pi}\left((\log(\frac{DN}{Q})+1)\log(\frac{x^2N}{Q}) + \frac{\log^2(\frac{x^2N}{Q})}{2}\right) + \\ + \frac{2\pi}{N}\sqrt{Q/N}\tau(N/Q)\log(x)e^{-2\pi/x}. \tag{2.15}$$

Cuando $N = Q$, hay un término extra $\frac{\pi}{3}\frac{xe^{\frac{-2\pi}{x}}\tau(D)}{ND^{3/2}}$ correspondiente al valor $c = D$. Usando el hecho de que $B_{N,Q}(x) = A_{N,Q}(D^2N/x)$, tenemos la cota

$$|B_{N,Q}(x)| \leq |A_{N,Q}(D^2N/x)| + \delta_{Q=N}\frac{\pi}{3}\frac{\sqrt{D}}{x}\tau(D)e^{\frac{-2\pi x}{ND^2}}. \tag{2.16}$$

Recordemos que $(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} = (a_1, L_\chi)_{2p^2}^{+_{p^2}} - \frac{1}{p-1}(a_1, L_\chi)_{2p}^{\chi(p)_p}$ (ver [55, Lema 4.1]). Por lo tanto, las fórmulas $(6.1), (6.2)$ de [55] resultan de la siguiente forma:

$$\frac{1}{2\pi}(a_1, L_\chi)_{2p^2}^{+_{p^2},\text{new}} \geq \frac{(p-2)}{(p-1)}e^{-2\pi/x} - \Big(|A_{2p^2,1}(x)| + |A_{2p^2,p^2}(x)| + \frac{|A_{2p,1}(x)|}{p-1} + \frac{|A_{2p,p}(x)|}{p-1} + \\ + |B_{2p^2,2p^2}(x)| + |B_{2p^2,2}(x)| + \frac{|B_{2p,2p}(x)|}{p-1} + \frac{|B_{2p,2}(x)|}{p-1}\Big). \tag{2.17}$$

Tomando x de la misma magnitud que p (en nuestras aplicaciones tomaremos $x = p \cdot \kappa$ para una constante numérica computada κ), el lado derecho es una función creciente en p, por lo tanto al encontrar un valor positivo ya tenemos nuevamente una cota explícita para la Proposición 2.4.7.

El primo 2 **no se parte en** $K/\mathbb{Q}$

En caso de que 2 no se parta en $K/\mathbb{Q}$ no todo está perdido, pues como fue mencionado al comienzo de la Sección 2.4.5, el problema de descartar las formas con multiplicación compleja puede ser parcialmente resuelto mediante la Proposición 2.4.6. Dicho resultado, junto con el Lema 3.1.8 (respectivamente Lema 4.1.9) y con la siguiente observación, permitirá descartar las formas con multiplicación compleja bajo ciertas hipótesis de congruencia en p, sabiendo exactamente qué soluciones estamos dejando de lado (ver ejemplo $d = 6$ para la ecuación (1)).

Observación 16. La razón por la cual podremos eliminar las formas con multiplicación compleja es la siguiente: supongamos que f es una forma nueva con multiplicación compleja en $\mathscr{O}_L$, el anillo de enteros de un cuerpo de números L. Si p es un primo que se parte en L entonces, por Proposición 1.2.20, la representación residual módulo p de la forma f tiene imagen proyectiva en el normalizador de un subgrupo de Cartan split. Luego, esto contradice la Proposición 2.4.6, siempre y cuando exista un primo que no divida a 6 para el cual la curva (respectivamente $\widetilde{E}_{(a,b,c)}$) tenga reducción multiplicativa, problema que ya fue discutido anteriormente en la Sección 2.4.1.

Capítulo 3

La ecuación $x^4 - dy^2 = z^p$

In mathematics you don't understand things.
You just get used to them.

J. Von Neumann.

En 2004 Ellenberg estudió las $\mathbb{Q}$-curvas, obteniendo así importantes resultados sobre sus representaciones de Galois (ver [38]). Por su aplicación natural en la resolución de ecuaciones diofánticas vía el método modular, fue capaz de probar lo siguiente:

Teorema (Ellenberg)**.** *Sea $p > 211$ un número primo. La ecuación $x^4 + y^2 = z^p$ no tiene solución primitiva no trivial.*

Con esto, ecuaciones aptas para ser estudiadas vía el aporte de las $\mathbb{Q}$-curvas en el método modular fueron ganando interés. En 2009 Dieulefait y Jiménez-Urroz logran resolver el Paso 1 del método para la ecuación (1) con d un entero cualquiera (ver [37]). Es decir, dada una hipotética solución (a, b, c) de la ecuación (1), definieron la curva

$$E_{(a,b,c)} : y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{d}b)x, \tag{3}$$

que como veremos en la Sección 3.1 cumple con las propiedades esperadas. Más aún, demuestran lo siguiente:

Teorema (Dieulefait, Jiménez-Urroz)**.** *Sea $d = -2$ (respectivamente $d = -3$). Entonces la ecuación*

$$x^4 - dy^2 = z^p$$

no tiene soluciones primitivas no triviales para los primos $p > 349$ (respectivamente $p > 131$).

Años más tarde, Bennet, Ellenberg y Ng logran refinar en [4] los resultados anteriores, encontrando todas las soluciones primitivas no triviales para $d = -1, -2$ y p un número natural cualquiera mayor a 4. En esta tesis doctoral daremos una receta para aplicar el método modular a la ecuación (1) con d un entero general. Luego pondremos en práctica esto para encontrar resultados asintóticos para nuevos valores de d en la ecuación (1). Dichos aportes están basados en los artículos [64] y [65], en colaboración con Ariel Pacetti.

Como fue mencionado en el Capítulo 2, la hipótesis de primitividad en las soluciones es necesaria para garantizar la finitud de soluciones, pues al rebajar dicha hipótesis se obtienen infinitas soluciones. El siguiente resultado es una prueba de ello. Queremos agradecer a Andrew Granville por remarcarnos este hecho, dando una prueba del Lema 3.0.1.

Lema 3.0.1. *Sea $p > 3$ un número primo. La ecuación*

$$x^4 - dy^2 = z^p$$

tiene infinitas soluciones no primitivas.

Demostración. Supongamos que $p \equiv 1 \pmod 4$. Sean $u, v \in \mathbb{Z}$ arbitrarios tales que $r = u^4 - dv^2$ no es igual a ± 1. Entonces el punto $(ur^{\frac{p-1}{4}}, vr^{\frac{p-1}{2}}, r)$ es solución de la ecuación (1). Si $p \equiv 3 \pmod 4$ entonces el punto $(ur^{\frac{3p-1}{4}}, vr^{\frac{3p-1}{2}}, r^3)$ es solución de la ecuación (1). □

Observación 17. Notemos que en el caso de la ecuación (1) es claro que basta analizar los casos en donde d es un entero libre de cuadrados, pues supongamos que $d = d_1^2 \cdot d_2$. Luego, si (a, b, c) es solución de la ecuación $x^4 + dy^2 = z^p$ entonces (a, bd_1, c) es solución de la ecuación $x^4 + d_2y^2 = z^p$.

Para seguir la estrategia detallada en el Capítulo 2, este capítulo se desarrollará de la siguiente forma: primero analizaremos las propiedades más importantes la curva (3) (Sección 3.1). Luego, en la Sección 3.2.1 daremos la construcción explícita del caracter χ (separando en casos según el signo de d). Por último, daremos una sección de ejemplos de valores de d para los cuales resolvemos la ecuación (1).

Observación 18. Notemos que si $(a, b, c) \in \mathbb{Z}^3$ es una solución de (1), entonces $(a, b\sqrt{d}, c)$ es una solución de $x^4 - y^2 = z^p$ en el anillo de enteros $\mathcal{O}_K$ del cuerpo $K = \mathbb{Q}(\sqrt{d})$. Esta observación fue la que motivó al autor a estudiar la ecuación $x^4 - y^2 = z^p$ sobre cuerpos de números en [82]. Sin embargo, dicho trabajo no será desarrollado en la presente tesis.

3.1 Paso 1: La curva $E_{(a,b,c)}$ y sus propiedades

Sea (a, b, c) una solución de (1). Como mencionamos al comienzo del capítulo, en [37] se adjunta la curva $E_{(a,b,c)}$ definida como en (3). Su discriminante y su j-invariante son

$$\Delta(E_{(a,b,c)}) = 512(a^2 + \sqrt{d}b)c^p, \quad j(E_{(a,b,c)}) = \frac{64(5a^2 - 3\sqrt{d}b)^3}{c^p(a^2 + \sqrt{d}b)}.$$

Sea $\tau \in G_{\mathbb{Q}}$ un elemento cuya restricción a $\mathbb{Q}(\sqrt{d})$ no coincida con la identidad, y sea ψ_{-2} el caracter cuadrático correspondiente a la extensión cuadrática $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$.

Proposición 3.1.1. *La curva elíptica $E_{(a,b,c)}$ es una $\mathbb{Q}$-curva totalmente definida sobre el cuerpo $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$. Más aún, $\tau(E_{(a,b,c)})$ es isógena al twist cuadrático $E_{(a,b,c)} \otimes \psi_{-2}$.*

Demostración. Este resultado está explicado en [37]. Sea τ un generador no trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. El punto $(0, 0)$ tiene orden dos, y (como se explica por ejemplo en [78, Ejemplo 4.5]) el cociente tiene ecuación

$$y^2 = x^3 - 8ax^2 + 8(a^2 - \sqrt{d}b)x.$$

Un cambio de variables sencillo prueba que esta última es igual al twist cuadrático por -2 de $\tau(E_{(a,b,c)})$. En particular, la curva y sus isogenías están todas definidas sobre el cuerpo $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$. □

En particular, si (a, b, c) es una solución no trivial, la curva $E_{(a,b,c)}$ no está definida sobre $\mathbb{Q}$. Sea $K = \mathbb{Q}(\sqrt{d})$, el cuerpo donde la curva está naturalmente definida y $\mathcal{O}_K$ su anillo de enteros. A continuación veremos una serie de lemas que proveen información sobre el comportamiento de $E_{(a,b,c)}$ en un ideal primo $\mathfrak{q}$ de $\mathcal{O}_K$.

Lema 3.1.2. *Supongamos que q es un primo racional impar que ramifica en $K/\mathbb{Q}$ y denotemos por $\mathfrak{q}$ el (único) ideal primo en $\mathscr{O}_K$ que divide a q. Entonces $\mathfrak{q} \nmid \Delta(E_{(a,b,c)})$.*

Demostración. Como q ramifica, $\mathfrak{q} \mid \sqrt{d}$, y como (a,b,c) es primitiva, $\mathfrak{q} \nmid a$. Luego $\mathfrak{q} \nmid c^p(a^2 + \sqrt{d}b)$. □

Lema 3.1.3. *Sea $\mathfrak{q}$ un ideal primo impar de $\mathscr{O}_K$ tal que $\mathfrak{q} \mid \Delta(E_{(a,b,c)})$. Entonces $E_{(a,b,c)}$ tiene reducción multiplicativa en $\mathfrak{q}$.*

Demostración. Por Lema 3.1.2 sabemos que los primos que dividen a $\Delta(E_{(a,b,c)})$ no ramifican en $K/\mathbb{Q}$; en particular, si $\mathfrak{q}$ es un primo impar que divide a $\Delta(E_{(a,b,c)})$, $\mathfrak{q} \nmid 4a$, luego claramente la reducción de (3) módulo $\mathfrak{q}$ es multiplicativa. □

Lema 3.1.4. *Sea $\mathfrak{q}$ un ideal primo impar de $\mathscr{O}_K$. Entonces $v_{\mathfrak{q}}(\Delta(E_{(a,b,c)})) \equiv 0 \pmod{p}$.*

Demostración. Claramente si $\mathfrak{q} \mid \text{mcd}(a^2+\sqrt{d}b, a^2-\sqrt{d}b)$ entonces $\mathfrak{q} \mid 2$, pues (a,b,c) es primitiva. Luego, como $c^p = a^4 - db^2 = (a^2+\sqrt{d}b)(a^2-\sqrt{d}b)$,

$$v_{\mathfrak{q}}(a^2+\sqrt{d}b) = \begin{cases} 0 & \text{si } \mathfrak{q} \nmid (a^2+\sqrt{d}b), \\ v_{\mathfrak{q}}(c^p) & \text{caso contrario.} \end{cases}$$

□

Los últimos dos resultados son los necesarios para remover los primos que dividan a c del conductor de la representación residual (vía un teorema de Ribet). Denotemos por $N(E_{(a,b,c)})$ al conductor de $E_{(a,b,c)}$. Asumamos que $p \geq 11$ para evitar cálculos extras cuando 2 se parta en $K/\mathbb{Q}$.

Lema 3.1.5. *Sea $\mathfrak{p}_2$ un ideal primo en $\mathscr{O}_K$ que divida a 2.*

1. *Si 2 es inerte en K entonces $E_{(a,b,c)}$ tiene reducción de tipo* III *en $\mathfrak{p}_2$, con $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 8$.*
2. *Si 2 ramifica en K entonces $E_{(a,b,c)}$ tiene reducción de tipo I_2^* ó I_4^* en $\mathfrak{p}_2$, con $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) \in \{10, 12\}$.*
3. *Si $(2) = \mathfrak{p}_2\bar{\mathfrak{p}}_2$ entonces $E_{(a,b,c)}$ tiene o bien reducción tipo* III *en ambos primos, en donde $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = v_{\bar{\mathfrak{p}}_2}(N(E_{(a,b,c)})) = 8$ o $E_{(a,b,c)}$ es un twist de una curva con reducción multiplicativa, con lo cual los primos pueden ser tomados de manera que $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 6$ y $v_{\bar{\mathfrak{p}}_2}(N(E_{(a,b,c)})) \in \{1, 4\}$.*

Demostración. La prueba consiste en aplicar el algoritmo de Tate [79]. Los invariantes de $E_{(a,b,c)}$ son: $a_6 = 0$, $b_2 = 16a$, $b_6 = 0$ y $b_8 = -4(a^2+\sqrt{d}b)^2$.

1. Por hipótesis $d \equiv 5 \pmod{8}$ y 2 es primo en $\mathscr{O}_K$. Notemos que, por Lema 2.1.1, $2 \nmid a^2+\sqrt{d}b$ y entonces $v_2(\Delta(E_{(a,b,c)})) = 9$. Como se satisface que: $2 \mid b_2$, $2^2 \mid a_6$, $2^3 \nmid b_8$, la curva tiene tipo de reducción III y $v_2(N(E_{(a,b,c)})) = v_2(\Delta(E_{(a,b,c)})) - 1 = 8$.

2. Sea $\mathfrak{p}_2$ el único primo en $\mathscr{O}_K$ que divide a 2 y sea π el uniformizador local. Por Lema 2.1.1, $\mathfrak{p}_2 \nmid (a^2+\sqrt{d}b)$, luego $v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) = 18$. Para facilitar la notación, consideremos la curva

$$y^2 = x^3 + 4\alpha x^2 + 2\beta x, \tag{3.1}$$

donde $\mathfrak{p}_2 \nmid \beta$. Claramente $\mathfrak{p}_2 \mid b_2$, $\mathfrak{p}_2^2 \mid a_6$, $\mathfrak{p}_2^3 \mid b_8$ y $\mathfrak{p}_2^3 \mid b_6$. Siguiendo la notación de Tate, sea $a_{n,m} = \frac{a_n}{\pi^m}$. El polinomio $P = x^3 + a_{2,1}x^2 + a_{4,2}x + a_{6,3}$ tiene una raíz doble en $x = 1$, por lo que trasladamos, $x \to x + \pi$ en (3.1), para obtener la nueva ecuación

$$y^2 = x^3 + (4\alpha + 3\pi)x^2 + (8\pi\alpha + 3\pi^2 + 2\beta)x + 4\pi^2\alpha + \pi^3 + 2\beta\pi. \tag{3.2}$$

Escribimos $\tilde{a}_i$ para los nuevos coeficientes. Si d es par (con lo cual podríamos tomar $\pi = \sqrt{d}$) y b es impar, o d es impar (con lo cual podríamos tomar $\pi = 1 + \sqrt{d}$) y b es par (y por lo tanto a impar), $v_{\mathfrak{p}_2}(\pi^2 + 2\beta) = 3$ y por lo tanto $v_{\mathfrak{p}_2}(\tilde{a_4}) = 4$, y el polinomio $Y^2 + \tilde{a}_{3,2}Y - \tilde{a}_{6,4}$ tiene una raíz doble distinta de cero. Aunque necesitamos realizar una traslación (para llevar dicha raíz al 0), tal procedimiento no cambiará $\tilde{a}_{4,3}$, que tiene valuación 3. Con lo cual, el tipo es I_2^* y $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) - 6 = 12$.

Supongamos que d es par y b también. Si $\frac{d}{2} \equiv 3 \pmod 4$ entonces $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 6$ y $v_{\mathfrak{p}_2}(\tilde{a}_4) = 4$, con lo cual se puede prescindir de trasladar. Entonces el tipo es I_4^* y $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 18 - 8 = 10$. Si $\frac{d}{2} \equiv 1 \pmod 4$ entonces $v_{\mathfrak{p}_2}(\tilde{a}_6) = 4$ y $v_{\mathfrak{p}_2}(\tilde{a}_4) \geq 5$, por lo que el polinomio $Y^2 + \tilde{a}_{3,2}Y - \tilde{a}_{6,4}$ tiene una raíz doble distinta de cero, y luego de trasladarla a 0, obtenemos que a_4 tiene valuación 4, por lo que la misma cuenta funciona.

Por último, si $d \equiv 3 \pmod 4$ y b es impar, $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 5$ y $v_{\mathfrak{p}_2}(\tilde{a}_4) = 4$, entonces nuevamente el tipo es I_4^* y $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 18 - 8 = 10$.

3. Sea $\mathfrak{p}_2$ un primo arriba de 2. Consideremos los siguientes casos:

   - Si a o b es par (y por lo tanto el otro impar) entonces $v_{\mathfrak{p}_2}(a^2+\sqrt{d}b) = 0$ y $v_{\mathfrak{p}_2}(\Delta(E_{(a,b,c)})) = 9$ (para ambos primos). Claramente $v_{\mathfrak{p}_2}(b_2) \geq 4$ y $v_{\mathfrak{p}_2}(b_8) = 2$, por lo que el tipo de reducción es III y $v_{\mathfrak{p}_2}(N(E_{(a,b,c)})) = 9 - 1 = 8$ (en los dos primos).
   - Si ambos a, b son impares, podemos asumir que $v_{\mathfrak{p}_2}(a^2 + \sqrt{d}b) > 1$ y $v_{\bar{\mathfrak{p}_2}}(a^2 + \sqrt{d}b) = 1$ (ya que $\frac{a^2+\sqrt{d}b}{2}$ es un entero y $v_{\bar{\mathfrak{p}_2}}(a^2 + \sqrt{d}b) = v_{\mathfrak{p}_2}(a^2 - \sqrt{d}b) = v_{\mathfrak{p}_2}(a^2 + \sqrt{d}b - 2\sqrt{d}b)$). Más aún, el hecho de asumir $p \geq 11$ implica que $v_{\mathfrak{p}_2}(a^2 + \sqrt{d}b) \geq 11$ y luego $v_{\mathfrak{p}_2}(j(E_{(a,b,c)})) < 0$. En particular $E_{(a,b,c)}$ tiene reducción potencialmente multiplicativa. La ecuación no es minimal en $\mathfrak{p}_2$ y bajo un cambio de variables tenemos

   $$y^2 = x^3 + ax^2 + \frac{(a^2 + \sqrt{d}b)}{2^5}x,$$

   que ya tiene reducción multiplicativa. Por lo tanto su conductor es $\mathfrak{p}_2$ o $\mathfrak{p}_2^4$. Para calcular su tipo en $\bar{\mathfrak{p}_2}$, notamos que la hipótesis también implica que $v_{\bar{\mathfrak{p}_2}}(j(E_{(a,b,c)})) < 0$, con lo cual la curva tiene reducción potencialmente multiplicativa, pero resulta un twist cuadrático (por el caracter de conductor 8) de una curva con reducción multiplicativa; luego su conductor en $\bar{\mathfrak{p}}_2$ es $\bar{\mathfrak{p}}_2^6$.

□

El siguiente lema técnico es necesario sólo para calcular el conductor de la representación extendida cuando $d \equiv 7 \pmod 8$, con lo cual recomendamos al lector esquivarlo en una primera leída.

Lema 3.1.6. *Supongamos que $d \equiv 7 \pmod 8$ y b es impar. Sea $\mathfrak{p}_2$ el primo que divide a 2, $\pi = 1 + \sqrt{d}$ y ϵ una unidad. Entonces, en $\mathfrak{p}_2$, la curva elíptica $E_{(a,b,c)}$ twisteada por $\epsilon\pi$ con ecuación*

$$\epsilon\pi y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{d}b)x,$$

tiene exponente 8 en el conductor si $b \equiv 1 \pmod 4$ y 6 si $b \equiv 3 \pmod 4$.

Demostración. La prueba también sigue el algoritmo de Tate. El efecto de twistear nuestra curva en la ecuación (3.2) es que el coeficiente a_i se convierte en $a_i(\pi\varepsilon)^{-i}$, con lo cual la valuación del discriminante decrece en 6 y los coeficientes a_i decrecen su valuación por i. Luego, si $b \equiv 1 \pmod 4$, las valuaciones son $v_{\mathfrak{p}_2}(\tilde{a}_2) = 0$, $v_{\mathfrak{p}_2}(\tilde{a}_4) \geq 4$ mientras que $v_{\mathfrak{p}_2}(\tilde{a}_6) = 2$ (ya que $\frac{\pi^2}{2} + b\sqrt{d}$ es divisible por π pero no por π^3). Siguiendo el Paso 6 del algoritmo de Tate, realizamos el cambio de variables

$y \to y + x + \pi$ para obtener los nuevos coeficientes $\tilde{a}_2 - 1$, $\tilde{a}_4 - 2\pi$ y $\tilde{a}_6 - \pi^2$, con valuaciones 2, 3 y 3 respectivamente, con lo cual el tipo de reducción es I_0^* y el conductor es igual a $18 - 6 - 4 = 8$.

Por otro lado, si $b \equiv 3 \pmod 4$ entonces $v_{\mathfrak{p}_2}(\tilde{a}_2) = 0$, $v_{\mathfrak{p}_2}(\tilde{a}_4) = 2$ (ya que $2 \mid \frac{3\pi^2}{2} + b\sqrt{d}$ pero π^3 no) mientras que $v_{\mathfrak{p}_2}(\tilde{a}_6) \geq 4$. Siguiendo el algoritmo de Tate, aplicamos el cambio de variables $y \to y + x$ para obtener los coeficientes $\alpha_1 = 2$, $\alpha_2 = \tilde{a}_2 - 1$, $\alpha_3 = 0$, $\alpha_4 = \tilde{a}_4$ y $\alpha_6 = \tilde{a}_6$ con $v_{\mathfrak{p}_2}(\alpha_2) = 2$, $v_{\mathfrak{p}_2}(\alpha_4) = 2$ y $v_{\mathfrak{p}_2}(\alpha_6) \geq 4$. Como la reducción del polinomio $t^3 + \frac{\alpha_2}{\pi}t^2 + \frac{\alpha_4}{\pi^2}t + \frac{\alpha_6}{\pi^3}$ tiene una raíz doble y una simple, el tipo de reducción es I_n^*. Realizando el cambio de variables $x \to x + \pi$ el nuevo coeficiente a_4 es igual a $3\pi^2 + \frac{2}{\pi^2}\beta + 3$, que tiene valuación 3 en $\mathfrak{p}_2$, y por lo tanto el tipo es I_2^* y la valuación del conductor es $18 - 6 - 6 = 6$, como se afirmó. □

A continuación vemos que todas las soluciones primitivas triviales corresponden a curvas muy especiales.

Lema 3.1.7. *La solución trivial* $(0, 0, 0)$ *da lugar a una curva singular. El resto de las soluciones primitivas triviales de (1) son las siguientes:*

- *La solución* $(1, 0, 1)$*, correspondiente a la curva con etiqueta LMFDB* 256-a2 *y multiplicación compleja por* $\mathbb{Z}[\sqrt{-2}]$.
- *La solución* $(-1, 0, 1)$*, correspondiente a la curva son etiqueta LMFDB* 256-d2 *y multiplicación compleja por* $\mathbb{Z}[\sqrt{-2}]$.
- *La solución* $(0, \pm 1, 1)$ *(cuando* $d = 1$*), correspondiente a la curva con etiqueta LMFDB* 256-c2 *y multiplicación compleja por* $\mathbb{Z}[\sqrt{-1}]$.

Demostración. La solución $(0, 0, 0)$ claramente da una curva singular. Cualquier otra solución trivial debe cumplir que $b = 0$ o $a = 0$. En el primer caso, la hipótesis de primitividad implica que la solución es igual a $(\pm 1, 0, 1)$. Si $a = 0$, y q es un primo que divide a d, debe dividir a c, pero como la solución es primitiva, q no puede dividir a b. Esto implica que tal primo no puede existir, y por lo tanto la última es solución precisamente cuando $d = 1$, con solución trivial $(0, \pm 1, 1)$. □

Observación 19. El conductor de la curva $E_{(\pm 1,0,1)}$ sobre K tiene valuación 8 en los primos que dividen a 2 cuando 2 no ramifica en $K/\mathbb{Q}$, valuación 10 cuando $2 \mid d$ y valuación 12 cuando 2 ramifica en $K/\mathbb{Q}$ pero $2 \nmid d$ (equivalentemente, cuando $d \equiv 3 \pmod 4$).

Para aquellas soluciones primitivas que no son triviales tenemos el siguiente resultado.

Lema 3.1.8. *Sea* d *entero tal que* $d \notin \{17, 33, 41, 89\}$ *y sea* (a, b, c) *solución primitiva no trivial de la ecuación (1). Entonces la curva* $E_{(a,b,c)}$ *tiene multiplicación compleja si y sólo si vale alguna de las siguientes:*

- $(a, b, c, d, p) = (\pm 3, \pm 5, \pm 16, -7, 2)$*, en cuyo caso* $E_{(a,b,c)}$ *tiene multiplicación compleja por* $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ *y* j*-invariante* -3375.
- $(a, b, c, d) = (\pm 7, \pm 20, 1, 6)$ *para todo* p*, en cuyo caso* $E_{(a,b,c)}$ *tiene multiplicación compleja por* $\mathbb{Z}[\sqrt{-2}]$ *y* j*-invariante* $188837384000 \pm 77092288000\sqrt{6}$.

Demostración. Supongamos primero que $d < 0$. Recordar que si E es una curva elíptica con multiplicación compleja por un orden $\mathscr{O}$ entonces el orden del grupo de clases de $\mathscr{O}$ es igual al grado $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ (ver [76, Teorema 5.7]). Nuestra curva $E_{(a,b,c)}$ satisface que su j-invariante pertenece a $\mathbb{Q}(\sqrt{d})$, por lo que $[\mathbb{Q}(j(E_{(a,b,c)})) : \mathbb{Q}] \leq 2$. Pero si el grado es dos, entonces el grupo de clases tiene orden 2 y la extensión $\mathbb{Q}(j(E_{(a,b,c)}))$ es totalmente real (ver [76, (5.4.3)]). Luego, el grado es

1 y por lo tanto $j(E_{(a,b,c)}) \in \mathbb{Q}$. Como $j := j(E_{(a,b,c)})$ es racional, de su ecuación se deduce lo siguiente.

$$\begin{cases} jc^p = -14400a^4b - 1728db^2 = 0, \\ jc^p = 8000a^4 + 8640a^2b^2d = 0. \end{cases}$$

Restando las ecuaciones se obtiene que

$$175a^4 = 81db^2.$$

Luego, suponiendo que la solución no es trivial se obtiene que $\frac{a^2}{b} = \pm\frac{9}{5}\sqrt{\frac{-d}{7}}$, de donde se deduce que $d = -7$, pues la solución es entera y d es libre de cuadrados. Sustituyendo, llegamos a lo enunciado.

Si $d > 0$, existen finitos valores de d para los cuales el cuerpo $K = \mathbb{Q}(\sqrt{d})$ admite curvas definidas sobre K con j-invariante no racional y multiplicación compleja, a saber $d \in \{2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 61, 89\}$ (ver [26, Tabla 1]). Por lo tanto de ahora en más asumiremos que d pertenece a dicho conjunto. Si $E_{(a,b,c)}$ tiene multiplicación compleja entonces no tiene un primo de reducción multiplicativa. Luego, por Lema 3.1.3, c está soportado en 2. Ahora, si suponemos que $d \notin \{17, 33, 41, 89\}$, se tiene que $d \not\equiv 1 \pmod 8$. Luego, c es impar, y por lo tanto $c = \pm 1$. Las soluciones con $c = \pm 1$ se corresponden con las de la ecuación (3.27), que como veremos más adelante, son conocidas para los valores de d en el conjunto anterior. Luego, reemplazando d y (a, b, c) por cada uno de sus posibles valores se obtiene que la única curva que tiene multiplicación compleja es $E_{(\pm 7, \pm 20, 1)}$ cuando $d = 6$. □

3.2 Paso 2

3.2.1 Construcción del caracter de Hecke en el caso $t = 2$

En la presente sección nos dedicaremos a dar la construcción del caracter de Hecke χ por el cual vamos a twistear para extender la representación de $\rho_{E_{(a,b,c)},p}$. Como fue anticipado (Sección 1.7.1) primero definiremos un caracter ε que resultará ser el Nebentypus de la forma asociada a la representación extendida. Antes, dividimos los primos impares divisores de d en cuatro conjuntos, a saber:

$$Q_i = \{p \text{ primo } : \ p \neq 2, \quad p \mid d, \quad p \equiv i \pmod 8\},$$

para $i = 1, 3, 5, 7$; con lo cual $d = \text{sgn}(d) \cdot 2^{v_2(d)} \cdot \prod_{Q_i} p$, donde el producto se recorre sobre $Q_1 \cup Q_3 \cup Q_5 \cup Q_7$ y sgn es la función signo, i.e.

$$\text{sgn(d)} = \begin{cases} 1 & \text{si } d > 0, \\ -1 & \text{si } d < 0. \end{cases}$$

d	$\#Q_3$	$\#Q_5$	$\#Q_7$	d	$\#Q_3$	$\#Q_5$	$\#Q_7$
1	0	0	1	5	0	1	1
	1	1	0		1	0	0
3	0	1	0	7	0	0	0
	1	0	1		1	1	1
2	0	0	1	6	0	0	0
	0	1	1		0	1	0
	1	0	0		1	0	1
	1	1	0		1	1	1

Tabla 3.2.1: Muestra el valor de $\#Q_i \pmod 2$ cuando $d < 0$.

Antes de definir el caracter ε, introduciremos un poco de notación. Sean ψ_{-1}, ψ_2, ψ_{-2} los caracteres de $\mathbb{Z}$ correspondientes a las extensiones cuadráticas $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2})$ respectivamente y sean δ_{-1}, δ_2, δ_{-2} sus componentes locales en el primo 2 (ver Tabla 3.2.2 para ver los valores que toman).

Char	1	3	5	7
δ_{-1}	1	-1	1	-1
δ_{-2}	1	1	-1	-1
δ_2	1	-1	-1	1

Tabla 3.2.2

El caracter ε: Definimos un caracter par $\varepsilon : \mathbb{I}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ ramificado en los primos en $Q_3 \cup Q_5$ y a veces en 2, con componente local ε_p como se sigue:

- Para primos $p \in Q_1 \cup Q_7$, el caracter $\varepsilon_p : \mathbb{Z}_p^{\times} \to \mathbb{C}^{\times}$ es trivial.
- Para primos $p \in Q_3$, el caracter $\varepsilon_p = \delta_p$, donde δ_p es el caracter cuadrático $\delta_p(n) = \left(\frac{n}{p}\right)$.
- Para $p \in Q_5$, sea ε_p un caracter de orden 4 y conductor p.
- Para $p = 2$, $\varepsilon_2 = \delta_{-1}^{\#Q_3 + \#Q_5}$.
- El caracter ε_∞ (la componente arquimediana) es trivial.

Por construcción, el caracter ε satisface la condición de compatibilidad, a saber

$$\prod_p \varepsilon_p(-1)\varepsilon_\infty(-1) = \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(-1)\varepsilon_2(-1) = (-1)^{\#Q_3 + \#Q_5}\varepsilon_2(-1) = 1.$$

Esto da un caracter de Hecke ε de $\mathbb{I}_{\mathbb{Q}}$ bien definido correspondiente a un cuerpo totalmente real L cuyo grado es 1 si $Q_3 = Q_5 = \emptyset$, 2 si $Q_3 \neq Q_5 = \emptyset$ y 4 en caso contrario. Por teoría de cuerpos de clases, ε se identifica con un caracter $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$. Denotemos por N_ε su conductor, dado por $N_\varepsilon = 2^e \prod_{p \in Q_3 \cup Q_5} p$, donde $e = 0$ si $\#Q_3 + \#Q_5$ es par y 2 en caso contrario.

Observación 20. En la Tabla 3.2.1 se encuentran los posibles valores de $\#Q_3$, $\#Q_5$ y $\#Q_7$ módulo 2, dependiendo de la congruencia de d módulo 8. Notar en particular que cuando d es impar, la paridad de $\#Q_3 + \#Q_5$ (y por lo tanto la definición de ε_2) depende sólo del valor de $d \pmod 8$.

Teorema 3.2.1. *Existe un caracter de Hecke $\chi : G_K \to \overline{\mathbb{Q}}^{\times}$ tal que:*

1. *$\chi^2(\sigma) = \varepsilon(\sigma)$ para todo $\sigma \in G_K$,*
2. *χ es no ramificado en primos que no dividen a $2\prod_{p \in Q_1 \cup Q_5 \cup Q_7} p$,*
3. *Si $\tau \in G_{\mathbb{Q}}$ es tal que su restricción a K no es trivial, entonces ${}^{\tau}\chi = \chi \cdot \psi_{-2}$, vistos como caracteres de G_K (ver fórmula (2.1)).*

Por lo dicho en la Sección 1.7.1, a la hora de construir nuestro caracter χ, necesitamos verificar que el producto de sus componentes locales en una unidad sea 1. Recordemos que cuando K es cuadrático imaginario tiene en general dos unidades (1 y -1). Es por eso que comenzaremos definiendo a χ para el caso K imaginario y luego para el caso real veremos que la definición se puede extender sin inconvenientes.

Caso $d < 0$

Recordemos que este caso se corresponde a tomar K imaginario.

Demostración (del Teorema 3.2.1; caso $d < 0$). Recordar que para cada primo ramificado p en K hay un isomorfismo de grupos natural $(\mathscr{O}_\mathfrak{p}/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$ (donde $\mathscr{O}_\mathfrak{p}$ denota la completación de $\mathscr{O}_K$ en $\mathfrak{p}$). En particular, denotaremos por δ_p ó ε_p al mismo caracter de $(\mathscr{O}_\mathfrak{p}/\mathfrak{p})^\times$. Siguiendo la estrategia descripta anteriormente en la Sección 1.7.1, sea $\chi_p : \mathscr{O}_\mathfrak{p}^\times \to \overline{\mathbb{Q}}^\times$ el caracter dado por:

- Si $\mathfrak{p}$ es un primo impar (i.e. $\mathfrak{p} \nmid 2$) no ramificado, $\chi_\mathfrak{p}$ es el caracter trivial.
- Si p es un primo impar que ramifica en $K/\mathbb{Q}$ y $\mathfrak{p} \mid p$,

$$\chi_\mathfrak{p} = \varepsilon_p \delta_p. \tag{3.3}$$

- La componente arquimediana de χ es trivial.

Su definición local en los lugares que dividen a 2 es más complicada. Supongamos que 2 no se parte en K, y sea $\mathfrak{p}_2$ el único primo que lo divide 2. El caracter $\chi_{\mathfrak{p}_2}$ tiene por conductor un divisor de 2^3; la estructura de grupo de $(\mathscr{O}_{\mathfrak{p}_2}/2^n)^\times$ y sus generadores están dados en la Tabla 3.2.3. Los generadores están ordenados de manera tal que el orden del generador i coincida con el factor i de la estructura del grupo, mientras que las normas de los elementos están dadas módulo 8. Definimos $\chi_{\mathfrak{p}_2}$ en el conjunto de generadores de la siguiente forma:

d	n	Estructura	Generadores	Normas
3	3	$\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$	$\{\sqrt{d}, 1+2\sqrt{d}, -1\}$	$\{5, 5, 1\}$
5	3	$\mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	$\{\zeta_3, \sqrt{d}, 3+2\sqrt{d}, -1\}$	$\{1, 3, 5, 1\}$
7	3	$\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$	$\{\sqrt{d}, 1+2\sqrt{d}, 5\}$	$\{1, 5, 1\}$
par	2	$\mathbb{Z}/4 \times \mathbb{Z}/2$	$\{1+\sqrt{d}, -1\}$	$\{3, 1\}$

Tabla 3.2.3

- Si $d \equiv 15 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.
- Si $d \equiv 7 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = -1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(5) = -1$.
- Si $d \equiv 5 \pmod{8}$, $\chi_{\mathfrak{p}_2}(\zeta_3) = 1$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = i$, $\chi_{\mathfrak{p}_2}(3+2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = 1$.
- Si $d \equiv 11 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- Si $d \equiv 3 \pmod{16}$, $\chi_{\mathfrak{p}_2}(\sqrt{d}) = -1$, $\chi_{\mathfrak{p}_2}(1+2\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- Si $d \equiv 6 \pmod{8}$ y $\#Q_3 + \#Q_5$ es par, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = 1$.
- Si $d \equiv 6 \pmod{8}$ y $\#Q_3 + \#Q_5$ es impar, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = i$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- Si $d \equiv 2 \pmod{8}$ y $\#Q_3 + \#Q_5$ es par, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = 1$, $\chi_{\mathfrak{p}_2}(-1) = -1$.
- Si $d \equiv 2 \pmod{8}$ y $\#Q_3 + \#Q_5$ es impar, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = i$, $\chi_{\mathfrak{p}_2}(-1) = 1$.

Por último,

- Si $d \equiv 1 \pmod{8}$, el primo 2 se parte como $2 = \mathfrak{p}_2\overline{\mathfrak{p}}_2$. Sea $\chi_{\mathfrak{p}_2} := \delta_{-2}$ y $\chi_{\overline{\mathfrak{p}}_2} := 1$ (trivial) o tomamos $\chi_{\mathfrak{p}_2} := \delta_2$ y $\chi_{\overline{\mathfrak{p}}_2} := \delta_{-1}$.

Para mantener la consistencia en la prueba, denotamos por $\chi_2 = \prod_{\mathfrak{p}_2|2} \chi_{\mathfrak{p}_2}$. Definimos χ en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ como trivial en $K^\times$ y el producto de las componentes locales en el segundo factor. Incluso sin saber si nuestro caracter χ satisface la condición de compatibilidad, y sin siquiera haberlo extendido a todo el grupo de idèles, satisface las tres propiedades del enunciado, por Lema 3.2.3.

Una propiedad importante de nuestro caracter en 2 es que su restricción a los enteros 2-ádicos siempre satisface

$$\chi_2|_{\mathbb{Z}_2^\times} = \delta_2^{v_2(d)+1} \delta_{-1}^{\#Q_5+\#Q_7}. \tag{3.4}$$

Compatibilidad: el subgrupo de unidades de K es generado por raíces de orden 2, 6 y 4 (para $\mathbb{Q}(\sqrt{-1})$). Como todos los caracteres tienen orden una potencia de 2, la relación de compatibilidad en la raíces de orden 3 (si K tiene alguna) es trivial. Si $K = \mathbb{Q}(\sqrt{-1})$, todos los conjuntos Q_i, $i = 1, 3, 5, 7$ son vacíos y la compatibilidad en $\sqrt{-1}$ se sigue del hecho de que $\chi_2(\sqrt{-1}) = 1$ en dicho caso.

A continuación realizaremos el siguiente abuso de notación: para un ideal primo $\mathfrak{p}$ de $\mathscr{O}_K$, denotaremos por $\mathfrak{p} \in Q_i$ al hecho de que el único primo en $\mathfrak{p} \cap \mathbb{Z}$ pertenezca a dicho conjunto. La compatibilidad en -1 se sigue de

$$\chi(-1) = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(-1) = \prod_{\mathfrak{p} \in Q_1 \cup Q_5 \cup Q_7} \chi_{\mathfrak{p}}(-1)\chi_2(-1) = (-1)^{\#Q_5+\#Q_7} \delta_{-1}(-1)^{\#Q_5+\#Q_7} = 1. \tag{3.5}$$

Extensión: Como fue explicado anteriormente, para extender χ a todo el grupo de idèles $\mathbb{I}_K$, es suficiente definir en idèles cuya imagen por Id (en 2.2) generan el grupo de clases de K. Sean $\{\mathfrak{r}_1, \cdots, \mathfrak{r}_\mathfrak{h}\}$ ideales primos de K que generan $\mathrm{Cl}(K)$ (podemos y asumiremos que no ramifican en $K/\mathbb{Q}$). Como $\mathfrak{r}_i$ no es principal, debe partirse en $K/\mathbb{Q}$, con lo cual si $r_i = \mathscr{N}(\mathfrak{r}_i)$, el elemento a_i en $\mathbb{I}_K$ con componente infinita trivial y componentes finitas:

$$(a_i)_\mathfrak{p} = \begin{cases} r_i & \text{si } \mathfrak{p} = \mathfrak{r}_\mathfrak{i}, \\ 1 & \text{caso contrario.} \end{cases}$$

es una preimagen de $\mathfrak{r}_i$ por Id. Como queremos que χ sea un caracter, es suficiente dar sus valores en cada elemento $(a_i)_\mathfrak{p}$. Para cada ideal $\mathfrak{r}_i$ de orden una potencia de 2 en la descomposición p-primaria definimos

$$\chi(a_i) = \sqrt{\varepsilon(\mathscr{N}(a_i))} \tag{3.6}$$

(realmente no es importante qué raíz se toma).

Sea $\mathfrak{r}_i$ un ideal cuyo orden es $p_i^{r_i}$ con p_i un primo impar. El valor $\chi(a_i)$ no puede ser arbitrario; como p_i es impar, existe un ideal $\mathfrak{t}$ tal que $\mathfrak{t}^2$ vive en la misma clase que $\mathfrak{r}_i$. En particular, si b_i denota un idèle en la preimagen de $\mathfrak{t}$ por Id, debe existir $\alpha \in K^\times$, $u \in \prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ tal que $a_i = \alpha u b_i^2$. Como queremos que χ sea un caracter, se debe satisfacer que

$$\chi(a_i) = \chi(u)\chi(b_i^2) = \chi(u)\chi(b_i)^2 = \chi(u)\varepsilon(\mathscr{N}(b_i)), \tag{3.7}$$

con lo cual hay un único posible valor para $\chi(a_i)$. Para chequear su correcta definición, supongamos que

$$a_i = \alpha u b_i^2 = \tilde{\alpha}\tilde{u}\tilde{b_i}^2.$$

Por un lado, $(b_i/\tilde{b_i})^2$ se corresponde a un ideal principal. Luego, por Lema 3.2.4 $\chi((b_i/\tilde{b_i})^2) = \varepsilon(\mathscr{N}((b_i/\tilde{b_i})))$. Por otro lado,

$$\begin{aligned} \varepsilon(\mathscr{N}(b_i))\chi(u) &= \varepsilon(\mathscr{N}(\tilde{b_i}))\frac{\varepsilon(\mathscr{N}(b_i))}{\varepsilon(\mathscr{N}(\tilde{b_i}))}\chi(u) \\ &= \varepsilon(\mathscr{N}(\tilde{b_i}))\chi(b_i^2/\tilde{b_i}^2)\chi(u) \\ &= \varepsilon(\mathscr{N}(\tilde{b_i}))\chi(\tilde{u}/u)\chi(u) = \varepsilon(\mathscr{N}(\tilde{b_i}))\chi(\tilde{u}). \end{aligned}$$

Por lo tanto, la definición dada en (3.7) es correcta. Luego simplemente extendemos a χ multiplicativamente a todo el grupo de idèles. Recordar que ya probamos que χ^2 y $\varepsilon \circ \mathscr{N}$ coinciden en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ con lo cual con esta definición coincidirán en todo el grupo de idèles $\mathbb{I}_K$.

En este punto hay una posible inconsistencia: ¡No es claro por qué la función multiplicativa que definimos esté bien definida! Una vez más, una potencia del idèle a_i vive en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$, por lo tanto debemos probar que nuestra definición realmente extiende la anterior. Para evitar confusiones, por el momento denotemos por $\tilde{\chi}$ a la función cuyo valor en los idèles a_i está dado por (3.7) y (3.6) y sea χ el caracter en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ definido anteriormente; si el idèle a_i corresponde a un ideal de orden s en el grupo de clases, la relación de consistencia se traduce en la igualdad $\tilde{\chi}(a_i)^s = \chi(a_i^s)$. Es suficiente probarla en los siguientes dos casos:

• El ideal $\mathfrak{r}_i$ tiene orden impar s en el grupo de clases. Luego, como fue explicado anteriormente, existe $b_i \in \mathbb{I}_K$, $\alpha \in K^\times$ y $u \in \prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ tales que $a_i = \alpha u b_i^2$. Notar que $\mathrm{Id}(b_i^s)$ también es un ideal principal, con lo cual b_i^s vive en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$. Luego, por (3.7) y el hecho de que $\chi^2 = \varepsilon \circ \mathscr{N}$ en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$, tenemos que

$$\tilde{\chi}(a_i)^s = \chi(u)^s \varepsilon(\mathscr{N}(b_i))^s = \chi(u)^s \varepsilon(\mathscr{N}(b_i^s)) = \chi(u)^s \chi^2(b_i^s) = \chi(u^s b_i^{2s}) = \chi(a_i^s).$$

• El ideal $\mathfrak{r}_i$ tiene orden una potencia de 2, digamos 2^s, y no es un cuadrado (pues genera el grupo de clases). Por definición queremos probar la igualdad

$$\chi(a_i^{2^s}) = \tilde{\chi}(a_i)^{2^s} = \varepsilon(\mathscr{N}(a_i))^{2^{s-1}} = \varepsilon(\mathscr{N}(a_i^{2^{s-1}})).$$

Sea $b_i = a_i^{2^{s-1}}$, un idèle cuyo cuadrado satisface que $\mathrm{Id}(b_i^2)$ es principal. El Lema 3.2.4 implica que

$$\chi(b_i^2) = \varepsilon(\mathscr{N}(b_i)),$$

de lo cual se sigue el resultado.

Ahora que definimos el caracter χ en todo el grupo de idèles y probamos que está bien definido, sólo resta verificar que nuestra extensión también satisface que

$${}^\tau\chi = \chi \cdot (\psi_{-2} \circ \mathscr{N})$$

para todos los elementos de $\mathbb{I}_K$. Como esto ya fue probado para los elementos de $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$, es suficiente probarlo para los idèles a_i (definidos como antes) con componentes finitas locales

$$(a_i)_{\mathfrak{p}} = \begin{cases} r_i & \text{si } \mathfrak{p} = \mathfrak{r}_i, \\ 1 & \text{caso contrario.} \end{cases}$$

Notar que $\tau(a_i)$ es el idèle de K con valor r_i en $\overline{\mathfrak{r}_i}$ y 1 en todos los demás lugares. Entonces

$${}^\tau\chi(a_i) = \chi(\tau(a_i)) = \chi(a_i)^{-1}\chi(a_i\tau(a_i)) = \chi(a_i)^{-1}\chi\left(\frac{a_i\tau(a_i)}{r_i}\right), \tag{3.8}$$

donde $\frac{1}{r_i}$ denota la imagen de $K^\times \hookrightarrow \mathbb{I}_K$. Notar que $\frac{a_i\tau(a_i)}{r_i}$ es una unidad en todos los lugares, entonces

$$\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi_2(r_i)^{-1} \prod_{\mathfrak{p} \in Q_1 \cup Q_5 \cup Q_7} \chi_{\mathfrak{p}}(r_i)^{-1}. \tag{3.9}$$

Por la fórmula del producto (Teorema 1.3.5),

$$1 = \varepsilon(r_i) = \varepsilon_{r_i}(r_i)\varepsilon_2(r_i) \prod_{p \in Q_3 \cup Q_5} \varepsilon_p(r_i). \tag{3.10}$$

Como $\varepsilon_{r_i}(r_i) = \varepsilon(\mathscr{N}(a_i)) = \chi^2(a_i)$, multiplicando (3.9) y (3.10) y usando que $\chi_{\mathfrak{p}}(r_i) = \varepsilon_p(r_i)\delta_p(r_i)$ tenemos que

$$\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi^2(a_i)\chi_2(r_i)^{-1}\varepsilon_2(r_i)\prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7}\delta_p(r_i). \tag{3.11}$$

Recordar que r_i se parte en K, con lo cual $\left(\frac{d}{r_i}\right) = 1$ y reciprocidad cuadrática implica que

$$1 = \left(\frac{2}{r_i}\right)^{v_2(d)}\left(\frac{-1}{r_i}\right)^{\#Q_3+\#Q_7+1}\prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7}\delta_p(r_i).$$

En particular, el lado derecho de (3.8) es igual a

$$\chi(a_i)\chi_2(r_i)^{-1}\varepsilon_2(r_i)\delta_2(r_i)^{v_2(d)}\delta_{-1}(r_i)^{\#Q_3+\#Q_7+1} = \\ \chi(a_i)\cdot\left(\delta_2(r_i)\delta_{-1}(r_i)^{\#Q_5+\#Q_7}\varepsilon_2(r_i)\delta_{-1}(r_i)^{\#Q_3+\#Q_7+1}\right).$$

Una cuenta similar (pero más simple) muestra que $\psi_{-2}(\mathscr{N}(a_i)) = \delta_{-2}(r_i)$, por lo que el resultado se sigue de que

$$\delta_2(r_i)\varepsilon_2(r_i)\delta_{-1}(r_i)^{\#Q_3+\#Q_5+1} = \delta_2(r_i)\delta_{-1}(r_i) = \delta_{-2}(r_i).$$

□

Aunque construimos un caracter de Hecke que satisface

$${}^{\tau}\chi = \chi\cdot\psi_{-2},$$

lo cual es suficiente para nuetro problema, es natural tratar de encontrar todos los posibles caracteres de Hecke de orden finito que satisfagan la misma condición. Notar que si χ es tal caracter, y ν es un caracter de $G_{\mathbb{Q}}$, entonces $\chi\cdot\nu$ también satisface la misma condición.

Teorema 3.2.2. *Sean χ_1 y χ_2 caracteres de Hecke de orden finito tales que ${}^{\tau}\chi_i = \chi_i\cdot\psi_{-2}$ para $i = 1, 2$. Entonces existe un caracter racional $\nu : G_{\mathbb{Q}} \to \mathbb{C}^{\times}$ tal que $\chi_2 = \chi_1\cdot\nu$.*

Demostración. Denotemos por $\tilde{\nu}$ al cociente $\frac{\chi_1}{\chi_2}$, un caracter en $\mathbb{I}_K$. La hipótesis ${}^{\tau}\chi_i = \chi_i\cdot\psi_{-2}$ implica que ${}^{\tau}\tilde{\nu} = \tilde{\nu}$. Sea $\mathbb{I}_K^1$ el núcleo de la función norma $\mathscr{N} : \mathbb{I}_K \to \mathbb{I}_{\mathbb{Q}}$.

Afirmación: el caracter $\tilde{\nu}$ es trivial en $\mathbb{I}_K^1$.

Para probar la afirmación, sea v un lugar de $\mathbb{Q}$ que no se parta en K, y sea w el lugar de K que lo divide. En particular $K_w/\mathbb{Q}_v$ es una extensión cuadrática de Galois. Si $k \in K_w$ tiene norma uno, el Teorema 90 de Hilbert implica que existe $t \in K_w$ tal que $k = \frac{t}{\sigma(t)}$ para $\sigma \in \mathrm{Gal}(K_w/\mathbb{Q}_v)$ no trivial. La hipótesis ${}^{\tau}\tilde{\nu} = \tilde{\nu}$ entonces implica que $\tilde{\nu}(k) = 1$. Si el lugar v se parte, sean w_1, w_2 los dos lugares de K que lo dividen, y sea $(k_1, k_2) \in K_{w_1}\times K_{w_2}$ un elemento de norma uno, i.e. $k_1\cdot k_2 = 1$. La hipótesis ${}^{\tau}\tilde{\nu} = \tilde{\nu}$ implica que $\tilde{\nu}_{w_1} = \tilde{\nu}_{w_2}$, luego $\tilde{\nu}_{w_1}(k_1)\tilde{\nu}_{w_2}(k_2) = \tilde{\nu}_{w_1}(k_1\cdot k_2) = 1$, como se afirmó.

Luego, el caracter $\tilde{\nu}$ da un caracter bien definido en $\mathscr{N}(\mathbb{I}_K)$, subgrupo de $\mathbb{I}_{\mathbb{Q}}$, y podemos extenderlo a $\mathbb{Q}^{\times}\mathscr{N}(\mathbb{I}_K)$ haciéndolo trivial en los elementos de $\mathbb{Q}^{\times}$. Recordar que $\mathbb{Q}^{\times}\mathscr{N}(\mathbb{I}_K)$ tiene índice finito en $\mathbb{I}_{\mathbb{Q}}$, así que sea ν cualquier extensión de $\tilde{\nu}$ a todo el grupo de idèles $\mathbb{I}_{\mathbb{Q}}$. Entonces, por construcción $\tilde{\nu}$ coincide con $\nu\circ\mathscr{N}$ en $\mathbb{I}_K$, en particular $\chi_1 = \chi_2\cdot(\nu\circ\mathscr{N})$. □

Lemas utilizados en la demostración del Teorema 3.2.1

Lema 3.2.3. *El caracter χ definido en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ satisface las tres propiedades del Teorema 3.2.1.*

Demostración. 1. Necesitamos verificar que la igualdad

$$\chi^2 = \varepsilon \circ \mathscr{N}$$

se satisface para todo elemento en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$. El enunciado es claro para los elementos de $K^\times$ (ya que ambos términos son triviales) y para los elementos de $\mathbb{C}^\times$ por la misma razón, lo cual nos conduce a verificarlo para cada componente local. La prueba para ideales primos impares $\mathfrak{p}$ es la siguiente: si $\mathfrak{p}$ no ramifica en $K/\mathbb{Q}$, entonces el resultado es claro (pues todos los caracteres son triviales), mientras que en primos ramificados, se sigue de (3.3) junto con el Lema 2.2.1.

Finalmente, es fácil de ver que $\chi_2^2 = \varepsilon_2 \circ \mathscr{N}$ usando los valores del caracter de la Tabla 3.2.2, la paridad de la Tabla 3.2.1 y la norma de los generadores dada en la Tabla 3.2.3.

2. De la definición de ε y χ se sigue claramente la hipótesis sobre la ramificación.

3. De su definición, es claro que para todos los primos impares ${}^\tau\chi_{\mathfrak{p}} = \chi_{\mathfrak{p}}$, con lo cual la tercera condición también se satisface. La razón por la que vale para los primos $\mathfrak{p}_2$ que dividen a 2 es que ${}^\tau\chi_{\mathfrak{p}_2} \cdot \chi_{\mathfrak{p}_2} = \chi_{\mathfrak{p}_2} \circ \mathscr{N}$, por lo tanto ${}^\tau\chi_{\mathfrak{p}_2} = \chi_{\mathfrak{p}_2}^{-1} \cdot (\chi_{\mathfrak{p}_2} \circ \mathscr{N})$. Un simple análisis caso por caso en los generadores muestra que ${}^\tau\chi_{\mathfrak{p}_2} = \chi_{\mathfrak{p}_2} \cdot (\delta_{-2} \circ \mathscr{N})$.

□

Lema 3.2.4. *Sea b_i, un idèle cuyo cuadrado satisface que $\mathrm{Id}(b_i^2)$ es principal, entonces el caracter definido en (3.6) satisface que*

$$\chi(b_i^2) = \varepsilon(\mathscr{N}(b_i)). \tag{3.12}$$

Demostración. Es bien sabido que el subgrupo de 2-torsión del grupo de clases es generado por los ideales primos $\mathfrak{q} = \langle q, \sqrt{d}\rangle$, donde q es un primo impar que divide a d, y también el primo $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{d}\rangle$ cuando $d \equiv 3 \pmod 4$. Sea q un primo impar que divide a d y sea b_q el idèle de K definido como

$$(b_q)_{\mathfrak{p}} = \begin{cases} 1 & \text{si } \mathfrak{p} \neq \mathfrak{q}, \\ \sqrt{d} & \text{si } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

Luego $\mathrm{Id}(b_q) = \mathfrak{q}$. Similarmente, si $d \equiv 3 \pmod 4$, sea b_2 el idèle definido por

$$(b_2)_{\mathfrak{p}} = \begin{cases} 1 & \text{si } \mathfrak{p} \neq \mathfrak{p}_2, \\ 1 + \sqrt{d} & \text{si } \mathfrak{p} = \mathfrak{p}_2. \end{cases}$$

Afirmación: es suficiente probar (3.12) para los elementos b_q.

Supongamos que la igualdad (3.12) se satisface para dichos elementos. Sea b un idèle que cumple que $\mathrm{Id}(b)^2$ es principal. Entonces

$$\mathrm{Id}(b) = \prod_{q|2d} \mathrm{Id}(b_q)^{\epsilon_q},$$

para algún $\epsilon_q \in \{0, 1\}$, con lo cual existe $\alpha \in K^\times$, y $u \in \prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$ tal que $b = \alpha u \prod_{q|2d} b_q^{\epsilon_q}$. Por la propiedad multiplicativa del caracter χ,

$$\chi(b^2) = \chi(u)^2 \prod_{q|2d} \chi(b_q^2)^{\epsilon_q} = \varepsilon(\mathscr{N}(u)) \prod_{q|2d} \varepsilon(\mathscr{N}(b_q))^{\epsilon_q} = \varepsilon(\mathscr{N}(b)).$$

Sea q un primo impar que divide a d. Para probar (3.12) para los elementos b_q, calculamos ambos lados de la igualdad y probaremos que coinciden. Notar que $b_q^2 = qc_q$, donde $q \in K^\times$ y $c_q = b_q^2/q$ tiene la propiedad de que es una unidad en todos los lugares finitos. Entonces

$$\chi(b_q^2) = \chi_{\mathfrak{q}}\left(\frac{d}{q}\right)\chi_2\left(\frac{1}{q}\right)\prod_{\mathfrak{p}\in Q_1\cup Q_5\cup Q_7}\chi_{\mathfrak{p}}\left(\frac{1}{q}\right), \tag{3.13}$$

donde el producto corre sobre todos los primos $\mathfrak{p} \neq \mathfrak{q}$. Por otro lado, el lado derecho de (3.12) es igual a

$$\varepsilon(\mathscr{N}(b_q)) = \varepsilon_q(-d) = \varepsilon_q(-d/q)\varepsilon_2(q)^{-1}\prod_{p\in Q_3\cup Q_5}\varepsilon_p(q)^{-1}, \tag{3.14}$$

donde el producto corre sobre los primos distintos de q. Recordar que para cada primo ramificado, bajo el isomorfismo $(\mathscr{O}_K/\mathfrak{p})^\times \simeq (\mathbb{Z}/p)^\times$, tenemos la igualdad $\chi_{\mathfrak{p}} = \varepsilon_p\delta_p$. En particular, ambos lados se evalúan igual en elementos de $\mathbb{Z}_p^\times$. Usando tal relación en (3.13) para todos los primos impares ramificados y pegando junto con los términos que involucran a ε tenemos

$$\chi(b_q^2) = \chi_2^{-1}(q)\varepsilon_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_1\cup Q_3\cup Q_5\cup Q_7\\ p\neq q}}\varepsilon_p^{-1}(q)\cdot\delta_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_1\cup Q_3\cup Q_5\cup Q_7\\ p\neq q}}\delta_p(q) =$$

$$= \varepsilon_q(-d)\left(\chi_2^{-1}(q)\varepsilon_q(-1)\varepsilon_2(q)\delta_q(2)^{v_2(d)}\right)\cdot\left(\delta_q(2)^{v_2(d)}\delta_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_1\cup Q_3\cup Q_5\cup Q_7\\ p\neq q}}\delta_p(q)\right). \tag{3.15}$$

Nuestro objetivo es probar que el producto de todos los factores de la última expresión excepto el primero es igual a 1, para que se siga el resultado. Cuando $q \equiv 1 \pmod 4$, la reciprocidad cuadrática implica que $\delta_q(p) = \delta_p(q)$ y $\delta_q(-1) = 1$, luego el último factor (entre paréntesis) en (3.15) es igual a 1. Por otro lado, para $q \equiv 3 \pmod 4$ la reciprocidad cuadrática implica que $\delta_q(p) = \delta_p(q)\delta_p(-1)$. Notar que q es uno de los elementos en $Q_3 \cup Q_7$, con lo cual el último factor en (3.15) es igual a $(-1)^{\#Q_3+\#Q_7}$. En ambos casos, el último factor es igual a $\delta_{-1}(q)^{\#Q_3+\#Q_7}$.

Con respecto al segundo factor, nuevamente la reciprocidad cuadrática implica que $\delta_q(2) = \delta_2(q)$ (recordar la definición de δ_2 de Tabla 3.2.2). Por definición, $\varepsilon_2 = \delta_{-1}^{\#Q_3+\#Q_5}$ y en elementos de $\mathbb{Z}_2^\times$, $\chi_2 = \delta_2^{v_2(d)+1}\delta_{-1}^{\#Q_5+\#Q_7}$ (ver (3.4)), luego el lado derecho de (3.15) es igual a

$$\varepsilon_q(-d)\delta_2(q)\varepsilon_q(-1)\delta_{-1}(q)^{2\#Q_3+2\#Q_5+2\#Q_7} = \varepsilon_q(-d)\delta_2(q)\varepsilon_q(-1).$$

Luego, esto nos conduce a probar que $\varepsilon_q(-1)\delta_2(q) = 1$, que se sigue de las definiciones, ya que:

- Si $q \equiv \pm 1 \pmod 8$, $\varepsilon_q(-1) = 1 = \delta_2(q)$.
- Si $q \equiv \pm 3 \pmod 8$, $\varepsilon_q(-1) = -1 = \delta_2(q)$.

Supongamos ahora que $d \equiv 3 \pmod 4$, que es cuando además tenemos que chequear la compatibilidad en b_2. Una cuenta similar a la anterior da como resultado lo siguiente:

$$\varepsilon_2(1-d) = \varepsilon_2\left(\frac{1-d}{2}\right)\cdot\prod_{p\in Q_3\cup Q_5}\varepsilon_p(2)^{-1},$$

mientras que

$$\chi(b_i^2) = \chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right)\cdot\prod_{p\in Q_3\cup Q_5}\varepsilon_p(2)^{-1}\cdot\prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7}\delta_p(2).$$

Por reciprocidad cuadrática, $\prod_{p\in Q_1\cup Q_3\cup Q_5\cup Q_7}\delta_p(2) = (-1)^{\#Q_3+\#Q_5}$, luego el enunciado se sigue de los siguientes hechos fáciles de verificar (directo de sus definiciones):

- Si $d \equiv 7 \pmod 8$, entonces $\varepsilon_2\left(\frac{1-d}{2}\right) = 1$, $\chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) = 1$ y $\#Q_3 + \#Q_5$ es par.
- Si $d \equiv 11 \pmod{16}$, entonces $\varepsilon_2\left(\frac{1-d}{2}\right) = -1$, $\chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) = 1$ y $\#Q_3 + \#Q_5$ es impar.
- Si $d \equiv 3 \pmod{16}$, entonces $\varepsilon_2\left(\frac{1-d}{2}\right) = 1$, $\chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) = -1$ y $\#Q_3 + \#Q_5$ es impar.

□

Caso $d > 0$

Es natural estudiar cuándo nuestra construcción se puede extender a valores positivos de d, i.e. a cuerpos cuadráticos reales. El problema ahora es que necesitamos cierto control en la unidad fundamental. Veremos a continuación que el Teorema 3.2.1 vale para cuerpos cuadráticos reales, donde se impone una condición extra en el lugar arquimediano. Tomamos precisamente las mismas definiciones locales para χ que en el caso anterior. En este caso la sucesión exacta corta (2.2) se reescribe como

$$0 \longrightarrow K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2) \longrightarrow \mathbb{I}_K \xrightarrow{\text{Id}} \mathrm{Cl}(K) \longrightarrow 0.$$

Recordar que como $(\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times (\mathbb{R}^\times)^2) \cap K^\times = \mathscr{O}_K^\times$, la condición de compatibilidad nos implica que el producto de las componentes locales en las unidades es igual a 1. Como ahora $d > 0$, tenemos que $\mathscr{O}_K^\times = \langle -1, \epsilon \rangle$, donde ϵ denota una unidad fundamental. Con lo cual, es suficiente chequear la condición en -1 y ϵ.

Unidad fundamental de norma -1:

En el caso en el que la unidad fundamental ϵ tenga norma -1, la prueba es más directa.

Demostración (del Teorema 3.2.1; caso $d > 0$ y $\mathscr{N}(\epsilon) = -1$). Un hecho importante a considerar es que al cambiar el signo de d, cambia la Tabla 3.2.1 y por lo tanto a la hora de probar (3.5), obtenemos un factor -1 extra. Por lo tanto necesitamos añadir ramificación a uno de los lugares arquimedianos (luego especificaremos a cuál).

Sea ϵ una unidad fundamental (fija). La prueba funciona mutatis mutandis una vez que chequeamos la compatibilidad de χ en ϵ. La ventaja de asumir que ϵ tiene norma -1 es que $Q_3 = Q_7 = \emptyset$, pues si $\epsilon = a + b\sqrt{d}$, con $2a, 2b \in \mathbb{Z}$, la condición $a^2 - db^2 = -1$ implica que -1 es un cuadrado para todos los primos impares que dividen a d. Más aún, para tales primos, la reducción de ϵ tiene orden 4, con lo cual $\chi_p(\epsilon) = \pm 1$ si $p \in Q_1$ y es una raíz cuarta primitiva de la unidad si $p \in Q_5$. Afirmamos que $\chi_2(\epsilon) \prod_{p \in Q_5} \chi_p(\epsilon) = \pm 1$ (y por lo tanto $\chi_2(\epsilon) \prod_{p \in Q_1 \cup Q_5} \chi_p(\epsilon) = \pm 1$).

- Si $d \equiv 1 \pmod 8$ entonces $\#Q_5$ es par y χ_2 es cuadrático, con lo cual se verifica lo enunciado.
- Si $d \equiv 5 \pmod 8$ entonces $\#Q_5$ es impar, 2 es inerte, χ_2 tiene orden 4 y evaluado en cualquier elemento de orden 4 da un raíz cuarta primitiva de la unidad.
- Si $d \equiv 2 \pmod 8$ y $\#Q_5$ es par, χ_2 tiene orden 2, mientras que si $\#Q_5$ es impar, χ_2 tiene orden 4 y ϵ tiene orden 8 (se sigue de la Tabla 3.2.3, ya que su norma es -1) entonces $\chi_2(\epsilon)$ es una raíz cuarta primitiva de la unidad.

Luego, si $\chi_2(\epsilon) \prod_{p \in Q_1 \cup Q_5} \chi_p(\epsilon) = 1$, definimos χ como trivial en la componente arquimediana que toma valor negativo en ϵ y el caracter signo en la otra componente, mientras que si el producto anterior es -1, tomamos la elección opuesta. Como $\mathscr{N}(\epsilon) = -1$, la compatibilidad se satisface y la misma prueba del caso cuadrático imaginario se aplica. □

Unidad fundamental de norma 1**:**

Para el resto de los cuerpos cuadráticos reales la prueba es más sutil. Como la compatibilidad ya fue probada para el caso en que ϵ tenga norma -1 entonces luego de reemplazar ϵ por $-\epsilon$ en caso de ser necesario, podemos asumir que ϵ es totalmente positivo. El principal obstáculo es tener algún entendimiento de la reducción de una unidad fundamental positiva módulo primos que ramifican en K. Queda así establecido el siguiente problema.

Problema: Sea $K/\mathbb{Q}$ un cuerpo cuadrático real, y ϵ una unidad fundamental totalmente positiva, ¿Qué se puede decir acerca de la extensión $K(\sqrt{\epsilon})/K$?

En lo que resta de la sección, d será un discriminante fundamental positivo. Sea $p \mid d$ un primo impar y sea $\mathfrak{p}$ el único primo de K que lo divide. La hipótesis $\mathscr{N}(\epsilon) = 1$ implica que $\epsilon \equiv \pm 1 \pmod{\mathfrak{p}}$. Sea

$$\mathcal{P}_{\pm} = \{p \mid d,\ p \text{ impar} \ : \ \epsilon \equiv \pm 1 \pmod{\mathfrak{p}}\}.$$

Si 2 ramifica en $K/\mathbb{Q}$, sea $\mathfrak{p}_2$ el único primo de K que lo divide. Queremos agradecer a Yingkun Li por ofrecernos una prueba del siguiente teorema.

Teorema 3.2.5. *Sea* $\omega := \prod_{p \in \mathcal{P}_-} p$*. Entonces:*

- *si* 2 *no ramifica en* $K/\mathbb{Q}$*, tenemos que* $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$*,*
- *si* 2 *sí ramifica en* $K/\mathbb{Q}$*,* $K(\sqrt{\epsilon}) = K(\sqrt{2\omega})$ *o* $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$*.*

Más aún, si $8 \mid d$*, el último caso ocurre precisamente cuando* $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$*.*

Demostración. Recordemos algunos resultados conocidos sobre el grupo de clases estrecho de un cuerpo cuadrático real. El resultado fue demostrado mayormente por Gauss [44] (ver también [9] para una presentación más moderna), aunque el aporte de Gauss fue vía el estudio formas cuadráticas binarias indefinidas. Entre tales formas, existen algunas llamadas "formas ambiguas" (ver [9] página 7 del Capítulo 1 y página 24 del Capítulo 3), que son precisamente los elementos de orden dos bajo la ley de composición de Gauss. El número total de clases ambiguas (incluída la trivial) es igual a 2^{t-1}, donde t es el número de divisores primos de d (por [9, Proposición 4.7] y su prueba).

Recordar que hay una correspondencia entre clases de equivalencia estrictas de formas cuadráticas binarias indefinidas de discriminante d y clases de ideales del grupo de clases estrecho de K. Bajo esta correspondencia, las formas ambiguas se corresponden con ideales de orden dos en el grupo de clases estrecho. Pero tales ideales se corresponden precisamente con los ideales primos que ramifican en K (indexados por divisores de d), por [9, Corolario 4.9]. En particular, existe un único ideal principal no trivial y libre de cuadrados $\mathfrak{d}$ (generado por un elemento totalmente positivo α) dividiendo al diferente $\mathcal{D}$ de K. Si $\omega := \mathscr{N}\,\mathfrak{d} = \mathscr{N}(\alpha) = \alpha\overline{\alpha}$, entonces $\omega \mid d$.

Como todos los primos ramificados son invariantes bajo conjugación, y $\mathfrak{d}$ es divisible sólo por primos ramificados, $\overline{\mathfrak{d}} = \mathfrak{d}$. Entonces el cociente $\frac{\alpha}{\overline{\alpha}} \in \mathscr{O}_K$ es una unidad totalmente positiva que no puede ser trivial (ya que en ese caso $\alpha \in \mathbb{Q}_{>0}$, pero debe dividir al diferente de K y también generar un ideal libre de cuadrados de $\mathscr{O}_K$, con lo cual es igual a 1). Sustituyendo α por $\epsilon^k\alpha$ cambia el cociente $\frac{\alpha}{\overline{\alpha}}$ por un factor ϵ^{2k}. Luego, podemos asumir que

$$\frac{\alpha}{\overline{\alpha}} = \epsilon. \tag{3.16}$$

Entonces $\sqrt{\epsilon} = \frac{\sqrt{\alpha\overline{\alpha}}}{\overline{\alpha}}$ y luego $K(\sqrt{\epsilon}) = K(\sqrt{\omega})$. Esto nos conduce a determinar el conjunto de los primos que dividen a ω. Sea $\mathfrak{p}$ un ideal primo que divide a $\mathcal{D}$ y asumamos que $\mathfrak{p} \nmid 2$.

- El hecho de que $\alpha + \overline{\alpha} \in \mathfrak{d} \cap \mathbb{Z} = \langle\omega\rangle$ (que genera sobre K el ideal $\mathfrak{d}^2$) implica que $\alpha + \overline{\alpha} \in \mathfrak{d}^2$, luego $\epsilon + 1 = \frac{\alpha}{\overline{\alpha}} + 1 = \frac{\alpha+\overline{\alpha}}{\overline{\alpha}} \in \mathfrak{d}$ y por lo tanto $\epsilon \equiv -1 \pmod{\mathfrak{d}}$. En particular, $\epsilon \equiv -1 \pmod{\mathfrak{p}}$ para todos los ideales primos $\mathfrak{p} \mid \mathfrak{d}$.

- Por otro lado, si $\mathfrak{p} \mid \mathcal{D}$ pero $\mathfrak{p} \nmid \mathfrak{d}$ (en particular $\mathfrak{p} \nmid \alpha$), $\epsilon - 1 = \frac{\alpha - \overline{\alpha}}{\overline{\alpha}} \equiv 0 \pmod{\mathfrak{p}}$ y luego $\epsilon \equiv 1 \pmod{\mathfrak{p}}$.

Si $2 \nmid d$ entonces $\omega = \prod_{p \in \mathcal{P}_-} p$ y el enunciado se sigue. Si d es par, la única ambigüedad es cuándo ω es par o no. Supongamos que $8 \mid d$. Sea $\mathfrak{p}_2$ el ideal primo que divide a 2 ($\mathfrak{p}_2 = \langle 2, \sqrt{d/4} \rangle$). Claramente $v_{\mathfrak{p}_2}(\alpha) = v_{\mathfrak{p}_2}(\bar{\alpha}) = v_2(\omega)$. Un análisis elemental caso por caso muestra que $v_{\mathfrak{p}_2}(\alpha) \in \{0, 2\}$ si y sólo si $v_{\mathfrak{p}_2}(\epsilon - 1) \geq 3$ y $v_{\mathfrak{p}_2}(\epsilon + 1) = 2$. Similarmente, $v_{\mathfrak{p}_2}(\alpha) \in \{1, 3\}$ si y sólo si $v_{\mathfrak{p}_2}(\epsilon + 1) \geq 3$ y $v_{\mathfrak{p}_2}(\epsilon - 1) = 2$. □

Demostración (del Teorema 3.2.1; caso $d > 0$ y $\mathscr{N}(\epsilon) = 1$). Manteniendo la notación previa, sea $\chi_{\mathfrak{p}} : \mathscr{O}_{\mathfrak{p}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ definido como para el caso K imaginario. Ahora, para los lugares arquimedianos $\{v_1, v_2\}$, tomamos χ_{v_1} el caracter trivial y χ_{v_2} la función signo (el orden de los lugares arquimedianos no importa, ambas elecciones funcionan). Para un primo $\mathfrak{p}_2$ que divide a 2, reescribimos por comodidad para el lector la definición del caracter $\chi_{\mathfrak{p}_2}$, teniendo en cuenta que ahora d es un discriminante fundamental. Para facilitar la notación, sea

$$\tilde{d} = \begin{cases} d & \text{si } d \equiv 1 \pmod{4}, \\ d/4 & \text{caso contrario.} \end{cases}$$

- Si $\tilde{d} \equiv 1 \pmod{8}$, el primo 2 se parte como $2 = \mathfrak{p}_2 \overline{\mathfrak{p}}_2$. Sea $\chi_{\mathfrak{p}_2} := \delta_{-2}$ y $\chi_{\overline{\mathfrak{p}}_2} := 1$ (trivial) o tomamos $\chi_{\mathfrak{p}_2} := \delta_2$ y $\chi_{\overline{\mathfrak{p}}_2} := \delta_{-1}$.
- Si $\tilde{d} \equiv 5 \pmod{8}$, $\chi_{\mathfrak{p}}(\zeta_3) = 1$, $\chi_{\mathfrak{p}}(\sqrt{\tilde{d}}) = i$, $\chi_{\mathfrak{p}}(3 + 2\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(-1) = 1$.
- Si $\tilde{d} \equiv 7 \pmod{16}$, $\chi_{\mathfrak{p}}(\sqrt{\tilde{d}}) = -1$, $\chi_{\mathfrak{p}}(1 + 2\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(5) = -1$.
- Si $\tilde{d} \equiv 15 \pmod{16}$, $\chi_{\mathfrak{p}}(\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(1 + 2\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(5) = -1$.
- Si $\tilde{d} \equiv 3 \pmod{16}$, $\chi_{\mathfrak{p}}(\sqrt{\tilde{d}}) = -1$, $\chi_{\mathfrak{p}}(1 + 2\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(-1) = -1$.
- Si $\tilde{d} \equiv 11 \pmod{16}$, $\chi_{\mathfrak{p}}(\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(1 + 2\sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(-1) = -1$.
- Si $\tilde{d} \equiv 6 \pmod{8}$ y $\#Q_3 + \#Q_5$ es par, $\chi_{\mathfrak{p}}(1 + \sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(-1) = 1$, $\chi_{\mathfrak{p}}(5) = 1$.
- Si $\tilde{d} \equiv 6 \pmod{8}$ y $\#Q_3 + \#Q_5$ es impar, $\chi_{\mathfrak{p}}(1 + \sqrt{\tilde{d}}) = i$, $\chi_{\mathfrak{p}}(-1) = -1$, $\chi_{\mathfrak{p}}(5) = 1$.
- Si $\tilde{d} \equiv 2 \pmod{8}$ y $\#Q_3 + \#Q_5$ es par, $\chi_{\mathfrak{p}}(1 + \sqrt{\tilde{d}}) = 1$, $\chi_{\mathfrak{p}}(-1) = -1$, $\chi_{\mathfrak{p}}(5) = 1$.
- Si $\tilde{d} \equiv 2 \pmod{8}$ y $\#Q_3 + \#Q_5$ es impar, $\chi_{\mathfrak{p}}(1 + \sqrt{\tilde{d}}) = i$, $\chi_{\mathfrak{p}}(-1) = 1$, $\chi_{\mathfrak{p}}(5) = 1$.

Nuevamente para hacer la prueba consistente denotamos $\chi_2 = \prod_{\mathfrak{p}_2 \mid 2} \chi_{\mathfrak{p}_2}$. Dado que en este caso d es positivo, tenemos que $\tilde{d} = 2^{v_2(\tilde{d})} \prod_{p \in Q_1 \cup Q_2 \cup Q_3 \cup Q_5} p$ y por lo tanto el caracter satisface que

$$\chi_2|_{\mathbb{Z}_2^{\times}} = \delta_2^{v_2(d)+1} \delta_{-1}^{\#Q_5 + \#Q_7 + 1}. \tag{3.17}$$

Nuevamente, extendemos χ a $K^{\times} \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^{\times} \times (\mathbb{R}^{\times})^2)$ haciéndolo trivial en $K^{\times}$. La misma prueba del Teorema 3.2.1 funciona para ver que $\chi^2 = \varepsilon \circ \mathscr{N}$.

Compatibilidad: el subgrupo de unidades en K es generado por $\{-1, \epsilon\}$, por lo tanto es suficiente probar la compatibilidad en ambos elementos. Al cambiar el signo de d no se modifica la parte local de χ para los primos impares, pero sí en los primos que dividen a 2. Para tales primos, la restricción del caracter local a $\mathbb{Z}_2^{\times}$ difiere en δ_{-1}. En el Teorema 3.2.1 probamos la compatibilidad en -1 para cuerpos cuadráticos imaginarios. Como $\delta_{-1}(-1) = -1$, en este caso la compatibilidad en -1 se

sigue del signo extra por la contribución del caracter arquimediano. Probar la compatibilidad en ϵ toma más esfuerzo. El caracter toma valor $\chi_{\mathfrak{p}}(\epsilon) = 1$ para todos los primos que no ramifican y para los que están en $\mathcal{P}_- \cap (Q_1 \cup Q_3)$. Su valor en primos de $\mathcal{P}_- \cap (Q_5 \cup Q_7)$ es -1. Como el caracter δ_{-2} también satisface que toma el valor -1 en los primos de $Q_5 \cup Q_7$ y $+1$ en el resto de los primos, debemos probar la siguiente identidad

$$\chi_2(\epsilon) \cdot (-1)^{\#(\mathcal{P}_- \cap (Q_5 \cup Q_7))} = \chi_2(\epsilon)\delta_{-2}(\omega) = 1, \tag{3.18}$$

donde $\omega = \prod_{p \in \mathcal{P}_-} p$ como antes. La prueba del Teorema 3.2.5 implica que existe $\alpha \in \mathscr{O}_K$ tal que $\omega = \epsilon\overline{\alpha}^2$ o $2\omega = \epsilon\overline{\alpha}^2$. En el primer caso,

$$\chi_2(\overline{\alpha}^2) = \chi_2^2(\overline{\alpha}) = \varepsilon_2(\mathscr{N}(\alpha)) = \varepsilon_2(\omega).$$

Como ε_2 es como mucho cuadrático, es igual a su inverso y por lo tanto $\chi_2(\epsilon) = \chi_2(\omega)\varepsilon_2(\omega)$. Entonces la ecuación (3.18) es equivalente a

$$\chi_2(\omega)\varepsilon_2(\omega)\delta_{-2}(\omega) = 1. \tag{3.19}$$

Un hecho clave es que la hipótesis $\mathscr{N}(\alpha) = \omega$ impone limitaciones en los posibles valores de ω. Usando la ecuación (3.17), la prueba se sigue estudiando cada uno de los siguientes casos:

- Si $\tilde{d} \equiv 1 \pmod 8$, entonces $\chi_2 = \delta_{-2}$ y ε_2 es trivial, con lo cual (3.19) se satisface.
- Si $\tilde{d} \equiv 3 \pmod 8$, la condición de la norma implica que ω es congruente a 1 ó 5 módulo 8. Por definición $\chi_2|_{\mathbb{Z}_2^\times} = \delta_{-2}$ y $\varepsilon_2 = \delta_{-1}$, que es trivial en $\{1, 5\}$ y por lo tanto se verifica (3.19).
- Si $\tilde{d} \equiv 5 \pmod 8$, por definición $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ y $\varepsilon_2 = \delta_{-1}$, con lo cual (3.19) se satisface.
- Si $\tilde{d} \equiv 7 \pmod 8$, la condición de la norma implica que ω es congruente a 1 ó 5 módulo 8. Por definición $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ y $\varepsilon_2 = 1$. Pero δ_2 y δ_{-2} toman los mismos valores en $\{1, 5\}$, luego (3.19) se satisface.
- Si $\tilde{d} \equiv 2 \pmod 8$, la condición de la norma implica que ω es congruente a 1 ó 7 módulo 8. Por definición $\chi_2|_{\mathbb{Z}_2^\times} \cdot \varepsilon_2 = \delta_{-1}$, que coincide con δ_{-2} en $\{1, 7\}$, luego (3.19) vale.
- Si $\tilde{d} \equiv 6 \pmod 8$, la condición de la norma implica que ω es congruente a 1 ó 3 módulo 8. Por definición $\chi_2|_{\mathbb{Z}_2^\times} \cdot \varepsilon_2 = 1$ pero δ_{-2} es trivial en $\{1, 3\}$, con lo cual (3.19) se satisface.

Si d es impar, la igualdad $\omega = \epsilon\bar{\alpha}^2$ siempre se satisface, con lo cual se sigue el resultado. Asumamos que 2 ramifica en $K/\mathbb{Q}$ y que $2\omega = \epsilon\bar{\alpha}^2$. Sea $\mathfrak{p}_2$ el único primo de K que divide a 2. Recordemos que $K(\sqrt{\epsilon})$ no ramifica en $\mathfrak{p}_2$ si y sólo si ϵ es un cuadrado módulo 4 (ver por ejemplo [24, Lema 3.4]). La igualdad $2\omega = \epsilon\overline{\alpha}^2$ implica que

$$\left(\frac{2}{\overline{\alpha}}\right)^2 \omega = 2\epsilon. \tag{3.20}$$

Notemos que $\frac{2}{\overline{\alpha}}$ tiene valuación positiva en $\mathfrak{p}_2$, con lo cual podemos reducir la igualdad (3.20) módulo 16 para calcular para cada posible valor de ϵ el correspondiente valor de ω (salvo cuadrados) vía cálculos computacionales. No todos los elementos de $(\mathscr{O}_K/8)^\times$ corresponden a un posible valor de ϵ, ya que el hecho de que $K(\sqrt{\epsilon})/\mathbb{Q}$ sea bicuadrático impone una gran limitación. Antes de presentar los resultados de los cálculos, notemos lo siguiente: si $d_1 \equiv d_2 \pmod{16}$, entonces $\mathbb{Z}[\sqrt{d_1}]/2^4 \simeq \mathbb{Z}[\sqrt{d_2}]/2^4$ (como anillos) vía el mapa natural que manda $\sqrt{d_1}$ a $\sqrt{d_2}$. Aplicando esto a la igualdad

(3.20) se prueba que el valor ω asociado a una unidad fundamental de la forma $a + b\sqrt{d_1}$ es igual a la de $a + b\sqrt{d_2}$. En particular, es suficiente realizar la cuenta para $\tilde{d}$ módulo 16.

Si $\tilde{d} \equiv 3 \pmod 4$ y $t \mid d$ la extensión $K(\sqrt{t})$ ramifica en $\mathfrak{p}_2$ precisamente cuando t es par (y no divisible por 4). Luego, bajo nuestras hipótesis, la extensión $K(\sqrt{\epsilon})/K$ ramifica en $\mathfrak{p}_2$. Tomamos $\{\sqrt{\tilde{d}}, 1 + 2\sqrt{\tilde{d}}, -1\}$ como generadores del grupo de elementos invertibles módulo 16 cuando $\tilde{d} \equiv 3 \pmod 8$ y $\{\sqrt{\tilde{d}}, 1 + 2\sqrt{\tilde{d}}, 5\}$ cuando $\tilde{d} \equiv 7 \pmod 8$. Consideremos los siguientes casos, teniendo en cuenta una vez más que la condición de que 2ω sea una norma implica que $\omega \equiv 3, 7 \pmod 8$ cuando $\tilde{d} \equiv 3 \pmod 8$ y $\omega \equiv 1, 5 \pmod 8$ cuando $\tilde{d} \equiv 7 \pmod 8$:

- Si $\tilde{d} \equiv 3, 7 \pmod{16}$, los posibles valores para ϵ (dados en términos de los generadores) y los valores de ω están dados en la Tabla 3.2.4. Como $\chi_2((a, b, c)) = (-1)^{a+c}$ (nuevamente como exponentes) la igualdad $\chi_2(\epsilon) = \delta_{-2}(\omega)$ se sigue recordando que $\delta_{-2}(1) = \delta_{-2}(3) = 1$ y $\delta_{-2}(5) = \delta_{-2}(7) = -1$.

$\tilde{d} \pmod{16}$	Exp.	ω	Exp.	ω	Exp.	ω	Exp.	ω
3	$(1,1,0)$	7	$(1,1,1)$	3	$(1,3,0)$	7	$(1,3,1)$	3
3	$(3,1,0)$	7	$(3,1,1)$	3	$(3,3,0)$	7	$(3,3,1)$	3
7	$(1,0,0)$	5	$(1,0,1)$	1	$(1,2,0)$	5	$(1,2,1)$	1
7	$(3,0,0)$	5	$(3,0,1)$	1	$(3,2,0)$	5	$(3,2,1)$	1

Tabla 3.2.4: Relación entre ϵ y ω para $\tilde{d} \equiv 3, 7 \pmod{16}$.

- Si $\tilde{d} \equiv 11, 15 \pmod{16}$ los posibles valores para ϵ y los valores de ω están dados en la Tabla 3.2.5. Como $\chi_2((a, b, c)) = (-1)^c$ en este caso, vale la igualdad $\chi_2(\epsilon) = \delta_{-2}(\omega)$

$\tilde{d} \pmod{16}$	Exp.	ω	Exp.	ω	Exp.	ω	Exp.	ω
11	$(1,1,0)$	3	$(1,1,1)$	7	$(1,3,0)$	3	$(1,3,1)$	7
11	$(3,1,0)$	3	$(3,1,1)$	7	$(3,3,0)$	3	$(3,3,1)$	7
15	$(1,0,0)$	1	$(1,0,1)$	5	$(1,2,0)$	1	$(1,2,1)$	5
15	$(3,0,0)$	1	$(3,0,1)$	5	$(3,2,0)$	1	$(3,2,1)$	5

Tabla 3.2.5: Relación entre ϵ y ω para $\tilde{d} \equiv 11, 15 \pmod{16}$.

Cuando $8 \mid d$, el Teorema 3.2.5 implica que el caso $2\omega = \epsilon\bar{\alpha}^2$ ocurre precisamente para $\epsilon \equiv -1 \pmod{\mathfrak{p}_2^3}$. Recordemos que $(\mathscr{O}_{\mathfrak{p}_2}/2^3)^\times$ está generado por los elementos $\{-1, 5, 1 + \sqrt{\tilde{d}}\}$ (de orden $2, 2, 8$). Usando la congruencia de ϵ módulo $\mathfrak{p}_2^3$, la condición (3.20) y el hecho de que 2ω sea la norma de un elemento, buscamos todos los posibles valores de ϵ y ω.

- Si $\tilde{d} \equiv 2 \pmod{16}$ (respectivamente $d \equiv 10 \pmod{16}$) entonces $\#Q_3 + \#Q_5$ es par (respectivamente impar). El hecho de asumir que 2ω es una norma implica que $\omega \equiv 1, 7 \pmod 8$ (respectivamente $\omega \equiv 3, 5 \pmod 8$). Todos los posibles valores de ϵ para cada ω están dados en la Tabla (3.2.6), de donde se sigue que (3.18) se satisface.

$\tilde{d} \pmod{16}$	ϵ	ω	ϵ	ω	ϵ	ω	ϵ	ω
2	-1	7	$(1+\sqrt{d})^2$	1	$-(1+\sqrt{d})^4$	7	$(1+\sqrt{d})^6$	1
10	-1	3	$(1+\sqrt{d})^2$	5	$-(1+\sqrt{d})^4$	3	$(1+\sqrt{d})^6$	5
6	-1	5	$5(1+\sqrt{d})^2$	7	$-(1+\sqrt{d})^4$	5	$5(1+\sqrt{d})^6$	7

Tabla 3.2.6: Relación entre ϵ y ω para $\tilde{d} \equiv 2, 6, 10 \pmod{16}$.

- Si $\tilde{d} \equiv 6 \pmod{16}$ entonces $\#Q_3 + \#Q_5$ es impar. La condición de la norma implica que $\omega \equiv 1, 7 \pmod{8}$. Los posibles valores de ϵ y ω están dados en la Tabla (3.2.6).
- Si $\tilde{d} \equiv 14 \pmod{16}$ entonces $\#Q_3 + \#Q_5$ es par, y por lo tanto χ_2 es trivial. La condición de ser norma implica que $\omega \equiv 1, 3 \pmod{8}$, por lo que (3.18) se satisface.

Una vez que la compatibilidad es verificada, la prueba del caso imaginario funciona, teniendo en cuenta el cambio en la Tabla 3.2.1. □

Observación 21. Para ser más precisos, el conductor $\mathfrak{f}$ de $\chi_{\mathfrak{p}_2}$ tiene valuación:

$$v(\mathfrak{f}) = \begin{cases} 5 & \text{si } d \equiv 7 \pmod{8}, \\ 3 & \text{si } d \equiv 2, 3, 5 \pmod{8}, \\ 3 & \text{si } d \equiv 6 \pmod{8} \text{ and } 2 \nmid \#Q_3 + \#Q_5, \\ 0 & \text{si } d \equiv 6 \pmod{8} \text{ and } 2 \mid \#Q_3 + \#Q_5. \end{cases}$$

Cuando $d \equiv 1 \pmod{8}$ es $0, 2$ ó 3, dependiendo de su elección.

3.2.2 Extensión y modularidad

Recordar que por Proposición 3.1.1 el conjugado de Galois de la curva elíptica $E_{(a,b,c)}$ es una curva isógena a su twist cuadrático por ψ_{-2}. En particular si χ denota el caracter construido en el Teorema 3.2.1 entonces la representación twisteada $\rho_{E_{(a,b,c)},p} \otimes \chi$ es invariante bajo la acción del grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$. Luego podría extenderse a una representación de dimensión 2 de $G_{\mathbb{Q}}$. En esta sección probaremos que este es el caso y, más aún, calcularemos el determinante y el conductor de la extensión. Comenzamos enunciado un resultado importante sobre representaciones inducidas.

Teorema 3.2.6. *Sea E/F una extensión finita de cuerpos locales, y sea ρ un representación n-dimensional de W_E. Entonces el conductor de la representación inducida $\mathrm{Ind}_{W_E}^{W_F}$ es igual a*

$$v(\mathrm{cond}(\mathrm{Ind}_{W_E}^{W_F} \rho)) = n\delta(E/F) + f(E/F)v(\mathrm{cond}(\rho)), \tag{3.21}$$

donde $\delta(E/F)$ denota la valuación del diferente de la extensión y $f(E/F)$ el grado de inercia.

Demostración. Ver por ejemplo [72], página 105 (luego de la Proposición 4). □

Sea ε el caracter racional construido en la Sección 3.2.1 y sea $S(E_{(a,b,c)})$ el conjunto de primos de mala reducción de $E_{(a,b,c)}$ que a su vez no dividen a $2d$ (donde la curva tiene reducción multiplicativa por Lema 3.1.3). Abusando de la notación, diremos que un primo racional $q \in S(E_{(a,b,c)})$ si existe un primo de $S(E_{(a,b,c)})$ que divida a q. Por último, para facilitar la notación, sea $\rho_p = \rho_{E_{(a,b,c)},p} \otimes \chi$.

Proposición 3.2.7. *Sea $K/\mathbb{Q}$ una extensión cuadrática. Entonces la representación twisteada ρ_p se extiende a una representación $\tilde{\rho}_p$ de $G_{\mathbb{Q}}$ de dimensión 2 y conductor*

$$N(\tilde{\rho}_p) = 2^e \cdot \prod_{q \in S(E_{(a,b,c)})} q \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2.$$

El valor e es uno de los siguientes:

$$e = \begin{cases} 1, 8 & \textit{si } 2 \textit{ se parte}, \\ 8 & \textit{si } 2 \textit{ es inerte}, \\ 7, 8 & \textit{si } d \equiv 3 \pmod{8}, \\ 5, 8 & \textit{si } d \equiv 7 \pmod{8}, \\ 8, 9 & \textit{si } 2 \mid d. \end{cases}$$

Demostración. Como fue mencionado anteriormente, la existencia de la extensión fue probada por Ribet en [71]. A continuación daremos una prueba alternativa basada en representaciones de Galois (bien conocida por los expertos) para tener control en el nivel y el conductor.

Veamos que podemos asumir que ρ_p es irreducible. La única manera de que la representación ρ_p fuera reducible es que $E_{(a,b,c)}$ tenga multiplicación compleja por su cuerpo de definición, es decir, por $\mathbb{Q}(\sqrt{d})$. Si $d > 0$ entonces eso no puede pasar porque las curvas elípticas siempre tienen multiplicación compleja por un cuerpo cuadrático imaginario. Si $d < 0$ y la curva elíptica $E_{(a,b,c)}$ tiene multiplicación compleja, entonces su j-invariante es racional (como vimos en el Lema 3.1.8). Esto implica que la curva es un twist cuadrático de una curva racional, con lo cual la existencia es automática. Asumamos entonces que ρ_p es irreducible.

El conductor de ρ_p divide a $\text{mcm}\{N(E_{(a,b,c)}), \text{cond}(\chi)^2\}$ y su Nebentypus coincide con ε restringido a G_K (por la primera afirmación del Teorema 3.2.1). Sea τ un elemento como en el Teorema 3.2.1 (i.e. un elemento de $G_{\mathbb{Q}}$ cuya restricción a $\text{Gal}(K/\mathbb{Q})$ es no trivial). Es suficiente definir la extensión de ρ_p en τ y chequear lo enunciado sobre el Nebentypus en dicho elemento.

Recordar que ${}^{\tau}\rho_p$ denota la representación de Galois definida en σ por ${}^{\tau}\rho_p(\sigma) = \rho_p(\tau\sigma\tau^{-1})$. Por la tercera propiedad del Teorema 3.2.1, ρ_p y ${}^{\tau}\rho_p$ son isomorfas (ya que tienen la misma traza cuando se evaluan en un Frobenius). En particular, existe $A \in \text{GL}_2(\overline{\mathbb{Q}}_p)$ tal que $\rho_p = A({}^{\tau}\rho_p)A^{-1}$. Más aún, como ρ_p es irreducible, el Lema de Schur implica que la matriz A es única salvo escalar. Como τ tiene orden 2, la igualdad $\rho_p(\sigma) = {}^{\tau^2}\rho_p(\sigma) = A^2\rho_p(\sigma)A^{-2}$ implica que $A^2 = \lambda$ (una matriz escalar).

Supongamos que existe una extensión $\tilde{\rho}_p : G_{\mathbb{Q}} \to \text{GL}_2(\overline{\mathbb{Q}}_p)$. Entonces para $\sigma \in G_K$,

$$\tilde{\rho}_p(\tau\sigma\tau^{-1}) = \tilde{\rho}_p(\tau)\tilde{\rho}_p(\sigma)\tilde{\rho}_p(\tau)^{-1} = \tilde{\rho}_p(\tau)\rho_p(\sigma)\tilde{\rho}_p(\tau)^{-1}.$$

La unicidad de la matriz A implica que existe una constante μ tal que $\tilde{\rho}_p(\tau) = \mu A$. Como $\tilde{\rho}_p^2(\tau) = \rho_p(\tau^2) = 1$, se deduce que $\mu^2 = \frac{1}{\lambda}$.

Esto sugiere que debemos definir $\tilde{\rho}_p(\tau) = \frac{1}{\sqrt{\lambda}}A$ y es fácil de verificar que dicha definición de hecho da una extensión (la otra elección de raíz cuadrada da otra posible extensión; difieren en un twist por el caracter correspondiente a la extensión $K/\mathbb{Q}$).

Sea $\mathfrak{q}$ un primo impar no ramificado en $K/\mathbb{Q}$. Entonces χ no ramifica en $\mathfrak{q}$, por lo que la valuación del conductor de $\rho_{E_{(a,b,c)},p} \otimes \chi$ es uno para los primos en $S(E_{(a,b,c)})$ y cero para los restantes. La validez del segundo factor en la fórmula para $N(\tilde{\rho}_p)$ entonces se sigue del hecho de que el conductor de una representación no cambia cuando se la restringe al grupo de Galois absoluto de una extensión no ramificada.

Sea $\mathfrak{q}$ un primo impar que sí ramifica en $K/\mathbb{Q}$ y q el primo racional al cual divide (que no es igual a p). La representación local inducida satisface que

$$\text{Ind}_{G_{K_{\mathfrak{q}}}}^{G_{\mathbb{Q}_q}}(\rho_{E_{(a,b,c)},p}|_{G_{K_{\mathfrak{q}}}} \otimes \chi_{\mathfrak{q}}) = \tilde{\rho}_p|_{G_{K_{\mathfrak{q}}}} \oplus (\tilde{\rho}_p|_{G_{K_{\mathfrak{q}}}} \otimes \chi_{K_{\mathfrak{q}}}),$$

donde $\chi_{K_{\mathfrak{q}}}$ es el caracter cuadrático de la extensión local $K_{\mathfrak{q}}/\mathbb{Q}_q$. Ahora aplicaremos el Teorema 3.2.6. Por construcción, $\chi_{\mathfrak{q}}$ es no ramificado para $q \in Q_3$ y de conductor $\mathfrak{q}$ para $q \in Q_1 \cup Q_5 \cup Q_7$, con lo cual el lado derecho de (3.21) es igual a 2 para primos en Q_3 y 4 para primos en $Q_1 \cup Q_5 \cup Q_7$. Notar que ambos $\tilde{\rho}_p$ y $\tilde{\rho}_p \otimes \chi_{K_{\mathfrak{q}}}$ tienen el mismo Nebentypus, por lo que ambos deben ramificar en los primos de Q_3 con exponente 1 en el conductor. Como $\chi_{K_{\mathfrak{q}}}$ tiene exponente 1 en el conductor para el primo q, entonces twistear $\tilde{\rho}_p$ por $\chi_{K_{\mathfrak{q}}}$ no puede variar el exponente del conductor de 1 a 3 (o de 0 a 4). Por lo tanto, para los primos en $Q_1 \cup Q_5 \cup Q_7$ ambos $\tilde{\rho}_p$ y $\tilde{\rho}_p \otimes \chi_{K_{\mathfrak{q}}}$ tienen exponente 2 como se afirmó.

El valor de e es igual al valor del exponente del conductor de $\rho_{E_{(a,b,c)},p}$ cuando 2 no ramifica; esto nos da el caso inerte. Más aún, en el caso en que 2 se parte (digamos $2 = \mathfrak{p}_2\overline{\mathfrak{p}}_2$) podemos elegir el caracter local $\chi_{\mathfrak{p}_2}$ de manera que el twist de $E_{(a,b,c)}$ por $\chi_{\mathfrak{p}_2}$ tenga reducción multiplicativa split de conductor $\mathfrak{p}_2$ para dar con lo enunciado.

Si 2 ramifica en $K/\mathbb{Q}$ usamos nuevamente la fórmula (3.21). Notar que si $d \not\equiv 1 \pmod 8$ entonces el valor del conductor de $\rho_{E_{(a,b,c)},p}$ en $\mathfrak{p}_2$ es más grande que el doble del valor del conductor de χ en $\mathfrak{p}_2$ (ver Observación 21) por lo que la fórmula se sigue fácilmente del Lema 3.1.5 notando que una vez más el conductor en 2 de $\tilde{\rho}_p$ coincide con que el de $\tilde{\rho}_p \otimes \chi_{K_\mathfrak{q}}$. Cuando $d \equiv 1 \pmod 8$, el caracter local $\chi_{\mathfrak{p}_2}$ se corresponde a una extensión mansa (generada por la raíz cuadrada de $1+\sqrt{d}$ por una unidad), entonces Lema 3.1.6 implica que la representación twisteada tiene valuación 8 en el conductor (cuando $b \equiv 1 \pmod 4$) o 6 (cuando $b \equiv 3 \pmod 4$) cuando b es impar y 12 cuando b es par. Como podemos asumir (cambiando b por $-b$) que $b \equiv 3 \pmod 4$, el resultado se sigue. □

El siguiente resultado será de utilidad para el caso K real a analizar en el Teorema 3.2.9.

Lema 3.2.8. *Sea $K/\mathbb{Q}$ tal que existe un primo impar que ramifica. Sean $\sigma \in G_\mathbb{Q}$ y χ_K el caracter cuadrático correspondiente a $K/\mathbb{Q}$. Entonces,*

$$\chi(\sigma^2) = \varepsilon(\sigma)\chi_K(\sigma).$$

Demostración. Si $\sigma \in G_K$, entonces la primera propiedad del Teorema 3.2.1 implica que $\chi(\sigma^2) = \chi(\sigma)^2 = \varepsilon(\sigma)$. Luego, el enunciado es claro para todos los elementos de G_K (pues $\chi_K(\sigma) = 1$). Como G_K tiene índice dos en $G_\mathbb{Q}$, es suficiente probar que la igualdad se satisface en un elemento de $G_\mathbb{Q} \setminus G_K$. Sea p un primo impar que ramifica en la extensión $K/\mathbb{Q}$, y sea $L = \mathbb{Q}(\zeta_p)$ la extensión ciclotómica. El grupo de Galois $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al grupo cíclico $(\mathbb{Z}/p)^\times$. Sea g un generador. Por teoría de cuerpos de clases, $\mathrm{Gal}(L/\mathbb{Q})$ es también isomorfo al cociente $\mathbb{I}_\mathbb{Q}/\mathscr{N}_{L/\mathbb{Q}}(\mathbb{I}_L)$. Sea σ_p el elemento de $\mathrm{Gal}(L/\mathbb{Q})$ correspondiente al idèle ι_p con coordenadas locales:

$$(\iota_p)_v = \begin{cases} g & \text{si } v = p, \\ 1 & \text{caso contrario.} \end{cases}$$

Denotemos además por σ_p a cualquier extensión a todo el grupo de Galois $G_\mathbb{Q}$ que no sea la identidad en K. Como se mencionó anteriormente, es suficiente probar la igualdad para σ_p. Claramente $\sigma_p^2 \in G_K$, y más aún, coincide con el transfer map de $G_\mathbb{Q}^{\mathrm{ab}}$ a G_K^{ab} (ver por ejemplo [73, Capítulo 8] para la definición del transfer map). En el lado de los idèles, el transfer map es el mapa natural $\mathbb{I}_\mathbb{Q} \to \mathbb{I}_K$, por lo que el elemento ι_p se corresponde al idèle ι_p^K de $\mathbb{I}_K$ con componentes locales

$$(\iota_p^K)_v = \begin{cases} g & \text{si } v = \mathfrak{p}, \\ 1 & \text{caso contrario.} \end{cases}$$

Entonces, el valor $\chi(\sigma_p^2)$ es igual a $\chi(\iota_p^K) = \chi_\mathfrak{p}(g)$, y una de las propiedades claves impuestas a χ y ε es que para todos los primos impares ramificados $\chi_\mathfrak{p} = \varepsilon_p \delta_{K,p}$, vía la identificación natural de $(\mathbb{Z}/p)^\times$ con $(\mathscr{O}_K/\mathfrak{p})^\times$. Luego, se sigue el enunciado. □

Teorema 3.2.9. *Sea $K/\mathbb{Q}$ una extensión cuadrática tal que satisface alguna de las siguientes dos propiedades:*

- *$K/\mathbb{Q}$ es imaginaria, o*
- *$K/\mathbb{Q}$ tiene un primo $q > 3$ que ramifica.*

Entonces la representación twisteada $\rho_{E_{(a,b,c)},p} \otimes \chi$ se extiende a una representación de $G_\mathbb{Q}$ de dimensión 2 asociada a una forma nueva $f_{(a,b,c)}$ de peso 2, Nebentypus ε y nivel $N(a,b,c)$ dado por

$$N(a,b,c) = 2^e \cdot \prod_{q \in S(E_{(a,b,c)})} q \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2.$$

El valor e es uno de los siguientes:

$$e = \begin{cases} 1, 8 & \textit{si } 2 \textit{ se parte}, \\ 8 & \textit{si } 2 \textit{ es inerte}, \\ 7, 8 & \textit{si } d \equiv 3 \pmod 8, \\ 5, 8 & \textit{si } d \equiv 7 \pmod 8, \\ 8, 9 & \textit{si } 2 \mid d. \end{cases}$$

Más aún, el cuerpo de coeficientes de $f_{(a,b,c)}$ es una extensión a lo sumo cuadrática de $\mathbb{Q}(\chi)$.

Demostración. Por Proposición 3.2.7, la representación $\rho_p = \rho_{E_{(a,b,c)},p} \otimes \chi$ se extiende a una representación $\tilde{\rho}_p$ de $G_{\mathbb{Q}}$.

Afirmación: $\det(\tilde{\rho}_p) = \varepsilon\chi_{\text{cyc}}$ (donde χ_{cyc} denota el caracter ciclótomico p-ádico).

Asumiendo la afirmación anterior, la modularidad de la representación $\tilde{\rho}_p$ se sigue de las conjeturas de Serre (Teorema 1.5.3) y de los trabajos de Wiles [87] y Taylor-Wiles [80], por lo que sabemos que tenemos adjunta una forma modular de peso 2, Nebentypus ε y nivel $N(a, b, c) = N(\tilde{\rho}_p)$. Luego, resta probar la validez de la afirmación.

Para calcular el determinante de la representación extendida $\tilde{\rho}_p$, notar que $\det(\rho_p) = \varepsilon\chi_{\text{cyc}}$ como caracter de G_K. Luego, el determinante de $\tilde{\rho}_p$ es igual a $\varepsilon\,\chi_{\text{cyc}}$ o $\varepsilon\chi_K\,\chi_{\text{cyc}}$ (donde χ_K denota el caracter cuadrático correspondiente a la extensión $K/\mathbb{Q}$). Notar que es suficiente verificar que $\det(\tilde{\rho}_p)$ y $\varepsilon\chi_{\text{cyc}}$ coinciden en un elemento de $G_{\mathbb{Q}}$ que no pertenece a G_K.

Caso K imaginario: Nuevamente, sea τ un elemento de $G_{\mathbb{Q}}$ cuya restricción a $\text{Gal}(K/\mathbb{Q})$ es no trivial, y más aún, supongamos que corresponde a la conjugación compleja (aunque esto no sea realmente necesario). Por [71, Teorema 4.4], sabemos que cualquier extensión es impar, i.e. $\det(\tilde{\rho}_p)(\tau) = -1$. Pero también $\varepsilon(\tau)\chi_{\text{cyc}}(\tau) = -1$ (pues ε es par). Luego, $\det(\tilde{\rho}_p) = \varepsilon\chi_{\text{cyc}}$.

¡Cuando $K/\mathbb{Q}$ es real ambos caracteres toman el mismo valor en la conjugación compleja! ¿Cómo podemos saber cuál es el Nebentypus de la representación $\tilde{\rho}_p$ cuando la extensión es real? La solución es trabajar con otro elemento de un subgrupo de inercia de $K/\mathbb{Q}$.

Caso K real: Fijemos una base para el módulo de Tate de la curva elíptica $E_{(a,b,c)}$ (luego podemos asumir que la imagen de nuestra representación vive en $\text{GL}_2(\mathbb{Q}_p)$). Como nuestro cuerpo K es cuadrático real, sabemos que la representación de Galois $\rho_{E_{(a,b,c)},p}$ es absolutamente irreducible. En particular, cualquier matriz que conmute con su imagen debe ser una matriz escalar, por Lema de Schur.

Sea S el conjunto de primos que ramifican en $K/\mathbb{Q}$, y para cada primo $q \in S$ sea $\mathfrak{q}$ el primo de K que lo divide. Fijemos un primo $q > 3$ en S, distinto de p. Sea $I_q \subset G_{\mathbb{Q}}$ un subgrupo de inercia en q y $I_{\mathfrak{q}}$ su subgrupo de índice dos. Por [64, Lema 2.5] la curva $E_{(a,b,c)}$ tiene buena reducción en $\mathfrak{q}$. Por lo tanto, (por el criterio de Néron-Ogg-Shafarevich) $\rho_p|_{I_{\mathfrak{q}}}$ es una matriz escalar. Sea $\sigma_q \in I_q \setminus I_{\mathfrak{q}}$ y sea ${}^{\sigma_q}\rho_p(\tau) := \rho_p(\sigma_q\tau\sigma_q^{-1})$. El caracter χ fue construido de manera tal que ${}^{\sigma_q}\rho_p \sim \rho_p$, por lo que ambas representaciones son conjugadas bajo una matriz de $\text{GL}_2(\mathbb{Q}_p)$. Como $\tilde{\rho}_p$ extiende a ρ_p, $\tilde{\rho}_p(\sigma_q)$ es tal matriz. Consideremos los siguientes dos casos:

- Si ${}^{\sigma_q}\rho_p = \rho_p$, entonces $\tilde{\rho}_p(\sigma_q)$ es una matriz escalar (por el lema de Schur), digamos $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$. En particular, $\det(\tilde{\rho}_p(\sigma_q)) = \lambda^2$. Por otro lado, $\tilde{\rho}_p(\sigma_q)^2 = \rho_p(\sigma_q^2) = \left(\begin{smallmatrix} \chi(\sigma_q^2) & 0 \\ 0 & \chi(\sigma_q^2) \end{smallmatrix}\right)$. Luego, en particular $\lambda^2 = \chi(\sigma_q^2) = \varepsilon(\sigma_q)\chi_K(\sigma_q)$ por Lema 3.2.8, entonces $\det(\tilde{\rho}_p) = \varepsilon\chi_K\,\chi_{\text{cyc}}$.

- Si ${}^{\sigma_q}\rho_p \neq \rho_p$, entonces $\tilde{\rho}_p(\sigma_q)^2 = \rho_p(\sigma_q^2)$ es una matriz escalar. Luego, podemos elegir otra base del módulo de Tate para que la matriz $\tilde{\rho}_p(\sigma_q)$ sea igual a la matriz $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & -\lambda \end{smallmatrix}\right)$. Entonces $\det(\tilde{\rho}_p(\sigma_q)) = -\lambda^2$. Una vez más, $\tilde{\rho}_p(\sigma_q)^2 = \rho_p(\sigma_q^2) = \left(\begin{smallmatrix} \chi(\sigma_q^2) & 0 \\ 0 & \chi(\sigma_q^2) \end{smallmatrix}\right)$ por lo que en particular

el Lema 3.2.8 (y el hecho de que $\chi_K(\sigma_q) = -1$) implica que $\det(\tilde{\rho}_p(\sigma_q)) = -\lambda^2 = -\chi(\sigma_q^2) = -\varepsilon(\sigma_q)\chi_K(\sigma_q) = \varepsilon(\sigma_q)$, luego $\det(\tilde{\rho}_p) = \varepsilon\,\chi_{\text{cyc}}$.

Luego, basta probar que ${}^{\sigma_q}\rho_p \neq \rho_p$ (un resultado independiente del primo $q \in S$). Recordar que $\rho_p = \rho_{E_{(a,b,c)},p} \otimes \chi$, por lo que el enunciado es equivalente a probar que ${}^{\sigma_q}\rho_{E_{(a,b,c)},p} \neq \rho_{E_{(a,b,c)},p} \cdot \delta_{-2}$ (pues ${}^{\sigma_q}\chi = \chi\delta_{-2}$) . Consideremos ambas acciones en los puntos de $E_{(a,b,c)}$ de orden p^n: el lado izquierdo es igual a $\sigma_q \cdot \tau \cdot \sigma_q^{-1}(P)$, mientras que el lado derecho es igual a $\delta_{-2}(\tau)\tau(P)$.

Consideremos la 2-isogenía $\phi : E_{(a,b,c)} \to \overline{E_{(a,b,c)}}$ explícitamente dada por

$$\phi(x,y) = (\phi_1(x,y), \phi_2(x,y)) = \left(\frac{-y^2}{2x^2}, \frac{y(2a^2 + 2\sqrt{d}b - x^2)}{2\sqrt{-2}x^2}\right).$$

Notar que en particular

$$\delta_{-2}(\tau) \cdot \tau \circ \phi = \phi \circ \tau \text{ para todo } \tau \in G_K, \tag{3.22}$$

donde consideramos $\delta_{-2}(\tau)$ como un endomorfismo de $E_{(a,b,c)}$. La hipótesis de p siendo impar implica que para cada entero positivo n, el mapa $\phi : E_{(a,b,c)}[p^n] \to \overline{E_{(a,b,c)}}[p^n]$ es biyectivo. Entonces si $P \in E_{(a,b,c)}[p^n]$, tenemos

$$\sigma_q \cdot \tau \cdot \sigma_q^{-1}(P) = (\sigma_q \cdot \phi^{-1})(\phi\tau\phi^{-1})(\sigma_q \cdot \phi^{-1})^{-1}(P) = \delta_{-2}(\tau)(\sigma_q \cdot \phi^{-1})\tau(\sigma_q \cdot \phi^{-1})^{-1}(P),$$

donde la última igualdad se sigue de (3.22). Sea n suficientemente grande tal que la representación en los puntos de p^n-torsión (que denotamos ρ_n) es absolutamente irreducible.

Luego, por el lema de Schur, ${}^{\sigma_q}\rho_n = \rho_n \cdot \delta_{-2}$ si y sólo si el endomorfismo $\sigma_q\phi^{-1}$ actúa como una matriz escalar en $E_{(a,b,c)}[p^n]$. Como la representación de Galois de una curva elíptica es parte de una familia compatible (y el Nebentypus no depende de la elección del primo p), es suficiente considerar el caso $p = 3$ y probar que $\sigma_q\phi^{-1}$ actuando en los puntos de 3-torsión no es igual a multiplicar por ± 1 (luego no puedo actuar como la multiplicación por un entero en los puntos de orden 3^n).

Notar que -1 actúa trivialmente en las coordenada x de los puntos de torsión, por lo que es suficiente probar que en la coordenada x de los puntos de 3-torsión, los elementos σ_q y ϕ no coinciden. Sea $M = K(x(E_{(a,b,c)}[3]))$ la extensión de K que se obtiene por añadir a K las coordenadas x de todos los puntos en $E_{(a,b,c)}[3]$ (una subextensión de $K(E_{(a,b,c)}[3])$ de grado 2). Notar por un lado que ϕ mapea las coordenadas x de los puntos de 3-torsión de $E_{(a,b,c)}$ a las coordenadas x de los puntos de 3-torsión de $\overline{E_{(a,b,c)}}$, pero además, el mapa ϕ_1 está dado por un polinomio en x con coordenadas en K. Más concretamente,

$$\phi_1(x) = -\frac{x^3 + 4ax^2 + 2(a^2 + \sqrt{d}b)x}{2x^2}. \tag{3.23}$$

Esto implica que M es una extensión de Galois de $\mathbb{Q}$. Claramente ambos K y $\mathbb{Q}(\sqrt{-3})$ son subcuerpos de M (pues el determinante de nuestra representación es el caracter ciclotómico módulo 3). En particular, $\mathbb{Q}(\sqrt{-3d})$ está contenido en M. Como el grado de ramificación de q en $M/\mathbb{Q}$ es 2 (pues $E_{(a,b,c)}$ tiene buena reducción en los primos que dividen a q), debe ser el caso en que $\mathbb{Q}(\sqrt{-3}) \subset M^{\sigma_q}$ (ya que σ_q no puede fijar a $\sqrt{d}$ ni $\sqrt{-3d}$).

Para una curva genérica $y^2 = x^3 + \alpha x^2 + \beta x$, su polinomio de 3-división (cuyas raíces generan la extensión M/K) está dado por

$$\psi_3(x) = 3x^4 + 4\alpha x^3 + 6\beta x^2 - \beta^2. \tag{3.24}$$

(recordar que en nuestro caso, $\alpha = 4a$ mientras que $\beta = 2(a^2 + \sqrt{d}b)$).

Sean $\theta_1, \ldots, \theta_4$ las raíces de ψ_3 y sea $\bar{\beta} = \frac{\alpha^2 - 4\beta}{4}$ (en nuestro caso $\bar{\beta}$ coincide con el conjugado de β). Luego,

$$\frac{\Delta(\psi_3)}{2^{12} \cdot 3^2 \cdot \beta^4 \cdot \bar{\beta}^2} = \left(\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^6 \cdot 3 \cdot \beta^2 \cdot \bar{\beta}} \right)^2 = -3. \tag{3.25}$$

En particular, como σ_q fija $\sqrt{-3}$, debe fijar al cociente $\frac{\prod_{i<j}(\theta_i - \theta_j)}{2^6 \cdot 3 \cdot \beta^2 \cdot \bar{\beta}}$, y como σ_q no es la identidad en K, debe mandar β a $\bar{\beta}$ y vice-versa. En particular,

$$\sigma_p \left(\prod_{i<j}(\theta_i - \theta_j) \right) = \prod_{i<j}(\sigma_p(\theta_i) - \sigma_p(\theta_j)) = \prod_{i<j}(\theta_i - \theta_j) \cdot \frac{\bar{\beta}}{\beta}.$$

Por otro lado, para $i \neq j$, usando (3.23) obtenemos

$$\phi_1(\theta_i) - \phi_1(\theta_j) = -\frac{\theta_i^2 + \alpha\theta_i + \beta}{2\theta_i} + \frac{\theta_j^2 + \alpha\theta_j + \beta}{2\theta_j} = (-1)(\theta_i - \theta_j)\frac{(\theta_i\theta_j - \beta)}{2\theta_i\theta_j}.$$

No es difícil de verificar que $\{\theta_1, \ldots, \theta_4\}$ son raíces de un polimonio mónico $x^4 + A_1x^3 + A_2x^2 + A_3x + A_4$. Entonces

$$\prod_{i<j}(\theta_i\theta_j - \beta) = \beta^6 - A_2\beta^5 + (A_1A_3 - A_4)\beta^4 + (2A_4A_2 - A_4A_1^2 - A_3^2)\beta^3 + (A_4A_3A_1 - A_4^2)\beta^2 - A_4^2A_2\beta + A_4^3.$$

Usando esta fórmula para ψ_3, tenemos que

$$\prod_{i<j}(\theta_i\theta_j - \beta) = \frac{16\beta^5}{27}(\alpha^2 - 4\beta) = \frac{64\beta^5\bar{\beta}}{27}.$$

Luego,

$$\prod_{i<j}(\phi_1(\theta_i) - \phi_1(\theta_j)) = (-1)^6 \prod_{i<j}(\theta_i - \theta_j) \left(\frac{-\bar{\beta}}{\beta} \right).$$

En particular, ϕ_1 y σ_q no actúan de la misma forma en las raíces θ_i, por lo que la afirmación se sigue. □

Observación 22. El mismo resultado vale para $K = \mathbb{Q}(\sqrt{3})$ o $\mathbb{Q}(\sqrt{6})$ reemplazando los cálculos en los puntos de 3-torsión con los de 5-torsión (para el primo $q = 3 \in S$). Mientras trabajamos con los puntos de 5-torsión, la fórmula (3.25) se convierte en

$$\frac{\Delta(\psi_5)}{2^{88} \cdot 5^{10} \cdot b^{44} \cdot (a^2 - 4b)^{22}} = 5.$$

El caso $K = \mathbb{Q}(\sqrt{2})$ es más sutil ya que no es clara la elección de un elemento de orden dos en el grupo de Galois $\mathrm{Gal}(K(E_{(a,b,c)}[p])/\mathbb{Q})$. En ejemplos particulares calculados el resultado vale, pero no tenemos una prueba general de este hecho.

Observación 23. El cuerpo de coeficientes puede ser calculado de la siguiente forma: si p es un primo inerte en $K/\mathbb{Q}$ entonces $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_p))^2 = a_p(E_{(a,b,c)})\chi(\mathrm{Frob}_p) + 2\varepsilon(\mathrm{Frob}_p)p$. Luego, es suficiente realizar dicho cálculo para un primo inerte de $K/\mathbb{Q}$.

3.3 Paso 3: Baja de nivel

Sea $\tilde{\rho}_p$, como en la sección anterior, la extensión de $\rho_{E_{(a,b,c)},p} \otimes \chi$, una representación modular de $G_{\mathbb{Q}}$.

Corolario 3.3.1. *Supongamos que $p \nmid 2d$ y supongamos que la representación de Galois residual $\overline{\tilde{\rho}_p}$ es absolutamente irreducible. Entonces existe una forma $f \in S_2(\Gamma_0(N), \varepsilon)$, donde*

$$N = 2^e \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2,$$

para e como en Teorema 3.2.9, tal que $\overline{\rho}_{E_{(a,b,c)},p} \equiv \overline{\rho_{f,K,p} \otimes \chi^{-1}} \pmod{\mathfrak{p}}$, donde $\rho_{f,K,p}$ es la restricción de la representación $\rho_{f,p}$ al grupo de Galois G_K, $\mathfrak{p}$ es un ideal primo de $\overline{\mathbb{Q}}$ que divide a p y χ es el caracter construido en la sección anterior.

Demostración. Sea $\mathfrak{q}$ un ideal primo de $\mathscr{O}_K$ que divide a $N(E_{(a,b,c)})$ pero que no divide a p. Por Lema 3.1.4 y por Teorema 1.2.16, la representación residual $\overline{\rho}_{E_{(a,b,c)},p}$ es no ramificada en $\mathfrak{q}$. Como χ es no ramificado en $\mathfrak{q}$, lo mismo vale para $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi}$, y como $K/\mathbb{Q}$ es no ramificado en $\mathfrak{q}$, la imagen de la inercia de $\overline{\tilde{\rho}_p}$ coincide con la de $\overline{\rho}_{E_{(a,b,c)},p}$. En particular, $\overline{\tilde{\rho}_p}$ es no ramificada en todos los primos que no dividen a $2dp$. La hipótesis de finitud (para remover también a p del nivel) en $\mathfrak{p}$ para primos $\mathfrak{p}$ que dividen a p se sigue de la Proposición 1.5.4, bajo la suposición de que p no ramifica en $K/\mathbb{Q}$ (y que por lo tanto χ no ramifica en $\mathfrak{p}$). Nuestra suposición de absoluta irreducibilidad implica que estamos en la hipótesis del Teorema 1.5.6. Luego, existe una forma nueva $f \in S_2(\Gamma_0(N), \varepsilon)$ (en nuestro caso por construcción $\varepsilon = \varepsilon(\overline{\tilde{\rho}_p})$) con N sólo divisible por los primos que ramifican y quizá por los primos arriba de 2, que es congruente a la representación $\tilde{\rho}_p$ módulo $\mathfrak{p}$ para algún ideal primo $\mathfrak{p}$ que divida a p. □

Es importante remarcar que el nivel, el peso y el Nebentypus de la forma nueva f no depende ni de la solución (a, b, c) ni del primo p.

Proposición 3.3.2. *Las extensiones de las representaciones asociadas a las soluciones $(\pm 1, 0, 1)$ se corresponden con formas $f_\pm$ con multiplicación compleja en el espacio $S_2(\Gamma_0(N), \varepsilon)$, donde*

$$N = 2^8 \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2.$$

Demostración. Por Lema 3.1.7 y Observación 19 el exponente del conductor de la curva elíptica correspondiente a las soluciones $(\pm 1, 0, 1)$ es igual a 8 cuando 2 no ramifica en $K/\mathbb{Q}$, a 12 si $d \equiv 3 \pmod 4$ y 10 si $2 \mid d$. En todos los casos, la fórmula (3.21) implica que la extensión tiene valuación 8 en el exponente, en el primo 2. □

Recordemos que para garantizar que la representación $\tilde{\rho}_p$ tiene imagen absolutamente irreducible (hipótesis requerida en el corolario anterior) utilizamos los resultados vistos en la Sección 1.7.1. El caso en que (a, b, c) es una solución que satisface que existe un primo $q > 3$ que divide a c está cubierto por Proposición 2.3.1. Resta demostrar el siguiente resultado.

Proposición 3.3.3. *Si (a, b, c) es una solución primitiva tal que c está soportado en $\{2, 3\}$ entonces existe una cota N_K tal que si $p > N_K$ la representación $\rho_{E_{(a,b,c)},p}$ tiene imagen absolutamente irreducible.*

Demostración. La prueba es similar a [37] (caso (ii)). Supongamos que $c = 2^\alpha 3^\beta$, por lo que la curva tiene conductor $2^\alpha \cdot 3^\beta$, donde $\alpha \leq 12$, $\beta \leq 1$ (por Lema 3.1.5). Sea $\epsilon_3 = 1$ si $3 \mid c$ y 0 en caso

contrario. Entonces $N_{\tilde{\rho}_p} = 2^s \cdot 3^{\epsilon_3} \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2$, donde $s \leq 9$ por Teorema 3.2.9. Supongamos que la imagen residual de $\tilde{\rho}_p$ es reducible, i.e.

$$\overline{\tilde{\rho}_p}^{s.s} \sim \nu \oplus \varepsilon \nu^{-1} \overline{\chi}_{\text{cyc}}, \tag{3.26}$$

donde χ_{cyc} denota el caracter ciclotómico p-ádico. En particular, como el conductor de la representación reducida divide el conductor de $\tilde{\rho}_p$, entonces $\text{cond}(\nu) \mid N(\tilde{\rho})$. Sea ℓ un primo tal que $\ell \equiv 1 \pmod{\text{mcm}(4d, \text{cond}(\nu))}$. En particular, ℓ se parte en $K/\mathbb{Q}$, digamos $\ell = \mathfrak{l}\bar{\mathfrak{l}}$. Luego, por un lado $\text{Tr}(\tilde{\rho}_p(\text{Frob}_\ell)) = a_{\mathfrak{l}}(E_{(a,b,c)})\chi(\mathfrak{l})$ es un entero (ya que la forma tiene twist interno) y por la cota de Hasse satisface que $|a_{\mathfrak{l}}(E_{(a,b,c)})| \leq 2\sqrt{\ell}$. Por otro lado, (3.26) y nuestra suposición en ℓ implican que $\text{Tr}(\overline{\tilde{\rho}_p}^{s.s}(\text{Frob}_\ell)) = \ell + 1$. En particular $p \mid \ell + 1 - a_{\mathfrak{l}}(E_{(a,b,c)})\chi(\mathfrak{l})$ (distinto de 0), que no puede ocurrir si $p > 2\sqrt{\ell} + \ell + 1$. □

Observación 24. La constante N_K depende del primer primo congruente a 1 mód $\text{mcm}(4d, \text{cond}(\nu))$. Podemos mejorar la cota para el conductor de ν en el teorema anterior. De (3.26) se sigue que $\text{cond}(\nu) \cdot \text{cond}(\nu^{-1}\varepsilon) \mid N(\tilde{\rho}_p)$. Si $3 \mid c$ entonces ε es no ramificada en 3, y $\tilde{\rho}_p$ tiene exponente 1 en el conductor, para el primo 3. Luego $3 \nmid \text{cond}(\nu)$. Para primos impares ramificados q, como el conductor de ε es libre de cuadrados, $v_q(\text{cond}(\nu)) \leq 1$. Luego, si $\tilde{d} = \frac{d}{2^{v_2(d)}}$ entonces $\text{cond}(\nu) \mid 2^4 \cdot \tilde{d}$, con lo cual podemos reemplazar el mínimo común múltiplo por $16\tilde{d}$.

Con respecto al menor primo ℓ congruente a 1 módulo $16\tilde{d}$, de acuerdo con el teorema de Dirichlet, $1/\varphi(16\tilde{d})$-avos de los primos son congruentes a 1 módulo $16\tilde{d}$, pero dar una cota precisa para el primero de tales primos es muy inefectivo, en términos computacionales.

En particular, como $E_{(a,b,c)}$ es $\mathbb{Q}$-curva de grado 2, si N_K es como en la proposición anterior y $p > \max\{13, N_K\}$ entonces la imagen de $\overline{\tilde{\rho}_p}$ es absolutamente irreducible y tenemos garantizada la existencia de una forma f como en el Corolario 3.3.1.

3.4 Paso 4: Resolviendo la ecuación $x^4 - dy^2 = z^p$

En la presente sección estudiaremos las soluciones de (1) para distintos valores de d libres de cuadrados. Para ello, seguiremos la estrategia descripta en el Capítulo 2.

El método modular da una respuesta positiva para primos p suficientemente grandes (una constante explícita) con una condición de congruencia cuando $d > 0$. Un resumen de los resultados obtenidos se encuentra en la Tabla 3.4.1. La tabla contiene también la dimensión del espacio de formas nuevas de peso 2 (calculado para descartar posibles soluciones), así como la dimensión del espacio de formas modulares de Hilbert de peso paralelo 2 (si uno deseara aplicar el método modular clásico sobre K cuando K es real, i.e., $d > 0$). Notar que la dimensión del espacio de Hilbert se vuelve muy grande rápidamente, siendo imposible de calcular desde un punto de vista computacional.

d	Teorema	Condición en p	$\dim(S_2(\Gamma_0(N), \varepsilon))$	Dim. esp. de Hilbert
-5	3.4.1	$p > 499$	$72, 140$	–
-6	3.4.2	$p > 563$	$28, 64$	–
-7	3.4.3	$p > 349$	$3, 318$	–
6	3.4.4	$p > 7, p \neq 17, p \equiv 1, 3 \pmod 8$	$28, 64$	$96, 384$
10	3.4.5	$p > 19, p \equiv 1, 3 \pmod 8$	$140, 288$	$448, 1792$
11	3.4.6	$p > 19, p \equiv 1, 3 \pmod 8$	$48, 92$	$224, 896$
19	3.4.7	$p > 19, p \neq 43, 113, p \equiv 1, 3 \pmod 8$	$80, 156$	$608, 2432$
129	3.4.8	$p > 900$ o $p > 19, p \equiv 1, 3 \pmod 8, p \neq 43$	$16, 1400$	$100, 600, 38400$

Tabla 3.4.1: Resumen de los resultados principales para la ecuación (1).

Los algoritmos usados para los siguientes ejemplos están disponibles en [83], así como los resultados de los cálculos.

3.4.1 Ejemplos para $d < 0$

Analicemos primero los casos en donde d es libre de cuadrados y $-10 < d < -1$.

La ecuación $x^4 - dy^2 = z^p$, con $d = -1, -2, -3$

Como fue mencionado en el comienzo del capítulo, estos casos fueron considerados en los artículos [38], [4] y [37].

La ecuación $x^4 + 5y^2 = z^p$

Esta ecuación no fue considerada anteriormente, y aplicando nuestro método obtenemos el siguiente resultado.

Teorema 3.4.1. *Sea $p > 499$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^4 + 5y^2 = z^p.$$

Demostración. Por Teorema 3.2.9, ε es un caracter de orden 4 y conductor $4 \cdot 5$, mientras que χ tiene orden 8. Sea (a, b, c) una solución primitiva no trivial. Como $d \not\equiv 1 \pmod 8$, c no puede ser par (por Lema 2.1.1), con lo cual c es una potencia de 3, o es divisible por un primo mayor a 3. En el último caso, la Proposición 2.3.1 implica que si $p > 13$ la imagen es absolutamente irreducible. Si c es una potencia de 3, podemos aplicar la Proposición 3.3.3 (y la Observación 24) con el primo $\ell = 241$, obteniendo la cota $N_K = 273$. En particular, si $p > 273$ estamos en la hipótesis de bajada de nivel. Luego, por Corolario 3.3.1 existe una forma f en $S_2(\Gamma_0(2^7 \cdot 5^2), \varepsilon)$ o en $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$ cuya representación de Galois es congruente a la de $E_{(a,b,c)} \otimes \chi$ módulo p.

• El espacio $S_2(\Gamma_0(2^7 \cdot 5^2), \varepsilon)$ tiene 12 clases de conjugación de Galois (de formas nuevas), ninguna de ellas con multiplicación compleja. Usando el truco de Mazur (ver Proposición 2.4.1) para primos $3 \leq q \leq 30$ distintos de 5 y toda f en el espacio, concluimos que $p \in \{2, 7, 13\}$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$ tiene 55 clases de conjugación de Galois, 24 de ellas con multiplicación compleja (y dos de ellas correspondientes a las soluciones triviales, por Proposición 3.3.2). Aplicando el truco de Mazur para primos $3 \leq q \leq 20$ distintos de 5 a cada forma sin multiplicación compleja tenemos que $p \in \{2, 3, 5, 7, 11\}$. Si c es una potencia de 3, entonces las formas con multiplicación compleja deberían satisfacer la hipótesis de bajada de nivel, i.e., que $p \mid N(16\varepsilon^{-1}(3) - a_3(g)^2)$ (ver discusión en la Sección 2.4.1). Esto implica que $p \in \{2, 3, 5, 29, 101, 139\}$.

Si c es divisible por un primo mayor a 3 entonces podemos aplicar el Teorema 2.4.8, que nos asegura que nuestra forma no puede ser congruente a una que tenga multiplicación compleja, para $p > 499$. □

Este es un ejemplo de cómo funciona el código: basta cargar en `Magma` el archivo `Eq1d5.mg` para obtener lo afirmado anteriormente.

```
> load "Eq1d5.mg";
Loading "Eq1d5.mg"
Loading "Mazur42p.mg"
Forms in Space 2^7*5^2:
Forms with CM:
[]
Primes obtained via Mazur's trick for non-CM forms:
```

```
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 13 @}
{@ 13 @}
{@ 13 @}
{@ 13 @}
Forms in Space 2^8*5^2:
Forms with CM:
[ 1, 2, 3, 4, 5, 6, 7, 8, 13, 14, 17, 18, 21, 22, 23, 24, 29, 30, 31, 32,
33, 34, 44, 45 ]
Primes obtained via Mazur's trick for non-CM forms:
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 11, 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 2, 7 @}
{@ 7 @}
{@ 7 @}
{@ 7 @}
{@ 7 @}
{@ 3 @}
{@ 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 3, 7 @}
{@ 3, 7 @}
{@ @}
{@ @}
{@ 2, 3, 5, 7 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 3 @}
{@ 3 @}
{@ 3 @}
{@ 3 @}
{@ 2, 5 @}
{@ 2, 5 @}
Primes obtained via Mazur's trick for CM forms:
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
{@ 2 @}
```

```
{@ 2 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 3 @}
{@ 2, 5 @}
{@ 2, 5 @}
{@ 2 @}
{@ 2 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 3, 139 @}
{@ 2, 29 @}
{@ 2, 29 @}
{@ 5, 101 @}
{@ 5, 101 @}
```

La ecuación $x^4 + 6y^2 = z^p$

En este caso podemos probar el siguiente resultado.

Teorema 3.4.2. *Sea $p > 563$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^4 + 6y^2 = z^p.$$

Demostración. Notar que como $6 \mid d$, el valor de c de una solución primitiva no trivial (a, b, c) no puede estar soportado en $\{2, 3\}$, con lo cual tenemos imagen absolutamente irreducible si $p > 13$ (por Proposición 2.3.1). El Teorema 3.2.9 implica que ε es un caracter de conductor $4 \cdot 3$ y orden 2, mientras que χ tiene orden 4. El Corolario 3.3.1 implica la existencia de una forma nueva f correspondiente a (a, b, c) que reside en $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ o $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$, cuya representación es congruente módulo p a $\rho_{E_{(a,b,c)},p} \otimes \chi$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ tiene 10 clases de conjugación de Galois. Seis de ellas tienen multiplicación compleja (dos de ellas correspondientes a las soluciones triviales, por Proposición 3.3.2). Corriendo el truco de Mazur para $q = 5$ y $q = 7$ para cada forma sin multiplicación compleja concluimos que $p \in \{2, 7\}$.

• El espacio $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$ tiene 13 clases de conjugación de Galois, tres de ellas con multiplicación compleja. Aplicando el truco de Mazur para cado primo $5 \leq q \leq 20$ a cada forma sin multiplicación compleja concluimos que $p \in \{2, 5, 7\}$.

Por último, en ambos espacios las formas sin multiplicación compleja puede ser descartadas si $p > 563$, por Teorema 2.4.8. □

Observación 25. Si la constante de Ellenberg en el Teorema 2.4.8 se pudiera mejorar a 13 (como esperamos), el resultado anterior valdría también para $p > 13$.

La ecuación $x^4 + 7y^2 = z^p$

Nuestro método nos permite probar el siguiente resultado.

Teorema 3.4.3. *Sea $p > 349$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^4 + 7y^2 = z^p.$$

Demostración. Sea (a, b, c) una solución primitiva no trivial. Como $-7 \equiv 2 \pmod 3$ concluimos que c no puede ser divisible por 3 (por Lema 2.1.1), pero sí puede ser una potencia de 2. Luego, para asegurar que la imagen sea absolutamente irreducible necesitamos aplicar la Proposición 3.3.3. La Observación 24 implica que podemos utilizar la Proposición 3.3.3 con $\ell = 113$, obteniendo imagen absolutamente irreducible para todo primo $p \geq 127$ (si c es divisible por un primo mayor que 3 entonces la imagen es absolutamente irreducible para $p > 13$, por Proposición 2.3.1).

Teorema 3.2.9 implica que ε es trivial, mientras que el caracter χ es el caracter cuadrático de conductor $7 \cdot 8$. Corolario 3.3.1 implica que existe una forma nueva f en $S_2(\Gamma_0(2 \cdot 7^2))$ o $S_2(\Gamma_0(2^8 \cdot 7^2))$ tal que su representación es congruente a $\rho_{E_{(a,b,c)},p} \otimes \chi$ módulo p.

Veamos dos formas diferentes de descartar las formas en el primer espacio. Si $f \in S_2(\Gamma_0(2 \cdot 7^2))$ es una forma nueva (candidata a una solución primitiva) su cambio de base a K da una forma modular de Bianchi cuyo twist por χ^{-1} debe corresponder a una forma modular de Bianchi de nivel $(\frac{1+\sqrt{-7}}{2})^6 \cdot (\frac{1-\sqrt{-7}}{2})$. Tal espacio puede ser calculado fácilmente (usando el algoritmo de Cremona [21], disponible en https://github.com/JohnCremona/bianchi-progs/releases/tag/v20200713). El resultado disponible en la página LMFDB [58]. Hay dos formas cuyo nivel tiene norma 128, dadas por 2.0.7.1-128.4 y 2.0.7.1-128.5, cuyo nivel es igual a $(\frac{1+\sqrt{-7}}{2})^3(\frac{1-\sqrt{-7}}{2})^4$ y su conjugada de Galois, por lo que ninguna proviene de una solución primitiva.

• El espacio $S_2(\Gamma_0(2 \cdot 7^2))$ tiene 2 clases de conjugación de Galois, una de ellas con coeficientes racionales (por lo tanto correspondiente a una curva elíptica) y la otra con coeficientes en la extensión cuadrática correspondiente al polinomio $x^2 - 2x - 7$. Ninguna tiene multiplicación compleja. El truco de Mazur para primos $3 \leq q \leq 50$ diferente de 7 descarta la forma racional si p no está en $\{2, 7, 17\}$. La segunda forma no puede ser descartada usando el truco de Mazur. Como no aparece en el espacio de formas modulares de Bianchi, su tipo local en 7 no puede ser el correcto (por lo que el twist por χ^{-1} de su cambio de base a K es ramificado en $\sqrt{-7}$). De hecho, `Magma` puede calcular dicho tipo local, dando que la componente local es de hecho supercuspidal, inducida por una caracter de orden 8 de la extensión cuadrática no ramificada de $\mathbb{Q}_7$. Tal tipo local no coincide con el de la nuestra curva (inducida por un caracter de orden 4 de la misma extensión). Por lo tanto no pueden ser congruentes, por Proposición 2.4.2 si $p > 3$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 7^2))$ tiene 98 clases de conjugación de Galois, 17 de ellas con coeficientes racionales y 30 formas con multiplicación compleja (dos de ellas correspondientes a las soluciones triviales por Proposición 3.3.2). El truco de Mazur (para primos $3 \leq q \leq 20$ distintos de 7) permite eliminar las formas sin multiplicación compleja cuando p no pertenece al conjunto $\{2, 3, 5, 7, 11, 17, 23, 27, 31\}$.

Las formas con multiplicación compleja de ambos espacios pueden ser descartadas si $p > 349$, por Teorema 2.4.8. □

3.4.2 Ejemplos para $d > 0$

Para la ecuación (1) es claro que (a, b, c) es solución para todo p primo mayor a 2 si y sólo si $c \in \{-1, 0, 1\}$. El caso $c = 0$ sólo sucede con la solución $(0, 0, 0)$, que da lugar a una curva singular (Lema 3.1.7), con lo cual no genera inconvenientes. Para $d < 0$, el caso $c = \pm 1$ sólo puede ocurrir con la solución $(\pm 1, 0, 1)$, ¡Sin embargo, esto deja de ser cierto cuando $d > 0$! Esto deriva a la pregunta de cuándo la curva

$$x^4 - dy^2 = \pm 1 \tag{3.27}$$

admite soluciones no triviales. Para $1 < d < 20$ (casos que analizaremos), las únicas soluciones no triviales están dadas por

$$(a, b, c, d) \in \{(\pm 1, \pm 1, -1, 2), (\pm 3, \pm 4, 1, 5), (\pm 7, \pm 20, 1, 6), (\pm 2, \pm 1, 1, 15), (\pm 2, \pm 1, 1, 17)\}. \tag{3.28}$$

La ecuación (3.27) fue estudiada en muchos artículos (ver por ejemplo [86]). Es sabido que la ecuación con $+1$ en el lado derecho tiene a lo sumo una solución no trivial (ver [56]), excepto cuando $d = 1785$. Más aún, en [20] todas las soluciones para $1 \leq d \leq 150000$ fueron calculadas. La ecuación con -1 en el lado derecho fue estudiada en [57], donde es además probado que en todos los casos existe como máximo una solución no trivial, y una condición para la existencia es presentada. A priori, el método modular no es compatible con los casos en donde exista una solución no trivial de la ecuación (3.27) (ver las obstrucciones del método presentadas en la Sección 1.7.1). Aún así, veremos en breve que sí funcionará para $d = 6$.

En esta sección, aplicamos el método para estudiar la ecuación (1) para valores libres de cuadrados $1 \leq d \leq 20$ y $d = 129$. El cuerpo $\mathbb{Q}(\sqrt{6})$ es el primero en donde la unidad fundamental tiene norma 1 y además tiene una solución no trivial para todo primo p. El caso $d = 129$ es el primer caso en donde 2 se parte (con lo cual podemos aplicar lo visto en Seccion 2.4.5) y además en donde todas las formas pueden ser descartadas usando el truco de Mazur. Para $d \in \{3, 5, 7, 14\}$ existen formas modulares sin multiplicación compleja que no pueden ser descartadas con los métodos de la Sección 2.4 (por lo que el método modular falla).

El caso $d = 6$

Como fue mencionado anteriormente, aunque el caso $d = 6$ pareciera estar fuera del alcance del método modular, resulta que las curvas de Frey provenientes de las soluciones $(\pm 7, \pm 20, 1)$ también tienen multiplicación compleja (esto parece ser una coincidencia fortuita, a diferencia de lo que ocurre para otros valores). Las soluciones triviales dan curvas elípticas con j-invariante 8000 (con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$). Sobre $\mathbb{Q}(\sqrt{6})$ sólo hay dos clases de isomorfismo extras de curvas elípticas con multiplicación compleja cuyo j-invariante no es racional (ver [26]), con j-invariante $188837384000 \pm 77092288000\sqrt{6}$ ¡Las curvas de Frey $E_{(\pm 7, \pm 20, 1)}$ tienen precisamente tales j-invariantes!

Teorema 3.4.4. *Sea $p > 7$ un número primo tal que $p \neq 17$ y $p \equiv 1, 3 \pmod 8$. Entonces, $(\pm 7, \pm 20, 1)$ son las únicas soluciones primitivas no triviales de la ecuación*

$$x^4 - 6y^2 = z^p.$$

Demostración. Supongamos que (a, b, c) es una solución primitiva no trivial. Si $c = \pm 1$ entonces, por (3.28), $(a, b, c) = (\pm 7, \pm 20, 1)$. Consideremos ahora el caso $c \neq \pm 1$ (en particular c es divisible por un primo mayor a 3). Para aplicar el teorema de bajada de nivel de Ribet, debemos probar que la representación residual de $E_{(a,b,c)}$ módulo p es irreducible. Para eso, podemos aplicar Proposición 2.3.1. Luego, si $p > 7$, el Corolario 3.3.1 implica que tenemos que calcular los espacios $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ y $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$, donde ε es el caracter correspondiente a la extensión $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 3), \varepsilon)$ tiene 10 clases de conjugación de Galois, 6 de ellas con multiplicación compleja. Corriendo el truco de Mazur para primos $5 \leq q \leq 10$ podemos descartar todas las formas excepto tres que tienen multiplicación compleja, si $p \notin \{2, 5, 7\}$. Las únicas formas que no pueden ser descartadas en este espacio son las tres formas correspondientes a las soluciones $(\pm 1, 0, 1)$ y $(\pm 7, \pm 20, 1)$, con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$.

• El espacio $S_2(\Gamma_0(2^9 \cdot 3), \varepsilon)$ tiene 13 clases de conjugación de Galois, 3 de ellas con multiplicación compleja. Nuevamente, el truco de Mazur para primos $5 \leq q \leq 20$ nos permite descartar todas las formas si $p \notin \{2, 3, 5, 7, 17\}$.

Luego, asumiendo $p > 7$ y $p \neq 13, 17$ podemos bajar el nivel y descartar todas las posibles formas nuevas, excepto las tres del primer espacio antes mencionadas, con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$. Para descartar las tres restantes, necesitamos imponer una condición de congruencia en p. Si $p \equiv 1, 3 \pmod 8$, entonces p se parte en $\mathbb{Q}(\sqrt{-2})$. Luego, por Proposición 1.2.20, la representación residual módulo p de las formas nuevas con multiplicación compleja tiene imagen contenida en el normalizador de un subgrupo de Cartan split. Esto contradice la Proposición 2.4.6 (pues c es divisible por un primo mayor a 3). □

El caso $d = 10$

En este caso tenemos el siguiente resultado.

Teorema 3.4.5. *Sea $p > 19$ un número primo tal que $p \equiv 1, 3 \pmod 8$. Entonces, no hay soluciones primitivas no triviales de la ecuación*

$$x^4 - 10y^2 = z^p.$$

Demostración. Sea (a, b, c) una supuesta solución primitiva no trivial. En este caso, el Teorema 3.2.1 implica que ε es un caracter de orden 4 y conductor $4 \cdot 5$, mientras que χ tiene orden 8. Como puede ocurrir que c esté soportado en 3, para probar que $\overline{\rho}_{E_{(a,b,c)},p}$ es irreducible y obtener una cota más óptima (evitando usar Proposición 3.3.3), aplicaremos el Teorema 2.3.2 (y la Observación 11) para los primos $q = 5, 7$. Con esto, obtenemos que $\overline{\rho}_{E_{(a,b,c)},p}$ es irreducible si p no pertenece a $\{2, 3, 5, 7, 13, 31, 37\}$. Luego, por Corolario 3.3.1, existe una forma nueva f en $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$ o en $S_2(\Gamma_0(2^9 \cdot 5^2), \varepsilon)$ cuya representación de Galois es congruente a $\rho_{E_{(a,b,c)},p} \otimes \chi$ módulo p.

• El espacio $S_2(\Gamma_0(2^8 \cdot 5^2), \varepsilon)$ tiene 55 clases de conjugación de Galois, 22 de ellas con multiplicación compleja. Corriendo el truco de Mazur para todas las formas nuevas f y primos $3 \leq q \leq 37$ tales que $q \neq 5, 31$, obtenemos que todas las formas pueden ser descartadas si $p \notin \{2, 3, 5, 7, 11, 17, 19, 23\}$, excepto por las dos formas que provienen de las soluciones triviales (ver Proposición 3.3.2), con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$.

• El espacio $S_2(\Gamma_0(2^9 \cdot 5^2), \varepsilon)$ tiene 40 formas, 10 de ellas con multiplicación compleja. En este caso, el truco de Mazur para los primos $q \neq 5$ tales que $3 \leq q \leq 20$, descarta todas las formas en el espacio si $p \notin \{2, 3, 5, 7, 11, 13, 17, 23\}$.

Luego, asumiendo $p \notin \{2, 5, 7, 11, 13, 17, 19, 23, 31, 37\}$, sólo resta descartar las dos formas con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$ pertenecientes al primer espacio. Como la solución es primitiva, c es impar (ver Lema 2.1.1). Si c es divisible por 3, entonces podemos usar el truco de Mazur con $q = 3$, obteniendo que $p \mid \mathscr{N}(16\varepsilon^{-1}(3) - a_3(f)^2)$, luego $p \in \{2, 5\}$ (absurdo). Por lo tanto, c no es divisible por 3 y estamos en las hipótesis de la Proposición 2.4.6. Luego, una vez más, podemos descartar las formas restantes aplicando la Proposición 1.2.20, cuando $p \equiv 1, 3 \pmod 8$. □

El caso $d = 11$

En este caso tenemos el siguiente resultado.

Teorema 3.4.6. *Sea $p > 19$ un número primo tal que $p \equiv 1, 3 \pmod 8$. Entonces, no hay soluciones primitivas no triviales de la ecuación*

$$x^4 - 11y^2 = z^p.$$

Demostración. Sea (a, b, c) una solución primitiva no trivial. Por Teorema 3.2.1 tenemos que ε es de orden 2 y conductor $4 \cdot 11$, y χ es de orden 4. Como $\text{mcd}(6, c) = 1$ (ver Lema 2.1.1) entonces por Proposición 2.3.1 $\overline{\rho}_{E_{(a,b,c)},p}$ es absolutamente irreducible si $p > 11$. Luego, Corolario 3.3.1 implica que existe una forma f en $S_2(\Gamma_0(2^7 \cdot 11), \varepsilon)$ o en $S_2(\Gamma_0(2^8 \cdot 11), \varepsilon)$ tal que su representación es congruente módulo p a $\rho_{E_{(a,b,c)},p} \otimes \chi$.

• El espacio $S_2(\Gamma_0(2^7 \cdot 11), \varepsilon)$ tiene 4 clases de conjugación de Galois, ninguna de ellas con multiplicación compleja. Corriendo el truco de Mazur para los primos $3 \leq q \leq 10$ podemos descartar todas las formas, asumiendo $p > 7$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 11), \varepsilon)$ tiene 15 clases de conjugación de Galois, 7 de ellas con multiplicación compleja (dos de ellas correspondientes a las soluciones triviales, por Proposición 3.3.2). Corriendo el truco de Mazur para las demás 13 formas, para primos $q \neq 11$ tales que $3 \leq q \leq 43$, podemos descartarlas si $p > 19$. Para descartar las restantes dos necesitamos la hipótesis $p \equiv 1, 3 \pmod 8$ y aplicar las Proposiciones 1.2.20 y 2.4.6. □

El caso $d = 19$

En este caso tenemos el siguiente resultado.

Teorema 3.4.7. *Sea $p > 19$ un número primo tal que $p \neq 43, 113$ y $p \equiv 1, 3 \pmod 8$. Entonces, no hay soluciones primitivas no triviales de la ecuación*

$$x^4 - 19y^2 = z^p.$$

Demostración. Sea (a, b, c) una solución primitiva no trivial. Nuevamente, como c puede estar soportado en 3, para probar que la representación de $E_{(a,b,c)}$ módulo p es absolutamente irreducible aplicamos el Teorema 2.3.2 para $q = 19$ y seguimos la Observación 11 para el primo $q = 7$, obteniendo que $\rho_{E_{(a,b,c)},p}$ tiene reducción absolutamente irreducible si $p \notin \{2, 3, 5, 11, 13, 17, 19, 31, 43, 113, 115597\}$, por lo que asumiremos dicha hipótesis en p de ahora en adelante.

El caracter ε tiene orden 2 y conductor $4 \cdot 19$, mientras que χ es de orden 4. Luego, el Corolario 3.3.1 implica que debemos buscar una forma nueva f en $S_2(\Gamma_0(2^7 \cdot 19), \varepsilon)$ o $S_2(\Gamma_0(2^8 \cdot 19), \varepsilon)$.

• El espacio $S_2(\Gamma_0(2^7 \cdot 19), \varepsilon)$ tiene 4 clases de conjugación de Galois, ninguna con multiplicación compleja. Usando el truco de Mazur con primos $3 \leq q \leq 17$ podemos descartar todas las formas (de hecho, sólo necesitamos asumir $p > 2$ para esto).

• El espacio $S_2(\Gamma_0(2^8 \cdot 19), \varepsilon)$ tiene 18 clases de conjugación de Galois, 7 de ellas con multiplicación compleja. Con la suposición impuesta en p (y de hecho asumiendo sólo $p > 19$), podemos usar el truco de Mazur con los primos $3 \leq q \leq 17$ y descartar todas las formas nuevas excepto por dos, correspondientes a las soluciones triviales (ver Proposicion 3.3.2).

Para descartar las restantes formas, procedemos como antes. Por Lema 2.1.1, c es impar. Supongamos que c es divisible por 3. Entonces, el hecho de que $p \mid \mathcal{N}(16\varepsilon(3)^{-1} - a_3(f)^2)$, implica que $p \in \{2, 3\}$, lo cual contradice lo asumido. Luego c no es divisible por 3 y por lo tanto estamos en las hipótesis de la Proposición 2.4.6, por lo que podemos descartar las formas asociadas a las soluciones triviales, bajo la hipótesis de $p \equiv 1, 3 \pmod 8$ (por Proposición 1.2.20). □

El caso $d = 129$

El primo 2 se parte en $\mathbb{Q}(\sqrt{129})/\mathbb{Q}$, por lo que la Proposición 2.4.7 (como fue descripto en la Sección 2.4.5) puede ser aplicada para descartar las formas con multiplicación compleja.

Teorema 3.4.8. *Sea $p > 19$ un número primo que satisface que $p > 900$ o $p \equiv 1, 3 \pmod 8$ y $p \neq 43$. Entonces, no hay soluciones primitivas no triviales de la ecuación*

$$x^4 - 129y^2 = z^p.$$

Demostración. Como antes, sea (a, b, c) una solución primitiva no trivial, y sea $E_{(a,b,c)}$ la curva de Frey adjuntada a tal solución. En este caso, c podría estar soportado en 2, con lo cual la Proposición 2.3.1 no es suficiente para obtener la irreducibilidad de $\rho_{E_{(a,b,c)},p}$. Además, el Teorema 2.3.2 prueba que la imagen residual es absolutamente irreducible para primos no pertenecientes a $\{2, 3, 5, 7, 11, 13, 17, 43, 53, 251, 313, 661, 2593, 3371, 411577\}$. Como esta cota es grande, seguiremos la estrategia descripta en [62, Lema 3.2]. Supongamos que la representación residual extendida $\tilde{\rho}_p$ en el primo p es reducible, digamos con semisimplificación dada por $\theta_1 \oplus \theta_2$. Entonces la representación residual de $\rho_{E_{(a,b,c)},p}$ es isomorfa a $\chi^{-1}\theta_1|_{G_K} \oplus \chi^{-1}\theta_2|_{G_K}$. Para facilitar la notación, sea $\psi_i = \chi^{-1}\theta_i|_{G_K}$. Como la curva $E_{(a,b,c)}$ tiene reducción aditiva sólo en los primos que dividen a 2, ambos ψ_1 y ψ_2 son no ramificados fuera de los primos que dividen a 2 y p. Más aún, por [53, Lema 1], uno de los caracteres es no ramificado fuera de p (digamos ψ_1).

El primo 2 se parte en $\mathbb{Q}(\sqrt{129})/\mathbb{Q}$, digamos $\langle 2\rangle = \mathfrak{p}_2\bar{\mathfrak{p}}_2$. Por Lema 3.1.5, el conductor de $E_{(a,b,c)}$ en $(\mathfrak{p}_2, \bar{\mathfrak{p}}_2)$ es igual a $(8, 8), (1, 6)$ o $(4, 6)$, por lo que el caracter ψ_1 tiene conductor a lo sumo $2^4, \mathfrak{p}_2^3$ o $4 \cdot \mathfrak{p}_2$ (o sus conjugados). El grupo de clases de rayos de tales conductores tiene exponente 4 en el primer caso y 2 en los otros dos casos (calculados usando `PARI/GP`). En particular la curva (o un twist cuadrático de ella) tiene un punto racional sobre una extensión de grado 2 o 4 sobre $\mathbb{Q}$. Luego $p \leq 17$ por [33, Teorema 1.2].

El Corolario 3.3.1 y la prueba del Lema 3.1.5 implican que $\rho_{E_{(a,b,c)},p} \otimes \chi$ es congruente módulo p a la representación de Galois de una forma nueva en $S_2(2\cdot 3\cdot 43, \varepsilon)$ (cuando c es par) o en $S_2(2^8\cdot 3\cdot 43, \varepsilon)$ (cuando c es impar), donde ε corresponde a la extensión $\mathbb{Q}(\sqrt{129})/\mathbb{Q}$.

• El espacio $S_2(\Gamma_0(2 \cdot 3 \cdot 43), \varepsilon)$ tiene 4 clases de conjugación de Galois, una de ellas con multiplicación compleja. Usando el truco de Mazur para los primos $5 \leq q \leq 20$, todas las formas pueden ser descartadas asumiendo $p > 5$.

• El espacio $S_2(\Gamma_0(2^8 \cdot 3 \cdot 43), \varepsilon)$ tiene 36 clases de conjugación de Galois, 18 de ellas con multiplicación compleja. Usando el truco de Mazur para los primos $5 \leq q \leq 20$, las primeras 33 formas (en el orden de `Magma`) pueden ser descartadas asumiendo $p \notin \{2, 5, 7, 11, 13, 17, 23, 43\}$, excepto por cuatro formas con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$. Las últimas tres no tienen multiplicación compleja, pero tienen cuerpo de coeficientes grande y `Magma` no consigue calcular las normas sobre estos cuerpos, por lo que utilizamos `Magma` para calcular los coeficientes a_5 y a_7 de cada una de dichas formas y aplicamos el truco de Mazur en `PARI/GP` para $q = 5, 7$ a mano (donde las normas son calculadas en unos pocos segundos). Se sigue que pueden ser descartadas si $p \notin \{2, 5, 7, 37\}$.

Como 2 se parte, entonces podemos utilizar los resultados de la Sección 2.4.5 para descartar formas con multiplicación compleja. Luego de una búsqueda por el mínimo x, obtenemos que tomar $x = 49885$ en (2.17) (usando las desigualdades (2.15) y (2.16)) hace que el lado derecho sea positivo si $p > 900$. Esto puede ser chequeado con el siguiente comando (en `PARI/GP`):

```
? read("RemoveCM");
? Bound(129,907,49885)
%1 = 0.039412707010082109791157365950637933812
```

Para primos chicos, el mismo argumento que en los ejemplos anteriores funciona; notar que c es divisible por un primo mayor que 3 porque no puede ser divisible por 3 (por Lema 2.1.1) y no es divisible por 2 porque las formas modulares que no pueden ser descartadas aparecen en el espacio $S_2(\Gamma_0(2^8 \cdot 3 \cdot 43), \varepsilon)$. Luego, nuevamente estamos en las hipótesis de la Proposición 2.4.6, que

descarta las formas con multiplicación compleja por $\mathbb{Z}[\sqrt{-2}]$ para los primos $p \equiv 1, 3 \pmod 8$, por Proposición 1.2.20. □

Observación 26. La cota de Ellenberg obtenida en el ejemplo anterior probablemente pueda ser mejorada si se mejoran las cotas en los cálculos de la Sección 2.4.5. Si el valor final no es muy grande, una forma $f \in S_2(2p^2)$ con las propiedades deseadas (del Teorema 2.4.7) se puede encontrar en el rango intermedio vía una búsqueda computacional (ver Observación 15).

Capítulo 4

La ecuación $x^2 - dy^6 = z^p$

Los analistas no podrán entender

C. García, Cerca de la revolución.

Al final de Capítulo 1 vimos que en la actualidad no se conocen todas las soluciones de la ecuación (1.9). La ecuación (4.1) expuesta a continuación es más débil, pues si (a, b, c) es solución de (4.1) entonces (a, b^2, c) es solución de (1.9). En 2012, Bennet y Chen logran probar, combinando los resultados de $\mathbb{Q}$-curvas en [38] junto la técnica del multi Frey (ver [10, 12]) el siguiente resultado (ver [3]).

Teorema 4.0.1 (Bennett-Chen)**.** *Sea $n \geq 3$ un entero. Entonces la ecuación*

$$x^2 + y^6 = z^n \tag{4.1}$$

no tiene soluciones primitivas no triviales.

Para ello, en el Paso 1 de la estrategia general, los autores introducen una curva elíptica definida sobre $\mathbb{Q}(\sqrt{-1})$ que resulta ser 3-isógena a su conjugada, sobre $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-1})$ (es decir que es $\mathbb{Q}$-curva totalmente definida sobre L). Siguiendo la misma estrategia, Chen demuestra lo siguiente (ver [17]).

Teorema 4.0.2 (Chen)**.** *Sea p un número primo tal que $p \equiv 1, 7 \pmod{24}$ y $p \neq 7$. La única solución primitiva no trivial de la ecuación*

$$x^2 - 2y^6 = z^p$$

es $(x, y, z) = (\pm 1, \pm 1, -1)$ para todo p.

Más recientemente, en el año 2020, Koutsianas logra definir una $\mathbb{Q}$-curva sobre $\mathbb{Q}(\sqrt{-3})$ que le permite probar lo siguiente (ver [51]).

Teorema 4.0.3 (Koutsianas)**.** *Sea $n \geq 3$ un entero. La única solución primitiva de la ecuación*

$$x^2 + 3y^6 = z^n$$

es $(x, y, z, n) = (\pm 47, \pm 2, \pm 7, 4)$.

Al igual que antes, la hipótesis de primitividad de la solución es fundamental puesto que, removiendo dicha hipótesis nuevamente tendríamos infinitas soluciones.

Lema 4.0.4 (Granville)**.** *Sea $p > 3$ un número primo. La ecuación*

$$x^2 + dy^6 = z^p,$$

tiene infinitas soluciones no primitivas.

Demostración. La prueba sigue la misma idea que el Lema 3.0.1. Supongamos que $p \equiv 1 \pmod 6$. Sean $u, v \in \mathbb{Z}$ arbitrarios tales que $r = u^2 + dv^6$ no es igual a ± 1. Entonces el punto $(ur^{(p-1)/2}, vr^{(p-1)/6}, r)$ es solución de la ecuación (2). Si $p \equiv 5 \pmod 6$, entonces el punto $(ur^{(5p-1)/2}, vr^{(5p-1)/6}, r^5)$ es solución de la ecuación (2). □

Similar al Capítulo 3, el objetivo del presente capítulo es estudiar la ecuación (2) para d un entero mediante el método modular. A diferencia de la ecuación (1), en este caso no contamos con una curva definida para un d arbitrario, con lo cual primero deberemos encargarnos de ello (a pesar de ser pronosticado que dicha curva no existiría en general; ver [51, Introducción]). Los resultados expuestos en este capítulo están basados en el artículo [64], en colaboración con Ariel Pacetti, y en [46], junto con Franco Golfieri y Ariel Pacetti.

4.1 Paso 1: La curva $\widetilde{E}_{(a,b,c)}$ y sus propiedades

La construcción de la curva de Frey en [3] para el caso $d = -1$ no muestra explícitamente la 3-isogenía a su conjugada. Asumiendo que nuestra curva tendrá un punto de 3-torsión, es natural comenzar con la parametrización de la familia de curvas que tienen un punto de 3-torsión, dada por Kubert en [54, Tabla 1]. Es así como, dada (a, b, c) una solución primitiva de (2) construimos la curva elíptica

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{d}xy - 4d(a + b^3\sqrt{d})y = x^3. \tag{4}$$

Su discriminante es igual a $\Delta(\widetilde{E}_{(a,b,c)}) = -2^8 3^3 d^4 c^p (a + b^3\sqrt{d})^2$; notar que su discriminante es divisible por d (a diferencia de la curva (3)). Su j-invariante es $j(\widetilde{E}_{(a,b,c)}) = \frac{2^4 3^3 b^3\sqrt{d}(4a-5b^3\sqrt{d})^3}{c^p(a+b^3\sqrt{d})^2}$.

Sea ψ_{-3} el caracter cuadrático correspondiente a la extensión cuadrática $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$.

Proposición 4.1.1. *La curva elíptica $\widetilde{E}_{(a,b,c)}$ es una $\mathbb{Q}$-curva totalmente definida sobre el cuerpo $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$. Más aún, $\tau(\widetilde{E}_{(a,b,c)})$ es isógena al twist cuadrático $\widetilde{E}_{(a,b,c)} \otimes \psi_{-3}$.*

Demostración. Como es explicado en [54, Tabla 1], todas las curvas elípticas que tienen un punto de 3-torsión tienen un modelo minimal de la forma

$$E : y^2 + a_1xy + a_3y = x^3,$$

donde $P = (0, 0)$ es un punto de orden 3. Su curva 3-isógena (obtenida como el cociente de la curva por el grupo de orden 3 generado por P) tiene ecuación

$$y^2 + a_1xy + a_3y = x^3 - 5a_1a_3x - a_1^3a_3 - 7a_3^2.$$

Nuestra curva $\widetilde{E}_{(a,b,c)}$ se corresponde a tomar los valores $a_1 = 6b\sqrt{d}$, $a_3 = -4d(a + b^3\sqrt{d})$. La fórmula anterior implica que el cociente de $\widetilde{E}_{(a,b,c)}$ por $\langle(0, 0)\rangle$ tiene ecuación

$$y^2 + 6b\sqrt{d}xy - 4d(a + b^3\sqrt{d})y = x^3 + (-120b^4d^2 + 120abd\sqrt{d})x + 976b^6d^3 - 1088ab^3d^2\sqrt{d} - 112a^2d^2. \tag{4.2}$$

Por otro lado, si τ genera el grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, claramente $\tau(\widetilde{E}_{(a,b,c)}) = \widetilde{E}_{(a,-b,c)}$. El twist cuadrático de $\widetilde{E}_{(a,-b,c)}$, por $\sqrt{-3}$ (que puede ser calculado usando `PARI/GP`) se corresponde a la ecuación

$$y^2 + 6b\sqrt{d}xy + 12d(-a + b^3\sqrt{d})y = x^3 + 36b^2dx^2 + \\ (144abd\sqrt{d} + 144b^4d^2)x + 288ab^3d^2\sqrt{d} + 144b^6d^3 - 144a^2d^2. \quad (4.3)$$

Vía el cambio de variables usual (haciendo $a_1 = a_3 = a_2 = 0$) es fácil de ver que ambas (4.3) y (4.2) se transforman en

$$y^2 = x^3 + (108abd\sqrt{d} - 135b^4d^2)x - 756ab^3d^2\sqrt{d} + 594b^6d^3 - 108a^2d^2.$$

En particular, $\tau(\widetilde{E}_{(a,b,c)})$ es isógena al twist cuadrático de $\widetilde{E}_{(a,b,c)}$ por $\sqrt{-3}$. Luego, $\widetilde{E}_{(a,b,c)}$ es una $\mathbb{Q}$-curva y su cuerpo de definición es igual a $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$. □

Al igual que en la Sección (3.1), tenemos algunos resultados básicos que la curva $\widetilde{E}_{(a,b,c)}$ debe satisfacer. Nuevamente, sea $K = \mathbb{Q}(\sqrt{d})$ y $\mathscr{O}_K$ su anillo de enteros.

Lema 4.1.2. *Sea* $\mathfrak{q}$ *un ideal primo de* $\mathscr{O}_K$ *tal que* $\mathfrak{q} \nmid 6d$ *y* $\mathfrak{q} \mid \Delta(\widetilde{E}_{(a,b,c)})$. *Entonces* $\widetilde{E}_{(a,b,c)}$ *tiene reducción multiplicativa en* $\mathfrak{q}$.

Demostración. La prueba es similar a la del Lema 3.1.3. □

Lema 4.1.3. *Sea* $\mathfrak{q}$ *un ideal primo de* $\mathscr{O}_K$ *tal que* $\mathfrak{q} \nmid 6d$. *Entonces* $v_{\mathfrak{q}}(\Delta(\widetilde{E}_{(a,b,c)})) \equiv 0 \pmod{p}$.

Demostración. La prueba es similar a la del Lema 3.1.4. □

Una diferencia importante entre la ecuación (1) y la ecuación (2) es que no podremos remover (con ningún resultado de bajada de nivel) los primos ramificados impares del conductor de la representación residual.

Lema 4.1.4. *Supongamos que* q *es un primo impar que ramifica en* $K/\mathbb{Q}$ *y denotemos por* $\mathfrak{q}$ *el (único) ideal primo de* $\mathscr{O}_K$ *que divide a* p. *Entonces* $v_{\mathfrak{q}}(\Delta(\widetilde{E}_{(a,b,c)})) = 8 + 3v_{\mathfrak{q}}(3)$.

Demostración. Como q ramifica, $\mathfrak{q} \mid \sqrt{d}$, y como (a, b, c) es una solución primitiva, $\mathfrak{q} \nmid a$. Entonces, usando que $\mathfrak{q} \nmid c^p(a + b^3\sqrt{d})$ y que $v_{\mathfrak{q}}(d) = 2$ el resultado se sigue. □

Observación 27. La curva $\widetilde{E}_{(a,b,c)}$ tiene mala reducción potencialmente buena en todos los primos impares que ramifican en $K/\mathbb{Q}$. Sin embargo, sobre la extensión $K(\sqrt[6]{-d})$ obtiene buena reducción (vía el cambio usual de variables $(x, y) \to (\sqrt[3]{(-d)^2}x, dy)$). Si $q \mid d$ es tal primo impar, sea $\mathfrak{q} = \langle q, \sqrt{d}\rangle$ el ideal en K que lo divide. Si $q \equiv 1 \pmod 3$, la extensión $K_{\mathfrak{q}}(\sqrt[6]{-d})/K_{\mathfrak{q}}$ es una extensión abeliana, por lo tanto el tipo local de la representación de Weil-Deligne en $\mathfrak{q}$ es una serie principal (dada por un caracter de orden 3), mientras que si $q \equiv 2 \pmod 3$ la curva adquiere buena reducción sobre una extensión no abeliana, luego su tipo local coincide con el de una representación supercuspidal (obtenida induciendo un caracter de orden 3 de la extensión cuadrática no ramificada $K_{\mathfrak{q}}(\zeta_3)/K_{\mathfrak{q}}$).

Sea $N(\widetilde{E}_{(a,b,c)})$ el conductor de $\widetilde{E}_{(a,b,c)}$ y supongamos que $p > 3$.

Lema 4.1.5. *Sea* $\mathfrak{p}_2$ *un ideal primo de* $\mathscr{O}_K$ *que divide a* 2. *Entonces:*

1. *Si* 2 *es inerte en* $K/\mathbb{Q}$ *entonces* $\tilde{E}$ *tiene tipo de reducción* IV^* *en* $\mathfrak{q}$ *con* $v_2(N(\widetilde{E}_{(a,b,c)})) = 2$.
2. *Si* 2 *se parte en* $K/\mathbb{Q}$ *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene tipo de reducción* IV^* *ó* I_n *en* $\mathfrak{p}_2$, *con* $v_{\mathfrak{p}_2}(N(\widetilde{E}_{(a,b,c)})) = 1, 2$ *en ambos primos que dividen a* 2.

3. *Si* 2 *ramifica en* $K/\mathbb{Q}$ *pero* $2 \nmid d$ *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene tipo de reducción* IV *en* $\mathfrak{p}_2$ *con* $v_{\mathfrak{p}_2}(N(\widetilde{E}_{(a,b,c)})) = 2$.

4. *Si* $2 \mid d$ *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene buena reducción en* $\mathfrak{p}_2$.

Demostración. Consideremos cada caso por separado:

1. Si 2 es inerte, $2 \nmid c$, por Lema 2.1.1. Claramente $2 \mid b_2$, $4 \mid a_6$, $8 \mid b_8$ pero como $2 \nmid (a + b^3\sqrt{d})$, el polinomio $y^2 + \frac{a_3}{4}y - a_6$ tiene raíces distintas, con lo cual el Paso 8 del algoritmo de Tate implica que la reducción es de tipo IV^* y el conductor es igual a $v_2(\Delta(\widetilde{E}_{(a,b,c)})) - 6 = 2$.

2. Supongamos que 2 se parte y que $\mathfrak{p}_2$ es un primo que lo divide. La hipótesis de primitividad implica que uno de $\{a, b\}$ es par y el otro impar o ambos son impares. En el primer caso, $v_{\mathfrak{p}_2}(a_1) \geq 1$ y $v_{\mathfrak{p}_2}(a_3) = 2$, luego nuevamente estamos en el Paso 8 del algoritmo de Tate (tipo IV^*) y entonces el exponente del conductor es 2. Por otro lado, si ambos a y b son impares, el modelo no es minimal, ya que $v_{\mathfrak{p}_2}(a_1) = 1$ y $v_{\mathfrak{p}_2}(a_3) \geq 3$; su modelo minimal tiene a $\tilde{a_1}$ como unidad (por lo tanto a $\tilde{b_2}$ como unidad) y la curva tiene tipo $\mathrm{I_n}$. En particular, su exponente en el conductor es 1.

3. Supongamos que 2 ramifica pero $2 \nmid d$ y sea π un uniformizador local. La hipótesis de primitividad implica $v_\pi(a + b^3\sqrt{d}) = 0$ (i.e. $a \not\equiv b \pmod 2$). El modelo no es minimal; el cambio de variables $y \to \pi^3 y$, $x \to \pi^2 x$ da un modelo minimal con valuaciones $v_\pi(\tilde{a_1}) \geq 1$ y $v_\pi(\tilde{a_3}) = 1$. En particular, $v_\pi(\tilde{b_6}) = 2$ con lo cual estamos en el Paso 5 del algoritmo de Tate, que implica que la reducción es de tipo IV y el exponente de su conductor es igual a $v_\pi(\Delta(\widetilde{E}_{(a,b,c)})) - 2 = 2$.

4. Si $2 \mid d$ entonces $2 \nmid a$ (pues la solución es primitiva), entonces el cambio de variables $x \to 2^2 x$, $y \to 2^3 y$ da lugar a una curva no singular.

□

Por último, necesitamos información en los primos que dividen a 3.

Lema 4.1.6. *Sea* $\mathfrak{p}_3$ *un ideal primo de* $\mathcal{O}_K$ *que divide a* 3.

1. *Si* 3 *es inerte en* K *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene tipo de reducción* II *ó* III *en* 3, *con* $v_3(N(\widetilde{E}_{(a,b,c)})) \in \{2, 3\}$.

2. *Si* $3 = \mathfrak{p}_3\bar{\mathfrak{p}}_3$ *en* K *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene tipo de reducción* II *ó* III *en* $\mathfrak{p}_3$, *con* $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = v_{\bar{\mathfrak{p}}_3}(N(\widetilde{E}_{(a,b,c)})) \in \{2, 3\}$ *o* $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 2$ *y* $v_{\bar{\mathfrak{p}}_3}(N(\widetilde{E}_{(a,b,c)})) = 1$.

3. *Si* 3 *ramifica en* K *entonces* $\widetilde{E}_{(a,b,c)}$ *tiene tipo de reducción* IV^* *en* $\mathfrak{p}_3$, *con* $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 8$.

Demostración. Consideremos los distintos casos:

1. Si 3 es inerte, la hipótesis de primitividad implica que c no es divisible por 3 y $v_3(a_3) = 0$, con lo cual el punto singular no está en el origen pero va al origen bajo la traslación $(x, y) \to (x - a_3^6, y + a_3)$ (estamos usando que en el cuerpo residual elevar a la potencia octava es el mapa constante). Denotemos por a_1, a_3 los coeficientes correspondientes de $\tilde{E}$ (para facilitar la notación). Entonces el modelo se convierte en

$$y^2 + a_1xy + (3a_3 - a_1a_3^6)y = x^3 - 3a_3^6x^2 - a_1a_3x + (a_1a_3^7 - a_3^{18} - 2a_3^2). \tag{4.4}$$

Denotemos por $\tilde{a_i}$ tales coeficientes. Si $3 \mid b$ entonces $v_3(a_1) \geq 2$ y $v_3(\tilde{a_6}) = 1$, con lo cual estamos en el Paso 3 del algoritmo de Tate. Por lo tanto la curva tiene reducción de tipo II y el exponente en el conductor es 3. Si $3 \nmid b$, $v_3(a_1) = 1$. Si $9 \nmid a_1 a_3^7 - a_3^{18} - 2a_3^2$ estamos nuevamente en el caso II (con exponente 3). Caso contrario, se sigue la siguiente igualdad:

$$\frac{a_1}{3} \equiv a_3^3 \left(\frac{a_3^{16} + 2}{3} \right) \pmod 3.$$

El coeficiente $\tilde{b_2}$ es igual a $-4a_1^2 a_3^{18} + 6a_1 a_3^{13} + 12a_3^{24} - 3a_3^8$. Usando la ecuación de arriba, un simple cálculo muestra que su valuación en 3 es igual a 2, luego el tipo de reducción es III y el exponente del conductor es 2.

2. Si 3 se parte en K, sea $\mathfrak{p}_3$ un primo que lo divide. Si $3 \mid a$ entonces $3 \nmid b$, luego $v_{\mathfrak{p}_3}(a_1) = 1$ y $v_{\mathfrak{p}_3}(a_3) = 0$. Esta situación coincide con el caso previo y un cálculo similar prueba que el tipo es II o III y la valuación del exponente es 3 o 2 en ambos $\mathfrak{p}_3$ y $\bar{\mathfrak{p}_3}$. Si $3 \mid b$ entonces $3 \nmid a$, luego $v_{\mathfrak{p}_3}(a_1) \geq 2$ y $v_{\mathfrak{p}_3}(a_3) = 0$ y como en el caso previo se corresponde con un tipo II con exponente en el conductor 3.

   Supongamos entonces que $3 \nmid ab$. Esto implica que uno de los primos (digamos $\mathfrak{p}_3$) divide a $a + b^3\sqrt{d}$ mientras que el otro no. Como $c^p = (a + b^3\sqrt{d})(a - b^3\sqrt{d})$, la hipótesis $p \geq 5$ implica que (sin pérdida de generalidad) $v_{\mathfrak{p}_3}(a+b^3\sqrt{d}) > 3$ entonces $\mathfrak{p}_3$ divide el denominador del j-invariante. Más aún, el modelo no es minimal, y bajo el cambio usual de variables (mandando $(x, y) \to (3^2x, 3^3y)$ obtenemos una curva con reducción multiplicativa, con lo cual el exponente en el conductor es 1. En el primo $\bar{\mathfrak{p}}_3$ la curva es un twist cuadrático (por el caracter de conductor 3) de una curva con reducción multiplicativa, de donde se sigue el enunciado.

3. Si 3 ramifica en K entonces $3 \mid d$ y la hipótesis de primitividad implica que $3 \nmid a$. Denotemos por $\mathfrak{p}_3$ el ideal primo que divide a 3 en K. Entonces $v_{\mathfrak{p}_3}(a_1) \geq 2$ y $v_{\mathfrak{p}_3}(a_3) = 2$, luego estamos en el Paso 8 del algoritmo de Tate, el tipo de reducción es IV^* y el exponente de conductor es $14 - 6 = 8$.

□

Observación 28. Si 3 es inerte en $K/\mathbb{Q}$ y la curva tiene tipo de reducción III (el caso de valuación del conductor igual a 2), el cambio de variables $(x, y) \to (\sqrt[4]{3}x, \sqrt{3}y)$ en la ecuación (4.4) da una curva con buen tipo de reducción. Como las raíces cuartas de la unidad están en K_3, el tipo local de la representación de Weil-Deligne es una serie principal (cuya inercia está dada por un caracter de orden 4).

Lema 4.1.7. *Sea q un primo que ramifica en $K/\mathbb{Q}$ tal que $q \nmid 6$ y sea $\mathfrak{q}$ el ideal primo de $\mathcal{O}_K$ que lo divide. Entonces $\widetilde{E}_{(a,b,c)}$ tiene tipo de reducción IV^* en $\mathfrak{q}$ y $v_{\mathfrak{q}}(N(\widetilde{E}_{(a,b,c)})) = 2$.*

Demostración. Como (a, b, c) es solución primitiva, entonces $q \nmid a$, $v_{\mathfrak{q}}(a_3) = 2$ y $v_{\mathfrak{q}}(b_6) = 4$. Además, $v_{\mathfrak{q}}(b_2) \geq 2$ lo que implica que estamos en el Paso 8 del algoritmo de Tate, con lo cual el resultado se sigue del Lema 4.1.4. □

Nuevamente, las soluciones triviales corresponden a curvas especiales.

Lema 4.1.8. *La solución trivial $(0, 0, 0)$ da lugar a una curva singular. Las demás soluciones primitivas triviales de (2) son las siguientes:*

- *La solución $(0, \pm 1, 1)$ (cuando $d = 1$), correspondiente a la curva elíptica con etiqueta LMFDB 2.0.4.1-324.1-a3 y multiplicación compleja por $\mathbb{Z}[\sqrt{-1}]$.*

- *La solución* $(\pm 1, 0, 1)$*, correspondiente a un twist cúbico por* $\sqrt[3]{d}$ *de la curva elíptica con etiqueta LMFDB* 108-a2*. Tal twist tiene multiplicación compleja por* $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Demostración. La solución $(0, 0, 0)$ claramente da una curva singular. Las demás soluciones primitivas deben ser de la forma $(\pm 1, 0, 1)$ o $(0, \pm 1, 1)$. El último caso sólo puede ocurrir cuando $d = 1$ (pues d es libre de cuadrados), dando la primera ecuación. La solución $(\pm 1, 0, 1)$ se corresponde con la curva elíptica

$$\widetilde{E}_{(\pm 1,0,1)} : y^2 \pm 4dy = x^3.$$

Cuando $d = 1$, se corresponde con la curva elíptica con etiqueta LMFDB 108-a2, que tiene multiplicación compleja por $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. El hecho de que las raíces cúbicas de la unidad actúen en la curva permite definir twist cúbicos de la curva, y el caso general es precisamente el twist cúbico por $\sqrt[3]{d}$ del caso $d = 1$. □

Observación 29. La solución trivial $(\pm 1, 0, 1)$ se corresponde con una curva elíptica sobre K con multiplicación compleja cuyo conductor tiene valuación:

- 2 para todos los primos $\mathfrak{q}$ que dividen a d pero no a 3,
- 2 si $\mathfrak{p}_2 \mid 2$ y $2 \nmid d$,
- 0 si $\mathfrak{p}_2 \mid 2$ y $2 \mid d$,
- 3 si $\mathfrak{p}_3 \mid 3$ y $3 \nmid d$,
- 8 si $\mathfrak{p}_3 \mid 3$ y $3 \mid d$.

Más aún, el siguiente resultado caracteriza todas las soluciones primitivas que dan lugar a curvas elípticas con multiplicación compleja en el caso en donde K es imaginario, que es el que será de interés en la Sección 4.3.1.

Lema 4.1.9. *Sea* $d < 0$ *un entero libre de cuadrados y* (a, b, c) *una solución primitiva no trivial de (2). Entonces la curva* $\widetilde{E}_{(a,b,c)}$ *tiene multiplicación compleja si y sólo si* $(a, b, c, d, p) = (\pm 5, \pm 1, 3, -2, 3)$*, con multiplicación compleja por* $\mathbb{Z}[\sqrt{-2}]$.

Demostración. Recordemos que el j-invariante es $j(\widetilde{E}_{(a,b,c)}) = 2^4 3^3 \sqrt{d} b^3 \cdot \frac{(4a-5b^3\sqrt{d})^3}{c^p(a+b^3\sqrt{d})^2} \in \mathbb{Q}(\sqrt{d})$. Si E tiene multiplicación compleja, entonces por el mismo argumento que en el Lema 3.1.8, $j(\widetilde{E}_{(a,b,c)}) \in \mathbb{Q}$. La parte imaginaria de $j(\widetilde{E}_{(a,b,c)})$ se factoriza como

$$864ab^3 \cdot \frac{(2a^2 - 25db^6)(16a^2 - 11db^6)}{c^{3p}}. \tag{4.5}$$

Se anula si y sólo si $a = 0$ (dado soluciones no primitivas), $b = 0$ (solución trivial) o uno de los dos últimos términos se anula. Como d es libre de cuadrados y nuestra solución es primitiva, esto sólo puede ocurrir cuando $d = 2$, $a = \pm 5$ y $b = \pm 1$, correspondiente al punto $(\pm 5, \pm 1, 3)$ para $p = 3$. □

4.2 Paso 2

4.2.1 Construcción del caracter de Hecke para un primo $t \equiv 3 \pmod 4$

Los cálculos a realizar son similares a los de la Sección 3.2.1. Sea $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$ (libre de cuadrados). Utilizaremos la notación $p \equiv \square \pmod t$ para decir que p es un cuadrado módulo t. En esta oportunidad, definimos los siguientes conjuntos:

- $Q_{++} = \{p \mid d,\ p \nmid 2t,\ p \equiv \square \pmod 4,\ p \equiv \square \pmod t\}$.
- $Q_{+-} = \{p \mid d,\ p \nmid 2t,\ p \equiv \square \pmod 4,\ p \not\equiv \square \pmod t\}$.
- $Q_{-+} = \{p \mid d,\ p \nmid 2t,\ p \not\equiv \square \pmod 4,\ p \equiv \square \pmod t\}$.
- $Q_{--} = \{p \mid d,\ p \nmid 2t,\ p \not\equiv \square \pmod 4,\ p \not\equiv \square \pmod t\}$.

Luego, en este caso tenemos que $d = -2^{v_2(d)} \cdot t^{v_t(d)} \cdot \prod_{p \in Q_{\pm\pm}} p$. El siguiente lema elemental clarificará luego algunos cálculos.

Lema 4.2.1. *Supongamos que t es no ramificado en K. Entonces el primo t se parte en K precisamente cuando la siguiente igualdad se satisface:*

$$(-1)^{\#Q_{+-}+\#Q_{--}} \delta_t(2)^{v_2(d)} = -1.$$

Similarmente, es inerte cuando $(-1)^{\#Q_{+-}+\#Q_{--}} \delta_t(2)^{v_2(d)} = 1$.

Demostración. Se sigue fácilmente del hecho de que t se parte en $\mathbb{Q}(\sqrt{d})$ si y sólo si d es un cuadrado módulo t. □

El caracter ε: Definimos un caracter par $\varepsilon : \mathbb{I}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ ramificado en los primos que viven en Q_{++}, Q_{-+}, Q_{+-} y eventualmente en 2 y t. Su componente local ε_p se define de la siguiente forma:

- Para primos $p \in Q_{++} \cup Q_{-+}$, el caracter $\varepsilon_p : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ es cuadrático, i.e., $\varepsilon_p = \delta_p$.
- Para primos $p \in Q_{+-}$, el caracter $\varepsilon_p : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ es cualquier caracter de orden $2^{v_2(p-1)}$.
- Para $p = t$ definimos $\varepsilon_t = \begin{cases} \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+v_2(d)+1} & \text{si } t \equiv 3 \pmod 8, \\ \delta_t^{\#Q_{+-}+\#Q_{--}+v_t(d)+1} & \text{si } t \equiv 7 \pmod 8. \end{cases}$

  Por Lema 4.2.1, ε_t es trivial si t se parte en K y es igual a δ_t si t es inerte en K.
- Para $p = 2$ definimos $\varepsilon_2 = \begin{cases} \delta_{-1}^{\#Q_{-+}+\#Q_{--}+v_t(d)+v_2(d)+1} & \text{si } t \equiv 3 \pmod 8, \\ \delta_{-1}^{\#Q_{-+}+\#Q_{--}+v_t(d)+1} & \text{si } t \equiv 7 \pmod 8. \end{cases}$
- Para todos los primos restantes, ε_p es trivial.
- El caracter ε_∞ (la componente arquimediana) es trivial.

Por Lema 4.2.1, ε_t es trivial si t se parte en K y es igual a δ_t si t es inerte en K. Un resultado similar para ε_2 es el siguiente.

Lema 4.2.2. *El caracter ε_2 definido más arriba satisface que*

$$\varepsilon_2 = \begin{cases} 1 & \text{si } d \equiv 3 \pmod 4, \\ \delta_{-1} & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Demostración. Como $2 \nmid d$, el primo 2 ramifica en K si y sólo si $d \equiv 3 \pmod 4$. Recordamos que el primo t no es un elemento de $Q_{\pm\pm}$, por lo que los divisores primos de d congruentes a 3 módulo 4 son precisamente los de $Q_{-+} \cup Q_{--}$ y posiblemente t. Luego, el primo 2 ramifica en K precisamente cuando $\#Q_{-+} + \#Q_{--} + v_t(d)$ es par. Como $2 \nmid d$, ε_2 es igual a δ_{-1} cuando 2 ramifica y 1 cuando no ramifica. □

Un simple cálculo de las definiciones anteriores muestra que

$$\prod_p \varepsilon_p(-1)\varepsilon_\infty(-1) = (-1)^{\#Q_{-+}+\#Q_{+-}}\varepsilon_2(-1)\varepsilon_t(-1) = 1.$$

Teorema 4.2.3. *Existe un caracter de Hecke $\chi : G_K \to \overline{\mathbb{Q}}^\times$ tal que:*

1. *$\chi^2(\sigma) = \varepsilon(\sigma)$ para todo $\sigma \in G_K$,*
2. *χ es no ramificado en primos que no dividen a $2t\prod_{p\in Q_{+-}\cup Q_{--}} p$,*
3. *Si $\tau \in G_{\mathbb{Q}}$ no es la identidad en K, ${}^\tau\chi = \chi\cdot\psi_{-t}$ como caracteres de G_K.*

Demostración. Nuevamente, seguimos la estrategia general para definir las componentes locales $\chi_p : \mathscr{O}_{\mathfrak{p}}^\times \to \overline{\mathbb{Q}}^\times$ del caracter χ:

- Si $\mathfrak{p}$ es un primo impar no ramificado, entonces, $\chi_{\mathfrak{p}}$ es el caracter trivial.
- Si $p \in Q_{\pm\pm}$ y $\mathfrak{p} \mid p$,
$$\chi_{\mathfrak{p}} = \varepsilon_p\delta_p. \tag{4.6}$$
- Para primos $\mathfrak{t}$ que dividen a t, definimos el caracter $\chi_{\mathfrak{t}}$ como:
  - Si t ramifica en K, $\chi_{\mathfrak{t}} = \varepsilon_t$.
  - Si t se parte en K, digamos $t = \mathfrak{t}\bar{\mathfrak{t}}$, sea $\chi_{\mathfrak{t}} = \delta_t$ y $\chi_{\bar{\mathfrak{t}}} = 1$.
  - Si t es inerte en K, $\chi_{\mathfrak{t}}$ es un caracter de orden 4 (luego su restricción a $\mathbb{F}_t^\times$ es trivial).

  En todos los casos denotamos $\chi_t = \prod_{\mathfrak{t}\mid t}\chi_{\mathfrak{t}}$.
- En un primo $\mathfrak{p}_2$ que divide a 2, definimos el caracter $\chi_{\mathfrak{p}_2}$ de la siguiente forma:
  - Si 2 no ramifica en $K/\mathbb{Q}$, es trivial.
  - Si 2 ramifica en $K/\mathbb{Q}$ pero $2 \nmid d$, entonces definimos $\chi_{\mathfrak{p}_2}$ como:
    - Si $t \equiv 3 \pmod 8$, el caracter de conductor 2 que manda $\sqrt{d}$ a -1.
    - Si $t \equiv 7 \pmod 8$, el caracter trivial.
  - Si $2 \mid d$ entonces $\chi_{\mathfrak{p}_2}$ es el caracter de conductor $\mathfrak{p}_2^5$ cuyo valor en los generadores 5, -1 y $1+\sqrt{d}$ es igual: $\chi_{\mathfrak{p}_2}(5) = -1$, $\chi_{\mathfrak{p}_2}(-1) = \delta_2(t)$ y
    - Si $d \equiv 2 \pmod 8$, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = \begin{cases} 1 & \text{si } t \equiv 3 \pmod 8, \\ \sqrt{-1} & \text{si } t \equiv 7 \pmod 8. \end{cases}$
    - Si $d \equiv 6 \pmod 8$, $\chi_{\mathfrak{p}_2}(1+\sqrt{d}) = \begin{cases} \sqrt{-1} & \text{si } t \equiv 3 \pmod 8, \\ -1 & \text{si } t \equiv 7 \pmod 8. \end{cases}$

    Abusando de la notación, escribimos $\chi_2 = \chi_{\mathfrak{p}_2}$.
- La componente arquimediana de χ es trivial.

Recordemos algunas propiedades de los caracteres locales recién definidos (que motivaron dicha definición) que jugarán un rol muy importante luego.

(P1) El producto $\varepsilon_t\chi_t$ en elementos de $\mathbb{Z}_t^\times$ es igual a

$$\varepsilon_t\chi_t = \begin{cases} \delta_t & \text{si } t \nmid d, \\ 1 & \text{si } t \mid d. \end{cases}$$

(P2) Si $d \equiv 1 \pmod 4$ entonces $\chi_2(\sqrt{d}) = \delta_t(2)$.

(P3) Si $2 \mid d$, entonces $\chi_2^2(1+\sqrt{d}) = \chi_2(1-d)$.

(P4) Si $2 \mid d$ entonces $\chi_2|_{\mathbb{Z}_2^\times} = \delta_{-2}$ si $t \equiv 3 \pmod 8$ y $\chi_2|_{\mathbb{Z}_2^\times} = \delta_2$ si $t \equiv 7 \pmod 8$.

(P5) En todos los casos $\chi_2(-1) = \delta_2(t)^{v_2(d)}$ y $\chi_2(t) = 1$.

Como en el Teorema 3.2.1, definimos χ en $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ como trivial en los elementos de $K^\times$ y como el producto de las componentes locales en el segundo factor. Afirmamos que χ satisface las propiedades esperadas.

1. Debemos verificar que la igualdad
$$\chi^2 = \varepsilon \circ \mathscr{N}$$
se satisface para todos los elementos de $K^\times \cdot (\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$. Como antes, es suficiente probarlo componente a componente. Para los primos que no dividen a $2t$ el resultado se sigue de (4.6) junto con el Lema 2.2.1.

   Para primos que dividen a t, el caso en que t se parte y t ramifica se sigue del hecho tanto χ_t^2 como $\varepsilon_t \circ \mathscr{N}$ son triviales. En el caso inerte, es suficiente chequear la condición en un generador g de $\mathbb{F}_{t^2}^\times$: $\chi_t^2(g) = -1$ (pues χ_t tiene orden 4), y $\varepsilon_t(\mathscr{N}(g)) = -1$ porque $\mathscr{N}(g)$ genera $\mathbb{F}_t^\times$.

   Si $2 \nmid d$, el enunciado también es claro, pues χ_2^2 es trivial y ε_2 es trivial si 2 no ramifica (por Lema 4.2.2) y δ_{-1} cuando 2 ramifica. Pero la norma en el caso ramificado sólo toma los valores $\{0, 1, 2\}$ módulo 4, por lo que $\delta_{-1} \circ \mathscr{N}$ es trivial también. Por último, si $2 \mid d$, ambos χ_2^2 y $\varepsilon_2 \circ \mathscr{N}$ son triviales en los elementos de $\mathbb{Z}_2^\times$ y coinciden en $1+\sqrt{d}$ por (P3).

2. Lo enunciado sobre la ramificación es claro de la definición.

3. Para primos impares $\mathfrak{p}$ que no dividen a t, el caracter local $(\psi_{-t})_p \circ \mathscr{N}$ es trivial, mientras que ${}^\tau\chi_{\mathfrak{p}} = \chi_{\mathfrak{p}}$, por lo que se satisface lo enunciado. Para primos que dividen a 2, como $(\psi_{-t})_2 \circ \mathscr{N}$ también es trivial, necesitamos verificar que ${}^\tau\chi_2 = \chi_2$ (recordar la notación $\chi_2 = \chi_{\mathfrak{p}_2}$, donde $\mathfrak{p}_2$ es cualquier primo que divide a 2). Esto se sigue fácilmente de su definición cuando $2 \nmid d$. Cuando $2 \mid d$, sólo necesitamos verificar la propiedad en el elemento $1+\sqrt{d}$, pero
$${}^\tau\chi_2(1+\sqrt{d}) = \chi_2(1-\sqrt{d}) = \chi_2(1+\sqrt{d})^{-1}\chi_2(1-d) = \chi_2(1+\sqrt{d})$$
por (P3).

   Sea $\mathfrak{t}$ un primo que divide a t. Si t ramifica en K, $(\psi_{-t})_t \circ \mathscr{N}$ es trivial, mientras que ${}^\tau\chi_{\mathfrak{t}} = \chi_{\mathfrak{t}}$, y por lo tanto se satisface lo enunciado. Si t se parte, sin pérdida de generalidad podemos asumir que $\chi_{\mathfrak{t}}$ coincide con $(\psi_{-t})_t \circ \mathscr{N}$ y $\chi_{\bar{\mathfrak{t}}}$ es trivial, por lo que el resultado se sigue. Por último, supongamos que t es inerte en K. Sea g un generador de $\mathbb{F}_{t^2}^\times$; entonces ${}^\tau\chi_t(g)\chi_t(g) = \chi_t(\mathscr{N}(g)) = 1$ (pues χ_t es trivial en los elementos de $\mathbb{F}_t^\times$). Luego, ${}^\tau\chi_t = \chi_t^{-1}$. Por otro lado, $\delta_t(\mathscr{N}(g)) = -1$, pues $\mathscr{N}(g)$ es un generador de $\mathbb{F}_t^\times$. Luego, (como $\chi_t(g)$ es una raíz cuarta de la unidad) se cumple que
$${}^\tau\chi_t(g) = \chi_t(g)^{-1} = -\chi_t(g) = \chi_t(g) \cdot \psi_{-t}(\mathscr{N}(g)).$$

Compatibilidad: Como todos los caracteres tienen orden una potencia de 2, la relación de compatibilidad en raíces de orden 3 (si K tiene alguna) es trivial. El único caso en el que K tiene raíces de orden 4 es para $K = \mathbb{Q}(\sqrt{-1})$, en donde todos los conjuntos $Q_{\pm,\pm}$ son vacíos, mientras que t es inerte en K. Por definición:

1. $\chi_2(\sqrt{-1}) = -1$ si $t \equiv 3 \pmod 8$ y 1 si $t \equiv 7 \pmod 8$.

2. χ_t es un caracter de orden 4 (pues t es inerte en $\mathbb{Q}(\sqrt{-1})$) cuya restricción a $\mathbb{F}_t^\times$ es trivial.

Como $t \equiv 3 \pmod 4$, -1 no es un cuadrado en $\mathbb{F}_t$, por lo que $\sqrt{-1}$ es un elemento de $\mathbb{F}_{t^2}^\times$ y entonces $\chi_t(\sqrt{-1}) \in \{\pm 1\}$. Sea g un generador de $\mathbb{F}_{t^2}$, y sea $\sqrt{-1} = g^e$. Recordar que la potencia mínima de g en $\mathbb{F}_t^\times$ es $t+1$. Luego, si $t \equiv 3 \pmod 8$, e tiene valuación uno en 2 y entonces $\chi_t(\sqrt{-1}) = -1$, mientras que si $t \equiv 7 \pmod 8$, $4 \mid e$ y $\chi_t(\sqrt{-1}) = 1$.

Para chequear la condición en -1 (abusando un poco de la notación) tenemos que

$$\chi(-1) = \prod_{\mathfrak{p} \in Q_{+-} \cup Q_{--}} \chi_{\mathfrak{p}}(-1)\chi_2(-1)\chi_t(-1) = (-1)^{\#Q_{+-}+\#Q_{--}}\chi_2(-1)\chi_t(-1).$$

Recordar por la propiedad (P5) que $\chi_2(-1) = \delta_t(2)^{v_2(d)}$. Consideremos los siguientes casos:

- Si t no ramifica en K, el Lema 4.2.1 implica que t se parte en K (respectivamente es inerte en K) si y sólo si $(-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)} = -1$ (respectivamente 1). En el primer caso $\chi_t(-1) = -1$ mientras que en el segundo caso es igual a 1. En ambos casos,

  $$(-1)^{\#Q_{+-}+\#Q_{--}}\chi_2(-1)\chi_t(-1) = 1,$$

  como se espera.

- Si t ramifica en K, por definición $\chi_t = \varepsilon_t$. Su valor en -1 es igual a

  $$\varepsilon_t(-1) = (-1)^{\#Q_{+-}+\#Q_{--}}\delta_t(2)^{v_2(d)}.$$

Extensión: extendemos nuestro caracter χ a los idèles cuya imagen genera el grupo de clases $\mathrm{Cl}(K)$ exactamente igual como en la Sección 3.2.1, a saber, vía (3.7) para ideales de orden impar en el grupo de clases y vía (3.6) para aquellos cuyo orden es una potencia de 2. Luego, esto nos lleva a probar que, si para cada primo q que divide a d (y además para $q = 2$ si $d \equiv 3 \pmod 4$), b_q denota el idèle

$$(b_q)_{\mathfrak{p}} = \begin{cases} 1 & \text{si } \mathfrak{p} \neq \mathfrak{q}, \\ \sqrt{d} & \text{si } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

entonces

$$\chi(b_q^2) = \varepsilon(\mathscr{N}(b_i)). \tag{4.7}$$

Una vez más, calculamos ambos lados de la ecuación para verificar que coinciden. Comencemos suponiendo que $q \neq t$. Entonces, el lado izquierdo es igual a

$$\chi(b_q^2) = \chi_{\mathfrak{q}}\left(\frac{d}{q}\right)\chi_2\left(\frac{1}{q}\right)\chi_t\left(\frac{1}{q}\right)\prod_{\mathfrak{p} \in Q_{\pm\pm}}\chi_{\mathfrak{p}}\left(\frac{1}{q}\right), \tag{4.8}$$

donde el producto es sobre los primos que no dividen a q. Asimismo, el lado derecho es igual a

$$\varepsilon(\mathscr{N}(b_q)) = \varepsilon(-d) = \varepsilon_q(-d/q)\varepsilon_2(q)^{-1}\varepsilon_t(q)\prod_{p \in Q_{\pm\pm}}\varepsilon_p(q)^{-1}, \tag{4.9}$$

donde el producto corre sobre los primos distintos de q. Recordar que para todos los primos ramificados distintos de t, $\chi_{\mathfrak{p}} = \varepsilon_p\delta_p$. En particular, ambos lados se evalúan igual en los elementos de $\mathbb{Z}_p^\times$.

Usando tal relación en (4.8) para todos los primos impares que ramifican, distintos de t, tenemos que

$$\chi(b_q^2) = \chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_{\pm\pm}\\ p\neq q}}\varepsilon_p(q)^{-1}\cdot\delta_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_{\pm\pm}\\ p\neq q}}\delta_p(q) =$$
$$= \varepsilon_q(-d)\left(\chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_q(-1)\varepsilon_2(q)\varepsilon_t(q)^{-1}\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\right)\cdot$$
$$\left(\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\delta_q\left(\frac{d}{q}\right)\prod_{\substack{p\in Q_{\pm\pm}\\ p\neq q}}\delta_p(q)\right). \quad (4.10)$$

Nuestro objetivo es probar que el producto de todos los factores excepto el primero es igual a 1. Por reciprocidad cuadrática, si p, q son primos impares, entonces

$$\delta_p(q)\delta_q(p) = \begin{cases} 1 & \text{si } p \in Q_{+\pm},\\ \delta_{-1}(q) & \text{si } p \in Q_{-\pm}.\end{cases}$$

Luego, el último término de (4.10) es igual a $\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}}$. Con respecto al factor del medio, afirmamos que la siguiente igualdad se cumple (notar que no involucra al factor $\varepsilon_q(-1)$):

$$\left(\chi_2(q)^{-1}\chi_t(q)^{-1}\varepsilon_2(q)\varepsilon_t(q)\delta_q(2)^{v_2(d)}\delta_q(t)^{v_t(d)}\right)\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}} = \delta_q(t). \quad (4.11)$$

Como todos los valores anteriores pertenecen a $\{\pm 1\}$, podemos quitar los inversos. Por propiedad (P1), $\chi_t(q)\varepsilon_t(q) = \delta_t(q)^{1+v_t(d)}$, por lo que reciprocidad cuadrática implica que

$$\chi_t(q)\varepsilon_t(q)\delta_q(t)^{v_t(d)} = \delta_q(t)\delta_{-1}(q)^{1+v_t(d)},$$

y la afirmación es equivalente a la igualdad

$$\left(\chi_2(q)\varepsilon_2(q)\delta_q(2)^{v_2(d)}\right)\delta_{-1}(q)^{\#Q_{-+}+\#Q_{--}+1+v_t(d)} = 1.$$

El último término es igual a $\varepsilon_2(q)$ cuando $t \equiv 7 \pmod 8$ y es igual a $\varepsilon_2(q)\delta_{-1}(q)^{v_2(d)}$ cuando $t \equiv 3 \pmod 8$. Pero recordar que χ_2 es trivial en los elementos de $\mathbb{Z}_2^\times$ cuando $2 \nmid d$, y cuando $2 \mid d$, es igual a δ_{-2} si $t \equiv 3 \pmod 8$ y a δ_2 si $t \equiv 7 \pmod 8$, por propiedad (P4). Luego, la afirmación se sigue de observar que $\delta_q(2) = \delta_2(q)$.

Para finalizar la prueba de compatibilidad cuando $q \neq t$, necesitamos verificar que $\delta_q(t)\varepsilon_q(-1) = 1$, igualdad que se sigue de las definiciones (recolectadas en la Tabla 4.2.1).

$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$	$q \pmod 4$	$q \pmod t$	$\varepsilon_q(-1)$	$\delta_q(t)$
1	□	1	1	3	□	-1	-1
1	⍁	-1	-1	3	⍁	1	1

Tabla 4.2.1: Utilizamos □ o ⍁ para decir si q es un cuadrado o no módulo t, respectivamente.

Si $q = t$ (en particular $t \mid d$) los cálculos son similares reemplazando q por t en (4.8) y en (4.9), pero omitiendo el factor con subíndice t. Notar que en este caso la propiedad (P1) dice que $\chi_t\varepsilon_t = 1$. Entonces el análogo de (4.10) se convierte en

$$\chi(b_t^2) = \chi_2(t)\varepsilon_t\left(\frac{d}{t}\right)\prod_{p\in Q_{\pm\pm}}\varepsilon_p(q)^{-1}\cdot\prod_{p\in Q_{\pm\pm}}\delta_p(q) = \varepsilon_t(-d)\left(\chi_2(t)\varepsilon_t(-1)\varepsilon_2(t)\right)\cdot\left(\prod_{p\in Q_{\pm\pm}}\delta_p(t)\right). \quad (4.12)$$

Reciprocidad cuadrática implica que $\delta_p(t)$ es igual a 1 si $p \in Q_{++} \cup Q_{--}$ y es igual a -1 si $p \in Q_{+-} \cup Q_{-+}$. Luego, el último factor es igual a $(-1)^{\#Q_{+-}+\#Q_{-+}} = \varepsilon_t(-1)\varepsilon_2(t)$ (pues $\delta_t(-1) = -1$ y $\delta_{-1}(t) = -1$) y entonces la validez de (4.12) se sigue de que $\chi_2(t) = 1$ (por la propiedad (P5)).

Por último, cuando $d \equiv 3 \pmod 4$, también debemos probar el mismo resultado para el idèle b_2, cuya componente local es igual a $1 + \sqrt{d}$ en el lugar $\mathfrak{p}_2$ y 1 en los demás lugares. Entonces,

$$\varepsilon_2(1-d) = \varepsilon_2\left(\frac{1-d}{2}\right) \cdot \prod_{p \in Q_{\pm\pm}} \varepsilon_p(2)^{-1} \cdot \varepsilon_t(2)^{-1}, \tag{4.13}$$

mientras que

$$\chi(b_i^2) = \chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) \prod_{p \in Q_{\pm\pm}} \varepsilon_p(2)^{-1}\delta_p(2) \cdot \chi_t(2)^{-1}. \tag{4.14}$$

Esto nos conduce a probar que

$$\varepsilon_2\left(\frac{1-d}{2}\right)\varepsilon_t(2)^{-1} = \chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) \prod_{p \in Q_{\pm\pm}} \delta_p(2) \cdot \chi_t(2)^{-1}.$$

Recordar por Propiedad (P1) que $\varepsilon_t(2)\chi_t(2) = \delta_t(2)^{1+v_t(d)}$. Además, la igualdad $\frac{(1+\sqrt{d})^2}{2} = \frac{1+d}{2} + \sqrt{d}$ implica que $\chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) = \chi_2(\sqrt{d}) = \delta_t(2)$ (por definición), por lo que

$$\varepsilon_t(2)\chi_t(2)^{-1}\chi_2\left(\frac{(1+\sqrt{d})^2}{2}\right) = \delta_t(2)^{v_t(d)}.$$

Con respecto a los demás términos:

- Si $d \equiv 7 \pmod 8$ entonces $\varepsilon_2\left(\frac{1-d}{2}\right) = 1$ y $\prod_{p \in Q_{\pm\pm}} \delta_p(2)\delta_t(2)^{v_t(d)} = 1$, por lo que se satisface lo enunciado.
- Si $d \equiv 3 \pmod 8$ entonces $\varepsilon_2\left(\frac{1-d}{2}\right) = -1$ y $\prod_{p \in Q_{\pm\pm}} \delta_p(2)\delta_t(2)^{v_t(d)} = -1$, por lo que se satisface lo enunciado.

Ahora que tenemos un caracter bien definido en todo el grupo de idèle $\mathbb{I}_K$, debemos verificar que la condición

$${}^{\tau}\chi = \chi \cdot (\psi_{-t} \circ \mathscr{N})$$

se satisface para la extensión. Una vez más, es suficiente probarlo en los idèles a_i en $\mathbb{I}_K$ con componente trivial en el infinito y componentes finitas

$$(a_i)_{\mathfrak{p}} = \begin{cases} r_i & \text{si } \mathfrak{p} = \mathfrak{r}_i, \\ 1 & \text{caso contrario,} \end{cases}$$

donde los ideales primos no ramificados $\{\mathfrak{r}_i\}$ generan el grupo de clases, y donde r_i es la norma de $\mathfrak{r}_i$. El mismo cálculo que el realizado en (3.8), (3.9) y (3.10) hace que la ecuación (3.11) se convierta en

$${}^{\tau}\chi(a_i) = \chi(a_i)^{-1}\chi\left(\frac{a_i\tau(a_i)}{r_i}\right) = \chi(a_i)\chi_2(r_i)^{-1}\chi_t(r_i)^{-1}\varepsilon_2(r_i)\varepsilon_t(r_i) \prod_{p \in Q_{\pm\pm}} \delta_p(r_i).$$

El hecho de que r_i se parta en K implica que $\left(\frac{d}{r_i}\right) = 1$, por lo que la reciprocidad cuadrática nos da que

$$1 = \left(\frac{2}{r_i}\right)^{v_2(d)} \left(\frac{t}{r_i}\right)^{v_t(d)} \left(\frac{-1}{r_i}\right)^{\#Q_{-+}+\#Q_{--}+1} \prod_{p \in Q_{\pm\pm}} \delta_p(r_i).$$

Como $\psi_{-t}(\mathscr{N}(a_i)) = \delta_t(r_i)$, debemos verificar que

$$\chi_2(r_i)^{-1}\chi_t(r_i)^{-1}\varepsilon_2(r_i)\varepsilon_t(r_i)\delta_{r_i}(2)^{v_2(d)}\delta_{r_i}(t)^{v_t(d)}\delta_{-1}(r_i)^{\#Q_{-+}+\#Q_{--}+1} = \delta_t(r_i),$$

que se sigue directo de (4.11) . □

El Teorema 3.2.2 y su prueba se aplica mutatis mutandis con el caso $t \equiv 3 \pmod 4$ estudiado en esta sección, por lo que en particular χ es único salvo un caracter de $G_{\mathbb{Q}}$.

Observación 30. El conductor $\mathfrak{f}$ de $\chi_{\mathfrak{p}_2}$ tiene valuación:

$$v(\mathfrak{f}) = \begin{cases} 0 & \text{si } d \equiv 1 \pmod 4, \\ 2 & \text{si } d \equiv 3 \pmod 4 \text{ y } t \equiv 3 \pmod 8, \\ 0 & \text{si } d \equiv 3 \pmod 4 \text{ y } t \equiv 7 \pmod 8, \\ 5 & \text{si } 2 \mid d. \end{cases}$$

4.2.2 Extensión y modularidad

Sea ε el caracter construido en la sección anterior y sea $S(\widetilde{E}_{(a,b,c)})$ el conjunto de ideales primos que no dividen a $6d$ en donde la curva $\widetilde{E}_{(a,b,c)}$ tiene mal reducción. Abusando de la notación, si q es un primo racional, decimos que $q \in S(\widetilde{E}_{(a,b,c)})$ si existe un ideal de $\mathscr{O}_K$ que divide a q y está en el conjunto $S(\widetilde{E}_{(a,b,c)})$.

Antes de postular el enunciado de esta sección, veamos algunas observaciones acerca del conductor de la representación twisteada $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$. Sea $\mathfrak{q}$ un primo impar que ramifica en $K/\mathbb{Q}$ y que no divide a 3. La curva $\widetilde{E}_{(a,b,c)}$ tiene reducción aditiva en $\mathfrak{q}$ y su tipo local (por Observación 27) es el de una serie principal (dada por un caracter cuya inercia tiene orden 3) o el de una representación supercuspidal. Como la parte de la inercia de $\chi_{\mathfrak{q}}$ tiene orden una potencia de 2, no puede cancelar la contribución de la inercia de $\rho_{\widetilde{E}_{(a,b,c)},p}$. Luego, el conductor de la representación twisteada en $\mathfrak{q}$ continúa teniendo valuación 2.

En los primos que dividen a 2, la valuación del conductor $N(\widetilde{E}_{(a,b,c)})$ nunca coincide con el cuadrado del conductor de $\chi_{\mathfrak{p}_2}$ (ver Lema 4.1.5 y Observación 30), por lo que la representación twisteada tiene conductor el mínimo común múltiplo de ambos números. En los primos que dividen a 3 ocurre una situación en la que la representación twisteada tiene conductor menor que el de la curva elíptica. Esto ocurre precisamente cuando 3 es inerte en $K/\mathbb{Q}$ y $\widetilde{E}_{(a,b,c)}$ tiene valuación 2 en el conductor. En tal caso, el tipo local de la representación de Weil-Deligne es el de una serie principal cuya inercia está dada por un caracter de orden 4 (por Observación 28). Luego, twistear por χ_3 (otro caracter de orden 4 cuando es restringido al subgrupo de inercia) cancela uno de los caracteres y la representación tiene valuación 1.

Teorema 4.2.4. *Supongamos que $K/\mathbb{Q}$ es cuadrático imaginario. Entonces la representación twisteada $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$ se extiende a una representación de dimensión dos de $G_{\mathbb{Q}}$, asociada a una forma nueva $f_{(a,b,c)}$ de peso 2, Nebentypus ε y nivel $N(a,b,c)$ dado por*

$$N(a,b,c) = 2^{\alpha} \cdot 3^{\beta} \cdot \prod_{q \in S(\widetilde{E}_{(a,b,c)})} q \cdot \prod_{q \in Q_{\pm\pm}} q^2.$$

El valor de α es uno de los siguientes:

$$\alpha = \begin{cases} 2 & \text{si } 2 \text{ es inerte}, \\ 1, 2 & \text{si } 2 \text{ se parte}, \\ 4 & \text{si } 2 \text{ ramifica pero } 2 \nmid d, \\ 8 & \text{si } 2 \mid d. \end{cases}$$

y el valor de β es uno de los siguientes:

$$\beta = \begin{cases} 2, 3 & \text{si } 3 \text{ se parte}, \\ 1, 3 & \text{si } 3 \text{ es inerte}, \\ 5 & \text{si } 3 \text{ ramifica}. \end{cases}$$

Más aún, el cuerpo de coeficientes de $f_{(a,b,c)}$ es una extensión a lo sumo cuadrática de $\mathbb{Q}(\chi)$.

Demostración. La existencia de la extensión y la descripción de su Nebentypus se prueba exactamente igual que en el Teorema 3.2.9. La afirmación sobre el conductor es clara para los primos que no dividen a 6 y que no ramifican, pues la curva tiene reducción semiestable (por Lema 4.1.2) y χ no ramifica en tales primos.

Si $\mathfrak{q} \mid q$ es un ideal primo impar que no divide a 3, Lema 4.1.7 implica que $v_{\mathfrak{q}}(\rho_{\widetilde{E}_{(a,b,c)},p}) = 2$. Lo mismo vale para $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$ (como se mencionó anteriormente). Luego, la fórmula del conductor de la representación inducida (3.21) implica que la representación de dimensión 4 tiene valuación 4 en el conductor para tales primos, por lo que la representación extendida tiene valuación 2 en el conductor.

En el primo 2 el caracter χ_2 no ramifica cuando 2 no ramifica en $K/\mathbb{Q}$. Luego, el twist de la representación (y su extensión) tienen el mismo conductor que $\widetilde{E}_{(a,b,c)}$. Si $d \equiv 3 \pmod 4$ entonces χ_2 tiene conductor 2, por lo que la representación twisteada tiene valuación 4 en el conductor y su valuación en el conductor de la inducida es 8. Entonces $\tilde{\rho}_p$ tiene valuación 4 en el conductor, para el primo 2. Cuando $2 \mid d$, χ_2 tiene conductor 5. Luego, la representación twisteada tiene valuación 10, la inducida tiene valuación 16 y $\tilde{\rho}_p$ tiene valuación 8 en el conductor.

Finalmente, debemos analizar el exponente para el primo 3. Si 3 es un primo que ramifica en $K/\mathbb{Q}$, $v_{\mathfrak{p}_3}(N(\widetilde{E}_{(a,b,c)})) = 8$ (por Lema 4.1.6) y el caracter tiene valuación como mucho 1 en el conductor, por lo que la representación inducida tiene valuación 10 y $\tilde{\rho}_p$ tiene valuación 5. Si 3 se parte, la representación twisteada tiene exponente 2 o 3 en el conductor (luego $\tilde{\rho}_p$ también), mientras que en el caso inerte, como fue explicado anteriormente, la representación twisteada tiene valuación 1 o 3 en el conductor. □

4.3 Paso 3: Bajada de nivel

Denotemos por $\tilde{\rho}_p$ la extensión de $\rho_{\widetilde{E}_{(a,b,c)},p} \otimes \chi$.

Corolario 4.3.1. *Supongamos que $p \nmid 6d$ y supongamos que la representación de Galois residual $\overline{\tilde{\rho}_p}$ es absolutamente irreducible. Entonces existe una forma $f \in S_2(\Gamma_0(N), \varepsilon)$, donde*

$$N = 2^{\alpha} \cdot 3^{\beta} \cdot \prod_{q \in Q_{\pm\pm}} q^2,$$

para α y β como en el Teorema 4.2.4 tal que $\rho_{\widetilde{E}_{(a,b,c)},p} \equiv \rho_{f,K,p} \otimes \chi^{-1} \pmod{\mathfrak{p}}$, donde $\rho_{f,K,p}$ es la restricción de $\rho_{f,p}$ al grupo de Galois G_K, χ es como en el Teorema 4.2.3 y $\mathfrak{p}$ es un ideal primo de $\overline{\mathbb{Q}}$ que divide a p.

Demostración. La prueba es similar a la del Corolario 3.3.1. □

Podemos dar una fórmula precisa para el nivel de las formas correspondientes a las soluciones triviales $(\pm 1, 0, 1)$.

Proposición 4.3.2. *La extensión de las presentaciones asociadas a las soluciones* $(\pm 1, 0, 1)$ *se corresponden con formas* $f_\pm$ *con multiplicación compleja en el espacio* $S_2(\Gamma_0(N), \varepsilon)$*, donde* $N = 2^\alpha \cdot 3^\beta \cdot \prod_{q \in Q_{\pm\pm}} q^2$*, con*

$$\alpha = \begin{cases} 2 & \text{si } d \equiv 1 \pmod 4, \\ 4 & \text{si } d \equiv 3 \pmod 4, \\ 8 & \text{si } 2 \mid d. \end{cases}$$

y con

$$\beta = \begin{cases} 3 & \text{si } 3 \nmid d, \\ 5 & \text{si } 3 \mid d. \end{cases}$$

Demostración. La prueba es como en el Teorema 4.2.4 con la fórmula precisa para el exponente del conductor de $\tilde{E}_{(\pm 1,0,1)}$ dada en la Observación 29. □

Nuevamente, notemos que para poder aplicar el Corolario 4.3.1 precisamos que la reducción módulo p de $\tilde{\rho_p}$ sea absolutamente irreducible. Recordemos que esto no es un problema si c tiene un primo $q > 3$ que lo divida (ver Lema 4.1.2 y Proposición 2.3.1). Como fue mencionado durante la estrategia general, veremos a continuación que este va a ser siempre el caso para p suficientemente grande.

4.3.1 Otra curva de Frey

El objetivo de esta sección es probar que si (a, b, c) es una solución primitiva de (2), entonces c no está soportado en $\{2, 3\}$ si p es suficientemente grande. Para ello, la idea es explotar el hecho de que a la supuesta solución (a, b, c) podemos asociarle otra curva elíptica racional.

La técnica de multi Frey (desarrollada por Siksek en [10, 12]) tiene como idea adjuntar no una, sino muchas curvas a una hipotética solución. De este modo, aún si $B(q, f; a, b, c)$ se anula para una de las curvas (ver Sección 2.4.1), puede que no se anule para otra curva. Es decir que aún si el truco de Mazur falla cuando vemos las curvas de manera independiente, podría funcionar al analizarlas en simultáneo. Esto es precisamente lo que ocurre con la ecuación (2) para $d = 1$ (ver Sección 5 de [3]). Desafortunadamente, utilizando la misma técnica para otros valores de d, no conseguimos descartar ninguna otra solución que haya sorteado el truco de Mazur para nuestra $\mathbb{Q}$-curva original. Sin embargo, la existencia otra curva resultará beneficioso para notar que c no está soportado en $\{2, 3\}$. Más concretamente, a una supuesta solución (a, b, c) de (2), adjuntamos la curva elíptica racional

$$F_{(a,b,c)} \quad : \quad y^2 = x^3 - 3db^2x - 2da. \tag{4.15}$$

Su discriminante es $\Delta(F_{(a,b,c)}) = -1728 \cdot d^2 \cdot c^p$ y su j-invariante es $j(F_{(a,b,c)}) = \frac{-1728 \cdot d \cdot b^6}{c^p}$. Como (a, b, c) es primitiva, $\text{mcd}(d, c) = 1$, luego tiene reducción multiplicativa en los primos que dividen a c y reducción aditiva en todos los primos $\ell > 3$ que dividen a d si $\ell^6 \nmid d$.

Consideremos el caso particular de la ecuación (2), donde c está soportado en $\{2, 3\}$, i.e. la ecuación

$$C_p : x^2 - dy^6 = (2^\alpha 3^\beta)^p. \tag{4.16}$$

A una supuesta solución (a, b, c) (donde $c = 2^\alpha 3^\beta$) le adjuntamos la curva como en (4.15), con discriminante $-2^{\alpha p - 6} 3^{\beta p + 3} d^2$ y c-invariantes como se sigue:

$$c_4 = 2^4 3^2 dy^2, \quad c_6 = 2^6 3^3 dx. \tag{4.17}$$

Agradecemos a Mike Bennett por la siguiente descripción local de la curva $F_{(a,b,c)}$.

Proposición 4.3.3. *El modelo es minimal en todos los primos $\ell \geq 3$. Más aún, supongamos que d es libre de potencias sextas. Entonces si $N(F_{(a,b,c)})$ es el conductor de $F_{(a,b,c)}$, tenemos que:*

- *La curva tiene reducción aditiva en cada primo $\ell \mid d$, $\ell > 3$.*
- *Si $3 \nmid d$, el modelo es minimal en 3 y $v_3(N(F_{(a,b,c)})) \in \{2, 3\}$, con el último caso posible sólo si $b = 0$ o $(\beta, p) = (1, 2)$.*
- *Si $v_3(d) \in \{1, 2, 4, 5\}$, entonces $F_{(a,b,c)}$ es minimal en 3 y $v_3(N_F) = 5$.*
- *Si $v_3(d) = 3$, E es minimal en 3 y $v_3(N(F_{(a,b,c)})) \in \{2, 3\}$.*
- *Si $2 \nmid d$, y nuestro modelo es minimal en $\ell = 2$ y tenemos que $v_2(F_{(a,b,c)}) \in \{2, 3, 4, 5, 6\}$. Si no es minimal (por lo que necesariamente $\alpha p \geq 6$) un modelo minimal tiene c-invariantes $c_4 = -3^2db^2$, $c_6 = -3^3da$, discriminante minimal $\Delta(F_{(a,b,c)}) = -2^{\alpha p-6}3^{\beta p+3}d^2$ y $v_2(N(F_{(a,b,c)})) \in \{0, 1\}$.*
- *Si $2 \mid d$, $F_{(a,b,c)}$ es minimal en 2 si $8 \nmid d$. Más aún,*
  1. *Si $v_2(d) = 1$, $v_2(N(F_{(a,b,c)})) \in \{2, 3, 4, 7\}$.*
  2. *Si $v_2(d) = 2$, $v_2(N(F_{(a,b,c)})) = 6$.*
- *Si $\nu_2(d) = 3$, entonces o bien $F_{(a,b,c)}$ es minimal en 2 y $v_2(N(F_{(a,b,c)})) \in \{4, 5\}$, o $F_{(a,b,c)}$ no es minimal en 2, $2 \mid b$, y un modelo minimal cumple que $2 \nmid N(F_{(a,b,c)})$.*
- *Si $v_2(d) = 4$, entonces $F_{(a,b,c)}$ es minimal en 2 y $v_2(N(F_{(a,b,c)})) = 6$.*
- *Si $v_2(d) = 5$, entonces $F_{(a,b,c)}$ no es minimal en 2 y un modelo minimal cumple que $v_2(N(F_{(a,b,c)})) \in \{2, 3, 4\}$.*

Demostración. Se sigue de un cálculo sencillo usando [66]. □

Para un valor específico de d, podemos buscar las tablas de curvas elípticas de Cremona (ver [23]) disponibles en la página LMFDB [58] y por su discriminante, obtenemos una lista finita de posibilidades para α y β.

Proposición 4.3.4. *Sea $-19 \leq d \leq -2$ un entero libre de cuadrados. Entonces para cada valor de d, el valor de p en (4.16) está acotado por los valores de la Tabla 4.3.1.*

d	Cota	d	Cota	d	Cota	d	Cota
-2	3	-3	2	-5	2	-6	–
-7	7	-10	–	-11	3	-13	–
-14	–	-15	3	-17	2	-19	–

Tabla 4.3.1: Cotas para p en (4.16). El símbolo "–" significa que c no puede estar soportado en $\{2, 3\}$.

Demostración. Veamos cómo funciona el algoritmo con un ejemplo: sea $d = -2$. Entonces la Proposición 4.3.3 nos dice que $N(F_{(a,b,c)}) = 2^r3^s$ con $r \in \{2, 3, 4, 7\}$ y $s \in \{2, 3\}$. Ahora buscamos todas las curvas elípticas con conductor 2^r3^s que satisfacen que los invariantes (c_4, c_6, Δ) de un modelo minimal son compatibles con los de nuestra curva de Frey, por ejemplo, un requisito mínimo es que sean negativos (ver ecuación (4.17)) y que $288 \mid c_4$ y $3456 \mid c_6$. Hay una única curva que

satisface dichas condiciones requeridas en (4.17). Esto nos permite recuperar el valor de (a, b), a saber $(a, b) = (5, 1)$. Entonces, factorizando $a^2 + 2b^6$ obtenemos que p debe ser 3. Así es como se obtiene la misma respuesta con el código `Table.mg` escrito en `Magma`.

```
> ConductorCurve(2);
Elliptic Curve defined by y^2 = x^3 + 6*x + 20 over Rational Field
of conductor 1152 . In this case [a,b]= [ 5, 1 ]
and p is a divisor of 3
{}
```

Una cuenta similar fue hecha para cada valor de d, dando una lista finita de posibilidades para el valor de p presentado en la tabla. Queremos remarcar que el método anterior falla para el caso $d = -19$, puesto que involucra curvas elípticas de conductor 623808. Sin embargo, en este caso particular, no hay necesidad de realizar tal cálculo. La razón es que como 2 es inerte en $K/\mathbb{Q}$, $2 \nmid c$, y lo mismo ocurre con 3, por Lema 2.1.1.

Hay dos posibilidades de tratar de aplicar el mismo método utilizado en los demás casos para el caso $d = -19$ con el mismo método: una es calcular tal espacio de curvas elípticas usando el algoritmo de Cremona (esto fue hecho para nosotros por el profesor John Cremona), mientras que la otra es usar las tablas de curvas elípticas con mala reducción en un conjunto pequeño de primos, descripta en [85] (cuya base de datos está disponible en https://bmatschke.github.io/solving-classical-diophantine-equations/). □

Observación 31. El Lema 2.1.1 de hecho prueba que no hay soluciones no triviales de 4.16 si $d \not\equiv 1 \pmod 8$ y $d \not\equiv 1 \pmod 3$.

A continuación resumimos el principal resultado de esta sección con el siguiente corolario.

Corolario 4.3.5. *Sea $-20 \leq d \leq -2$ libre de cuadrados. Entonces la curva elíptica $\widetilde{E}_{(a,b,c)}$ asociada a una hipotética solución (a, b, c) tiene un primo de reducción multiplicativa que no divide a 6 si p es más grande que las cotas dadas en Tabla 4.3.1.*

4.4 Paso 4: Resolviendo la ecuación $x^2 - dy^6 = z^p$

Finalmente, en esta sección estudiaremos las soluciones primitivas de la ecuación (2) para $-20 \leq d \leq -1$ libre de cuadrados. Cabe destacar que mediante un procedimiento similar a lo hecho en el Capítulo 3, también se podrían analizar casos en donde d sea positivo.

Observación 32. La razón en este caso por la que nos restringimos a valores de d libres de cuadrados es la siguiente: si d no es libre de cuadrados, digamos $d = d_1 \cdot d_2^2$, entonces a una hipotética solución uno puede adjuntarle la misma curva elíptica (4), que está definida sobre el cuerpo cuadrático $\mathbb{Q}(\sqrt{-d_1})$. El caracter χ definido en la Sección 4.2.1 depende sólo de d_1 (como así también el Nebentypus de $\tilde{\rho}_p$). Sin embargo, la fórmula precisa para el nivel N de la forma modular f obtenida luego de bajar el nivel sí depende de d_2. En el apéndice de [46] damos una fórmula para N para un valor cualquiera d, y mostramos cómo se aplica en un ejemplo particular ($d = -4$).

d	Condición en p	Referencia	d	Condición en p	Referencia
-1	$p > 2$	[3, Teo. 1]	-7	$p > 283, p \equiv 5, 7 \pmod{12}$	Teo. 4.4.4
-2	$p > 257$	Teo. 4.4.1	-11	$p > 409, p \equiv 3 \pmod 4$	Teo. 4.4.5
-3	$p > 2$	[51, Teo. 1]	-13	$p > 1627$	Teo. 4.4.6
-5	$p > 547, p \equiv 2 \pmod 3$	Teo. 4.4.2	-15	$p > 457, p \equiv \pm 5, \pm 7, 15 \pmod{24}$	Teo. 4.4.7
-6	$p > 563$	Teo. 4.4.3	-19	$p > 683$	Teo. 4.4.8

Tabla 4.4.1: Resumen de los resultados principales para la ecuación (2).

La ecuación $x^2 + 2y^6 = z^p$

Este caso es muy interesante, ya que trabajando con formas modulares de Bianchi es suficiente para obtener un resultado.

Teorema 4.4.1. *Sea $p > 257$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^2 + 2y^6 = z^p.$$

Demostración. Siguiendo la notación de la Sección 4.2.1, los conjuntos $Q_{\pm,\pm}$ son todos vacíos; ε es el caracter trivial (i.e. la forma f no tiene Nebentypus) mientras que el caracter χ corresponde al caracter cuadrático δ_3 en uno de los primos que dividen a 3 en $\mathbb{Q}(\sqrt{-2})$. Este es un ejemplo muy interesante, ya que la curva $\widetilde{E}_{(a,b,c)}$ tiene siempre buena reducción en 2 y la parte del conductor que involucra al 3 es $3(1+\sqrt{-2})$, $3(1-\sqrt{-2})$, 9 ó 27. En particular, es más eficiente trabajar con formas de Bianchi que con las racionales (para evitar potencias de 2 en el nivel). La forma f satisface que su cambio de base a K y su twist por χ^{-1} (que es igual a χ, ya que es cuadrático) tiene sólo mala reducción en los primos que dividen a 3. Computando los respectivos espacios (usando el algoritmo de Cremona, disponible en LMFDB) resulta que no hay formas de Bianchi en ningún nivel, salvo en el de 3^3.

Sea (a, b, c) una solución primitiva no trivial. Si c está soportado en $\{3\}$, entonces la prueba del Lema 4.1.6 implica que nuestra curva tiene exponente 2 en uno de los primos que divide 3 y 1 en el otro. Sin embargo, el espacio de formas modulares de Bianchi de tal nivel es el trivial, con lo cual c no puede estar soportado en $\{3\}$ y entonces c debe ser divisible por un primo mayor que 3, con lo cual estamos en las hipótesis de la Proposición 2.3.1.

El espacio de formas modulares de Bianchi de peso 2 y nivel 3^3 contiene tres formas nuevas correspondientes a las curvas elípticas 2.0.8.1-729.4-a1, 2.0.8.1-729.4-b1 y 2.0.8.1-729.4-c1. La segunda curva tiene multiplicación compleja y cambio de base de una curva elíptica racional (se corresponde con la solución trivial, y no puede ser congruente a $\widetilde{E}_{(a,b,c)}$ si $p > 257$ por Teorema 2.4.8). Las otras dos (conjugadas complejas entre ellas) satisfacen que $a_5 = -1$. Es fácil calcular para cada posible valor de (a, b) módulo 5 el valor de $a_5(\widetilde{E}_{(a,b,c)})$ y verificar que pertenece al conjunto $\{2, -7, -10\}$. Por lo tanto, ambas curvas elípticas no pueden ser congruentes a la curva de Frey construida a partir de una solución primitiva no trivial si $p > 3$. □

La ecuación $x^2 + 3y^6 = z^p$

Este caso fue considerado en [51] (ver Teorema 4.0.3).

La ecuación $x^2 + 5y^6 = z^p$

Sea $K = \mathbb{Q}(\sqrt{-5})$ y sea $\mathfrak{p}_2 = \langle 2, 1+\sqrt{-5}\rangle$ tal que $\langle 2\rangle = \mathfrak{p}_2^2$. Sea $\mathfrak{p}_3 = \langle 3, 1+\sqrt{-5}\rangle$ tal que $\langle 3\rangle = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ y $\mathfrak{p}_5 = \langle\sqrt{-5}\rangle$.

Siguiendo los resultados de la Sección 4, tenemos que la curva $\widetilde{E}_{(a,b,c)}$ no es un twist cuadrático de una curva con buena reducción en los primos que dividen a $2, 3, 5$. Además, siguiendo la notación de la Sección 4.2.1 tenemos que $Q_{+-} = \{5\}$ mientras que los otros conjuntos son vacíos. El Nebentypus ε es de orden 4 y conductor 20. Recordar que $\mathbb{Q}(\sqrt{-5})$ tiene número de clases 2, por lo que el caracter de Hecke está unívocamente determinado por el valor en sus componentes locales restringidas a las unidades enteras y por su definición en los representantes del grupo de clases.

Observación 33. Hay dos posibles elecciones del caracter χ necesario para twistear la representación $\rho_{\widetilde{E}_{(a,b,c)},p}$, y así extenderla a $G_{\mathbb{Q}}$. Esto proviene del hecho de que $\#\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = 2$. Ambas

elecciones difieren del twist cuadrático por el caracter asociado al grupo de clases (correspondiente a la extensión $K(\sqrt{-1})/K$).

Por Corolario 4.3.1, una solución primitiva no trivial es congruente a una forma nueva en $S_2(\Gamma_0(2^4 \cdot 3^2 \cdot 5^2), \varepsilon)$ o en $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 5^2), \varepsilon)$. Más aún, cualquier solución (a, b, c) que satisface que $3 \nmid ab$ da una forma en el primer espacio (ver la prueba del Lema 4.1.6).

• El espacio $S_2(\Gamma_0(2^4 \cdot 3^2 \cdot 5^2), \varepsilon)$ tiene 15 clases de conjugación de Galois, 7 de las cuales tienen multiplicación compleja (que no pueden corresponder a soluciones no triviales si $p > 547$, por Teorema 2.4.8). El truco de Mazur prueba que las demás formas no pueden corresponder a soluciones si $p > 5$, excepto por cuatro formas, correspondientes a las formas $8, 11, 12$ y 13 en el orden de `Magma` (su cuerpo de coeficientes es una extensión de $\mathbb{Q}$ de grado 8 que contiene a las raíces cuartas de la unidad).

Por la construcción de Eichler-Shimura sabemos que a cada autoforma f le podemos asociar una variedad abeliana A_f definida sobre $\mathbb{Q}$ cuya dimensión es igual al grado del cuerpo de coeficientes (i.e. $\dim(A_f) = [\mathbb{Q}(\{a_n(f)\}) : \mathbb{Q}]$). Más aún, sus endomorfismos racionales cumplen $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \simeq \mathbb{Q}(a_n(f))$. En particular, la variedad A_f no se descompone sobre $\mathbb{Q}$. Sin embargo, sobre $\mathbb{C}$ (o $\overline{\mathbb{Q}}$) en general la variedad A_f es isógena a un producto de variedades abelianas simples, $A_f \sim B_1 \times \cdots \times B_r$. Cada variedad B_i se llama un *building block* de A_f. En el caso particular de las variedades abelianas provenientes de formas nuevas, todos los building blocks son isógenos entre sí, con lo cual $A_f \sim B^r$ (ver [69]).

La dimensión de un building block B puede ser mayor a 1 (ver [69]). Un primer posible chequeo (cuando es posible) es correr el algoritmo de Quer (implementado en `Magma` [7]) para asegurarse de que el building block tenga dimensión uno, y por lo tanto exista una curva elíptica asociada a nuestra variedad abeliana de dimensión 8. Además, el algoritmo de Quer da el cuerpo de definición del building block. Las cuatro formas tienen twist internos, y tienen un building block de dimensión uno (esto puede ser verificado con las rutinas `BrauerClass` y `DegreeMap` en `Magma`) definido sobre el cuerpo cuadrático $\mathbb{Q}(\sqrt{-5})$. Luego, podemos intentar encontrar tales curvas.

Antes de dar las ecuaciones de dichas curvas adjuntadas a nuestras formas modulares, veamos algunas observaciones:

- Las formas f_8, f_{12} y f_{13} son twist cuadráticos de formas cuyo nivel tiene 3 a la primera potencia (en particular, el tipo local de sus representaciones es Steinberg, como vimos en la Sección 2.4.2, donde el caracter χ es ramificado).

- La forma f_{11} es un twist cuadrático de una forma con buena reducción en 3, por lo que en particular el tipo local de su representación en 3 es el de una serie principal cuyo caracter tiene orden dos cuando es restringido al subgrupo de inercia.

Por la prueba del Lema 4.1.6, la curva $\widetilde{E}_{(a,b,c)}$ tiene en $\mathfrak{p}_3$ o bien reducción potencialmente multiplicativa u obtiene buena reducción sobre una extensión cuyo grado de ramificación es al menos 4 (pues el discriminante tiene valuación 3). Entonces la Proposición 2.4.2 implica que la forma f_{11} no puede corresponder a una solución si $p \geq 5$. Aún así, por completitud del algoritmo, buscaremos una ecuación para dicha forma también.

Buscamos curvas elípticas sobre $\mathbb{Q}(\sqrt{-5})$ con buena reducción fuera de $\{\mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3, \mathfrak{p}_5\}$ utilizando la implementación de `Magma`:

```
P<x> := PolynomialRing(Rationals()); K<a>:=NumberField(x^2+5);
O:=RingOfIntegers(K); I:=ideal<O|30>;
S:=EllipticCurveWithGoodReductionSearch(I,700);
```

Esto da un total de 89184 curvas elípticas. Utilizando unos pocos valores de a_p de las formas nuevas (usando (2.4) y twisteando por χ^{-1}) podemos descartar todas las curvas excepto las relacionadas con

nuestras formas. Notar que como $\mathbb{Q}(\sqrt{-5})$ no tiene número de clases uno, no hay un modelo minimal. Por Observación 33 hay (al menos) dos curvas elípticas adjuntadas a las formas modulares f_i (que son twist cuadráticos entre sí, por $K(\sqrt{-1})/K$), y sus complejos conjugados (que son isógenos por su twist por $\sqrt{-3}$). Luego sólo daremos una ecuación por cada una de estas cuatro curvas. Más aún, utilizamos la rutina `global_minimal_model(semi_global=True)` en `Sage` para obtener un modelo minimal de la curva en todos los primos menos en uno. Todos los cálculos y sus resultados se pueden ver en la carpeta `Minimal_model` (ver [83]).

Las curvas son las siguientes:

$$E_8 : y^2 + y = x^3 + (\sqrt{-5} - 1)x^2 + (\sqrt{-5} - 43)x - 21\sqrt{-5} + 113. \tag{4.18}$$

Notar que esta es la curva correspondiente a la solución no primitiva $2^2 + 5 \cdot 2^6 = 18^2$.

$$E_{11} : y^2 + (1 + \sqrt{-5})xy + (1 + \sqrt{-5})y = x^3 - \sqrt{-5}x^2 + (-4\sqrt{-5} + 29)x - 25\sqrt{-5} - 32. \tag{4.19}$$

El conjunto de curvas correspondientes a la forma f_{12} es más interesante, pues las curvas tiene una isogenía extra de grado 2 definida sobre K, por lo que tenemos ocho curvas diferentes (donde el gráfico de isogenías de cada curva tiene cuatro elementos).

$$E_{12} : y^2 + (1 + \sqrt{-5})xy = x^3 - x^2 + (-6\sqrt{-5} - 12)x - 10\sqrt{-5} + 2, \tag{4.20}$$

y su curva 2-isógena

$$y^2 + (\sqrt{-5} + 1)xy = x^3 - x^2 - (\sqrt{-5} + 2)x + 4.$$

Por último, la forma f_{13} está relacionada con la curva

$$E_{13} : y^2 = x^3 + (-\sqrt{-5} + 1)x^2 + (-1054\sqrt{-5} - 668)x - 16514\sqrt{-5} + 14618. \tag{4.21}$$

Una vez más, esta curva es la asociada a la solución primitiva $79^2 + 5 \cdot 2^6 = 3^8$.

Observación 34. ¿Cómo podemos verificar que la curva dada realmente corresponde a nuestra forma modular? Tomemos a la curva E_8 como ejemplo. La curva tiene una isogenía de grado tres, dada por la ecuación

$$y^2 + y = x^3 + (-15\sqrt{-5} - 375)x - 175\sqrt{-5} - 2744,$$

y es fácil de verificar (utilizando `Sage` por ejemplo) que su twist cuadrático por -3 es isomorfo al conjugado de E_8. El conductor de E_8 es igual a $\langle 3, \sqrt{-5} + 1\rangle \cdot \langle 3, \sqrt{-5} + 2\rangle^2 \cdot \langle \sqrt{-5}\rangle^2$. El caracter χ puede ser tomado para tener conductor $\langle 2\rangle \cdot \langle 3, \sqrt{-5} + 1\rangle \cdot \langle \sqrt{-5}\rangle$, y entonces la representación se extiende a una representación de $G_{\mathbb{Q}}$ con conductor $2^4 \cdot 3^2 \cdot 5^2$ (ver la prueba del Teorema 4.2.4). Por [71, Teorema 4.4] y las conjeturas de Serre, se corresponde a una forma nueva en el espacio $S_2(\Gamma_0(2^4 \cdot 3^2 \cdot 5^2), \varepsilon)$. Calcular uno pocos unos autovalores es suficiente para ver que f_8 es la única forma nueva cuyo q-ésimo coeficiente de Fourier sobre $\mathbb{Q}(\sqrt{-5})$ twisteado por χ^{-1} coincide con $a_q(E_8)$. Un cálculo similar fue llevado a cabo para las demás curvas.

A continuación, algunas observaciones triviales:

- la curva E_8 tiene buena reducción en $\mathfrak{p}_2$, por lo que su tipo local es el de una serie principal.
- La curva E_{11} tiene buena reducción en un primo que divide a 3.
- La curva E_{12} tiene buena reducción en $\mathfrak{p}_5$.

Por Lema 4.1.5, la curva $\widetilde{E}_{(a,b,c)}$ tiene reducción aditiva en el primo $\mathfrak{p}_2$, tipo Steinberg en los primos que dividen a 3 y tipo supercuspidal en el primo $\mathfrak{p}_5$, por Observación 27. La Proposición 2.4.2 implica que una solución primitiva no trivial no puede estar relacionada con ninguna de estas curva si $p \geq 5$.

Esto nos conduce a descartar la curva E_{13}. Un cálculo sencillo (usando `Sage`) muestra que la curva E_{13} no tiene un punto de 3-torsión (ni tampoco ninguna curva 3-isógena), por lo que podemos aplicar la estrategia descripta en el Teorema 2.4.5. Más concretamente, $a_{\mathfrak{p}_{43}}(E_{13}) = 1$ para ambos primos en $\mathbb{Q}(\sqrt{-5})$ que dividen a 43. En particular, $a_{\mathfrak{p}_{43}}(E_{13}) \not\equiv 43 + 1 \pmod 3$, por lo que E_{13} no puede provenir de una solución si $p > \max\{43 + 2\sqrt{43}, 4\sqrt{43}\}$. En particular, no hay soluciones primitivas no triviales si $3 \nmid ab$ y $p \geq 59$.

• El espacio $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 5^2), \varepsilon)$ tiene 24 clases de conjugación de Galois, 6 de ellas con multiplicación compleja (por lo que podemos descartarlas si $p > 547$). Para las restantes, el truco de Mazur las descarta si $p > 7$, excepto cuatro formas, correspondientes a los lugares $7, 8, 9$ y 10 en el orden de `Magma`. Es importante remarcar que twistear por $\sqrt{-3}$ preserva el espacio, por lo que en realidad podemos agrupar las formas en pares. El twist de la séptima forma es la novena, mientras que el twist de la octava es la décima. Procediendo como antes, calculamos las ecuaciones para sus building blocks y obtenemos

$$E_7 : y^2 = x^3 + (24\sqrt{-5} + 60)x + (-56\sqrt{-5} + 256), \tag{4.22}$$

y

$$E_8 : y^2 + (\sqrt{-5}+1)xy + (\sqrt{-5}+1)y = x^3 + (\sqrt{-5}+1)x^2 + (-46\sqrt{-5}-58)x + (-248\sqrt{-5}+126). \tag{4.23}$$

Notar que la primera curva tiene buena reducción en el primo $\mathfrak{p}_5$, por lo que no puede provenir de una solución primitiva (ya que su tipo local en $\mathfrak{p}_5$ de $\widetilde{E}_{(a,b,c)}$ es supercuspidal). Es fácil ver que la segunda curva proviene de la solución $2^2 + 5 \cdot 1^6 = 3^2$. Es 3-isógena a la curva elíptica

$$E_8' : y^2 + (\sqrt{-5}+1)xy + (\sqrt{-5}+1)y = x^3 + (\sqrt{-5}+1)x^2 + (-346\sqrt{-5}+692)x + (-1448\sqrt{-5}-11724),$$

que tiene un punto de 3-torsión, por lo que el Teorema 2.4.5 no aplica en este caso. Como $v_{\mathfrak{p}_5}(\Delta(E_8')) = 8 = v_{\mathfrak{p}_5}(\Delta(\widetilde{E}_{(a,b,c)}))$, el Teorema 2.4.4 implica que $E_8'[p]$ y $\widetilde{E}_{(a,b,c)}[p]$ son simplécticamente isomorfos y no son anti simplécticamente isomorfos. Más aún, aplicando [41, Teorema 11] obtenemos que ambos módulos son anti simplécticamente isomorfos si $\left(\frac{3}{p}\right) = -1$, pues

$$(v_{\mathfrak{p}_3}(c_4(E_8')), v_{\mathfrak{p}_3}(c_6(E_8')), v_{\mathfrak{p}_3}(\Delta(E_8'))) = (2, 3, 5),$$

y $v_{\mathfrak{p}_3}(\Delta(\widetilde{E}_{(a,b,c)})) = 3$. A partir de esto, obtenemos el siguiente resultado.

Teorema 4.4.2. *La ecuación $x^2 + 5y^5 = z^p$ no tiene soluciones primitivas no triviales (a, b, c) si $p > 547$ y alguna de las siguientes dos condiciones se cumplen:*

- $3 \nmid ab$.
- $p \equiv 2 \pmod 3$.

La ecuación $x^2 + 6y^6 = z^p$

Todos los conjuntos $Q_{\pm,\pm}$ son vacíos, el caracter ε es el caracter cuadrático de conductor 12, mientras que χ es un caracter cuadrático de conductor $3 \cdot \langle 2, \sqrt{-6}\rangle^5$. En este caso debemos calcular el espacio $S_2(\Gamma_0(2^8 \cdot 3^5), \varepsilon)$, que tiene 58 clases de conjugación. En este caso cualquier solución primitiva no trivial (a, b, c) satisface que c es divisible por un primo mayor a 3 y que entonces la curva $\widetilde{E}_{(a,b,c)}$ no tiene multiplicación compleja. Las primeras seis formas (dadas en el orden de Magma) tienen

multiplicación compleja, con lo cual pueden ser descartadas. El resto son eliminadas mediante el truco de Mazur para $p > 109$.

Directo del análisis anterior y de la cota $N_{-6} = 569$ en el Teorema 2.4.8 obtenemos el siguiente resultado.

Teorema 4.4.3. *Sea $p > 569$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^2 + 6y^6 = z^p.$$

La ecuación $x^2 + 7y^6 = z^p$

Este caso resulta muy interesante, debido a que la ecuación de Lebesgue-Nagell (4.24) es difícil de resolver. En [19] (Sección 6) Cohn conjeturó que todas las posibles soluciones de

$$x^2 + 7 = z^n \tag{4.24}$$

con $n \geq 3$ son aquellas con $|x| \in \{1, 3, 5, 11, 181\}$. La conjetura fue estudiada en [25] y completamente resuelta en [11]. Volviendo a la ecuación general $x^2 + 7y^6 = z^p$, tenemos que $Q_{-+} = \{7\}$ y el resto de los conjuntos son vacíos, con lo cual ε es el caracter cuadrático de conductor 21. De acuerdo al Corolario 4.3.1, en este caso debemos computar los espacios $S_2(\Gamma_0(2^r \cdot 3^s \cdot 7^2), \varepsilon)$, donde $r \in \{1, 3\}$ y $s \in \{1, 3\}$. Sea $\mathfrak{p}_7$ el único primo que divide a 7 y sea $\mathfrak{p}_2 = \langle \frac{1+\sqrt{-7}}{2} \rangle$ y $\overline{\mathfrak{p}}_2$ (su conjugado de Galois) los primos sobre 2.

• El espacio $S_2(\Gamma_0(2 \cdot 3 \cdot 7^2), \varepsilon)$ tiene dos clases de conjugación. El truco de Mazur permite descartar la segunda para $p > 7$, pero no es suficiente para la primera. Ésta corresponde a la curva elíptica

$$E_1 : y^2 + xy + \frac{1+\sqrt{-7}}{2} y = x^3 - x^2 + (950\sqrt{-7} - 46)x + \frac{7285\sqrt{-7} + 200449}{2}. \tag{4.25}$$

De hecho, esta curva se corresponde con la solución $181^2 + 7 \cdot (-1)^6 = 2^{15}$ (proveniente de una solución de (4.24)) pero también está relacionada con la solución $1^2 + 7 \cdot (-1)^6 = 2^3$ (pues las curvas $\widetilde{E}_{(181,-1,2)}$ y $\widetilde{E}_{(1,-1,2)}$ son isógenas). La curva tiene discriminante $\mathfrak{p}_7^8 \cdot \mathfrak{p}_2^{13} \cdot \overline{\mathfrak{p}}_2^{39} \cdot \langle 3 \rangle^3$ y un punto de orden 3 sobre K, a saber, el punto $(-5, -2\sqrt{-7} + 319)$. La curva tiene reducción multiplicativa en ambos primos arriba de 2, con lo cual podemos aplicar el Teorema 2.4.3. Recordemos que $v_{\mathfrak{p}_2}(\widetilde{E}_{(a,b,c)}) \equiv 8 \pmod{p}$ (y lo mismo vale para $\overline{\mathfrak{p}}_2$), luego ambas curvas son simplécticamente isomorfas para $\mathfrak{p}_2$ si y sólo si $\left(\frac{2 \cdot 13}{p}\right) = 1$ mientras que para $\overline{\mathfrak{p}}_2$ si y sólo si $\left(\frac{2 \cdot 13 \cdot 3}{p}\right) = 1$. Claramente ambos casos no pueden ocurrir si $\left(\frac{3}{p}\right) = -1$.

• El espacio $S_2(\Gamma_0(2^2 \cdot 3 \cdot 7^2), \varepsilon)$ tiene cuatro clases de conjugación, la primera (en el orden de `Magma`) con multiplicación compleja. Las tres restantes pueden ser descartadas con el truco de Mazur para $p > 7$.

• El espacio $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 7^2), \varepsilon)$ tiene siete clases de conjugación. Las primeras tres tienen multiplicación compleja (y por lo tanto pueden ser descartadas), mientras que las cuatro restantes pueden ser eliminadas mediante el truco de Mazur para $p > 7$.

• El espacio $S_2(\Gamma_0(2 \cdot 3^3 \cdot 7^2), \varepsilon)$ tiene seis clases de conjugación. Las últimas tres pueden ser descartadas con el truco de Mazur para $p > 7$, pero las primeras tres no. Éstas se corresponden a las siguientes curvas elípticas:

$$E_1 : y^2 + xy + \frac{-1+\sqrt{-7}}{2} y = x^3 - x^2 + \frac{115\sqrt{-7} - 91}{2} x + \frac{443\sqrt{-7} + 529}{2}. \tag{4.26}$$

Esta curva proviene de la solución $11^2 + 7 \cdot (-1)^6 = 2^7$ (también proveniente de la ecuación (4.24)). Su discriminante es $\mathfrak{p}_7^8 \cdot \mathfrak{p}_2^{15} \cdot \overline{\mathfrak{p}}_2^5 \cdot \langle 3 \rangle^3$. Tiene el punto de 3-torsión K-racional $(-5, -2\sqrt{-7} + 22)$ (con lo cual no puede ser descartada usando el argumento de la Sección 2.4.4). Para las restantes dos curvas escribimos el modelo (minimal) de un twist cuadrático.

$$E_2 : y^2 + xy + \frac{-1+\sqrt{-7}}{2} y = x^3 - x^2 + \frac{31\sqrt{-7} - 91}{2} x + \frac{121\sqrt{-7} - 157}{2}. \tag{4.27}$$

Notar que esta curva proviene de la solución $3^2 + 7 \cdot (-1)^6 = 2^4$. Su discriminante es $\mathfrak{p}_7^8 \cdot \mathfrak{p}_2^6 \cdot \overline{\mathfrak{p}}_2^2 \cdot \langle 3 \rangle^3$. Tiene el punto de 3-torsión K-racional $(-5, -2\sqrt{-7} + 8)$. La curva

$$E_3 : y^2 + xy + \frac{-1+\sqrt{-7}}{2} y = x^3 - x^2 - \left(\frac{53\sqrt{-7} + 91}{2} \right) x - \left(\frac{201\sqrt{-7} + 59}{2} \right), \tag{4.28}$$

proveniente de la solución $5^2 + 7 \cdot 1^6 = 2^5$. Tiene el punto de 3-torsión K-racional $(-5, -2\sqrt{-7} - 6)$.

Notemos que en los tres casos podemos usar nuevamente el criterio simpléctico en ambos primos que dividen a 2, obteniendo que la curva $\widetilde{E}_{(a,b,c)}$ no puede ser simplécticamente isomorfa a ninguna de éstas si $\left(\frac{3}{p}\right) = -1$. Como estamos asumiendo $p > 283$ para remover las formas con multiplicación compleja (usando Teorema 2.4.8), obtenemos el siguiente resultado.

Teorema 4.4.4. *Sea $p > 283$ un número primo tal que $p \equiv 5, 7 \pmod{12}$. Entonces no existen soluciones primitivas no triviales de la ecuación*

$$x^2 + 7y^6 = z^p.$$

La ecuación $x^2 + 10y^6 = z^p$

El Corolario 4.3.1 implica que para aplicar el método modular debemos calcular el espacio $S_2(\Gamma_0(2^8 \cdot 3^3 \cdot 5^2), \varepsilon)$, donde ε es un caracter de orden 4 y conductor 5. Computacionalmente esto no es posible actualmente.

La ecuación $x^2 + 11y^6 = z^p$

El primo 2 es inerte en $\mathbb{Q}(\sqrt{-11})$, mientras que 3 se parte (como en el caso $d = -5$). El único conjunto no vacío (siguiendo la notación de la Sección 4.2.1) es $Q_{--} = \{11\}$, por lo que el Nebentypus es trivial. El caracter χ es cuadrático de conductor 33. En particular, debemos calcular los espacios $S_2(\Gamma_0(2^2 \cdot 3^2 \cdot 11^2))$ y $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 11^2))$. Una vez más, cualquier forma asociada a una solución (a, b, c) que satisface que $3 \nmid ab$ reside en el primer espacio (por la prueba del Lema 4.1.6).

• El espacio $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 11^2))$ tiene 43 clases de conjugación, 11 de ellas con multiplicación compleja (que pueden ser descartadas si $p > 409$ por Teorema 2.4.8). Las demás formas del espacio se pueden descartar aplicando el truco de Mazur, para $p > 19$. En particular, no existen soluciones primitivas no triviales (a, b, c) con $3 \mid ab$, si $p > 19$.

• El espacio $S_2(\Gamma_0(2^2 \cdot 3^2 \cdot 11^2))$ tiene 26 órbitas de Galois, 6 de ellas con multiplicación compleja. Para las restantes, el truco de Mazur las descarta si $p > 11$, excepto dos de ellas que tienen cuerpo de coeficientes igual a $\mathbb{Q}(\sqrt{3})$ (correspondientes a los lugares 15 y 20 en el orden de `Magma`). La segunda es un twist cuadrático de una forma de nivel $2^2 \cdot 11^2$, por lo que su tipo local en 3 es el de una serie principal cuyo caracter tiene orden 2 restringido al subgrupo de inercia. Por la prueba del Lema 4.1.6, la curva $\widetilde{E}_{(a,b,c)}$ o bien tiene reducción potencialmente multiplicativa, o tiene buena reducción sobre una extensión con grado de ramificación al menos 4 (pues el discriminante tiene valuación 3), luego la Proposición 2.4.2 implica que estas dos representaciones no pueden ser congruentes si $p \geq 5$.

Para descartar la forma f_{15}, necesitamos encontrar una ecuación de la curva asociada (como explicamos anteriormente, verificamos la dimensión del building block y su cuerpo de definición con el algoritmo de Quer). Como el Nebentypus es trivial, existen dos formas distintas para encontrar la ecuación de la curva. Una opción es computar todas las posibles curvas con un conjunto dado de primos que ramifican usando `Magma`; posponemos la segunda construcción. Descartando las que no coinciden con nuestra forma, obtenemos la curva

$$E_{15} : y^2 = x^3 + \frac{1+\sqrt{-11}}{2}x^2 + \frac{1907\sqrt{-11} - 1615}{2}x - 19479\sqrt{-11} - 31012, \tag{4.29}$$

un twist cuadrático (isógeno) de la curva asociada a la forma f_{15}. Notar que ésta es la curva definida a partir de la solución no primitiva $40^2 + 11 \cdot (-4)^6 = 6^6$.

La curva E_{15} tiene un punto de orden 3 (sobre K), por lo que no podemos descartarla usando el Teorema 2.4.5. Necesitamos aplicar nuevamente el argumento simpléctico. El discriminante de E_{15} es igual a $\langle 3\rangle^9 \cdot \mathfrak{p}_{11}^8 \cdot \langle 2\rangle^8$, donde $\mathfrak{p}_{11} = \langle\sqrt{-11}\rangle$. Aplicando el Teorema 2.4.4 en el primo $\mathfrak{p}_{11}$ para los módulos $E_{15}[p]$ y $\widetilde{E}_{(a,b,c)}[p]$, tenemos que son simplécticamente isomorfos, porque la valuación del discriminante de ambas curvas es el mismo.

Consideremos el primo $\mathfrak{p}_3 = \langle\frac{1-\sqrt{-11}}{2}\rangle$ de reducción multiplicativa para ambas curvas. La curva E_{15} tiene valuación del discriminante 9 en $\mathfrak{p}_3$, mientras que la curva $\widetilde{E}_{(a,b,c)}$ tiene valuación del discriminante del modelo minimal $3pv_3(c) - 9$ en $\mathfrak{p}_3$ (ver la prueba de Lema 4.1.6). Entonces el Teorema 2.4.3 implica que los módulos son simplécticamente isomorfos si y sólo si $(-1/p) = 1$. En particular, cuando $(-1/p) = -1$ obtenemos una contradicción.

Teorema 4.4.5. *La ecuación $x^2+11y^6 = z^p$ no tiene solución primitiva no trivial (a, b, c) si $p > 409$ y alguna de las siguientes dos condiciones se cumple:*

- $3 \mid ab$,
- $p \equiv 3 \pmod 4$.

Un aporte diferente para calcular la curva. Aprovechamos la oportunidad para explicar en detalle un método para calcular la curva elíptica como se muestra en [22]. El mapa de Jacobi (y la relación de Eichler-Shimura) permite, dada una forma nueva f de peso dos, construir un retículo Λ_f adjuntado a una variedad abeliana de tipo GL_2 (cuyos puntos complejos corresponden a $\mathbb{C}^d/\Lambda_f$, donde $d = [K_f : \mathbb{Q}]$).

En nuestro caso particular, sea $f = f_{15}$ (para alivianar la notación). Recordar que como $K_f = \mathbb{Q}(\sqrt{3})$ es una extensión cuadrática, podemos construir un retículo de grado 4 obtenido integrando la homología contra la base $\{f, f^\sigma\}$, donde σ es el endomorfismo no trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$. Queremos partir el retículo como suma de dos de rango 2, proporcionando así el building block E_f que estamos buscando. Siguiendo la notación de Cremona, es fácil de verificar que para todo $\sigma \in G_{\mathbb{Q}}$,

$$\sigma(a_p(f)) = a_p(f)\chi(p),$$

donde χ es el caracter cuadrático correspondiente a la extensión $\mathbb{Q}(\sqrt{-11})/\mathbb{Q}$. Por [22, Teorema 2], el álgebra de endomorfismos de A_f es igual al álgebra de cuaterniones $B = \left(\frac{3,-11}{2}\right) \simeq M_2(\mathbb{Q})$ (pues 3 es la norma de $\frac{1+\sqrt{-11}}{2}$). Esto confirma que A_f es isógena al producto de dos curvas elípticas sobre $\mathbb{Q}(\sqrt{-11})$. Para partir la superficie, necesitamos encontrar un divisor de cero dentro del anillo de endomorfismos y claramente en B, el elemento $1 + 2i + j$ es un tal elemento (donde $i^2 = 3$, $j^2 = -11$ y $ij = -ji$). En términos del retículo, recordar que el operador twist η_χ (como elemento del anillo de endomorfismos) en la base elegida tiene matriz $\left(\begin{smallmatrix} 0 & \sqrt{-11} \\ \sqrt{-11} & 0 \end{smallmatrix}\right)$ (ver [75, Sección 2]). En particular, $\eta_\chi^2 = -11$ (el endomorfismo dado por multiplicar por -11), y $f^\sigma = \frac{\eta_\chi f}{\sqrt{-11}}$. Más aún,

$(1+2i+j)f = (1+2\sqrt{3})f + \sqrt{-11}f^\sigma$, por lo que podemos multiplicar (por la izquierda) el retículo por el vector $[1+2\sqrt{3}, \sqrt{-11}]$ para obtener el retículo complejo que estamos buscando. Notar que el divisor de cero no es único; un múltiplo racional de él dará otra curva elíptica isomorfa (sobre $\mathbb{C}$). Luego, debemos calcular el j-invariante de la curva elíptica obtenida vía este proceso, y encontrar el twist correspondiente de la curva que coincide con f.

A continuación mostramos cómo realizar las cuentas usando `Magma`. Una pequeña observación para explicar los cálculos computacionales: internamente `Magma` trabaja con bases racionales, por lo que en vez de calcular el período de la matriz relativa al par $\{f, f^\sigma\}$, utiliza la base $\{\frac{f+f^\sigma}{2}, \frac{f-f^\sigma}{2\sqrt{3}}\}$. Entonces debemos multiplicar por la inversa de la matriz correspondiente para obtener el retículo correcto.

```
SetDefaultRealFieldPrecision(100);
M:=ModularSymbols(2^2*3^2*11^2,2);
S:=NewSubspace(CuspidalSubspace(M)); new:=NewformDecomposition(S);
f:=new[15]; PP:=Periods(f,2000);
```

Esto da la matriz de períodos

$$\begin{pmatrix} -0.454169873046895263850024266849 - 6.310887241768094443293828522226 \cdot 10^{-30}\mathrm{I} & -0.048435665107411599011309623205 8 + 3.628760164016654304893951400 30 \cdot 10^{-29}\mathrm{I} \\ 0.227084936523447631925012133311 - 0.024656977008378975839071327941 9\mathrm{I} & 0.024217832553705799505654811613 3 - 0.129635417833054626720844898122\mathrm{I} \\ -1.516941058003016024958120502 26 - 0.462877184524300807679748661140\mathrm{I} & 0.057560108647507035385428452739 0 - 0.413563230507542856001606030888\mathrm{I} \\ -0.154431438862330233408047701838 + 0.413563230507542856001606005167\mathrm{I} & 0.202867103969741832419357322421 + 0.154292394841433602559916234538\mathrm{I} \end{pmatrix}$$

Para calcular el j-invariante de nuestra curva (y reconocerlo como un entero algebraico), es mejor usar `PARI/GP`. Así es como termina el cálculo:

```
\p 30
Periods=
[-0.45416987304689526385002426684 9 - 6.3108872417680944432938285222 6E-30*I,
-0.04843566510741159901130962320 58 + 3.6287601640166543048939514003 0E-29*I;
0.22708493652344763192501213331 1 - 0.024656977008378975839071327941 9*I,
0.02421783255370579950565481161 33 - 0.129635417833054626720844898122 *I;
-1.51694105800301602495812050226 - 0.462877184524300807679748661140*I,
0.05756010864750703538542845273 90 - 0.413563230507542856001606030888 *I;
-0.15443143886233023340804770183 8 + 0.413563230507542856001606005167 *I,
0.20286710396974183241935732242 1 + 0.154292394841433602559916234538 *I];
A=[1/2,1/2;1/2/sqrt(3),-1/2/sqrt(3)];
Candidate=[1+2*sqrt(3),sqrt(-11)]*1/A*Periods~; lindep(Candidate)
% 4 = [-7, -15, 1, -4]~
```

Esto prueba que el tercer elemento (en $\mathbb{C}$) es una combinación entera de los otros tres.

```
lindep([Candidate[1],Candidate[2],Candidate[4]]);
% 5 = [-1, -3, -2]~
```

Luego, nuestro retículo es generado por el segundo y el cuarto elemento. Calculamos la curva elíptica y su j-invariante sobre los complejos.

```
W=ellperiods([Candidate[2],Candidate[4]]);
E=ellinit([0,0,0,-elleisnum(W,4,1)/4,-elleisnum(W,6,1)/4]);
algdep(E.j,2)
% 8 = 531441*x^2 - 37711872000*x + 1441792000000000
```

Es fácil verificar que el j-invariante de la curva (4.29) es una raíz del polinomio dado.

Observación 35. Este método (al igual que el anterior) no es riguroso. Una vez que tenemos un "candidato" para nuestra curva, debemos aplicar un proceso de ingeniería inversa como el explicado anteriormente:

1. Probar que la curva es una $\mathbb{Q}$-curva. Más aún, probar que la conjugación compleja de la curva es isógena a su twist por $\sqrt{-3}$.

2. Calcular el nivel de la forma modular asociada a la curva (cuya existencia está garantizada por las conjeturas de Serre).

3. Calcular el espacio dado, y deducir que la forma asociada a la curva elíptica encontrada es la única cuyos primeros coeficientes de Fourier coinciden con los de f.

La ecuación $x^2 + 13y^6 = z^p$

Siguiendo la notación de la Sección 4.2.1, tenemos que el único conjunto no vacío es $Q_{++} = \{13\}$, su Nebentypus ε tiene orden 2 y conductor $4 \cdot 3 \cdot 13$. Por el Corolario 4.3.1 debemos calcular los espacios $S_2(\Gamma_0(2^4 \cdot 3 \cdot 13^2), \varepsilon)$ y $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 13^2), \varepsilon)$. Por Teorema 2.4.8 podemos descartar las formas con multiplicación compleja en ambos espacios asumiendo $p > 1627$.

• El espacio $S_2(\Gamma_0(2^4 \cdot 3 \cdot 13^2), \varepsilon)$ tiene 29 clases de conjugación, 7 de ellas con multiplicación compleja. Las formas restantes se pueden descartar por el truco de Mazur, para $p > 13$.

• El espacio $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 13^2), \varepsilon)$ tiene 68 clases de conjugación, 14 de ellas con multiplicación compleja. Las formas restantes pueden ser descartadas una vez más utilizando el truco de Mazur, para $p > 29$.

Teorema 4.4.6. *Sea $p > 1627$ un número primo. Entonces no hay soluciones primitivas no triviales de la ecuación*

$$x^2 + 13y^6 = z^p.$$

La ecuación $x^2 + 14y^6 = z^p$

Siguiendo la notación de la Sección 4.2.1, $Q_{-+} = \{7\}$, por lo que las posibles soluciones dan formas en los espacios $S_2(\Gamma_0(2^8 \cdot 3^2 \cdot 7^2), \varepsilon)$ y $S_2(\Gamma_0(2^8 \cdot 3^3 \cdot 7^2), \varepsilon)$, donde ε es el caracter cuadrático de conductor 28. Computacionalmente no es posible calcular estos espacios actualmente.

La ecuación $x^2 + 15y^6 = z^p$:

Sea $K = \mathbb{Q}(\sqrt{-15})$. El primo 2 se parte como $\langle 2 \rangle = \mathfrak{p}_2\overline{\mathfrak{p}}_2$, donde $\mathfrak{p}_2 = \langle 2, \frac{1+\sqrt{-15}}{2} \rangle$ mientras que el primo 3 es inerte en K. Como en el caso $d = 5$, el único conjunto no vacío es $Q_{+-} = \{5\}$. La diferencia es que el Nebentypus ramifica en 3 y no en 2. Por el Corolario 4.3.1 debemos calcular los espacios $S_2(\Gamma_0(2 \cdot 3^5 \cdot 5^2), \varepsilon)$ y $S_2(\Gamma_0(2^2 \cdot 3^5 \cdot 5^2), \varepsilon)$.

• El espacio $S_2(\Gamma_0(2 \cdot 3^5 \cdot 5^2), \varepsilon)$ tiene 21 clases de conjugación. El truco de Mazur nos permite eliminar, para $p > 71$, todas las formas excepto las primeras seis (dadas en el orden de `Magma`), que no tienen multiplicación compleja y tienen building blocks de dimensión 1. Como el primo 2 se parte en K, el caracter χ necesario para que la representación de Galois descienda es no ramificado en 2, por lo que los building blocks tienen reducción multiplicativa en los primos que dividen a 2, y lo mismo ocurre para $\widetilde{E}_{(a,b,c)}$. En particular, podemos asumir que $2 \nmid ab$. Para descartar las formas restantes buscamos curvas elípticas sobre $\mathbb{Q}(\sqrt{-15})$ con buena reducción fuera de $\{\mathfrak{p}_2, \overline{\mathfrak{p}}_2, \mathfrak{p}_3, \mathfrak{p}_5\}$ y encontramos 111264 curvas elípticas. Utilizando unos pocos a_p's de las formas, descartamos la mayoría, y obtenemos las siguientes ecuaciones para nuestras curvas (salvo conjugación):

$$E_1 : y^2 + xy - \frac{1-\sqrt{-15}}{2}y = x^3 - x^2 - \frac{421+23\sqrt{-15}}{2}x - \frac{2185+191\sqrt{-15}}{2}, \qquad (4.30)$$

proveniente de la solución $1^2 + 15 \cdot 1^6 = 2^4$;

$$E_2 : y^2 + xy - \frac{1-\sqrt{-15}}{2}y = x^3 - x^2 + (2\sqrt{-15} - 8)x + \frac{-7+7\sqrt{-15}}{2}; \tag{4.31}$$

$$E_3 : y^2 - \frac{1-\sqrt{-15}}{2}xy = x^3 + \frac{1+\sqrt{-15}}{2}x^2 + \frac{-111+87\sqrt{-15}}{2}x + \frac{65+375\sqrt{-15}}{2}; \tag{4.32}$$

$$E_4 : y^2 + xy + \frac{1+\sqrt{-15}}{2}y = x^3 - x^2 + (-211 + 137\sqrt{-15})x + \frac{1973+2333\sqrt{-15}}{2}; \tag{4.33}$$

$$E_5 : y^2 + \frac{1+\sqrt{-15}}{2}xy = x^3 + \frac{1-\sqrt{-15}}{2}x^2 - \frac{111+375\sqrt{-15}}{2}x + \frac{-9823+2793\sqrt{-15}}{2}; \tag{4.34}$$

y

$$E_6 : y^2 + xy + \frac{1+\sqrt{-15}}{2}y = x^3 - x^2 - (79\sqrt{-15} + 211)x - \left(\frac{1339\sqrt{-15}+835}{2}\right). \tag{4.35}$$

Las curvas E_2, E_3, E_4 y E_5 tienen buena reducción en $\mathfrak{p}_5$, mientras que nuestra curva $\widetilde{E}_{(a,b,c)}$ tiene reducción aditiva en $\mathfrak{p}_5$ (Observación 27). En particular, los tipos locales no coinciden, por lo que las dos representaciones no pueden ser congruentes si $p \geq 5$, por Proposición 2.4.2.

Las curvas E_1 y E_6 tienen un punto de 3-torsión (por ejemplo el punto $(-11, 2 - 4\sqrt{-15})$ y $(-11, -4\sqrt{-15} - 21)$ respectivamente). Luego, deberemos recurrir al argumento simpléctico para descartarlas. Las valuaciones de sus discriminantes son las siguientes:

- La curva E_1 tiene discriminante minimal con valuación 6 en $\mathfrak{p}_2$, 2 en $\overline{\mathfrak{p}}_2$, 14 en $\mathfrak{p}_3$ y 8 en $\mathfrak{p}_5$.
- La curva E_6 tiene discriminante minimal con valuación 12 en $\mathfrak{p}_2$, 4 en $\overline{\mathfrak{p}}_2$, 14 en $\mathfrak{p}_3$ y 8 en $\mathfrak{p}_5$.

Como $2 \nmid ab$, el modelo (4) no es minimal. Su discriminante minimal tiene valuación $v_{\mathfrak{p}_2}(\widetilde{E}_{(a,b,c)}) \equiv v_{\overline{\mathfrak{p}}_2}(\widetilde{E}_{(a,b,c)}) \equiv 8 - 12 \pmod{p}$. Si aplicamos el Teorema 2.4.3 a ambos primos arriba de 2, obtenemos lo siguiente:

- El argumento en el primo $\mathfrak{p}_2$ dice que $E_1[p]$ (respectivamente $E_6[p]$) y $\widetilde{E}_{(a,b,c)}[p]$ son simplécticamente isomorfos si y sólo si $\left(\frac{-6}{p}\right) = 1$ (respectivamente $\left(\frac{-3}{p}\right) = 1$).
- El argumento en el primo $\overline{\mathfrak{p}}_2$ dice que $E_1[p]$ (respectivamente $E_6[p]$) y $\widetilde{E}_{(a,b,c)}[p]$ son simplécticamente isomorfos si y sólo si $\left(\frac{-2}{p}\right) = 1$ (respectivamente $\left(\frac{-1}{p}\right) = 1$).

En particular, si $\left(\frac{3}{p}\right) = -1$ obtenemos una contradicción. Podemos mejorar aún más; notemos que $v_{\mathfrak{p}_5}(\widetilde{E}_{(a,b,c)}) = 8 = v_{\mathfrak{p}_5}(E_1)$ (respectivamente E_6), por lo que podemos aplicar el argumento simpléctico (Teorema 2.4.4) en $\mathfrak{p}_5$, obteniendo que los módulos son siempre simplécticamente isomorfos. Luego, podemos utilizar esta información para añadir más primos en nuestro resultado final. Para descartar ambas curvas cuando $\left(\frac{3}{p}\right) = 1$, necesitamos la hipótesis extra $\left(\frac{-2}{p}\right) = 1$ y $\left(\frac{-1}{p}\right) = -1$. En particular, si $p \equiv 5, 7, 15, 17, 19 \pmod{24}$ tenemos una contradicción (incrementamos el porcentaje de primos de $1/2$ a $5/8$).

• El espacio $S_2(\Gamma_0(2^2 \cdot 3^5 \cdot 5^2), \varepsilon)$ tiene 33 clases de conjugación. En este caso el truco de Mazur es suficiente para descartar a todas si $p > 19$, excepto a las primeras doce (en el orden de `Magma`), que tienen multiplicación compleja, y por lo tanto también pueden ser descartadas vía el Teorema 2.4.8 para $p > 457$. Cabe notar que las formas asociadas a soluciones (a, b, c) con $2 \mid ab$ deben pertenecer a este espacio, por Lema 4.1.5. En particular se sigue que no hay soluciones primitivas no triviales si $2 \mid ab$ y $p > 457$.

Teorema 4.4.7. *La ecuación $x^2 + 15y^6 = z^p$ no tiene soluciones primitivas no triviales (a, b, c) si $p > 457$ y alguna de las siguientes dos condiciones se satisface:*

- $2 \mid ab$.
- $p \equiv 5, 7, 15, 17, 19 \pmod{24}$.

La ecuación $x^2 + 17y^7 = z^p$

Siguiendo la notación de la Sección 4.2.1, el único conjunto no vacío es $Q_{+-} = \{17\}$. Luego, el Nebentypus ε tiene orden 16 y conductor $4 \cdot 17$. Debemos descartar formas en los espacios $S_2(\Gamma_0(2^4 \cdot 3^2 \cdot 17^2), \varepsilon)$ y $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 17^2), \varepsilon)$. Aunque la dimensión del primer espacio pareciera estar en el rango de lo computable (cerca del límite) `Magma` comunica un error interno mientras intentamos calcular dicho espacio. El segundo espacio es demasiado grande para computarlo.

La ecuación $x^2 + 19y^6 = z^p$

Siguiendo la notación de la Sección 4.2.1, el único conjunto no vacío es $Q_{-+} = \{19\}$. El Nebentypus ε tiene orden 2 y conductor $3 \cdot 19$. El caracter χ es de orden 4, ramificado solamente en el 3 (es inerte en $\mathbb{Q}(\sqrt{-19})/\mathbb{Q}$), con componente local en 3 un caracter de orden 4. Por el Corolario 4.3.1, debemos descartar formas en $S_2(\Gamma_0(2^2 \cdot 3 \cdot 19^2), \varepsilon)$ y $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 19^2), \varepsilon)$.

• El espacio $S_2(\Gamma_0(2^2 \cdot 3 \cdot 19^2), \varepsilon)$ tiene 10 clases de conjugación, tres de ellas con multiplicación compleja. Utilizando el truco de Mazur podemos descartar todas las formas sin multiplicación compleja, para $p > 19$.

• El espacio $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 19^2), \varepsilon)$ tiene 18 clases de conjugación. El truco de Mazur permite descartarlas para $p > 19$, excepto tres de ellas que tienen multiplicación compleja. Queremos remarcar que la última forma tiene un cuerpo de coeficientes muy grande y por alguna razón `Magma` no puede correr el truco de Mazur para dicha forma. Entonces, la descartamos usando `PARI/GP` (ver los resultados en el archivo para más detalles).

Recordar que debemos asumir $p > 683$ para remover las formas con multiplicación compleja (utilizando el Teorema 2.4.8). Luego, del análisis anterior tenemos el siguiente resultado.

Teorema 4.4.8. *Sea $p > 683$ un número primo. Entonces no existen soluciones primitivas no triviales de la ecuación*

$$x^2 + 19y^6 = z^p.$$

Bibliografía

[1] Sebastian Zuniga Alterman. Explicit averages of square-free supported functions: to the edge of the convolution method, 2020.

[2] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[3] Michael A. Bennett and Imin Chen. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$. *Algebra Number Theory*, 6(4):707–730, 2012.

[4] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng. The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. *Int. J. Number Theory*, 6(2):311–338, 2010.

[5] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties. *Proc. Amer. Math. Soc.*, 145(10):4111–4117, 2017.

[6] Nicolas Billerey, Imin Chen, Luis Dieulefait, Nuno Freitas, and Filip Najman. On Darmon's program for the Generalized Fermat equation, available at arXiv:2205.15861, 2022.

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] Josha Box. Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular. *Trans. Amer. Math. Soc.*, 375(5):3129–3172, 2022.

[9] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[10] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3):969–1018, 2006.

[11] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[12] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008.

[13] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[14] Ana Caraiani and James Newton. On the modularity of elliptic curves over imaginary quadratic fields, 2023.

[15] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[16] A. Cassels, J. & Frölich. *Algebraic Number Theory*. Academic Press Inc. (London) Ltd., 1967.

[17] Imin Chen. On the equations $a^2 - 2b^6 = c^p$ and $a^2 - 2 = c^p$. *LMS J. Comput. Math.*, 15:158–171, 2012.

[18] Imin Chen and Angelos Koutsianas. A modular approach to Fermat equations of signature $(p, p, 5)$ using Frey hyperelliptic curves, 2022.

[19] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[20] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[21] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984.

[22] J. E. Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc. (2)*, 45(3):404–416, 1992.

[23] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[24] John Cremona and Ariel Pacetti. On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1. *Proc. Lond. Math. Soc. (3)*, 118(5):1245–1276, 2019.

[25] John E. Cremona and Samir Siksek. On the Diophantine equation $x^2 + 7 = y^m$. *Acta Arith.*, 109(2):143–149, 2003.

[26] Harris B. Daniels and Álvaro Lozano-Robledo. On the number of isomorphism classes of CM elliptic curves defined over a number field. *J. Number Theory*, 157:367–396, 2015.

[27] Henri Darmon. The equation $x^4 - y^4 = z^p$. *C. R. Math. Rep. Acad. Sci. Canada*, 15(6):286–290, 1993.

[28] Henri Darmon. The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$. *Internat. Math. Res. Notices*, (10):263–274, 1993.

[29] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000.

[30] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Int. Press, Cambridge, MA, 1994.

[31] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[32] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[33] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree, 2017.

[34] Maarten Derickx, Filip Najman, and Samir Siksek. Elliptic curves over totally real cubic fields are modular. *Algebra Number Theory*, 14(7):1791–1800, 2020.

[35] J.-M. Deshouillers and F. Dress. Sommes de diviseurs et structure multiplicative des entiers. *Acta Arith.*, 49(4):341–375, 1988.

[36] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[37] Luis Dieulefait and Jorge Jiménez Urroz. Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. Reine Angew. Math.*, 633:183–195, 2009.

[38] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.

[39] Jordan S. Ellenberg. On the error term in Duke's estimate for the average special value of L-functions. *Canad. Math. Bull.*, 48(4):535–546, 2005.

[40] G. Faltings. Erratum: "Finiteness theorems for abelian varieties over number fields". *Invent. Math.*, 75(2):381, 1984.

[41] Nuno Freitas and Alain Kraus. On the symplectic type of isomorphims of the p-torsion of elliptic curves, 2016.

[42] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[43] Nuno Freitas and Samir Siksek. Criteria for irreducibility of $\mathrm{mod}\, p$ representations of Frey curves. *J. Théor. Nombres Bordeaux*, 27(1):67–76, 2015.

[44] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[45] Franco Golfieri Madriaga. El Último Teorema de Fermat. *Trabajo especial de la Licenciatura en Matemática, FAMAF, UNC*, disponible en https://rdu.unc.edu.ar/, 2021.

[46] Franco Golfieri Madriaga, Ariel Pacetti, and Lucas Villagra Torcomian. On the equation $x^2 + dy^6 = z^p$ for square-free $1 \leq d \leq 20$. *International Journal of Number Theory*, 19(05):1129–1165, 2023.

[47] Franco Golfieri Madriaga, Ariel Pacetti, and Lucas Villagra Torcomian. Asymptotic results for the equations $x^4 + dy^2 = z^p$ and $x^2 + dy^6 = z^p$, Preprint arXiv:2211.16334, 2022.

[48] Emmanuel Halberstadt and Alain Kraus. Courbes de Fermat: résultats et problèmes. *J. Reine Angew. Math.*, 548:167–234, 2002.

[49] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[50] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 280–293. Hindustan Book Agency, New Delhi, 2010.

[51] Angelos Koutsianas. On the generalized fermat equation $a^2 + 3b^6 = c^n$. *Bulletin of the Hellenic Mathematical Society*, 64:56–68, 2020.

[52] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[53] Alain Kraus. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4):611–633, 2007.

[54] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[55] Samuel Le Fourn. Nonvanishing of central values of L-functions of newforms in $S_2(\Gamma_0(dp^2))$ twisted by quadratic characters. *Canad. Math. Bull.*, 60(2):329–349, 2017.

[56] Wilhelm Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70, 1942.

[57] Wilhelm Ljunggren. Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$. In *Tolfte Skandinaviska Matematikerkongressen, Lund, 1953*, pages 188–194. Lunds Universitets Matematiska Inst., Lund, 1954.

[58] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2021.

[59] David Loeffler and Jared Weinstein. On the computation of local components of a newform. *Math. Comp.*, 81(278):1179–1200, 2012.

[60] Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *Algebra Number Theory*, 16(4):777–837, 2022.

[61] Ariel Pacetti Luis Dieulefait and Fernando Rodriguez Villegas. Representaciones de Galois. *Notas del AGRA III*, disponible en https://www.famaf.unc.edu.ar/~apacetti/agra3/index.html, 2018.

[62] Philippe Michaud-Rodgers. Fermat's last theorem and modular curves over real quadratic fields, 2021.

[63] Filip Najman and George C. Ţurcaş. Irreducibility of mod p galois representations of elliptic curves with multiplicative reduction over number fields. *International Journal of Number Theory*, 17(08):1729–1738, 2021.

[64] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations. *Math. Comp.*, 91(338):2817–2865, 2022.

[65] Ariel Pacetti and Lucas Villagra Torcomian. $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations II. *Publicacions Matemàtiques*, to appear, 2022.

[66] Ioannis Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2):119–152, 1993.

[67] PARI Group, Univ. Bordeaux. *PARI/GP version 2.12.2*, 2019. available from http://pari.math.u-bordeaux.fr/.

[68] Jordi Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc. (3)*, 81(2):285–317, 2000.

[69] Jordi Quer. Fields of definition of building blocks. *Math. Comp.*, 78(265):537–554, 2009.

[70] Kenneth A. Ribet. Lowering the levels of modular representations without multiplicity one. *Internat. Math. Res. Notices*, (2):15–19, 1991.

[71] Kenneth A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[72] Jean-Pierre Serre. *Corps locaux*. Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968. Deuxième édition.

[73] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[74] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[75] Goro Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25:523–544, 1973.

[76] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[77] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[78] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[79] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975.

[80] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[81] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*, 2021. https://www.sagemath.org.

[82] Lucas Villagra Torcomian. Asymptotic Fermat for signature $(4, 2, p)$ over number fields. *Journal of Number Theory*, 250:124–138, 2023.

[83] Lucas Villagra Torcomian. *Códigos utilizados para esta Tesis*, 2023. https://github.com/lucasvillagra/PhD-thesis.

[84] Lucas Villagra Torcomian. Correspondencia de Langlands en Dimensión 1. *Trabajo especial de la Licenciatura en Matemática, FAMAF, UNC*, disponible en https://rdu.unc.edu.ar/, 2019.

[85] Rafael von Känel and Benjamin Matschke. Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture, 2016.

[86] P. G. Walsh. Diophantine equations of the form $aX^4 - bY^2 = \pm 1$. In *Algebraic number theory and Diophantine analysis (Graz, 1998)*, pages 531–554. de Gruyter, Berlin, 2000.

[87] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.