
**UNIVERSIDAD DE BUENOS AIRES**
**Facultad de Ciencias Exactas y Naturales**
**Departamento de Matemática**

**Tesis de Licenciatura**

# Rango promedio de curvas elípticas y aritmética cuantitativa

**Ignacio Cordoba**

**Director:** Marcelo Paredes

Fecha de presentación: 27/06/25

# Índice

# Agradecimientos

El camino hasta esta tesis fue largo. Afortunadamente, lo hice acompañado de muchas personas que me ayudaron en la travesía. Lo que sigue es un extenso intento (plagado de apócopes) de agradecer por tal compañía. Lamento cualquier omisión: lo que la palabra esquive espero siempre poder demostrarlo con el acto. No sé si es costumbre que la longitud de esta parte sea tanta; en mi caso, les aseguro que es imprescindible.

Agradezco a mis amigos con quienes he cursado desde el inicio por hacer de mi paso facultativo una experiencia hermosa, divertida, y por mostrarme que siempre se puede aprender algo nuevo. Dirijo este agradecimiento en especial a Cami, Chanu, Facu, Juli, Pedro, Santi y Zenón. Otros, como Boris, Joa y Valen, prefirieron primero ser mis alumnos, y a ellos agradezco por su posterior amistad.

Agradezco a mis compañeros de (lo que quizá ya puedo empezar a llamar) área - Ian, Juan, Juli, Mateo y Pedro. De todos ustedes he aprendido mucho, no sólo matemáticamente.

Agradezco a quienes conocí en el transcurso de la carrera y compartieron muchos momentos lindos conmigo en Exactas, en seminarios, charlas de café y/o enseñando conmigo. Entre ellos me es importante mencionar a Carli, Charly, Darío, Dev, Facu M, Georgi, Ivo, Juan PG, Leo, Lola, Maki, Manu, Nahuel, Pablito y Santi R.

Agradezco a mis queridos amigos Agus, Emi, Guido, Lu, Lucas, Rama y Sol. Gracias por tantas salidas, por tantas risas, por tantos consejos, por tanta matemática y por tanto cariño.

Agradezco a mis amigos de siempre - Brandon, Hernán, Lucas, Lucio, Juanma, Juli, Martín, Mati y Seba por ser un pilar inamovible, al cual no hace falta llamar para saber que está ahí. Lamento si lo que consta luego no se entiende a la primera.

Agradezco a Avril, por su larga amistad y por escuchar siempre mis literarias inquietudes.

Agradezco a Lucía, por acompañarme desde el CBC en esta travesía. Tu amistad incondicional, tu inteligencia y tu constancia siempre fueron y serán algo que atesoro.

Agradezco a todos los profesores que me han formado. Especial agradecimiento es necesario dirigir a: Martín Mereb, de quien he aprendido muchísimo y quien siempre me ha aconsejado acerca de mi carrera; gracias, además, por ser jurado de esta tesis. A Román Sasyk, por ser jurado de esta tesis y por permitirme poner a prueba mi entendimiento en el seminario. Gracias, además, por ayudarme a que mi meta de continuar investigando se vuelva realidad. A Nicolás Sirolli, con quien aprendí gran parte de la teoría de números que sé y a quien debo la hermosa experiencia de haber ido a mi primera conferencia internacional.

Agradezco profusamente a mi director, Marcelo. Los agradecimientos que te debo deben incluso comenzar tempranamente, dado que aprendí a escribir y a demostrar siendo alumno tuyo en Taller. Asimismo, allí comenzó mi interés por la teoría de números, a pesar de que la vastedad del área lo haya hecho mermar algunas veces. No obstante, las grandes sugerencias de libros para leer y las conversaciones acerca de la naturaleza diofántica de las cosas siempre lograron cautivarme. Avanzando unos años, el agradecimiento continúa por haber dirigido mi tesis, eligiendo un tema que me permitió entender cómo era leer un paper y transversal a gran parte de la literatura. Gracias por orientarme con mis dudas y por explicarme tantas cosas, con la paciencia que te caracteriza, ahora y durante mi carrera. Finalmente, gracias por ayudarme a que mi meta de continuar investigando se vuelva realidad. Prometo estar a la altura.

Agradezco a Damián por acompañarme todos estos años, cursando conmigo, enseñándome y siendo el mejor de los amigos que se puede tener. Espero que sigamos conversando sobre matemática y sobre la vida por mucho tiempo más.

Agradezco de todo corazón a mis padres, que me han apoyado incansablemente durante todo este camino, permitiéndome perseguir mi sueño de estudiar Matemática. Gracias por siempre velar porque nada me falte, por siempre estar atentos a como me iba, por tantas comidas a horas insensatas cuando cursaba un sin fín de materias. Gracias por enseñarme el

valor de la educación y el valor del esfuerzo, aprendizaje del cual espero la existencia de esta tesis sea un fiel reflejo. Agradezco también con mucho amor a mi hermano, a mis abuelos Juan y Susana, a Jere, Lisi, Germán, Antú, Galo y Patricia. En general, extiendo mi gratitud a toda mi familia, que sé que estará igual de contenta que yo con esta tesis. Gracias a todos ustedes por su sempiterno amor.

Agradezco a la educación pública y a la UBA. Trataré siempre de retribuir todo lo que se me ha dado.

Agradezco a Cecilia por el infinito amor y por acompañarme en estos cinco exactenses años, desde que arribamos en Análisis I y Álgebra I. No sé que habría hecho sin tu apoyo, dulzura y sabiduría, y, por más que escriba, ningún párrafo bastaría para reflejar aunque sea una brisa de lo afortunado que me siento por estar a tu lado. Gracias por hacerme un mejor hombre y un mejor matemático cada día; espero que quieras seguir haciéndolo en la etapa que sigue.

Por último, gracias a Ester y a Matilde, a quienes ya les contaré, junto con José, a su debido tiempo y en más detalle, esta tesis.

# 1. Introducción

El objetivo de la presente tesis es la exposición de un resultado que arroja luz sobre un importante problema de la teoría de números: el comportamiento del rango de las curvas elípticas. Asimismo - como explicaremos a la brevedad - al estar este problema enmarcado en el área de la *estadística aritmética* o la *teoría cuantitativa o enumerativa de números*, aprovecharemos para exponer brevemente avances en otro problema de esta índole.

Nuestro principal objeto de interés son las curvas elípticas. Formalmente, una curva elíptica sobre un cuerpo $K$ es una curva definida sobre $K$, proyectiva, suave, de género 1 y con un punto $K$-racional distinguido. Las curvas elípticas se manifiestan de manera natural en la teoría de números, codificando la información aritmética de problemas tan antiguos como el *problema del número congruente*. Asimismo, en las curvas elípticas interactúan facetas algebraicas, geométricas, analíticas y aritméticas, que pueden combinarse para atacar problemas que, a primera vista, no tienen tanto que ver con ellas (como es el caso del teorema de Wiles).

Una de sus propiedades más básicas y fundamentales es que sus puntos obedecen una ley abeliana de grupo, y por ende es posible construir *nuevos* puntos a partir de otros ya conocidos - aunque en principio no es claro que estos puntos sean *genuinamente nuevos*, es decir, que sean independientes de los ya obtenidos. De especial interés es el caso de curvas elípticas sobre los números racionales y su grupo de puntos racionales. Una pregunta inmediata, ante la aparición de este grupo, es si es finito o infinito, y, en este segundo caso, otra pregunta natural es si es posible obtener *todos* los puntos de la curva en base a un conjunto de puntos particulares (y, más aún, si este conjunto de generadores es finito). La respuesta a esto último viene dada por el celebrado teorema de Mordell-Weil, y es afirmativa: el grupo de puntos $K$-racionales de una curva elíptica es finitamente generado. En particular, admite una parte libre, en la cual aparecen copias de $\mathbb{Z}$, y una parte de torsión. La cantidad de sumandos libres del grupo de puntos racionales de la curva elíptica se denomina **rango**. La parte de torsión está completamente entendida sobre $\mathbb{Q}$ (resultado el cual fue probado por Mazur en [Maz77]). En cambio, la parte libre es misteriosa,

y el *problema del rango* ha sido desde la prueba del teorema de Mordell-Weil una cuestión de intenso debate e investigación. Un entendimiento profundo del rango no sólo nos daría consecuencias importantes a nivel algorítmico, sino que el rango permite entender cómo se distribuyen las soluciones asociadas a la curva elíptica.
El problema puede resumirse en la siguiente pregunta:

**¿Cómo se comporta el rango de las curvas elípticas?**

Más precisamente, podríamos preguntarnos:

- ¿Está el rango de las curvas elípticas uniformemente acotado?
- ¿Hay una sucesión de curvas elípticas con rangos creciendo de manera no acotada?
- ¿Para cada natural, hay una curva elíptica que lo tiene por rango? ¿Hay infinitas?
- ¿Cómo calcular el rango de una curva elíptica?

La opinión de la comunidad matemática sobre esta pregunta está dividida hace mucho tiempo. Sobre $\mathbb{Q}$ es fácil probar que hay familias infinitas de curvas elípticas con rango 0, 1 y 2. El mayor natural tal que hay infinitas curvas de ese rango es 19 (ver las tablas de Dujella: [Duj]). Por otro lado, la curva elíptica con mayor rango conocido tiene rango $\geq 29$ (y rango exactamente 29 si asumimos la hipótesis de Riemann generalizada), y se debe a Elkies y Klagsbrun (ver: [Elk]). En contraste, sobre cuerpos de funciones $\mathbb{F}_p(t)$, los rangos no están acotados (ver [Ulm02]). Si uno espera que los cuerpos de números se parezcan a estos cuerpos de funciones (lo que se conoce como la *analogía de cuerpos de funciones*), esto parecería sugerir que los rangos no están acotados tampoco en el caso de $\mathbb{Q}$ y cuerpos de números. No obstante, se han podido producir muy pocas curvas de rango alto, lo cual, si el rango no estuviera acotado, parecería implicar que las curvas de rango alto son extrañas o difíciles de encontrar. Desde el lado de la acotación uniforme, una reciente heurística ( [PPVW19]) sugiere que hay *finitas* curvas de rango mayor a 22. Comentaremos brevemente heurísticas al respecto del rango en la sección 6.

La profunda dificultad del problema del rango ha llevado a la comunidad a evaluar el problema desde distintas ópticas, para ganar información

sobre el rango sin directamente tratar de construir curvas elípticas específicas. Por un lado, se sabe que un posible algoritmo para calcular el rango (el *método del descenso*) depende de la finitud de un grupo de cohomología asociado a la curva elíptica, el **grupo de Tate-Shafarevich**. La finitud de este grupo es otro importante problema abierto, el cual por el momento las herramientas de la teoría de números no pueden atacar. El grupo de Tate-Shafarevich, al igual que el grupo de puntos módulo duplicación, encajan en una sucesión exacta en la cual el término del medio es otro grupo de cohomología, el **grupo de Selmer**. Este grupo controla el co-núcleo de la isogenía que multiplica por 2, y se puede utilizar para dar una demostración del teorema de Mordell-Weil (ver [Sil09]). Por ende, controlar este grupo es de interés para tratar de controlar explícitamente el rango, y hay mucho trabajo puesto en entender el comportamiento de los grupos de Selmer en la actualidad.

En otra dirección, una forma de ganar información sobre los objetos aritméticos es entender su comportamiento o distribución "en promedio" o estadísticamente. Esto da lugar a los llamados problemas de *aritmética estadística*. Este campo busca entender cómo se distribuyen los objetos de la teoría de números a nivel asintótico - estadístico, donde este fenómeno se puede manifestar ya sea promediando sobre familias de representantes de los objetos, o buscando cotas en función de invariantes de los objetos. Simultáneamente, es posible tratar a los objetos determinados, como los cuerpos de números, como objetos "aleatorios" y tratar de predecir o estudiar su estructura probabilística. Por ejemplo, un problema clásico que se encuentra sin resolución actualmente es el problema de Gauss:

**Conjetura: 1.1.** *Existen infinitos cuerpos cuadráticos reales con número de clase igual a* 1*.*

De manera muy elemental, el comportamiento real cuadrático debería esperarse distinto al comportamiento imaginario cuadrático: en la fórmula del número de clases, las unidades y el regulador juegan un papel muy distinto, pues salvo finitos casos, las unidades en los cuerpos cuadráticos imaginarios son cíclicas de orden 2. La imposibilidad de atacar este problema con métodos directos permite preguntarse: *¿qué porcentaje de cuerpos cuadráticos reales tienen número de clase* 1*?¿Hay alguna manera de modelar o predecir la distribución de este fenómeno?* Las heurísticas más importantes al respecto hoy en día son las *heurísticas de Cohen-Lenstra* ( [CL84]). Además

de predecir comportamientos para el caso cuadrático, estas heurísticas describen el comportamiento de varias extensiones de cuerpos de números. En su forma más básica, predicen que el cardinal del grupo de automorfismos influye fuertemente en la "ciclicidad" de la extensión y en la cantidad de veces que "aparece naturalmente" un cuerpo de números. En particular, debería ser cierto que "mientras más grande es el grupo de automorfismos del objeto, menos común sería verlo".

Hay otros problemas de arimética estadística o cuantitativa que son representativos de esta filosofía:

- *La conjetura de Malle* ( [Mal02,Mal04]): sea $G$ un grupo finito, subgrupo de $S_n$, $K$ un cuerpo de números y $n$ un natural. Sea $N(K, G, n, X)$ la función que cuenta las extensiones de grado $n$ de $K$ con grupo de Galois de su clausura de Galois isomorfo (como grupo de permutaciones) a $G$ y discriminante acotado por $X$. La conjetura de Malle predice el comportamiento de $N(K, G, n, X)$. Esta conjetura está abierta e implica el problema inverso de Galois. Klüners encontró un contraejemplo ( [Kl5]) a la heurística inicial de Malle, la cual ha sido desde entonces refinada. Por otro lado, la conjetura de Malle se puede reintepretar en términos de stacks ( [ESZB23]), y en este contexto se vuelve un problema de conteo de puntos de altura acotada - esto se relaciona con conjeturas de Darda y Yasuda ( [DY24]). Esta relación da lugar a lo que se conoce como la conjetura de Batyrev-Manin-Malle ( [ESZB23]);

- La *conjetura de la $\ell$-torsión* predice el comportamiento de los grupos de torsión de los cuerpos de números y da su orden asintótico en función del discriminante. Nos abocamos a casos particulares de esta conjetura en la sección 7;

- La *conjetura de Linnik*: sea $N(n, X)$ la función que cuenta extensiones de $\mathbb{Q}$ de grado $n$ y discriminante acotado por $X$. La conjetura de Linnik predice que $N(n, X) \sim cX$, con $c$ una constante que depende de $n$ (ver [Coh03], [Pie22]). Esto da lugar en general a los *problemas de conteo de cuerpos*, en los cuales podemos tratar de obtener cotas generales para todo $n$, o bien asintóticas exactas luego de fijar el $n$. En el primer caso, trabajos fundamentales son el paper de Schmidt [Sch95] y el paper de Ellenberg-Venkatesh [EV06]. En

el segundo caso, se conocen resultados para $n = 2$ (Gauss), $n = 3$ (Davenport–Heilbronn) y $n = 4, 5$ (Cohen–Díaz–Olivier, Bhargava) - ver las referencias contenidas en el survey de Cohen [Coh03]. Se puede realizar la misma pregunta para $K$ cuerpo global y también se han obtenido resultados parciales (Yukie, Wright); para más sobre estos resultados, ver [Coh03];

- Siguiendo con el problema del rango, podemos preguntarnos cómo se distribuye el rango de las curvas elípticas, cómo se distribuye el rango del grupo de Selmer, cómo se distribuye la torsión del grupo de Tate-Shafarevich, entre otros.

El auge de este tipo de conjeturas que avanzan nuestro entendimiento de estos problemas, sirviendo de guía para investigarlos, vino aparejado por el desarrollo de nuevos métodos para ser aplicados en este campo. El caso al que nos abocamos es el del rango de las curvas elípticas, y expondremos el importante teorema de Bhargava–Shankar ( [BS15a]). En este paper, los autores demuestran que el rango de las curvas elípticas, cuando son ordenadas a menos de isomorfismo y por su altura, es menor o igual a $3/2$. En particular, esto da evidencia de que el rango podría estar acotado uniformemente. El método es una combinación de técnicas de geometría de números, y teoría de invariantes y grupos algebraicos. En primer lugar, usando resultados de Birch, Swinnerton-Dyer, Cremona y Fisher, los autores re-interpretan el problema de conteo para el grupo de Selmer asociado a la isogenía que multiplica por 2 como un problema de conteo de formas cuárticas con varias propiedades. A su vez, este problema se reduce vía la aplicación de técnicas de integración, parametrizaciones y diversas cribas a contar la cantidad de órbitas de formas cuárticas enteras irreducibles de discriminante acotado. Como una forma cuártica está determinada por sus coeficientes, esto es un problema de conteo de puntos enteros en una "caja" - aunque en realidad no estamos tratando con un conjunto compacto, sino con un conjunto que posee partes no acotadas que se van a infinito. Por ende, las técnicas usuales de geometría que dan un estimativo para la cantidad de puntos enteros (en general en función del volumen del compacto) no funcionan. Para salvar esto, los autores utilizan una "técnica de promediado", en la cual, al mover el conjunto a lo largo de un compacto de matrices, las partes largas que van a infinito se hacen "más anchas" y se "truncan", permitiendo aplicar las técnicas usuales.

La importancia del paper de Bhargava y Shankar no solo reviste en el importante resultado, que se conocía sólo para algunos casos y de manera condicional en conjeturas fuertes como la conjetura de Birch y Swinnerton-Dyer, y la hipótesis de Riemann (ver [Bru92], [HB04]), sino que la potencia de las técnicas que desarrollan en el proceso, así como lo innovativo de las mismas, han permitido atacar más problemas de esta índole. En particular, logran revitalizar las estrategias que utilizan teoría de invariantes al soslayar varias de las trabas existentes a llevarlas a cabo. Salvadas estas obstrucciones, dan una estrategia general para este tipo de problema de conteo (siguiendo ideas que también fueron usadas por Bhargava en su tesis de doctorado, ver [Bha04a] y sus tres partes siguientes). La estrategia se puede definir brevemente como la idea de transformar problemas aritméticos en problemas de conteo de objetos asociados a la teoría de invariantes, y atacar estos con diversas técnicas. En general, uno tiene una familia de estructuras aritméticas y la acción de un grupo algebraico permite parametrizarlas. Debe ocurrir que las órbitas de la acción estén capturando el fenómeno que se quiere estudiar, y que la acción tenga propiedades buenas (como ser corregular o "aritmética"). Si esto se cumple, el problema es ahora un problema de estimar órbitas, que en general se realiza con geometría de números. Hay otras formas de realizar esta parte del procedimiento: con métodos geométricos como cribas o el método de Bombieri-Pila (ver sección 5 y sección 7); con métodos proviniendo de la teoría de representaciones (ver [Tho13], [RT20]); en el caso de cuerpos de números en general, con una combinación de estos métodos, al aparecer espacios pre-homogéneos (ver [BG12]).

La organización de la tesis sigue el paper de Bhargava–Shankar, aunque con cambios de orden en la presentación de los temas, con excepción de las secciones 2 y 7, que no aparecen en dicho trabajo. Por otro lado, varias secciones han sido ampliadas con conocimiento necesario para leerlas tal y como aparecen en el paper. Asumimos conocimientos básicos de curvas elípticas, como pueden encontrarse en el capítulo 3 del libro de Silverman [Sil09]. En la sección 2 se presentan los rudimentos de la teoría cohomológica de una curva elíptica en grado 0 y 1, en aras de definir el grupo de Selmer. En la sección 3 se desarrolla la teoría de invariantes necesaria para atacar el problema, manteniendo el espíritu clásico de la misma. También se expone su relación con el grupo de Selmer. En la sección 4 se realiza el conteo de formas cuárticas bajo la acción del grupo general

lineal y se prueba un teorema de cambio de variable que permite calcular densidades locales y globales. En la sección 5 se expone el teorema de conteo uniforme. Esta es una de las etapas más delicadas del paper y una de las innovaciones más importantes, y se realiza mediante un argumento de criba llamado "embedding sieve". En la sección 6 se finaliza la prueba, usando la maquinaria desarrollada previamente. Es importante usar que el número de clase del grupo general lineal es 1. Aprovechamos esta propiedad para dar una introducción a los grupos algebraicos y la aproximación fuerte. En esta sección, también mencionamos brevemente conjeturas y heurísticas sobre el rango de las curvas elípticas. En la sección 7 exponemos algunos resultados parciales en otro problema de aritmética estadística. Con esto, la filosofía de parametrización y conteo se hace visible nuevamente, mostrando que las técnicas, por más avanzadas y fuertes, todavía están en su infancia, y queda mucho por hacer.

No hay pretensiones de originalidad en cuanto al contenido matemático de esta tesis; sí la hay en la autoría y en la organización del contenido, así como en algunas variaciones ínfimas de ciertas demostraciones (aunque cabe notar que el argumento utilizando la fórmula ambigua del número de clases no aparece en el paper [BST+20], pero el uso de alguna forma de teoría de género es implicado por el lenguaje de los autores).

# 2. Grupos de Selmer de curvas elípticas

## 2.1. Cohomología de Galois

Comencemos describiendo brevemente la cohomología de Galois en grados 0 y 1 de una curva elíptica, siguiendo el libro de Silverman [Sil09]. Sea $G$ un grupo finito. Un **$G$-módulo** es un grupo abeliano $M$ equipado con una acción a derecha de $G$ que conmuta con la suma. Si $M, N$ son $G$-módulos, un **morfismo de $G$-módulos** es un morfismo de grupos $M \to N$, que es $G$-equivariante. La cohomología de grupos nos da invariantes para entender nuestros espacios.

**Definición: 2.1.** El **0-ésimo grupo de cohomología de $G$ sobre $M$** es

$$H^0(G, M) = \{m \in M : m^g = m \ \forall g \in G\}.$$

Observar que el funtor $H^0(G, -)$ no es exacto a derecha. La obstrucción a la exactitud es el primer grupo de cohomología:

**Definición: 2.2.** Los **1-cociclos para $G$ sobre $M$** son las funciones

$$Z^1(G, M) = \{\xi : G \to M | \xi_{gh} = \xi_g^h + \xi_h\}.$$

Los **1-cobordes para $G$ sobre $M$** son las funciones

$$B^1(G, M) = \{\xi : G \to M | \text{ existe } m \in M \text{ tal que } \xi_g = m^g - m\}.$$

El **primer grupo de cohomología de $G$ sobre $M$** es

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}.$$

Tenemos la familiar sucesión exacta larga en cohomología:

**Teorema: 2.3.** *Sea*

$$0 \to M \to N \to P \to 0$$

*una sucesión exacta corta de $G$-módulos. Luego, hay una sucesión exacta larga*

$$0 \to H_0(G, M) \to H_0(G, N) \to H_0(G, P) \to \\ \to H_1(G, M) \to H_1(G, N) \to H_1(G, P).$$

El mapa $\delta : H_0(G,P) \to H^1(G,M)$ se llama **morfismo de conexión**. Podemos definirlo explícitamente de la siguiente manera: sean $\phi : N \to P$ y $\psi : M \to N$, sea $m \in H^0(G,P)$. Como $N \to P$ es suryectiva, hay un $n \in N$ tal que $\phi(n) = m$. Notar que $\phi(n^g - n) = \phi(n)^g - \phi(n) = m^g - m = 0$ para todo $g$, con lo cual $n^g - g \in Ker(\phi)$. Por exactitud de la sucesión de arriba, $n^g - n$ está en la imagen de $P$ en $M$. Como $\psi$ es una inyección, es una biyección a su imagen y podemos definir

$$\delta'(m) = \xi,\ \xi_g = \psi^{-1}(n^g - n).$$

Observar que, llamando $\rho = \psi^{-1}$, $\rho$ es equivariante, pues $\psi(\rho(m)^g) = (\psi\rho(m))^g = m^g$, tal que tomando $\rho$ se sigue lo dicho. En particular,

$$\xi_{gh} = \rho(n^{gh} - n) = \rho(n^g)^h - \rho(n) = \rho(n^g - n)^h + (\rho(n^h - n)) = \xi_g^h + \xi_h,$$

así que esto en efecto es un cociclo. Definimos $\delta(m)$ como la clase en cohomología de $\delta'(m)$.

Para extender esta definición al caso Galois infinito, involucramos consideraciones topológicas. Sea $K$ un cuerpo perfecto y $G := Gal(\overline{K}/K)$. Al ser un grupo profinito, tiene una topología inducida. Un $G$-módulo será un grupo abeliano $M$ con topología discreta, sobre el cual $G$ actúa continuamente con las topologías definidas. Definimos $H^0(G,M)$ análogamente, mientras que $H^1(G,M)$ serán las imágenes de cociclos continuos, módulo cobordes. En este caso, también recuperamos la sucesión exacta larga en cohomología.

## 2.2. Grupos de Selmer

Sea $K$ un cuerpo de números y sea $E$ una curva elíptica sobre $K$. Sea $\phi$ una isogenía no nula de $E$ en $E'$. Hay una sucesión exacta corta

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0,$$

donde denotamos $E[\phi]$ a $Ker\ \phi$. En general, si $M$ es un grupo abeliano y $\phi$ un morfismo que sale de $M$, notamos $M[\phi]$ a $Ker\ \phi$. Tomando cohomología de Galois, obtenemos la sucesión exacta larga en cohomología:

$$\begin{aligned} 0 \to E(K)[\phi] \to E(K) \to E'(K) \to \\ \to H^1(G_K, E[\phi]) \to H^1(G_K, E) \to H^1(G_K, E'), \end{aligned}$$

donde identificamos los $H^0$ con los puntos $K$-racionales y $G_K$ es el grupo de Galois absoluto de $K$, es decir, $Gal(\overline{K}/K)$. El morfismo

$$E'(K) \to H^1(G_K, E[\phi])$$

es el morfismo de conexión.
Haremos uso de un resultado homológico elemental.

**Proposición: 2.4.** *Sea*

$$0 \to A \to B \xrightarrow{f} C \xrightarrow{\delta} D \xrightarrow{g} E \xrightarrow{l} F$$

*sucesión exacta en la categoría de grupos abelianos. Luego,*

$$0 \to \frac{C}{Im\ f} \xrightarrow{\delta} D \to Ker\ l \to 0$$

*es sucesión exacta corta, donde los mapas son los inducidos.*

De especial interés es tomar $E' = E$ y $\phi = [m]$, el mapa multiplicar por $m$. La sucesión exacta larga pasa a una sucesión exacta corta:

$$0 \to \frac{E(K)}{mE(K)} \to H^1(G_K, E[m]) \to H^1(G_K, E)[m] \to 0,$$

donde $H^1(G_K, E)[m]$ es el kernel de la restricción de $[m]$ a la cohomología. Una forma de estimar $E(K)/mE(K)$ viene dada por estimar $H^1(G_K, E[m])$. Para aproximar la imagen de $E(K)/m(E(K))$ en $H^1(G_K, E[m])$ utilizaremos consideraciones locales.
Sea $M$ el conjunto de lugares de $K$. Para cada $v \in M$, fijemos una extensión $v$ a $\overline{K}$ y por ende un embedding $\overline{K} \to \overline{K_v}$, donde $K_v$ es la completación de $K$ bajo $v$. El embedding nos dota de un morfismo restricción de grupos de Galois $G_{K_v} \to G_K$ y de un mapa restricción del grupo de descomposición $G_v \to G_{K_v}$ ( [Ser79], I.7). Las restricciones pasan a la cohomología y tenemos un diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \longrightarrow & H^1(G_K, E[\phi]) & \longrightarrow & H^1(G_K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E'(K_v)/\phi(E(K_v)) & \longrightarrow & H^1(G_{K_v}, E[\phi]) & \longrightarrow & H^1(G_{K_v}, E)[\phi] & \longrightarrow & 0 \end{array} .$$

Especializando al caso $\phi = [m]$,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E[m]) & \longrightarrow & H^1(G_K, E(\overline{K}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_v)/mE(K_v) & \longrightarrow & H^1(G_{K_v}, E[m]) & \longrightarrow & H^1(G_{K_v}, E(\overline{K}))[m] & \longrightarrow & 0 \end{array}.$$

Observar que esto vale para cada lugar $v$. Si notamos $E[m]$ tanto a $E(\overline{K})[m]$ como a $E(\overline{K_v})[m]$, mientras que $E_v := E(\overline{K_v})$, tomando límite en $v$ se tiene:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E[m]) & \longrightarrow & H^1(G_K, E(\overline{K}))[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_{v\in M} E(K_v)/mE(K_v) & \to & \prod_{v\in M} H^1(G_{K_v}, E[m]) & \to & \prod_{v\in M} H^1(G_{K_v}, E_v)[m] & \to & 0 \end{array}.$$

Haremos las siguientes definiciones:

- El $m$**-grupo de Selmer** $Sel^m(E/K)$ de $E$ es el kernel del mapa inducido
$$H^1(G_K, E(\overline{K})[m]) \to \prod_{v\in M} H^1(G_{K_v}, E(\overline{K_v}));$$
- El **grupo de Tate-Shafarevich** de $E$ es $Ш(E/K)$, el kernel del mapa inducido
$$H^1(G_K, E(\overline{K})) \to \prod_{v\in M} H^1(G_{K_v}, E(\overline{K_v})).$$

Con estas definiciones, tenemos la sucesión exacta corta:

$$0 \to \frac{E(K)}{mE(K)} \to Sel^m(E/K) \to Ш(E/K)[m] \to 0. \tag{1}$$

Ya en este paso podemos ver que el grupo de Selmer controla el rango de la curva elíptica, en conjunto con el grupo de Shafarevich. En particular, controla a $E(K)/mE(K)$. La demostración del teorema de Mordell-Weil (ver [Sil09], VIII, o bien [JHS15], capítulo 3, para una versión sobre $\mathbb{Q}$), nos

dice que los generadores de la parte libre de $E$ se hallan levantando generadores en ese grupo cociente, sumando posiblemente finitos puntos. Por ende, el tamaño de $E(K)/mE(K)$ está controlado por el del grupo de Selmer, y el defecto en esta inyección es el Ш. Sin embargo, este último grupo es muy difícil de entender, por lo cual el posible algoritmo para calcular el grupo de puntos racionales de $E$ (ver [Sil09], capítulo X) no funciona siempre (es más, no es ni siquiera claro que termine en tiempo finito).

El grupo de Selmer $Sel^2(E/\mathbb{Q})$ es un 2-grupo elemental abeliano. Como tal, está bien definida su dimensión sobre $\mathbb{F}_2$, que denotamos $r_2$. Notamos, en general, $r_p$ a la dimensión de un $p$-grupo sobre $\mathbb{F}_p$. Sea $r(G)$ el rango del grupo $G$. Por la sucesión exacta corta (1), se tiene que

$$r_2(Sel^2(E)) = r_2(E(K)/2E(K)) + r_2(Ш(E/K)[2]).$$

Por el teorema de Mordell-Weil y el teorema de estructura para grupos abelianos, $E(K)$ se escribe como una suma de grupos abelianos, los cuales en la parte de torsión se ven de la forma $\mathbb{Z}/p^i\mathbb{Z}$. En aquellos factores en que $p$ sea impar, multiplicar por 2 es una suryección, pues no hay elementos de orden 2. Por ende,

$$r_2(Sel^2(E)) = r(E(\mathbb{Q})) + r_2(E(\mathbb{Q})[2]) + r_2(Ш(E)[2]).$$

Ahora bien,

$$\#Sel^2(E) = 2^{r_2(Sel^2(E))} \geq 2r_2(Sel^2(E)),$$

así que tenemos que

$$r(E(\mathbb{Q})) + r_2(E(\mathbb{Q})[2]) + r_2(Ш(E)[2]) \leq \frac{\#Sel^2(E)}{2}.$$

En particular, el tamaño promedio de cada uno de los sumandos está acotado por el tamaño promedio del grupo de 2-Selmer, sobre 2. Probaremos que el tamaño es 3, así que obtenemos la cota de $3/2$ para el promedio del rango de las curvas elípticas. Por otra parte, obtenemos también que el tamaño promedio de la 2-torsión del grupo de Tate-Shafarevich es $\leq 3/2$.

## 2.3. Cubrimientos localmente solubles y el grupo de Weil-Châtelet

En esta sección comentamos la interpretación de la cohomología en grado 1 de una curva elíptica como espacios geométricos asociados a la

curva. La principal referencia es la sección X.3 de [Sil09]. Sea $E/\mathbb{Q}$ una curva elíptica sobre $\mathbb{Q}$. Un **espacio homogéneo** para $E$ es una curva $C/\mathbb{Q}$, definida sobre $\mathbb{Q}$, sobre la cual $E$ actúa algebraica y transitivamente. Como tal, existe un mapa algebraico racional $\mu : C \times E \to C$ que cumple que, si $\mathcal{O}$ es el neutro de $E(\mathbb{Q})$ y si llamamos $\mu((c, P)) = c + P$:

- $c + \mathcal{O} = c$;
- $(c + P) + Q = c + (P + Q)$;
- Para todo $c \in C$, para todo $l \in C$, existe un único $P \in E$ tal que $c + P = d$.

Decimos que dos espacios homogéneos son **equivalentes** y notamos $C \sim C'$ si existe un isomorfismo de curvas $C \to C'$ que está definido sobre $\mathbb{Q}$ y es equivariante para la acción de $E$. Como $E$ actúa por traslaciones sobre sí mismo, es un espacio homogéneo. Llamamos a $[E]_\sim$ la **clase trivial**. Observar que si $C$ está en la clase trivial, tiene un punto racional, puesto que $E$ lo tiene. Y, dada cualquier curva $C$ que es un espacio homgéneo de $E$ con un punto racional, $C \sim E$. Denotemos

$$WC(E/\mathbb{Q}) := \{C : C \text{ es un espacio homogéneo para } E\}/\sim .$$

Lo llamamos **grupo de Weil-Châtelet**. Tenemos el siguiente:

**Teorema: 2.5** ( [Sil09], X.3, Teorema 3.6)**.** *Hay una biyección natural*

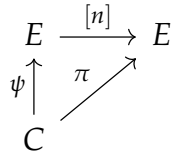
$$WC(E/\mathbb{Q}) \longleftrightarrow H^1(G_{\mathbb{Q}}, E),$$

*donde la clase de la curva $C$ es enviada a la clase del cociclo $[\xi_\sigma \to c^\sigma - c]$ para una elección de $c \in C$.*

Observar que, entonces, por cómo definimos el grupo $Ш(E)$, el grupo de Weil-Châtelet $WC(E/\mathbb{Q})$ contiene a todos los espacios homogéneos localmente solubles de $E$. Es decir, **podemos ver a los elementos del grupo de Tate-Shafarevich como espacios sobre los que $E$ actúa, y que tienen un punto en cada completación**.

Hay una noción muy relacionada que es la de **cubrimiento** de $E$. Sea $n \geq 1$. Un **$n$-cubrimiento** de $E$ es un par $(C, \pi)$, con $C$ una curva proyectiva suave y $\pi : C \to E$ un mapa definido sobre $\mathbb{Q}$, tal que $\pi$ se factoriza por la

multiplicación por $n$: hay mapas $\psi : C \to E$, $\phi : C \to E$, que verifican que el triángulo




conmuta, $\psi$ es un isomorfismo sobre $\mathbb{C}$ y $\phi$ está definida sobre $\mathbb{Q}$. Dos $n$-cubrimientos son equivalentes si son isomorfos sobre $\mathbb{Q}$ vía un isomorfismo que conmuta con los mapas $C \to E$. Observar que un $n$-cubrimiento es un espacio homogéneo para $E$. Lo que probaremos en la última subsección de la sección 3 es que los elementos de Selmer están parametrizados por cubrimientos con $n = 2$ y localmente solubles.

# 3. Formas cuárticas binarias

En esta sección describimos lo necesario de la teoría de formas cuárticas binarias para llevar a cabo el argumento de Bhargava–Shankar. Nos concentramos en ser concretos y en mantener el espíritu con el que la teoría de invariantes se desarrolló, para mostrar que el área de esta tesis es actual, pero con raíces que provienen desde hace más de un siglo. Seguimos el libro de Hilbert, [Hil06], y por lo tanto las formas cuárticas las tomaremos con coeficientes involucrando números combinatorios. Sin embargo, en futuras secciones dejaremos esta convención. Dado que estamos sobre $\mathbb{Q}$, confiamos en que el lector podrá adecuar las constantes que aparecen al pasar de un caso al otro.

Sea $K$ un cuerpo de característica 0. Una **forma cuártica binaria** es un polinomio homogéneo de grado 4 perteneciente a $K[X, Y]$. De ahora en más, hablaremos de formas cuárticas para referirnos a las formas cuárticas binarias. Sea $G$ un subgrupo de matrices de $GL_2(K)$. Hay una acción de $G$ sobre $V$, el conjunto de formas cuárticas, dada por:

$$\gamma \cdot f(x, y) = f((x, y) \cdot \gamma).$$

Nos van a interesar los casos $G = SL_2(K)$ y $G = GL_2(K)$, principalmente. Podemos escribir una forma cuártica general como

$$f = \sum_{i=0}^{4} \binom{4}{i} a_i X^{4-i} Y^i.$$

Llamamos a los $a_i$ los **coeficientes de la forma**. Tenemos la siguiente definición:

**Definición: 3.1.** Sea $f$ una forma cuártica. Un **invariante** para $f$ es un polinomio no nulo $I$ en los coeficientes de $f$, homogéneo, tal que para todo $\gamma \in GL_2(K)$,

$$I(\gamma \cdot f) = (det\ \gamma)^k I(f)$$

Llamamos a $k$ el **peso** de $I$.

Es decir, si tomamos una forma $f$ y una matriz $\gamma$, notando $a_i', 1 \leq i \leq 4$ a los coeficientes de la nueva forma $\gamma \cdot f$, vale que:

$$I(a_1', a_2', a_3', a_4') = (det\ \gamma)^k I(a_1, a_2, a_3, a_4).$$

Llamaremos **invariante**, sin especificar la forma $f$, a los invariantes para todo el espacio de formas cuárticas.
Tenemos también nociones más laxas de invarianza:

**Definición: 3.2.** Un **covariante** para $f$ es un polinomio no nulo y homogéneo $T$ en los 4 coeficientes de $f$ y en $x$ e $y$, tal que

$$T(\gamma \cdot f) = (det\ \gamma)^k T(f),$$

donde estamos aplicando la transformación $\gamma$ tanto a los $a_i$ como a $x$ e $y$.

Es decir, si tomamos una forma $f$ y una matriz $\gamma$, y llamamos como antes $a_i', 1 \leq i \leq 4$ a los coeficientes de la forma transformada $\gamma \cdot f$, mientras que llamamos $x', y'$ a los coeficientes del vector que resulta de aplicar $\gamma$ a $(x, y)$, es decir, de hacer

$$(x, y) \cdot \gamma,$$

tenemos que

$$T(a_1', a_2', a_3', a_4', x', y') = (det\ \gamma)^k T(a_1, a_2, a_3, a_4, x, y).$$

Nos interesa clasificar los invariantes según su grado y según su orden. Sean $l, u \in K$ no nulos. Luego la matriz $\gamma$ diagonal con entradas $(l, u)$ es inversible con determinante $lu$. Si $I$ es un invariante de grado $d$ y orden $k$, podemos escribir $I = \sum_{|\rho|=d} c_\rho X_0^{\rho_0} X_1^{\rho_1} \cdot \cdots \cdot X_4^{\rho_4}$, con $\rho = (\rho_1, \cdots, \rho_4)$ y $|\rho| = |\rho_1| + |\rho_2| + |\rho_3| + |\rho_4|$. Observar que por un lado:

$$I(\gamma \cdot f) = I(a_0 l^4, a_1 l^3 u, a_2 l^2 u^2, a_3 l u^3, a_4 u^4) = \sum_{|\rho|=d} c_\rho \prod_{i=0}^{4} a_i^{\rho_i} l^{(4-i)\rho_i} u^{i\rho_i},$$

lo cual es igual a

$$\sum_{|\rho|=d} c_\rho \prod_{i=0}^{4} a_i^{\rho_i} \prod_{i=0}^{4} l^{\rho_i(4-i)} \prod_{i=0}^{4} u^{\rho_i i} = I(a_0, \cdots, a_4) l^{\sum_{i=0}^4 \rho_i(4-i)} u^{\sum_{i=0}^4 \rho_i i}.$$

Por otro lado,

$$I(\gamma \cdot f) = (lu)^k I(a_0, \cdots, a_4).$$

En particular, se sigue que

$$\sum_{i=0}^{4} \rho_i (4-i) = k \tag{2}$$

$$\sum_{i=0}^{4} \rho_i i = k. \tag{3}$$

Sumando las ecuaciones, se observa que

$$\sum_{i=0}^{4} 4\rho_i = 2k.$$

Como $\sum_{i=0}^{4} 4\rho_i = 4\sum_{i=0}^{4} \rho_i$, llegamos a la ecuación fundamental:

$$4d = 2k.$$

En particular, $2d = k$.
Puede verse en ( [Hil06], lecture VII) que vale la siguiente recíproca parcial.
En el teorema que sigue, decimos que un polinomio es **isobárico** si todos sus términos tienen el mismo peso.

**Teorema: 3.3.** *Sea $P$ un polinomio homogéneo e isobárico, que es función de los 5 coeficientes de $f$. Si $P$ satisface la ecuación $4d - 2k = 0$, donde $d = deg\ P$ y $k$ es su peso, luego $P$ es un invariante para $f$ bajo matrices diagonales.*

## 3.1. El operador $D$

Consideremos ahora la matriz

$$\gamma = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}.$$

Decimos que una tal matriz es **de tipo** 2.
Debido a que $\gamma$ tiene determinante 1, debe valer que un invariante cumple

$I(\gamma \cdot f) = I(f)$. Aplicando $\gamma$ tenemos:

$$\begin{aligned}
\gamma \cdot f &= \sum_{i=0}^{4} \binom{4}{i} a_i (X + uY)^{4-i} Y^i = \\
&= \binom{4}{0} a_0 (X^4 + 4uX^3Y + 6u^2X^2Y^2 + 4u^3XY^3 + u^4Y^4) + \\
&+ \binom{4}{1} a_1 (X^3 + 3X^2uY + 3Xu^2Y^2 + u^3Y^3)Y + \\
&+ \binom{4}{2} a_2 (X^2 + 2uXY + u^2Y^2)Y^2 + \binom{4}{3} a_3 (X + uY)Y^3 + \binom{4}{4} a_4 Y^4 = \\
&= \binom{4}{0} a_0 X^4 + \left( \binom{4}{0} 4ua_0 + \binom{4}{1} a_1 \right) X^3Y + \\
&+ \left( \binom{4}{0} 6u^2 a_0 + \binom{4}{1} 3ua_1 + \binom{4}{2} a_2 \right) X^2Y^2 + \\
&+ \left( \binom{4}{0} 4u^3 a_0 + \binom{4}{1} 3u^2 a_1 + \binom{4}{2} 2ua_2 + \binom{4}{3} a_3 \right) XY^3 + \\
&+ \left( \binom{4}{0} u^4 a_0 + \binom{4}{1} u^3 a_1 + \binom{4}{2} u^2 a_2 + \binom{4}{3} ua_3 + \binom{4}{4} a_4 \right) Y^4.
\end{aligned}$$

Podemos reescribir esto en forma canónica como:

$$\begin{aligned}
\gamma \cdot f &= \\
&= \binom{4}{0} a_0 X^4 + \binom{4}{1} (ua_0 + a_1) X^3Y + \binom{4}{2} (u^2 a_0 + 2ua_1 + a_2) X^2Y^2 + \\
&+ \binom{4}{3} (u^3 a_0 + 3u^2 a_1 + 3ua_2 + a_3) XY^3 + \\
&+ \binom{4}{4} (u^4 a_0 + 4u^3 a_1 + 6u^2 a_2 + 4ua_3 + a_4) Y^4. \qquad (4)
\end{aligned}$$

Por otro lado, sea $a_i'$ el coeficiente nuevo de $f$ luego de actuar con $\gamma$. Tenemos la igualdad, uniforme en $u$, $I((a_i)) = I((a_i'))$. Derivando respecto $u$:

$$0 = \sum_{i=0}^{4} \frac{da_i'}{du} \frac{\partial I((a_i'))}{\partial a_i'}.$$

Como se ve de la expresión (4),

$$\frac{da_i'}{du} = i a_{i-1}'.$$

En particular, si $D$ es el operador diferencial

$$D(F) := \sum_{i=1}^{4} i x_{i-1} \frac{\partial F(x)}{\partial x_i},$$

obtenemos la siguiente identidad:

$$D(I(a')) = 0.$$

Esta ecuación es una caracterización parcial de la invarianza para formas con propiedades básicas. Enunciamos a continuación un tal resultado recíproco, que puede verse en ( [Hil06], lecture VIII).

**Teorema: 3.4.** *Sea $P$ un polinomio, que es función de los coeficientes de la forma $f$ y satisface la ecuación $D(P') = 0$. Luego, $P$ es un invariante para $f$ bajo sustituciones de tipo* 2 *(ver inicio de la subsección).*

## 3.2. Número de invariantes

Buscamos los invariantes de grado $d$ y peso $k$ para la familia de todas las formas cuárticas. Es evidente que la suma de invariantes de grado $d$ y peso $k$ tiene grado $d$ y peso $k$, y lo mismo para productos por escalares, con lo cual los invariantes son un espacio vectorial, y por ende nos interesan los invariantes a menos de dependencia lineal. Sea $w(d,k)$ la dimensión del espacio de invariantes. Recordando la identidad fundamental $2d = k$, deducimos que $k$ es par. Para el cómputo de $w(d,k)$ tenemos el siguiente teorema:

**Teorema: 3.5** ( [Hil06], Lecture XVI)**.** *Sea*

$$F(x,y) = \frac{1}{(1-y)(1-xy)(1-x^2y)(1-x^3y)(1-x^4y)}.$$

*Luego, $F$ puede escribirse en potencias de $x$ e $y$, y el coeficiente de la potencia $x^k y^d$ es $w(d,k)$.*

*Demostración.* Observar que a nivel formal

$$\prod_{j=0}^{4} \sum_{i=0}^{\infty} x^{ji} y^i = \prod_{j=0}^{4} \frac{1}{1-x^j y} = F(x,y).$$

Es decir, que el término de $x^d y^k$ se obtiene vía un producto $y^{\rho_0} x^{\rho_1} y^{\rho_1} x^{2\rho_2} y^{\rho_2} \cdots$. En particular,

$$x^k y^d = x^{\sum_{i=0}^{4} i\rho_i} y^{\sum_{i=0}^{4} \rho_i}.$$

Es decir, estamos contando todas las formas de elegir grados de los monomios para que sumen $d$, el grado del invariante, y para que, pesados por $i$, den el orden (recordar la identidad (3)). Esto dice que el término de $x^k y^d$ es $w(d,k)$. □

Un breve cálculo usando esto (ver [Hil06], Lecture XVI), muestra que:

**Corolario: 3.6.** *$w(d,k)$ es el coeficiente de $x^k$ en la expresión en potencias de $x$ de*

$$G(x) = \frac{\prod_{i=1}^{d}(1-x^{4+i})}{\prod_{i=2}^{d}(1-x^i)}.$$

Con esto, estamos en posición de probar el siguiente corolario.

**Corolario: 3.7.** *Las formas cuárticas binarias admiten dos invariantes linealmente independientes que generan el espacio de invariantes para $GL_2(K)$. Los llamamos $I$ y $J$; $I$ tiene grado 2 y peso 4, $J$ tiene grado 3 y peso 6.*

*Demostración.* Tenemos que por la identidad fundamental $2k = d$, se tiene que $w(d,k) = w(d,2d)$. Por otro lado, desarrollando la expresión de $g$ y quedándose con los términos que producen un $x^{2d}$, obtenemos que $w(d,k)$ es el coeficiente de $x^k$ en

$$\frac{1-x^{d+1}-x^{d+2}-x^{d+3}-x^{d+4}}{(1-x^2)(1-x^3)(1-x^4)},$$

es decir, la resta de los coeficientes de $x^{2d}$ en

$$\frac{1}{(1-x^2)(1-x^3)(1-x^4)}$$

y en

$$\frac{x^{d+1}\sum_{i=0}^{3} x^i}{(1-x^2)(1-x^3)(1-x^4)}.$$

En la segunda suma, notar que calcular el coeficiente de $x^{2d}$ es lo mismo que calcular el término de $x^d$ del polinomio dividido $x^d$. Luego, podemos cambiar el segundo polinomio por

$$\frac{x\frac{x^4-1}{x-1}}{(1-x^2)(1-x^3)(1-x^4))} = \frac{x(1-x^4)}{(1-x)(1-x^2)(1-x^3)(1-x^4)} = \\ = \frac{x}{(1-x)(1-x^2)(1-x^3)},$$

y buscar el coeficiente de $x^d$. Por otro lado, el coeficiente de $x^d$ en el polinomio es el mismo que el de $x^{2d}$ al reemplazar todas las $x$ por $x^2$, con lo cual podemos cambiar este último polinomio por

$$\frac{x^2}{(1-x^2)(1-x^4)(1-x^6)}$$

y buscar su coeficiente de $x^{2d}$. En resumen, tenemos que hallar el coeficiente de $x^{2d}$ en la resta

$$\frac{1}{(1-x^2)(1-x^3)(1-x^4)} - \frac{x^2}{(1-x^2)(1-x^4)(1-x^6)} = \\ = \frac{1\cdot(x^3+1)-x^2}{(1-x^2)(1-x^4)(1-x^6)}.$$

Primero estudiemos la expresión:

$$\frac{x^3}{(1-x^2)(1-x^4)(1-x^6)}.$$

Observar que:

$$\frac{x^3}{(1-x^2)(1-x^4)(1-x^6)} = x^3\sum_{i=0}^{\infty}x^{2i}\sum_{j=0}^{\infty}x^{4j}\sum_{l=0}^{\infty}x^{6l} = \\ = \sum_{i=0}^{\infty}x^{2i+1}\sum_{j=0}^{\infty}x^{4j+1}\sum_{l=0}^{\infty}x^{6l+1}.$$

Los términos de esta suma son de la forma $x^\delta$, con

$$\delta = (2i+1)(4j+1)(6k+1) = 2(i+2j+3k+1)+1,$$

así que todos los términos tienen grado impar. Por ende, sólo nos importa

$$\frac{1-x^2}{(1-x^2)(1-x^4)(1-x^6)} = \frac{1}{(1-x^4)(1-x^6)} = \sum_{i=0}^{\infty} x^{4i} \sum_{j=0}^{\infty} x^{6j}.$$

Es decir, hay tantos invariantes como soluciones a la ecuación $4n + 6m = 2d$, o bien, $2n + 3m = d$, en $\mathbb{N}_0$. Si $d = 2$, hay un sólo invariante, digamos $I$. Si $d = 3$, hay también un invariante, digamos $J$. Luego, $I^n J^m$ es un invariante de grado $2n + 3m$, con lo cual hay una biyección entre soluciones de la ecuación previa y monomios en $IJ$.

Resta ver que los monomios de esta forma son linealmente independientes. Para eso, vamos a construir explícitamente $I$ y $J$. Si $d = 2$, $k = 4$. Escribamos $I = \sum_{|\rho|=2} c_\rho \prod_{i=0}^{4} a_i^{\rho_i}$. Como $\rho$ tiene módulo $|\rho| = 2$, las partes homogéneas de $I$ deben ser de la forma $ba_i^2$ o bien $ba_i a_j$, donde $b$ es una constante. Sean $I_1 = ba_i a_j$, $I_2 = ca_v^2$. Luego, el operador $D$ verifica que:

$$D(I_1) = b(ia_{i-1}a_j + ja_{j-1}a_i),$$

y

$$D(I_2) = 2ca_{v-1}a_v.$$

Tomando $b = 1$, $c = 1$, $i = 0$, $j = 4$ y $v = 2$, vemos que $I_1 = a_0 a_4$, $I_2 = a_2^2$ verifican que:

$$D(I_1) = 4a_3 a_0, \tag{5}$$
$$D(I_2) = 4a_1 a_2. \tag{6}$$

Por otro lado, si $I_3 = a_1 a_3$,

$$D(I_3) = a_0 a_3 + 3a_2 a_1.$$

Juntando todo,

$$D(I_1 + I_2 + I_3) = 4a_3 a_0 + 4a_1 a_2 + a_0 a_3 + 3a_2 a_1.$$

Es fácil ver ahora que $I = I_1 + 3I_2 - 4I_3$ cumple que $D(I) = 0$. Es decir, es un invariante para $d = 2$ y $k = 4$.

Si $d = 3$, entonces $k = 6$. Un argumento similar muestra que

$$J = a_0a_2a_4 - a_0a_3^2 - a_1^2a_4 + 2a_1a_2a_3 - a_2^3 = det \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{pmatrix}$$

es un invariante de grado 3 y peso $k$.

Puede verse ahora, tomando una forma sin coeficientes $X^3Y$ y $X^2Y^2$, que $I^n$ y $J^m$ son linealmente independientes, con lo cual los polinomios invariantes están generados por $I^nJ^m$. □

Al invariante $J$ lo llamamos **catalecticante**.

## 3.3. Parametrizando el grupo de Selmer

El Grupo de Selmer controla el rango de la curva elíptica. Para poder atacarlo usando las técnicas de geometría de números, necesitamos algún tipo de parametrización que lo relacione con objetos de la teoría de invariantes. En este caso, el papel lo juegan las formas cuárticas, como se desarrolla en [CF09]. En general, como mencionamos en secciones anteriores, hay varias formas de interpretar la parametrización. El grupo de Selmer se puede interpretar como la familia de clases de equivalencia de cubrimientos localmente solubles de $E$. Los cubrimientos inducen divisores racionals de grado 2, que a su vez inducen cubrimientos que caen en $\mathbb{P}^1$ (ver [Har08], capítulo 4, sección 3). De estos cubrimientos se recuperan las formas cuárticas, a menos de equivalencia. En lo que sigue, damos una exposición más computacional de la parametrización del grupo de Selmer, debida a Cremona y Fisher (y que se complmenta con resultados de Birch y Swinnerton-Dyer).

Sea $K$ un cuerpo de característica 0 (en general, cualquier cuerpo de característica 0 o positiva $\geq 5$ sirve). Sea $f$ una forma cuártica sobre $K$, con coeficientes

$$f(X, Y) = aX^4 + bX^3Y + cX^2Y^2 + dXY^3 + eY^4,$$

(sin usar números combinatorios). Como se desarrolla en la sección anterior, podemos definir los invariantes asociados $I$, $J$, y podemos definir el discriminante $\Delta$:

$$I = 12ae - 3bd + c^2,\ J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3,\ \Delta = \frac{I^3 - 4J^2}{27}.$$

El sistema completo de invariantes y covariantes de una forma cuártica $f$ es conocido (ver [Hil06], lecture XXII; algunas normalizaciones difieren por constantes). En particular, está conformado por - además de la propia $f$ - dos invariantes y dos covariantes. Los invariantes ya los hemos calculado. A continuación definimos los covariantes, el **hessiano** $H$ y el covariante **séxtico** $g_6$:

$$\begin{aligned} H(X,Y) = &(3b^2 - 8ac)X^4 \\ &+ 4(bc - 6ad)X^3Y + 2(2c^2 - 24ae - 3bd)X^2Y^2 \\ &+ 4(cd - 6be)XY^3 + (3d^2 - 8ce)Y^4, \end{aligned}$$

$$\begin{aligned} g_6(X,Y) = &(b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y + \\ &+ 5(8abe + b^2d - 4acd)X^4Y^2 + 20(b^2e - ad^2)X^3Y^3 \\ &- 5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 \\ &- (d^3 + 8be^2 - 4cde)Y^6. \end{aligned}$$

Precisaremos también los llamados **semi-invariantes** de $f$, que se definen de la siguiente forma:

$$\begin{aligned} p &= 3b^2 - ac, \\ r &= b^3 + 8a^2d - 4abc, \\ q &= \frac{1}{3}(p^2 - 16a^2I). \end{aligned}$$

Asociamos a $f$ la cúbica $F(X) = X^3 - 3I(f)X + J(f)$, que llamamos **cúbica resolvente**. Consideremos el álgebra $L$ que viene dada por el cociente

$$K[\varphi] = K[X]/(F).$$

Notar que $L$ está caracterizada por el tipo de descomposición de $f$ en factores irreducibles. Esta descomposición puede ser de tres tipos:

$$\begin{cases} f \sim (1) & \text{si } f \text{ es irreducible,} \\ f \sim (12) & \text{si admite un factor lineal y uno cuadrático,} \\ f \sim (111) & \text{si } f \text{ se parte completamente en } K. \end{cases}$$

Con esta notación, la forma de $L$ es como sigue:

$$\begin{cases} K(\varphi) & f \sim (1), \\ K \times K' & f \sim (12),\ [K' : K] = 2, \\ K \times K \times K & f \sim (111). \end{cases}$$

Fijando un orden de los embeddings $L \to \overline{K}$, obtenemos un orden de las raíces de $F$ y un valor para $\varphi$. Asimismo, obtenemos una función norma $N_{L/K}$ para el álgebra $L$, tal que la norma de $\alpha$ es el determinante de la multiplicación por $\alpha$, $L_\alpha$. Extendemos esta norma por linealidad a un mapa $L[X, Y] \to K[X, Y]$. Notamos

$$L^* = \{l \in L : N_{L/K}(l) \neq 0\}.$$

Definamos ahora $G(X, Y)$ como

$$G(X, Y) = \frac{1}{3}(4\varphi f(X, Y) + H(X, Y)).$$

El invariante que definiremos estará dado a menos de cuadrados de unidades. Para hacer esto, es importante entender cómo se comporta la norma de $G$, para la buena definición. La clave para este cálculo es la existencia de **sizigias** entre los invariantes, covariantes y semi-invariantes, las cuales son relaciones de dependencia polinomial entre ellos. Tenemos el siguiente teorema:

**Teorema: 3.8** ( [Hil06], lecture XXII)**.** *Se tienen las siguientes sizigias:*

$$7r^2 = p^3 - 48Ia^2p - 64Ja^3, \tag{7}$$
$$27g_6^2 = H^3 - 48If^2H - 64Jf^3. \tag{8}$$

Observar que usando esto obtenemos que

$$g_6^2 = \frac{H^3 - 48If^2H - 64Jf^3}{27} = \left(\frac{H}{3}\right)^3 - 3 \cdot \left(\frac{4}{3}\right)^2 \left(\frac{H}{3}\right) - \left(\frac{4}{3}\right)^3 Jf^3.$$

La ecuación $g_6^2 = 0$ es equivalente a la ecuación

$$\lambda^3 - 3 \cdot \left(\frac{4}{3}\right)^2 I\lambda - \left(\frac{4}{3}\right)^3 J = 0,$$

donde $\lambda = \frac{H}{3f}$. Sean $\lambda_1, \lambda_2, \lambda_3$ las raíces de esta ecuación. Observar que por la definición de $F$,

$$\left(-\frac{4}{3}\varphi\right)^3 = -\left(\frac{4}{3}\right)^3 \varphi^3 = -\left(\frac{4}{3}\right)^3 (3I\varphi - J) = 3 \cdot \left(\frac{4}{3}\right)^2 I\left(-\frac{4}{3}\varphi\right) + \left(\frac{4}{3}\right)^3 J,$$

con lo cual

$$\left(-\frac{4}{3}\varphi\right)^3 - 3 \cdot \left(\frac{4}{3}\right)^2 I\left(-\frac{4}{3}\varphi\right) - \left(\frac{4}{3}\right)^3 J = 0.$$

Esto dice que, si $\varphi_1 := \varphi$, $\varphi_2$, $\varphi_3$ son los conjugados de $\varphi$, las raíces $\lambda_i$ que definimos antes coinciden con estos conjugados. En particular, podemos suponer que

$$\lambda_i = -\frac{4}{3}\varphi_i.$$

Ahora bien, del hecho de que $g_6^2$ es equivalente a la ecuación en $\lambda$, se sigue que

$$g_6^2 = (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3) = (H - 3\lambda_1 f)(H - 3\lambda_2 f)(H - 3\lambda_3 f).$$

Reemplazando el valor de $\lambda_i$, arribamos a

$$g_6^2 = \left(H + 3 \cdot \frac{4}{3}\varphi_1 f\right)\left(H + 3 \cdot \frac{4}{3}\varphi_2 f\right)\left(H + 3 \cdot \frac{4}{3}\varphi_3 f\right).$$

Por otro lado, observar que

$$N_{L/K}(G) = \prod_{i=1}^{3} \frac{1}{3}(4\varphi_i f + H) = \frac{1}{27}(H + 4\varphi_1 f)(H + 4\varphi_2 f)(H + 4\varphi_3 f).$$

Concluimos que

$$N_{L/K}(G) = 27 g_6^2.$$

En particular, salvo quizá 6 excepciones correspondientes a las raíces de $g_6$ en $\mathbb{P}^1$ (recordar que $g_6$ es séxtico), $G$ toma valores en $L^*$. Dadas nuestras suposiciones sobre $K$, podemos entonces elegir siempre un $v \in K \times K$ tal que $G(v) \in L^*$.

La siguiente proposición permite definir el invariante que usaremos para caracterizar la equivalencia de formas. La demostración es un cálculo formal que puede hacerse por computadora.

**Proposición: 3.9** ( [CF09], Lema 1). *Existe un polinomio cuadrático* $T \in K[X_1, Y_1, X_2, Y_2]$ *tal que*

$$G(1,0)G(X,Y) = T^2$$

*en* $\overline{K}$. *Explícitamente,*

$$\begin{aligned} 9F(X_1,Y_1,X_2,Y_2) = &(12a\varphi - 24ac + 9b^2 2)X_1^2X_2^2 + \\ &+ (6b\varphi - 36ad + 6bc)X_1X_2(X_1Y_2 + Y_1X_2) + \\ &+ (-2\varphi^2 + 2c\varphi - 9bd + 4c^2)(X_1^2Y_2^2 + Y_1^2X_2^2) + \\ &+ (4\varphi^2 + 8c\varphi - 144ae + 4c_2)X_1Y_1X_2Y_2 + \\ &+ (6d\varphi - 36be + 6cd)Y_1Y_2(X_1Y_2 + Y_1X_2) + \\ &+ (12e\varphi - 24ce + 9d^2)Y_1^2Y_2^2. \end{aligned}$$

Lo anterior permite definir el invariante $z$: para cualquier elección de un par $(x_0, y_0)$ tal que $G(x_0, y_0) \in L^*$, definimos

$$z(f) := G(x_0, y_0) \text{ mód } L^{*2}.$$

Trabajaremos con **doble equivalencia por** $GL_2$ **y** $GL_1$. Mientras que la primera acción es la usual, la de $GL_1$ es

$$\lambda \cdot f(x,y) = \lambda^2 f(x,y).$$

Dado un par $(M, \lambda) \in GL_2 \times GL_1$, notamos $\delta := det(M, \lambda) = det(M \cdot \lambda)$. Una equivalencia doble $f \sim f'$ se dice *propia* si $|det(M, \lambda)| = 1$. El hecho de usar doble equivalencia en vez de equivalencia ordinaria permitirá demostrar más fácilmente el teorema de parametrización. El siguiente teorema muestra que $z$ es constante en las formas con un factor racional:

**Teorema: 3.10.** *Sea* $f$ *con un factor racional. Luego,* $z(f) = 1$.

*Demostración.* Sea $(x, y)$ en $\mathbb{P}^1$ tal que $f(x, y) = 0$. Por el Teorema 3.8, se tiene que

$$H^3 = g_6^2.$$

Por otro lado, puede chequearse que ninguno de los dos es nulo: un cálculo de resultantes muestra que $Res_K(f, H)$, $Res_K(f, g_6)$ son múltiplos escalares de potencias del discriminante. Explícitamente, $Res_K(f, H) = \frac{\Delta^2}{3^2}$, y $Res_K(f, g_6) = \frac{\Delta^3}{3^9}$. En particular,

$$z(f) = G(x, y) = \frac{1}{3}(4\varphi G(x, y) + H(x, y)) = \frac{H(x, y)}{3} \equiv \frac{3g_6^2}{H^2} \equiv 1.$$

□

Afirmamos que vale la vuelta. Primero, observar que si $f \sim f'$,

$$I(f') = \delta^4 I(f),\ J(f') = \delta^6 J(f),\ \Delta(f') = \delta^{12}\Delta(f).$$

Por otro lado, los covariantes se transforman de la siguiente manera:

$$H(f') = \delta^2\lambda^2 M \cdot H(f),\ g_6(f') = \delta^3\lambda^3 M \cdot g_6(f).$$

En particular, los invariantes resultan invariantes para la doble equivalencia propia y el Hessiano verifica que

$$H((M, \lambda) \cdot f) = (M, \lambda) \cdot H(f),$$

si la equivalencia es propia. En particular, si transformamos $f$ por un par propio $(M, \lambda)$, la forma $G(x, y)$ se convierte en

$$(M, \lambda) \cdot G(x, y).$$

Notar que esto dice que **si dos cuárticas son propiamente equivalentes, el invariante** $z$ **vale lo mismo en ellas** (puesto que $z$ no depende del representante y $G$ es enviado a una transformación de sí mismo por $M$ y $\lambda$). En particular, este es un primer paso para probar que $z$ detecta equivalencias. Ahora, probemos la recíproca de la invarianza para formas con un factor racional:

**Proposición: 3.11.** *Todas las formas con invariantes $(I, J)$ y un factor lineal en $K$ son propiamente equivalentes, explícitamente a*

$$g(X, Y) = \frac{1}{27}(27X^3 - 9IXY^2 - JY^3)Y = -\frac{1}{27}Y^4 F\left(-\frac{3X}{Y}\right).$$

*En particular, $f$ tiene un factor racional si y solo si $z = 1$.*

*Demostración.* Consideremos una tal $f$ y $(x_0, y_0)$ el factor racional. Consideramos la matriz

$$M = \begin{pmatrix} x_0 & y_0 \\ 0 & 1 \end{pmatrix},$$

y el escalar $\lambda = x_0^{-1}$. A menos de cambiar la segunda fila de $M$ y el $\lambda$ (recordar que $(x_0, y_0) \in K \times K$), podemos propiamente transformar $f$ por $(M, \lambda)$ y poner $a = 0 \neq b$ (recordar que el primer coeficiente de $M \cdot f$ será $f(e_1 M)$). Cambiando ahora por

$$M = \begin{pmatrix} 1 & 0 \\ -c/3b & 1 \end{pmatrix},$$

podemos suponer que $c = 0$. Utilizando ahora

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix},$$

y $\lambda = \frac{1}{b}$, ponemos $b = 1$. Hasta ahora, $(a, b, c) = (0, 1, 0)$. En particular,

$$f \sim Y(X^3 + dXY^2 + eY^3),\ I = -3d,\ J = -27e.$$

Cambiando por $(3Id, \frac{1}{9})$ se obtiene el resultado. □

**Teorema: 3.12.** *Si $z(f) = 1$, $f$ tiene un factor racional.*

*Demostración.* Supongamos sin pérdida de generalidad que $G(1, 0)$ realiza $z(g)$. Luego, $z = \frac{4a\varphi + p}{3}$, y, como $\phi$ es cúbico, podemos escribir

$$h(Z) = Z^3 - pZ^2 + qZ - r^2$$

al minimal de $z$. Debemos probar que $z$ es un cuadrado en $L$. En particular, esto diría que $h(Z^2)$ se puede partir sobre $K$ como $-h_0(Z)h_0(-Z)$, con $h_0$ cúbica. En efecto, si $z = \omega^2$ y $h_0$ es el minimal de $\omega$, se puede escribir $h_0 = Z^3 + uZ^2 + vZ + r$ (salvo quizá elegir $-\omega$ en lugar de $\omega$). Comparando raíces de $h(Z^2)$ y $- - h_0(Z)h_0(-Z)$ se llega a la identidad. Ahora, se tendrá $v = \frac{1}{2}(u^2 - p)$, y $u$ cumple una ecuación cuártica $g(u) = (u^2 - p) - 8ru - 4q$. Observar que

$$ag(u) = f(u + b, -4a).$$

Si $a \neq 0$, esto completa la demostración, pues $-(u + b)/4a$ es raíz de $g$. Si no, $a = 0$, y $z = b^2$. □

Para probar el teorema de caracterización, citamos dos resultados de [CF09]:

**Proposición: 3.13** ( [CF09], Lema 9)**.** *Sean $f$, $f'$ con iguales invariantes. Supongamos que sus semi-invariantes $r$, $r' \neq 0$. Si $z(f) = z(f')$, $g = pf' - aH'$ tiene un factor racional.*

**Proposición: 3.14** ( [CF09], Lema 10)**.** *Si $f$ y $f'$ tienen los mismos invariantes, $r \neq 0$ y $g = pf - aH'$ tiene un factor racional, $f$ y $f'$ son propiamente equivalentes.*

Con esto, ya estamos en posición de probar uno de los teoremas principales de la sección.

**Teorema: 3.15.** *Sean $f$ y $f'$ con los mismos invariantes. Luego, $z(f) = z(f')$ si y solo si son propiamente equivalentes.*

*Demostración.* La suficiencia es consecuencia del Teorema 3.10 y la discusión posterior. Para la necesidad, por la Proposición 3.11, sabemos que podemos asumir que ninguna tiene un factor racional. Luego, $a$ y $a'$ son no nulos. A menos de equivalencia propia, podemos suponer que $r$, $r' \neq 0$, así que aplicando primero la Proposición 3.13 y luego la Proposición 3.14, vemos que $f$, $f'$ son equivalentes. □

Con lo conseguido hasta ahora tenemos un invariante, $z$, que detecta doble equivalencia propia para formas con invariantes prescriptos $I$, $J$. Sea $E/K$ una curva elíptica, que ponemos en forma

$$E : y^2 = x^3 - 27Ix - 27J.$$

Notar que la 2-torsión de $E$ son aquellos puntos de la forma $(\phi, 0)$, con $\phi$ raíz del polinomio en $x$ que define $E$, así como $\mathcal{O}$, el infinito. Tomemos $\varphi_j$ un conjugado de $\varphi$. Observar que

$$\varphi_j^3 = 3I\varphi_j - J,$$

así que $27\varphi_j^3 = 81I\varphi_j - 27J$. Concluimos entonces que si $\varphi_1 := \varphi$ y $\varphi_2, \varphi_3$ son los conjugados de $\varphi_1$,

$$E[2] = \{\mathcal{O}, (-3\varphi_1, 0), (-3\varphi_2, 0), (-3\varphi_3, 0)\}.$$

Consideremos los siguientes subconjuntos:

- $H \subseteq L^*/L^{*2}$ los elementos de norma un cuadrado;
- $S \subseteq F_K/\sim$, con $F_K$ las formas cuárticas sobre $K$ y $S$ el conjunto de clases propias de formas con invariantes prescriptos $I,\ J$.

Notamos que $H$ es un subgrupo. Tenemos un mapa

$$q : E(K)/2E(K) \to S,$$

dado por

$$\begin{aligned} &\mathcal{O} \mapsto P_K, \\ &(\xi, \eta) + 2E(K) \mapsto g_{\xi,\eta}. \end{aligned}$$

donde $P_K$ es la clase de formas con un factor racional (que ya sabemos que es una sola clase) y

$$g_{\xi,\eta}(X, Y) = X^4 - \frac{1}{6}\xi X^2Y^2 - \frac{1}{27}\eta XY^3 + \frac{1}{432}(-\xi^2 + 36I)Y^4.$$

Un cálculo de invariantes para la forma $g_{\xi,\eta}$ muestra que este mapa está bien definido.

También tenemos un mapa $S \to H$ dado por tomar invariante $z$. Lo que haremos ahora es mostrar cómo construir un mapa que complete el triángulo

$$\begin{array}{ccc} S & \xrightarrow{\quad z \quad} & H \\ {\scriptstyle q}\uparrow & \nearrow_{\delta} & \\ E(K)/2E(K) & & \end{array} \quad . \tag{9}$$

Esto fue hecho por Cassels y lo exponemos a continuación para el caso $K = \mathbb{Q}$, que es el que nos interesa. Seguimos a [Cas91], en específico la lecture 15.

**Teorema: 3.16** (Cassels)**.** *Sea $E/Q$ una curva elíptica definida por $y^2 = f(X)$. Sea $\theta$ la imagen de $X$ módulo $f$, y $L = \mathbb{Q}[X]/(f)$. Recordar que, en base a la factorización de $f$ en $\mathbb{Q}[X]$, el álgebra $L$ es un producto de finitos cuerpos, los cuales son extensiones simples, cuadráticas o cúbicas de $\mathbb{Q}$. Existe entonces un homomorfismo de grupos*

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xrightarrow{\mu} M \hookrightarrow \frac{L^*}{L^{*2}},$$

*donde, si $N$ es la norma del anillo $L/\mathbb{Q}$, $M$ consiste de aquellos elementos cuya norma es un cuadrado.*

*Demostración.* Sea $\mu : E(\mathbb{Q}) \to M$ dado por:

- Si $P = \mathcal{O}$, $\mu(P) = \overline{1}$;
- Si $P = (a, b)$ y $b \neq 0$, $\mu(P) = a - \theta$;
- Si $E$ tiene 2-torsión racional no trivial, procedemos de la siguiente forma: sabemos que existe $P = (a, 0)$ en $E(\mathbb{Q})$ y, pasando este elemento por el isomorfismo de $L$ al producto de cuerpos, en la coordenada correspondiente a $f(a) = 0$ hay una copia de $\mathbb{Q}$, que se anula al enviar $\theta \to a$. Reemplazamos ese 0 por un elemento cualquiera de $\mathbb{Q}^*$ que verifique que el nuevo elemento de $L$ está en $M$. En particular, si $E$ tiene dos puntos de 2-torsión, ponemos el discriminante de la ecuación que define la raíz no racional de $f$, y si tiene 4 puntos de 2-torsión, ponemos el producto de las otras dos raíces.

Sean $P$, $Q$, $R$ puntos de $E(\mathbb{Q})$. Supongamos que $P + Q + R = 0$ y que los tres puntos no son 2-torsión. Son entonces colineales y podemos tomar una recta $y = mx + b$ que pase por ellos. Escribamos $P = (a, b)$, $Q = (c, d)$ y $R = (e, f)$. Tenemos que el polinomio $G(X) = F(X) - (mX + b)^2$ se anula en $a, c, e$, con lo cual podemos escribir:

$$F(X) = (mX + b)^2 + (X - a)(X - c)(X - e).$$

Evaluando en $\theta$,

$$0 = (m\theta + b)^2 + (\theta - a)(\theta - c)(\theta - e).$$

Tomando módulo $L^*/L^{*2}$, se obtiene que

$$1 = \overline{(m\theta + b)^2} = \mu(P)\mu(Q)\mu(R).$$

Como al pasar al cociente los números se identifican con sus inversos, concluimos que $\mu(P)\mu(Q) = \mu(R)$.
En particular, tomando $R = -(P + Q)$ y notando que $\mu$ actúa igual en $P$ y en $-P$, obtenemos que es homomorfismo.

Si exactamente uno es torsión, digamos $R = (a_1, 0)$, con $a_1$ raíz racional de $F$, tenemos que

$$L = K_1K_2K_3 \cong \mathbb{Q}K_2K_3,$$

donde alguno de los $K_2, K_3$ posiblemente no aparece. Como las otras coordenadas no son torsión, el argumento anterior vale para $K_2$ y $K_3$, mientras que, por la definición de $\mu$, las normas son siempre un cuadrado, así que el lema vale para $K_1$.

Si toda la 2-torsión es racional, $L \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$. Observar que

$$(\theta - a_1) \to (0, a_2 - a_1, a_3 - a_1),$$

así que $\mu$ tomará el valor $\tau := (a_2 - a_1)(a_3 - a_1)$. Ahora bien,

$$N_{L/\mathbb{Q}}(\tau) = N_{L/\mathbb{Q}}(a_2 - a_1)N_{L/\mathbb{Q}}(a_3 - a_1) = F(a_1)^2 \equiv 0.$$

Concluimos así que $\mu$ es un morfismo.

Por otro lado, es evidente ahora que $2E(\mathbb{Q}) \subseteq Ker\ \mu$. Afirmamos que vale la otra contención. Si $\mu(a) \equiv 0$ en $(\mathbb{Q}^*[\theta])^2$, escribamos

$$a - \theta = (p_2\theta^2 + p_1\theta + p_0)^2.$$

Como $[L : \mathbb{Q}] = 3$, $p_0 \neq 0$. Escribiendo

$$(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) = r_1\theta + r_2,\ s_i, r_i \in \mathbb{Q},$$

podemos suponer que $s_1 \neq 0$ (pues $p_0 \neq 0$) y por ende que $s_1 = -1$. Ahora, al elevar al cuadrado,

$$(s_0 - \theta)^2(a - \theta) = (r_1\theta + r_0)^2.$$

Sea $G(X) = (r_1X + r_0)^2 - (s_0 - X)^2(a - X)$. Observar que $G(\theta) = 0$, $G$ es mónico y $G$ tiene grado 3. Luego, $G = F$. Se sigue que

$$F(X) = (r_1X + r_0)^2 - (s_0 - X)^2(a - X),$$

y que, si consideramos $L : Y = r_1X + r_0$, $L$ es una línea racional y corta $Y^2 = F(X)$ en los siguientes puntos: $(a, \pm b)$, $(s_0, t)$, $(s_0, t)$. Por Bézout, debe haber una repetición, y, por ende, $(a, b)$, $(s, t)$, $(s, t)$ están en la misma línea, así que

$$(a, b) + 2(s, t) = \mathcal{O},$$

con lo cual $(a, b) \in 2E(\mathbb{Q})$. □

Hecho esto, demostraremos el teorema central de esta sección. Decimos que una forma cuártica sobre $K$ es **$K$-soluble** si la ecuación $z^2 = f(x,y)$ tiene una solución $(x,y,z)$ en $K$ con $(x,y) \neq (0,0)$.

**Teorema: 3.17** (Parametrización del grupo $Sel^2(E)$, [CF09], Teorema 13)**.**

1. *Tenemos que el triángulo de* (9) *conmuta, y que todas las flechas son inyectivas;*

2. *La imagen de $q$ son las clases que se pueden representar por formas $K$-solubles;*

3. *La imagen de $z$ consiste en clases que se pueden representar por elementos de $L$ en $< 1, \varphi >$.*

*Demostración.*

1. Es evidente que $z$ es inyectivo pues distingue equivalencia propia. Por otro lado, $q$ también lo es, comparando coeficientes mixtos. Si vemos que $\delta$ es la composición a nivel mapas de conjuntos de $z$ y $q$, también será automáticamente inyectivo. Notar que para cada $(\xi, \eta)$,

$$z(q(\xi,\eta)) = \frac{4\varphi g(1,0) + H(1,0)}{3} = \frac{4\varphi + p}{3},$$

   y observar que esto es

$$z(g) = \frac{4\varphi + \frac{8}{6}\xi}{3} = \frac{2^2}{3^2}(3\varphi + \xi).$$

   En particular, $\delta = z \circ q$;

2. El coeficiente principal de $q(P)$ es un cuadrado, así que es soluble. Si $g$ es soluble pero no tiene una raíz $K$-racional, a menos de equivalencia podemos asumir que $a = 1$ y $g$ es mónica; además, podemos poner $b = 0$. Definiendo $\xi = -6c$, $\eta = -27d$, entonces se tiene $q(\xi,\eta) = g$;

3. Observar que $z$ se representa por un elemento en el subespacio generado por 1 y $\varphi$ por definición. Recíprocamente, si $z = u + v\varphi$ tiene

norma cuadrado $N = r^2$, tenemos dos casos: si $v = 0$, $z$ es un cuadrado y proviene de cualquier cuártica con un factor lineal racional. Si $v \neq 0$, ponemos

$$g(X,Y) = \frac{1}{12v}(X^4 - 6uX^2Y^2 + 8rXY^3 + (12Iv^2 - 3u^2)Y^4).$$

Luego, $z(g) = \frac{1}{v^2}(u + v\varphi)$.

□

Concluimos la sección con el Teorema 3.2 de [BS15a], en el cual la primera afirmación se deduce del Teorema 3.17, y la segunda se puede ver en [CF09, Sección 5, Remark 1].

**Teorema: 3.18.** *Sea $K$ un cuerpo con char $K = 0$ o char $K \geq 5$. Sea*

$$E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$$

*una curva elíptica sobre $K$. Hay una biyección*

$$q : \frac{E(K)}{2E(K)} \to S,$$

*donde $S$ es el conjunto de $PGL_2(K)$-órbitas de formas cuárticas $K$-solubles con invariantes $I$, $J$. El elemento identidad del dominio va a la clase de formas con un factor lineal en $K$. Más aún, cualquier forma $f$ en $V_K$ con discriminante no nulo e invariantes $(I, J)$ cumple que*

$$Stab_{PGL_2(K)}(f) \cong E(K)[2],$$

*con $E : x^3 - \frac{I}{3}x - \frac{J}{27}$.*

## 3.4. Elementos del grupo de Selmer como formas localmente solubles

Sea $E$ una curva elíptica. Podemos escribirla a menos de cambios que preservan la forma de Weierstrass como

$$y^2 = x^3 + Ax + B,$$

donde si un primo $p$ verifica que $p^4|A$, será entonces $p^6 \nmid B$. Sean los invariantes $I(E) = -3A$ y $J(E) = -27B$. La altura tradicional de $E = E_{A,B} = E^{I,J}$ se define como $\max(4|A|^3, 27B^2)$. En [BS15a], se usa la altura $H(E) = \max(|I(E)|^3, J(E)^2/4)$, que difiere de la altura tradicional por un factor racional positivo.

En [BSD63], se consideran 2-cubrimientos: curvas $C$ tales que admiten mapas $\psi : C \to E$, $\phi : C \to E$, que verifican que el triángulo

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ {\scriptstyle\psi}\uparrow & \nearrow_{\phi} & \\ C & & \end{array}$$

conmuta, $\psi$ es un isomorfismo sobre $\mathbb{C}$ y $\phi$ está definida sobre $\mathbb{Q}$. Tenemos que $\phi$ induce un mapa de divisores de grado 2 de $C$ a $E$, definido sobre $\mathbb{Q}$. El contenido del Lema 1 de [BSD63] es que si $C$ es localmente soluble, podemos hallar un divisor en $C$ que es positivo y con grado 2. Esbozamos el argumento: el mapa de divisores anterior preserva el grupo de clases de divisores. En particular, la fibra del punto en infinito $\mathcal{O}$ se parametriza por una curva de género 0, que, como $C$ es localmente soluble, tiene puntos en todas las completaciones. Por local-global, la curva tiene un punto racional, y el divisor asociado a este punto es positivo de grado 2.

Ahora bien, recordemos el teorema de Riemann-Roch: sea $C$ una curva algebraica, $D$ un divisor en $C$ y

$$L(D) := \{h : D + div(h) \geq 0\} \cup \{0\},$$

donde $h$ son funciones racionales en $C$. Luego, tenemos que:

**Teorema: 3.19** (Riemann-Roch, [Mil20a], Teorema 4.5)**.** *Consideremos $l(D) := dim_K\, L(D)$ y sea $g$ el género de $C$. Luego,*

$$l(D) \geq deg\ D + 1 - g.$$

*Si $deg\ D > 2g - 2$, vale el igual.*

Aplicándolo al caso de $C$ un 2-cubrimiento y $D$ un divisor racional sobre $C$ de grado 2, hallamos una función no constante $x$ con $div\ x > -D$.

Aplicándolo a $2D$, existe una función $v$ tal que $div\ v > -2D$, y $v \notin < 1, x, x^2 >$. Notar que $l(4D)$ es de dimensión 8, y además que

$$< 1, x, x^2, x^3, x^4, v, xv, x^2v, v^2 > \subseteq L(4D).$$

Por ende, son linealmente dependientes. Como $1, x, x^2, v$ son linealmente independientes, $v \notin \mathbb{Q}(X)$, y $v^2$ aparece en la dependencia lineal. Escribamos

$$\alpha + \beta x + \gamma x^2 + \delta x^3 + \epsilon x^4 + \eta v + \mu v^2 + \nu xv + \rho x^2 v = 0.$$

Podemos reescribir esta igualdad como

$$v^2 - 2v\left(\frac{\rho}{2}x^2 + \frac{\nu}{2}x + \frac{\eta}{2}\right) = \alpha + \beta x + \gamma x^2 + \delta x^3 + \epsilon x^4.$$

Sea $y := v - \frac{\rho}{2}x^2 - \frac{\nu}{2}x - \frac{\eta}{2}$, que no es constante. Se tiene que:

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e, \tag{10}$$

con $a, b, c, d, e \in \mathbb{Q}$. Como el cuerpo de funciones de $C$ es cuadrático sobre $\mathbb{Q}(x)$, debe ser igual a $\mathbb{Q}(x, y)$, lo cual dice que podemos tomar $C$ como la dada por la ecuación (10).

Si tomamos una curva dada por una cuártica $g$ como antes, por ( [Mil20a], Proposición 4.10), esta curva define un cubrimiento de su Jacobiana. Dos tales curvas $g$, $g'$ definen el mismo cubrimiento si son $\mathbb{Q}$-biracionalmente equivalentes y dicha equivalencia biracional preserva 2-torsión. Tal mapa existe siempre y cuando existan $\alpha, \beta, \gamma, \delta, \epsilon$ racionales con

$$g(x) = \epsilon^2(\gamma x + \delta)^4 g'\left(\frac{\alpha x + \beta}{\gamma x + \delta}\right).$$

Notar que esto dice que $g$ y $g'$ son doble equivalentes.

El desarrollo anterior implica que los cubrimientos provienen de formas cuárticas de la forma (10), y que una curva dada por una cuártica

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e,$$

es un cubrimiento doble de su Jacobiana $E : y^2 = x^3 - 27Ix - 27J$. El paso que nos falta es tener una noción de *forma reducida* que permita contar las formas. Podemos suponer que $g$ tiene coeficientes enteros, a menos

de cambiar sus invariantes por $n^4I$, $n^4J$, y podemos suponer, a menos de transformaciones que preservan la forma de Weierstrass de $E$, que $I$, $J$ están en forma minimal, es decir, que si un primo $p$ verifica que $p^4|I$, entonces será $p^6 \nmid J$. Tenemos el siguiente lema de Birch y Swinnerton-Dyer, que nos indica que podemos reducir fácilmente salvo que precisemos potencias de 2 y 3.

**Lema: 3.20** ( [BSD63], Lema 3)**.** *Supongamos que $g$ está dada por coeficientes enteros y tiene invariantes $I$ y $J$. Si $p > 4$ es un primo tal que $p^4|I$, $p^6|J$ y $g$ es localmente soluble (es decir, $y^2 = g(x)$ tiene solución en todas las completaciones de $\mathbb{Q}$), existe una forma $f$ doble equivalente a $g$ tal que es entera y sus invariantes son $Ip^{-4}$ y $Jp^{-6}$.*

La prueba es un cálculo elemental, separando en casos.
Tenemos el análogo para $p = 2$ y $p = 3$, cuyas demostraciones también son un cálculo como el anterior:

**Lema: 3.21** (p = 3)**.** *Si $3^5|I$ y $3^9|J$ y $g$ tiene un punto en $\mathbb{Q}_3$. Luego, hay una $f$ entera, doble equivalente a $g$, con invariantes $I \cdot 3^{-4}$ y $J \cdot 3^{-6}$.*

**Lema: 3.22** (p = 2)**.** *Si $2^6|I$ y $2^9|J$ y $2^{10}|(8I + J)$, y $g$ tiene un punto en $\mathbb{Q}_2$, hay una $f$ entera, doble equivalente a $g$, con invariantes $I \cdot 2^{-4}$ y $J \cdot 2^{-6}$.*

Notar que dijimos que podemos suponer que $g$ tiene coeficientes enteros a menos de cambiar sus invariantes por potencias cuartas y sextas de enteros. Por ende, primero podemos usar el lema para $p \neq 2, 3$, y suponer que, si los invariantes de $g$ son $m^4I$, $m^6J$, no hay ningún $p$ en $m$. Como $3|I(E)$ y $27|J(E)$, si $3|m$, $3^5|I$ y $3^9|J$, así que $g$ es doble equivalente a una forma entera cuyos invariantes no son divisibles por 3. Por último, si $4|m$, por el lema para $p = 2$ podemos ir sacando potencias pares de 2 de $m$, tal que, al final, $g$ es doble equivalente a una forma cuártica entera con invariantes $2^4I$, $2^6J$. Combinando el Teorema 3.18 y los Lemas 3.20, 3.21 y 3.22, y reintepretando la doble equivalencia como equivalencia bajo $PGL_2$, obtenemos el Lema 3.4 de [BS15a] y el Teorema 3.5 de [BS15a].

**Lema: 3.23.** *Toda forma cuártica $g$ racional localmente soluble con invariantes enteros $I$, $J$ tal que $2^4 \cdot 3|I$ y $2^6 \cdot 3^3|J$ es $PGL_2(\mathbb{Q})$-equivalente a una forma cuártica entera.*

**Teorema: 3.24** (Parametrización de $Sel^2(E)$)**.** *Sea $E = E^{I,J}$ una curva elíptica sobre $\mathbb{Q}$. Hay una biyección entre $Sel^2(E)$ y las clases de $PGL_2(\mathbb{Q})$-equivalencia de formas cuárticas localmente solubles enteras con invariantes $2^4I$ y $2^6J$.*

Usando el Teorema 3.18, tenemos que bajo esta correspondencia, aquellas formas con un factor lineal racional e invariantes $2^4 I$ y $2^6 J$ se corresponden con la clase de la identidad del grupo de Selmer.

# 4. Conteo de las formas cuárticas binarias

## 4.1. Preliminares sobre medidas de Haar

Sea $G$ un grupo topológico. Una **medida de Haar a izquierda** en $G$ es una medida no nula, Borel regular e invariante por traslación a izquierda. Recordemos el teorema de Haar (ver [Coh10], Teorema 9.2.2):

**Teorema: 4.1.** *Sea $G$ un grupo topológico localmente compacto. Existe una medida de Haar (izquierda) en $G$, y es única a menos de multiplicar por una constante.*

Sea $\mu$ una medida de Haar en $G$. Como es Borel, para cualquier compacto $Z \subseteq G$, $\mu(Z)$ es un número real. Luego, fijado un compacto $Z$ tal que $\mu(Z) := C > 0$, podemos normalizar $\mu$ vía definir una nueva medida de Haar $\nu := \mu/C$ que verifica $\nu(Z) = 1$. Vamos a utilizar este tipo de normalizaciones para construir una medida de Haar en un producto de grupos de matrices.

### 4.1.1. Medida de Haar en las unipotentes triangulares

Sea $U$ el grupo de unipotentes triangulares, es decir,

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} : u \in \mathbb{R} \right\}.$$

Notar que $U$ es isomorfo a $(\mathbb{R}, +)$ y admite como medida de Haar la medida de Lebesgue. En general, si $u$ está acotado en algún intervalo cerrado $I$, podemos normalizar la medida para que el volumen de $U$ sea 1 al dividir por $|I|$, la longitud de $I$.

### 4.1.2. Medida de Haar en el toro

Sea $\mathcal{A}$ el grupo de matrices:

$$\mathcal{A} = \left\{ \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} : 0 \neq t \right\}.$$

Notar que $\mathcal{A}$ es isomorfo a $(\mathbb{R}^*, \cdot)$ y admite una medida de Haar proveniente de la medida en $\mathbb{R}^*$. Observar que podemos definir en $\mathbb{R}^*$ la medida

$$\mu(B) = \int_B \frac{dt}{t},$$

donde la integral representa la medida de Lebesgue. Si $c \in \mathbb{R}$, $c \neq 0$, considerar la transformación $F : B \to cB$ que multiplica por $c$. Se tiene:

$$\mu(B) = \int_B \frac{dt}{t} dt = \int_{F(B)} \frac{1}{F(t)} |det\ F| dt = \int_{cB} \frac{1}{ct} c = \int_{cB} \frac{1}{t} dt = \mu(cB),$$

con lo cual $\mu$ es una medida de Haar en $\mathbb{R}^*$ (y por ende en $\mathcal{A}$).

### 4.1.3. Medida de Haar en los grupos ortogonales reales

Sea $K' = O(\mathbb{R})$ y $K = SO_2(\mathbb{R}) = O(\mathbb{R}) \cap SL_2(\mathbb{R})$. Ambos son subespacios de medida compactos de $GL_2(\mathbb{R})$ y $SL_2(\mathbb{R})$, respectivamente, y $GL_2(\mathbb{R})$ se sumerge en $\mathbb{R}^4$, heredando la topología localmente compacta. Por ende admite una medida de Haar. En cada caso, podemos considerar las normalizaciones tal que todo el espacio tiene volumen 1.

### 4.1.4. Medida de Haar en el centro positivo

Sea

$$\Lambda = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda > 0 \right\}$$

el centro con diagonal positiva. Es isomorfo a los reales positivos. La medida de Haar de los reales multiplicativos se restringe e induce una medida de Haar en $\Lambda$.

## 4.2. El dominio fundamental de $GL_2(\mathbb{Z})$ sobre $GL_2(\mathbb{R})$

Para contar las formas cuárticas usaremos lo que se llama **dominio fundamental** para la acción de $GL_2(\mathbb{Z})$ sobre $GL_2(\mathbb{R})$. Seguimos las definiciones de ( [Pla23], capítulo 4).

**Definición: 4.2.** Sea $G$ un grupo actuando a derecha sobre un espacio topológico $A$ como grupo discreto. Un subconjunto abierto $L \subseteq A$ es un **dominio fundamental** para la acción de $G$ sobre $A$ si:

- $\overline{L}G = A$;
- si $g \neq e$, $L \cap Lg = \emptyset$.

Tenemos el siguiente resultado:

**Teorema: 4.3.** *Sean*

$$N' = \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} : u \in \mathbb{R} \right\},$$
$$\hat{A} = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} : t \geq \frac{\sqrt[4]{3}}{\sqrt{2}} \right\}$$
$$\Lambda = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda > 0 \right\}.$$

*y $SO_2(\mathbb{R})$ el grupo especial ortogonal real. Luego, hay un dominio fundamental $\mathcal{F}$ para la acción de $GL_2(\mathbb{Z})$ sobre $GL_2(\mathbb{R})$, de la forma*

$$\mathcal{F} = \left\{ n \cdot \alpha \cdot k \cdot \lambda \mid n = n(u) \in N'(t) \subseteq N', \alpha(t) \in \hat{A}, k \in K, \lambda \in \Lambda \right\},$$

*donde*

$$N'(t) := \left\{ \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} : u \in v(t) \right\},$$

*y $v(t)$ es un intervalo o una unión de dos intervalos dentro de $[-1/2, 1/2]$ en función del valor de $t$.*

**Observación: 4.4.** Cada $t$ induce una correspondiente elección de un rango para $n(u)$, y lo que dirime si $v(t)$ es un intervalo o una unión de intervalos es si $t > 1$ o $t \leq 1$. De la demostración se ve que lo que hemos de mirar es cuando las matrices unipotentes de $N'(t)$ actúan en el semiplano complejo superior enviando $i$ al dominio fundamental de Gauss.

Para demostrar esta proposición, seguimos la estrategia de Aaron Landesman en sus notas [Lan20]. Primero, un lema ( [Pla23], Proposición 3.12):

**Lema: 4.5** (Descomposición de Iwasawa)**.** *Sean $K = O(2)$ el grupo ortogonal real, $A$ el grupo de diagonales positivas y $N$ las unipotentes triangulares superiores. Luego,*

$$GL_2(\mathbb{R}) = KAN.$$

**Observación: 4.6.**

1. Vía trasponer, tenemos que $GL_2(\mathbb{R}) = NAK$, con $N$ el grupo de unipotentes triangulares inferiores;

2. Tenemos una descomposición

$$SL_2(\mathbb{R}) = N(A \cap SL_2(\mathbb{R}))SO_2(\mathbb{R});$$

3. Supongamos que tenemos una matriz $D$ con diagonal positiva $(a, b)$. Llamando $t = \sqrt{\frac{b}{a}}$, $\lambda = \sqrt{ab} > 0$,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \sqrt{b}\sqrt{a} & 0 \\ 0 & \sqrt{a}\sqrt{b} \end{pmatrix} = \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

Así, usando que las matrices de $\Lambda$ están en el centro de $GL_2(\mathbb{R})$, obtenemos la descomposición

$$GL_2(\mathbb{R}) = N\mathcal{A}K\Lambda.$$

Procedemos a demostrar el Teorema 4.3.

*Demostración del Teorema 4.3.* Basta verlo para $GL_2^+(\mathbb{Z})\backslash GL_2^+(\mathbb{R})$, donde los supra-índices indican determinante positivo. Sea entonces $G = GL_2^+(\mathbb{R})$ el subgrupo de $GL_2(\mathbb{R})$ de matrices con determinante positivo y notar que $GL_2^+(\mathbb{Z})$ no es otra cosa que $SL_2(\mathbb{Z})$. $G$ actúa por transformaciones de Möebius (transpuestas) en el semiplano superior complejo $\mathcal{H}$, y el estabilizador de $i$ es el conjunto de matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ tal que } \frac{ai + c}{bi + d} = i.$$

Multiplicando por $bi + d$, vemos que

$$c + ai = -b + di,$$

así que $c = -b$ y $a = d$. Luego,

$$\begin{pmatrix} d & -c \\ c & d \end{pmatrix} = \begin{pmatrix} c^2 + d^2 & 0 \\ 0 & c^2 + d^2 \end{pmatrix} \begin{pmatrix} \frac{d}{c^2+d^2} & \frac{-c}{c^2+d^2} \\ \frac{c}{c^2+d^2} & \frac{d}{c^2+d^2} \end{pmatrix} \in \Lambda SO_2(\mathbb{R}).$$

Así que $Stab(i) = \Lambda SO_2(\mathbb{R})$. Por estabilizador - órbita,

$$\mathcal{H} \cong_G G/\Lambda SO_2(\mathbb{R}),$$

como $GL_2^+(\mathbb{R})$-conjuntos. Sabemos que la acción $SL_2(\mathbb{Z})$ en $\mathcal{H}$ por transformaciones de Möebius tiene un dominio fudamental dado por (ver [Sil94], Proposición 1.5)

$$\mathcal{G} = \left\{ z \in \mathcal{H} : |Re\, z| \leq \frac{1}{2},\ |z| \geq 1 \right\}.$$

Para calcular el dominio fundamental de $SL_2(\mathbb{Z})\backslash G$, observar que la acción de $SL_2(\mathbb{Z})$ sobre el semiplano complejo superior se traslada a una acción de $SL_2(\mathbb{Z})$ sobre $GL_2^+(\mathbb{R})/\Lambda SO_2(\mathbb{R})$. Por ende, si ahora tenemos una matriz en $G$, mirando su clase, podemos escribirla como $M \cdot \eta$ con $\eta \in \Lambda SO_2(\mathbb{R})$ y $M \in SL_2(\mathbb{Z})$. Para refinar esto aún más, observar que la matriz

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

se corresponde al complejo $z = a + ib$. Ahora sólo falta enviar, vía $nt \in NA$, a $i$ al dominio fundamental (ver [Mor15], ejemplo 7.2.1). Como

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot i = \begin{pmatrix} t & 0 \\ nt & t^{-1} \end{pmatrix} \cdot i = t^2 i + n,$$

si queremos que esto caiga en el dominio fundamental, debe ser que $|n| \leq \frac{1}{2}$, y que $t^4 + n^2 \geq 1$. Luego,

$$t^4 \geq 1 - \frac{1}{2} = \frac{3}{4},$$

con lo cual $t \geq \sqrt[4]{3}/2$. Una vez que hemos despejado $t$, el $n = n(t)$ se despeja en base al $t$ para que $t^2 i + n$ quede en el dominio fundamental de Gauss ( [Ser73], VII). □

**Observación: 4.7.** Realizando una demostración análoga con la acción ligeramente modificada vía:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{dz + b}{cz + a},$$

(ver, por ejemplo, [Pla23], página 180), obtenemos el mismo resultado que el Teorema 4.3, pero reemplazando $\hat{A}$ por

$$A' = \left\{ \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} : t \geq \frac{\sqrt[4]{3}}{\sqrt{2}} \right\}.$$

De ahora en más, utilizaremos este conjunto, en lugar de $\hat{A}$.

## 4.3. El conteo

Sea $V_{\mathbb{Z}}$ el espacio de formas cuárticas binarias, que puede identificarse con $\mathbb{Z}^5$. En general, notamos $V_R$ al espacio de formas cuárticas sobre un anillo $R$ (usualmente $R = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p, \mathbb{Q}_p$). Sea

$$\Delta(f) = \frac{4I(f)^3 - J(f)^2}{27}$$

el discriminante de la forma cuártica $f$, y sea

$$H(f) = \text{máx}\left(|I(f)|^3, \frac{J(f)^2}{4}\right)$$

la altura de $f$. Si $f$ tiene invariantes $(I, J)$, usualmente escribimos a la altura como $H(f) = H(I, J)$. Nos interesa estudiar **la función de conteo** $N(S,\ X)$, que recibe un subconjunto $GL_2(\mathbb{Z})$-invariante de $V_{\mathbb{Z}}$ y un real $X > 0$, y cuenta la cantidad de clases de $GL_2(\mathbb{Z})$-equivalencia de formas cuárticas binarias de $S$, enteras, irreducibles con altura acotada por $X$. Sea $V_{\mathbb{Z}}^i$ el subconjunto de $V_{\mathbb{Z}}$ de formas con $4 - 2i$ raíces reales en $\mathbb{P}^1_{\mathbb{C}}$. Si $i = 2$, las formas son siempre positivas o siempre negativas, y esto induce una partición de $V_{\mathbb{Z}}^2$ en $V_{\mathbb{Z}}^{2+}$ y $V_{\mathbb{Z}}^{2-}$. La distinción en cuanto las raíces es importante, como muestra el siguiente lema (ver [Cre01], Proposición 7):

**Lema: 4.8.** *Sean $f$ una cuártica y $p = 8ac - 3b^2$, $q = \frac{1}{3}(p^2 - 16a^2I)$ los semiinvariantes de la sección 3. Supongamos que $f$ tiene coeficientes reales y que es separable sobre $\mathbb{Q}$. Luego, podemos clasificar su tipo sobre $\mathbb{R}$ como:*

- *Si $\Delta > 0$, $y\ -p < 0$ o $q > 0$, $g \in V_{\mathbb{R}}^2$;*
- *Si $\Delta > 0$ $y\ -p > 0$ $y\ q < 0$, $g \in V_{\mathbb{R}}^0$;*
- *Si $\Delta < 0$, $g \in V_{\mathbb{R}}^1$.*

*Una vez fijados $I,\ J$, cuando $\Delta > 0$ hay 3 órbitas bajo $SL_2\mathbb{R}$: una para formas siempre positivas, una para formas siempre negativas, y otra para formas indefinidas; Si $\Delta < 0$, hay una sola órbita, en $V_{\mathbb{R}}^1$.*

Para contar las formas usaremos dominios fundamentales para las acciones de $GL_2(\mathbb{R})$ sobre cada $V_{\mathbb{R}}^i$:

**Lema: 4.9.** *La acción $GL_2(\mathbb{R})$ sobre $V_{\mathbb{Z}}^j$, $j \in \{0, 1, 2-, 2+\}$, admite conjuntos fundamentales de representantes (es decir, tienen un representante por cada clase), y en cada uno de ellos los coeficientes de las formas están acotados. Explícitamente:*

- $L^0 = \left\{ x^3y - \frac{1}{3}xy^3 - \frac{J}{27}y^4 : -2 < J < 2 \right\}$;
- $L^1 = L_1^1 \cup L_2^1 \cup L_3^1$, *con*

$$L_1^1 = \left\{ x^3y - \frac{I}{3}xy^3 + \frac{2}{27}y^4 : -1 \leq I < 1 \right\},$$

$$L_1^1 = \left\{ x^3y - \frac{I}{3}xy^3 - \frac{2}{27}y^4 : -1 \leq I < 1 \right\},$$

*y*

$$L_2^2 = \left\{ x^3y + \frac{1}{3}xy^3 - \frac{J}{27}y^4 : -2 < J < 2 \right\};$$

- $L^{2+} = \left\{ \frac{1}{16}x^4 - \frac{\sqrt{2-J}}{3\sqrt{3}}x^3y + \frac{1}{2}x^2y^2 + y^4 : -2 < J < 2 \right\}$;
- $L^{2-} = -L^{2+}$.

**Observación: 4.10.** ¿De dónde salen estos conjuntos? Observar que sabemos que $I(A \cdot f) = (det\ A)^4 I(f)$ y $J(A \cdot f) = (det\ A)^6 J(f)$, así que, por el Lema 4.8, dos formas $f,\ f'$ son equivalentes si y solo si hay un $\lambda > 0$ con $I(f') = \lambda^2 I(f)$, $J(f') = \lambda^3 J(f)$. En particular, como $H(f') = \lambda^6 H(f)$, y como siempre podemos tomar $\lambda$ tal que $H(\lambda^2 I, \lambda^3 J) = 1$, basta, para hallar los $L^i$, tomar una forma $f_{I,J}$ con $H(I, J) = 1$ para cada elección de $I,\ J$ (en base a si $27\Delta = 4I^3 - J^2$ es $< 0$ o $> 0$). Por ejemplo, dados $(I, J)$ con $\Delta < 0$, debe ser que $I^3 < \frac{J^2}{4}$. Luego, supongamos que $H(I, J) = \frac{J^2}{4}$. Pedimos entonces que $J = \pm 2$. Observar que en la expresión de los invariantes

$$I = 12ae - 3bd + c^2, \quad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3,$$

si ponemos $a = c = 0$, tenemos

$$I = -3bd,\ J = -27eb^2.$$

Ahora,

$$\begin{cases} I = -3bd \\ \pm 2 = -27eb^2 \end{cases},$$

de lo cual podmos despejar $\pm\frac{2}{27} = eb^2$. Poniendo $b = 1$, es

$$\begin{cases} I = -3d & , \\ \pm\frac{2}{27} = e & , \\ |I|^3 < \frac{I^2}{4} = 1. \end{cases}$$

De acá se deduce que podemos tomar las formas $x^3y - \frac{I}{3}xy^3 + \frac{\pm 2}{27}y^4$, para $-1 \leq I < 1$, como los miembros de $L^1$ si la altura es $\frac{I^2}{4}$. Los otros casos se deducen de manera análoga. No obstante, observar que estamos usando en este caso que podemos poner $a = 0$ pues $f$ tiene una raíz $(x, 1)$, y podemos transformarla por

$$\begin{pmatrix} x & 0 \\ 1 & 1 \end{pmatrix}$$

para eliminar el primer coeficiente.

Lo siguiente que necesitamos es el tamaño de los estabilizadores de las formas cuárticas. Esto es el contenido del siguiente lema, que probaremos en la sección 5.3.4.

**Lema: 4.11.** *Sea $f \in V^i_{\mathbb{R}}$ con $\Delta(f) \neq 0$. Sea $n_i$ dado por:*

$$\begin{cases} n_0 = n_{2-} = n_{2+} = 4 & , \\ n_1 = 2. \end{cases}$$

*Luego, $\#Stab(f) = 2n_i$.*

**Definición: 4.12.** Si $x,\ x'$ son formas cuárticas, decimos que son equivalentes, y notamos $x \sim x'$, si existe una matriz $\gamma$ tal que $\gamma \cdot x = x'$.

Observar ahora que dada cualquier forma $f \in V_{\mathbb{R}}$, hay una única forma equivalente en $L^i$, $f'$, y una matriz $A$ tal que $A \cdot f = f'$. Por otro lado, hay una única matriz $C \in \mathcal{F}$ tal que existe $B \in GL_2(\mathbb{Z})$ con $BA^{-1} = C$. Luego, $B \cdot f = CA \cdot f = C \cdot f'$, así que $\mathcal{F} \cdot L^i$ es un dominio fundamental para la acción de $GL_2(\mathbb{Z})$ sobre $V_{\mathbb{R}}$. Ahora bien, nuestro interés es contar formas con entradas enteras, en lugar de con entradas reales, y ello requiere entender cuántos representantes tiene cada clase entera en una

clase real. En general, podemos contar incluso moviendo por alguna $h$ fija en $GL_2(\mathbb{R})$; sea $\mathcal{F}h \cdot L^i$, conjunto el cual consideramos como multiset con peso $\omega(x) = \#\{g \in \mathcal{F} : x \in gh \cdot L^i\}$; es decir, es un conjunto pero en el cual *permitimos repeticiones*, y la cantidad de veces que se repite un elemento está dada por el peso $\omega$.

**Lema: 4.13.** *Sea $x \in V_{\mathbb{Z}} \cap \mathcal{F}h \cdot L^i$. Si $x \sim_{\mathbb{Z}} x'$, existe una $g' \in GL_2(\mathbb{R})$, con $x' = g' \cdot x_L$, donde $x_L$ es el único en $h \cdot L^i$ equivalente a $x$.*

*Demostración.* Sean $g' \in \mathcal{F}$, $x'' \in L^i$, $C \in GL_2(\mathbb{Z})$ con $x' = g'h \cdot x''$, $x' = C \cdot x$. Luego, $x$ es equivalente a $h \cdot x''$ vía $C^{-1}g'$. Como $x'' \in L^i$, es $x_L = x''$ y $x' = g' \cdot x_L$. □

**Lema: 4.14.** *Sea $x' \in V_{\mathbb{Z}} \cap \mathcal{F}h \cdot L^i$ y $x' \sim_{\mathbb{Z}} x$. Escribamos $x' = g' \cdot x_L$ y sea $g \in \mathcal{F}$ tal que $x = g \cdot x_L$. Luego, $g$ y $g'$ van a la misma coclase doble en el doble cociente $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})/Stab_{\mathbb{R}}x_L$.*

*Demostración.* Si $x' = g' \cdot x_L$, $x = g \cdot x_L$ y $x' = C \cdot x$, con $C \in GL_2(\mathbb{Z})$, luego $Cg \cdot x_L = g' \cdot x_L$, así que si tomamos $g_0 = g^{-1}C^{-1}g'$, $g_0 \in Stab_{\mathbb{R}}(x_L)$, y $g' = Cgg_0$. □

La cantidad de coclases en la doble coclase de $g'$ es

$$m(x) := \frac{\#gStab_{\mathbb{R}}(x_L)g^{-1}}{\#GL_2(\mathbb{Z}) \cap gStab_{\mathbb{R}}(x_L)g^{-1}} = \frac{\#Stab_{\mathbb{R}}(x)}{\#Stab_{\mathbb{Z}}(x)}.$$

Por ende, obtenemos que:

**Corolario: 4.15.** *La clase de $GL_2(\mathbb{Z})$-equivalencia de $x \in V^i_{\mathbb{R}}$ aparece $m(x)$ veces en $\mathcal{F}h \cdot L^i$.*

Observar que $-I$, $I$ están siempre en $Stab_{\mathbb{Z}}(x_L)$, con lo cual la multiplicidad $m(x)$ cumple que $1 \leq m(x) \leq n_i$. Sin embargo, notar que el conjunto de $x$ tales que $m(x) < n_i$ se contiene en

$$\bigcup_{\gamma \in GL_2(\mathbb{Z})\backslash\{-I,I\}} V_\gamma,$$

donde $V_\gamma$ es el conjunto de formas fijas por $\gamma$, que es una unión numerable de conjuntos de medida cero. Por ende, a menos de medida cero, todos los elementos de $\mathcal{F}h \cdot L^i$ tienen multiplicidad $n_i$, con lo cual, salvo medida cero, $\mathcal{F}h \cdot L^i$ es la unión de $n_i$ dominios fundamentales para la acción de $GL_2(\mathbb{Z})$ sobre $V_{\mathbb{Z}}$. De esa manera, se sigue que:

**Teorema: 4.16.** *$N(V^i_{\mathbb{Z}}, X)$ coincide con la cantidad de formas enteras irreducibles de altura acotada por $X$ de $\mathcal{F}h \cdot L^i$, independientemente de $h$ y salvo en un conjunto de medida nula, donde los puntos con estabilizador de cardinal $2r > 2$ se cuentan pesados por $\frac{1}{r}$.*

La región $\mathcal{F} \cdot L^i$ no es acotada, dada la aparición de factores de potencia positiva de $t$, que pueden tender a infinito. En particular, en dos de las 5 coordenadas, si $t \to \infty$, observamos que la región no está acotada, impidiendo, en principio, usar técnicas de conteo usuales, las cuales están preparadas para lidiar con conjuntos compactos. Para salvar esta obstrucción, analizaremos "truncamientos"del conjunto, lo cual nos permitirá lidiar con lo que en la literatura se conoce como "main body"(la parte acotada donde se concentran las formas irreducibles), mientras que vía un argumento de integración trataremos las partes no acotadas (lo que se conoce como "cusps", que contienen pocas formas tal que $y$ no las divide). A partir de ahora, notamos $R_X(h \cdot L^i)$ a:

$$R_X(h \cdot L^i) = \{w \in \mathcal{F}h \cdot L^i : |H(w)| < X\},$$

para $h \in GL_2(\mathbb{R})$.

### 4.3.1. Formas reducibles

La siguiente proposición nos muestra que en el "main body" la reducibilidad es escasa.

**Proposición: 4.17.** *Sea $\varepsilon > 0$, sea $h \in G_0$, $G_0 \subseteq GL_2(\mathbb{R})$ un compacto fijo. La cantidad de puntos $(a, b, c, d, e)$ enteros en $R_X(h \cdot L^i)$, con $a \neq 0$, que son reducibles sobre $\mathbb{Q}$ es $O_{\varepsilon, G_0}(X^{\frac{2}{3}+\varepsilon})$.*

*Demostración.* Observar que en $Kh \cdot L^i$ (donde recordar que $K = SO_2(\mathbb{R})$), los vectores tienen coordenadas acotadas, pues $K$ es compacto, $h$ está fijo y las formas de $L^i$ tienen coeficientes acotados. Por otro lado, si $x \in hL^i$, dado que los elementos del dominio fundamental $\mathcal{F}$ son de la forma $\gamma = n\alpha k\lambda$, con $n \in N'(t), \alpha \in \hat{A}, k \in K, \lambda \in \Lambda$, se tiene que $det(\gamma) = \lambda^2$. Por lo tanto, para que $x \in R_X(h \cdot L^i)$ debe valer que

$$X > H(nak\lambda x) = \lambda^{24} H(x) \geq \lambda^{24},$$

es decir

$$0 < \lambda < X^{\frac{1}{24}}.$$

Como los coeficientes de las matrices en $N$ están acotados y como para cada forma cuártica $F$ se cumple que la forma $F(t^{-1}x, tx)$ tiene coeficientes $\left(\frac{a}{t^4}, \frac{b}{t^2}, c, t^2d, t^4e\right)$, los coeficientes en $R_X(h \cdot L^i)$ cumplen

$$\begin{aligned} a &= O(\lambda^4) = O(X^{\frac{1}{6}}), \\ b &= O(\lambda^4) = O(X^{\frac{1}{6}}), \\ c &= O(\lambda^4) = O(X^{\frac{1}{6}}). \end{aligned}$$

No tenemos las mismas cotas para las entradas $d$ y $e$ por la presencia de los factores de $t$. Sin embargo, $ad = O(X^{\frac{2}{6}})$, $ae = O(X^{\frac{2}{6}})$ y $bd = O(X^{\frac{2}{6}})$. Luego, si $e = 0$, tenemos $O(X^{\frac{1}{6}})O(X^{\frac{1}{6}})O(X^{\frac{1}{6}})O(X^{1/6+\varepsilon}) = O(X^{4/6+\varepsilon})$ opciones para $(a, b, c, d)$.

Supongamos ahora que $f = (a, b, c, d, e)$ tiene $e \neq 0$ y un factor lineal $px + qy$. Luego, $p|a$ y $e|q$, así que, como la función divisores de $n$ es $O(n^\varepsilon)$, $p = O(X^\varepsilon)$ y $q = O(X^\varepsilon)$. Una vez que elegimos $(a, b, c, d)$, para lo cual tenemos $O(X^{\frac{4}{6}+\varepsilon})$ opciones, hay $O(X^\varepsilon)$ para elegir $p$, $q$, y al evaluar en $(-q, p)$ se despeja $c$ unívocamente. Luego, hay $O(X^{\frac{4}{6}+\varepsilon})$ opciones en este caso.

Supongamos ahora que $f$ tiene dos factores irreducibles y sean $f_0 = pX^2 + qXY + rY^2$, $f_1 = uX^2 + vXY + wY^2$ tales que $f = f_0 f_1$. Luego,

$$f = (pu)X^4 + (pv + uq)X^3Y + (pw + ur + qv)X^2Y^2 + (qw + vr)XY^3 + (rw)Y^4,$$

y como $ae = O(X^{\frac{1}{3}})$, la cantidad de pares de la forma $(a, e)$ es una $O(X^{\frac{1}{3}+\varepsilon})$, pues, si $\alpha = ae$, $\alpha = O(X^{\frac{1}{3}})$, una vez elegido $a$, . Una vez fijados $a, e$, $p$ divide a $a$ y $r$ divide a $e$, con lo cual $a = O(X^\varepsilon)$ y $r = O(X^\varepsilon)$. Luego, $(p, r)$ tiene $O(X^\varepsilon)$ posibilidades. Al despejar, podemos escribir las formas como $f_0 = pX^2 + qXY + rY^2$ y $f_1 = \frac{a}{p}X^2 + sXY + \frac{e}{r}Y^2$, con lo cual nos quedan las ecuaciones:

$$\begin{pmatrix} \frac{a}{p} & p \\ \frac{e}{r} & r \end{pmatrix} \begin{pmatrix} q \\ s \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}.$$

Si la matriz anterior es no-singular, el sistema tiene solución única y, una vez fijados $b,\ d$, los restantes $q,\ s$ quedan automáticamente determinados. Notar que una vez fijados $(a,b,d,e,p,q,r,s)$, $c$ se despeja del resto. Entonces, se estima la cantidad de óctuplas como sigue:

$$\#(a,e,b,c,d,p,r,q,s) = O(X^{\frac{1}{3}+\varepsilon})O(X^{\frac{1}{6}})O(X^{\frac{1}{6}})O(X^{\varepsilon}) = O(X^{\frac{2}{3}+\varepsilon}).$$

Si el sistema es compatible indeterminado, $\frac{ar}{p} - \frac{pe}{r} = 0$. En ese caso, la matriz queda

$$\begin{pmatrix} \frac{a}{p} & p \\ \frac{ar}{p^2} & r \end{pmatrix}.$$

Restando $\frac{r}{p}$ de la primer fila a la segunda, el sistema queda con una fila de ceros y obtenemos que $d = \frac{br}{p}$. Luego, una vez fijado $b$, queda automáticamente determinado $d$. Se calcula entonces que la cantidad de tuplas $(a,b,c,d,e)$ es

$$\#(a,b,c,d,e) = O(X^{\frac{1}{3}+\varepsilon})O(X^{\frac{1}{6}})O(X^{\frac{1}{6}}) = O(X^{\frac{2}{3}+\varepsilon}).$$

□

Además de controlar la reducibilidad en la parte amplia del conjunto, acotemos los estabilizadores grandes. Al igual que con el Lema 4.11, lo probaremos en la sección 5.3.4.

**Lema: 4.18.** *La cantidad de $GL_2(\mathbb{Z})$-órbitas de formas enteras $f$ con $\Delta(f) \neq 0$, $H(f) < X$ y tal que $\#Stab_{\mathbb{Q}}(f) > 2$ es una $O(X^{3/4+\varepsilon})$.*

### 4.3.2. Fórmula de conteo

En esta sección vamos a demostrar una forma general que describe cómo es la función de conteo. Para ello, sea $G$ un subconjunto compacto, semialgebraico (esto es, definido por inecuaciones $\leq$ usando polinomios), $SO_2(\mathbb{R})$ invariante a izquierda, tal que es la clausura de un abierto no vacío y tal que sus elementos tiene determinante mayor a 1, de $GL_2(\mathbb{R})$. Es claro que estos conjuntos existen:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \geq 1,\ a^2 + b^2 + c^2 + d^2 \leq 8 \right\}.$$

Vamos a utilizar este $G$ para realizar la técnica del promedio, la cual, moralmente, "ensancha" las cúspides al pasarlas a lo largo de un compacto fijo con interior no vacío. Para realizar la cuenta, tomaremos una medida de Haar normalizada. Para ver de donde aparece esta medida, seguimos nuevamente a [Lan20]. Sea $SL_2(\mathbb{R})$ parametrizado por coordenadas (cerca de la identidad)

$$(x, y, z) \to \begin{pmatrix} x & y \\ z & \frac{1+yz}{x} \end{pmatrix}.$$

Sea la medida $\omega = \frac{1}{x} dx\ dy\ dz = \frac{1}{x} dx \wedge dy \wedge dz$. Afirmamos que $\omega$ es $SL_2(\mathbb{R})$-invariante.

- Sea
$$A = \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix}$$
y observar que
$$A \begin{pmatrix} x & y \\ z & * \end{pmatrix} = \begin{pmatrix} t^{-1}x & t^{-1}y \\ tz & * \end{pmatrix}.$$
El pullback de la traslación $L_A$ se calcula:
$$L_A^*(\omega) = \frac{t}{x} d(t^{-1}x) \wedge d(t^{-1}y) \wedge d(tz) = \frac{t^{-2}t^2}{x} dx \wedge dy \wedge dz = \omega.$$
Análogamente se calculan los pullbacks por $n \in N, k \in K$;

- Observar que $\omega$ es enviada, vía el mapa de Iwasawa, a $\frac{1}{t^3} dn \wedge dt \wedge dk$. En efecto, cerca de la identidad tenemos coordenadas locales
$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \frac{\cos(\theta)}{t} & -\frac{\sin(\theta)}{t} \\ t\sin(\theta) + \frac{n\cos(\theta)}{t} & * \end{pmatrix}.$$
Es decir, que queremos calcular el pullback de $\omega$ por el mapa $F(x, y, z) = \left(\frac{\cos\theta}{t}, -\frac{\sin\theta}{t}, t\sin\theta + n\frac{\cos\theta}{t}\right)$. Tenemos que
$$F^*\omega = \frac{t}{\cos\theta} d\left(\frac{\cos\theta}{t}\right) \wedge d\left(\frac{-\sin\theta}{t}\right) \wedge d\left(t\sin\theta + \frac{n\cos\theta}{t}\right).$$
Por otro lado,
$$d\left(\frac{\cos\theta}{t}\right) = -\frac{\cos\theta}{t^2}\, dt - \frac{\sin\theta}{t}\, d\theta,$$

mientras que

$$d\left(\frac{-\sin\theta}{t}\right) = \frac{\sin\theta}{t^2}\,dt - \frac{\cos\theta}{t}\,d\theta;$$

por último,

$$d\left(t\sin\theta + \frac{n\cos\theta}{t}\right) =$$
$$= \left(\sin\theta - \frac{n\cos\theta}{t^2}\right)\,dt + \left(t\cos\theta - \frac{n\sin\theta}{t}\right)\,d\theta + \frac{\cos\theta}{t}\,dn.$$

Usando que $\wedge$ es antisimétrico y que $dt \wedge dt = d\theta \wedge d\theta = dn \wedge dn = 0$, se tiene que:

$$F^*\omega = \frac{\cos\theta}{t}\left(\frac{\cos^2\theta\cos\theta}{t^4}dt \wedge d\theta \wedge dn - \frac{\sin^2\theta\cos\theta}{t^4}d\theta \wedge dt \wedge dn\right) =$$
$$= \frac{1}{t^3}dn \wedge dt \wedge d\theta.$$

Como tenemos la siguiente sucesión exacta

$$0 \to SL_2(\mathbb{R}) \to GL_2(\mathbb{R}) \to \mathbb{R}^* \to 0,$$

donde el penúltimo mapa es el determinante, vemos que podemos inducir una medida de Haar en $GL_2(\mathbb{R})$ al mirar $SL_2(\mathbb{R}) \times \mathbb{R}^*$. La medida del toro sabemos que es $\frac{d\lambda}{\lambda}$, donde $d\lambda$ es la medida de Lebesgue de $\mathbb{R}$. Luego, normalizamos la medida de Haar $dh$ en $GL_2(\mathbb{R})$ vía poner

$$dh = t^{-2}\,du\,d^\times t\,dk\,d^\times\lambda,$$

donde $d^\times t = \frac{dt}{t}$ y $d^\times\lambda = \frac{d\lambda}{\lambda}$, mientras que tomamos $dn$ una medida de Haar en $N$ y $dk$ una medida de Haar en $SO_2(\mathbb{R})$ con $Vol(SO_2(\mathbb{R})) = 1$. Por las consideraciones anteriores, esto es una medida de Haar en $GL_2(\mathbb{R})$, y tenemos que para cualquier compacto $G$, $Vol(G) < \infty$.

Para cada $i \in \{0, 1, 2\pm\}$ tenemos que

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{n_i \int_{h\in G} N(V_{\mathbb{Z}}^{(i)}; X)dh}{n_i \int_{h\in G} dh}$$
$$= \frac{\int_{h\in G} \#\{w \in \mathcal{F}h \cdot L^{(i)} \cap V_{\mathbb{Z}}^{(i)Irr} : |H(w)| < X\}dh}{n_i \int_{h\in G} dh},$$

donde el supra-índice $Irr$ representa los elementos irreducibles. Con las normalizaciones anteriores sabemos que

$$n_i \int_{h\in G} dh := C_G(i)$$

es una constante que sólo depende de $G$ e $i$, y es positiva pues $G$ es la clausura de un abierto. El teorema siguiente transforma la integral que define $N(S, X)$ en una integral sobre el dominio fundamental, cuyo integrando cuenta puntos en una región definida en términos de $G$:

**Teorema: 4.19.** *Sea $S \subseteq V_{\mathbb{Z}}^{(i)}$. Luego, se tiene:*

$$C_G(i)N(S, X) = \int_{g\in N'(t)A'\Lambda} \#\{x \in S^{Irr} \cap B\}t^{-2}dnd^{\times}td^{\times}\lambda,$$

*donde $N'(t)$ y $\Lambda$ son como en 4.3, $A'$ como en la Observación 4.7 y $B = B(n, t, \lambda, X)$ es*

$$\left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} g : g \in G \right\} \cdot L^{(i)} \cap \{x \in V_{\mathbb{R}}^{i} : H(x) < X\}.$$

*Demostración.* Sea $x \in V_{\mathbb{R}}^{i}$. Sea $x_L$ el único en $L^i$ que es equivalente a $x$. Luego,

$$\int_{g\in N'(t)A'\Lambda} \#\{x \in S^{Irr} \cap B\}t^{-2}dh =$$
$$= \int_{h\in G_0} \sum_{\substack{x\in S^{irr}, \\ H(x)<X}} \#\{g \in \mathcal{F} : x = gh \cdot x_L\}dh. \tag{11}$$

Si fijamos $l \in GL_2(\mathbb{R})$ tal que $x = lx_L$, estamos contando soluciones en $\mathcal{F}$ a la ecuación $lx_L = ghx_L$. Por ende, si $g_1, \cdots, g_n \in GL_2(\mathbb{R})$ son todas las soluciones a $g_i x_L = x_L$ (recordar que los estabilizadores son finitos por 4.11), como la suma es de soporte finito, tenemos que el último término de (11) es igual a

$$\sum_{\substack{x \in S^{Irr}, \\ H(x)<X}} \int_{h \in G_0} \#\{g \in \mathcal{F} : x = gh \cdot x_L\} dh.$$

Por otra parte,

$$\begin{aligned}\int_{h \in G_0} \#\{g \in \mathcal{F} : x = gh \cdot x_L\} dh = \\ &= \sum_{j=1}^{n} \int_{h \in G_0} \#\{g \in \mathcal{F} : gh = g_j\} = \\ &= \sum_{j=1}^{n} \int_{h \in G_0} \chi_{\mathcal{F}^{-1} g_j}(h) dh.\end{aligned}$$

Lo que buscamos ahora es cambiar el conteo de puntos sobre $\mathcal{F}$, que puede ser complicado, por un conteo de puntos sobre un compacto. Esto involucra un truco integral para mejorar el integrando, pasando a integrar sobre $\mathcal{F}$. Seguimos manejando la suma:

$$\sum_{j=1}^{n} \int_{h \in G_0} \chi_{\mathcal{F}^{-1} g_j}(h) dh = \sum_{j=1}^{n} \int_{h \in G_0 \cap \mathcal{F}^{-1} g_j} dh = \sum_{j=1}^{n} Vol(G_0 \cap \mathcal{F}^{-1} g_j).$$

Usando que $dh$ es de Haar, $Vol(G_0 \cap \mathcal{F}^{-1} g_j) = Vol((G_0 \cap \mathcal{F}^{-1} g_j) g_j^{-1})$, así que

$$\sum_{j=1}^{n} Vol(G_0 \cap \mathcal{F}^{-1} g_j) = \sum_{j=1}^{n} Vol(G_0 g_j^{-1} \cap \mathcal{F}^{-1}) = \sum_{j=1}^{n} \int_{g \in \mathcal{F}} \#\{h \in G_0 : gh = g_j\} dg.$$

Volviendo a incluir la suma en el integrando y recordando la suma que teníamos afuera, vemos que:

$$\int_{g \in N'(t) A' \Lambda} \#\{x \in S^{Irr} \cap B\} dh = \int_{g \in \mathcal{F}} \#\{x \in S^{Irr} \cap g G_0 L^i : H(x) < X\} dh,$$

lo cual es una reformulación del teorema. □

La utilidad de este teorema viene dada por el hecho de que los conjuntos compactos y semialgebraicos son más tratables desde el punto de vista del conteo de puntos. En particular, tenemos la siguiente proposición, probada para el caso de conjuntos de multiplicidad 1 por Davenport en [Dav51]:

**Lema: 4.20** (Davenport). *Sea $R$ un multiset en $\mathbb{R}^n$ acotado, semialgebraico, con multiplicidad máxima $m$, definido por como mucho $k$ desigualdades y donde cada una de dichas desigualdades tiene grado $\leq l$. Luego, si $V(\mathbb{Z}) = R \cap \mathbb{Z}^n$ y $\pi(R)$ es el mayor volumen de una proyección de $R$ a un subespacio coordenado dado por poner $n-d$ coordenadas cero, $0 < d < n$,*

$$\#V(\mathbb{Z}) = Vol(R) + O(\text{máx}(1, \pi(R))),$$

*donde la $O$ depende de $n, m, k, l$.*

Vamos a aplicar esto a la región $B(n,t,\lambda,X)$. Sea $C$ tal que $C^4$ acota las coordenadas de todas las formas en $G_0 \cdot L^i$. Si llamamos a los coeficientes de $f$ como $a_1 = a,\ a_2 = b, \cdots, a_5 = e$ y tomamos $a_{i_1}, \cdots, a_{i_j}$, $i_j$ coeficientes entre los $a, b, c, d, e$, tenemos que el volumen de la proyección a esas coordenadas es $O\left(\lambda^{4j} \prod_{k=1}^{j} t^{2i_k - 6}\right)$. En particular, una vez que $t$ es una $O(\lambda)$, $t$ está acotado por arriba y por abajo, con lo que, a menos de una constante, el menor límite es $a$. Se sigue que la cantidad de puntos enteros en $B$, cuando $t$ está acotado, es

$$Vol(B) + O(\text{máx}(1, \lambda^{16} t^4)).$$

Con esto, tenemos:

**Proposición: 4.21.** *El número de puntos enteros $(a,b,c,d,e)$ en $B(n,t,\lambda,X)$ con $a \neq 0$ es 0, si $C\lambda < t$, y es $Vol(B(n,t,\lambda,X)) + O(\lambda^{16} t^4)$ en caso contrario.*

*Demostración.* Sólo basta notar que si $C\lambda < t$, como $0 \leq |a| = O(\frac{C^4 \lambda^4}{t^4})$, debe ser $a = 0$. □

Entonces, en $NA\lambda G_0^{Irr} \cdot L^i \cap \{H(x) < X\}$, tenemos que $0 < \lambda < X^{\frac{1}{24}}$ y, como $a \neq 0$, debe ser que $t \leq C\lambda$, y $\lambda \geq \frac{\sqrt[4]{3} C^{-1}}{\sqrt{2}}$. Se sigue que:

$$N(V_{\mathbb{Z}}^i,\ X) = \frac{1}{C_G(i)} \int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{\frac{1}{24}}} \int_{\frac{\sqrt[4]{3}}{\sqrt{2}}}^{C\lambda} \int_N (Vol(B) + O(t^4 \lambda^{16}))dh + O(X^{\frac{3}{4}+\varepsilon}),$$

donde el error aparece debido a que contamos las formas reducibles y las formas de estabilizador grande al utilizar el lema de Davenport. Calculando, vemos que:

$$\int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{1/24}} \int_{\frac{\sqrt[4]{3}}{\sqrt{2}}}^{C\lambda} \int_N O(\lambda^{16} t^4) dh = O(X^{\frac{3}{4}}),$$

mientras que

$$\frac{1}{C_G(i)} \int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{\frac{1}{24}}} \int_{\frac{\sqrt[4]{3}}{\sqrt{2}}}^{C\lambda} \int_N Vol(B) dh =$$
$$\frac{1}{C_G(i)} \left( \int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{\frac{1}{24}}} \int_{\frac{\sqrt[4]{3}}{\sqrt{2}}}^{\infty} \int_N Vol(B) dh - \int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{\frac{1}{24}}} \int_{C\lambda}^{\infty} \int_N Vol(B) dh \right).$$

Usando que en la primera integral estamos multiplicando por $\mathcal{F}$ a todo $G_0 L^i$, mientras que el volumen de $B$ se puede acotar de manera burda por $O(\lambda^{20})$, esto es:

$$\frac{1}{C_G(i)} \left( \int_{G_0} Vol(R_X(h \cdot L^i)) Vol(G_0) + O\left( \int_{\frac{\sqrt[4]{3}}{C\sqrt{2}}}^{X^{\frac{1}{24}}} \int_{C\lambda}^{\infty} \int_N O(\lambda^{20}) \right) \right),$$

lo cual evalúa a

$$\frac{Vol(R_X(h \cdot L^i))}{n_i} + O(X^{\frac{3}{4}}).$$

Obtenemos entonces el siguiente teorema (notar que el volumen de $R_X(h \cdot L^i)$ no depende de $h$):

**Teorema: 4.22.** *Tenemos que, para cada $i \in \{0, 1, 2-, 2+\}$,*

$$N(V^i_{\mathbb{Z}}, X) = \frac{Vol(R_X(L^i))}{n_i} + O(X^{\frac{3}{4}+\varepsilon}).$$

### 4.3.3. Cálculo del volumen I

Sólo resta calcular el volumen de $R_X(L^i)$ para tener una fórmula para la función de conteo. Para ello vamos a interpretar la acción en términos

de $PGL_2$. Como multiplicar por elementos del centro no afecta las clases proyectivas, consideremos el conjunto $R^i = \Lambda L^i$. Observar que, para cada $(I, J)$, estos conjuntos tienen un representante con invariantes $(I, J)$ (distinguiendo el caso $\Delta(I, J) > 0$ o $< 0$). Sea $R^i(X) = \{x \in R^i : H(x) < X\}$. Consideremos la acción de $GL_2(\mathbb{R})$ en $V(\mathbb{R})$ dada por

$$\gamma \cdot f(x, y) = \frac{f((x, y)\gamma)}{det^2(\gamma)}.$$

Observar que si $\lambda \in \mathbb{R}$,

$$(\lambda\ Id) \cdot f(x, y) = \frac{\lambda^4 f(x, y)}{\lambda^4} = f(x, y),$$

así que el centro actúa trivialmente y la acción pasa a $PGL_2(\mathbb{R})$. Sea $\pi : GL_2(\mathbb{R}) \to PGL_2(\mathbb{R})$ la proyección.

**Observación: 4.23.**

1. $\pi(\mathcal{F})$ es un dominio fundamental para la acción de $PGL_2(\mathbb{Z})$ sobre $PGL_2(\mathbb{R})$;
2. $\pi(\mathcal{F})R^i(X) = R_X(L^i)$.

Usando esto, tenemos que **podemos calcular el volumen de $R_X(L^i)$ vía calcular el volumen de** $\pi(\mathcal{F})R^i(X)$, que es la imagen de $\pi(\mathcal{F}) \times R^i(X)$ por el mapa $(\gamma, x) \to \gamma \cdot x$. Más aún, podemos identificar

$$R^i = \{(I, J) \in \mathbb{R}^2 : \Delta(I, J) < 0\}$$

si $i \neq 1$,

$$R^1 = \{(I, J) \in \mathbb{R}^2 : \Delta(I, J) > 0\},$$

con lo cual heredan la medida de Lebesgue de $\mathbb{R}^2$. Por otro lado, sea $\omega$ una forma de volumen para $PGL_2(\mathbb{R})$. Nuestro objetivo es recuperar el volumen de $\pi(\mathcal{F})R^i(X)$ vía un cambio de variables.

## 4.4. Teorema de cambio de variables

En esta sección exponemos el teorema de cambio de variables que es usado a lo largo del paper de Bhargava y Shankar.

**Teorema: 4.24** ( [BS15a, Proposición 3.10]). *Sea $R \subseteq \mathbb{C}^2$ un abierto y $s : R \to V_{\mathbb{C}}$ tal que es continua y, para cada $(I_0, J_0)$, $I(s_{I_0,J_0}) = I_0$, $J(s_{I_0,J_0}) = J_0$. Luego, existe $\mathcal{J} \in \mathbb{Q}$, no nulo, tal que para toda $\phi : V_{\mathbb{C}} \to \mathbb{R}$ medible,*

$$\int_{v \in PGL_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = |\mathcal{J}| \int_R \int_{PGL_2\mathbb{C}} \phi(g \cdot s_{I,J}) \omega(g) dI dJ, \tag{12}$$

*donde consideramos a $PGL_2(\mathbb{C}) \cdot s(R)$ como multiset.*

*Demostración.* Supongamos que $s$ es analítica. Por el teorema de cambio de variables,

$$\int_{v \in PGL_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = \int_{(I,J)} \int_{PGL_2(\mathbb{C})} \mathcal{J}_s(g, I, J) \phi(g \cdot s_{I,J}) \omega(g) dI dJ.$$

El objetivo es ver que $\mathcal{J} = \mathcal{J}_s(g, I, J)$, el jacobiano del mapa

$$(\gamma, (I, J)) \mapsto \gamma \cdot s_{I,J},$$

es constante.

- Independencia de $g$: sean $g_1, g_2 \in PGL_2(\mathbb{C})$ con $\mathcal{J}_s(g_1, I, J) \neq \mathcal{J}_s(g_2, I, J)$. Por continuidad y dado que $\omega$ es invariante, hay un $B$ abierto que contiene a $g_1$ tal que

  $$\int_B \mathcal{J}_s(g, I, J) dI dJ \neq \int_{g_2 g_1^{-1} B} \mathcal{J}_s(g, I, J) dI dJ.$$

  Ahora, usando continuidad en $(I, J)$, existe $N \subseteq R$ tal que

  $$\int_N \int_B \mathcal{J}_s(g, I, J) \omega(g) dI dJ \neq \int_N \int_{g_2 g_1^{-1} B} \mathcal{J}_s(g, I, J) dI dJ.$$

  Usando la igualdad (12), obtenemos que

  $$Vol(B \cdot N) \neq Vol(g_2 g_1^{-1} B \cdot N).$$

  Pero esto es imposible, pues el mapa $g_2 g_1^{-1} : V_{\mathbb{C}} \to V_{\mathbb{C}}$ preserva volumen.

- Independencia de $s$: Cualquier otra función $s'$ que cumple las mismas condiciones verifica que $PGL_2 \cdot s(R)$ es el mismo multiset que $PGL_2 \cdot s'(R)$. En particular, si tomamos $g_{I,J}$ tal que $g_{I,J} \cdot s_{I,J} = s'_{I,J}$ para cada $I, J$,

$$\int\limits_{v \in PGL_2(\mathbb{C}) \cdot s'(R)} \phi(v)dv = \int\limits_{v \in PGL_2(\mathbb{C}) \cdot (R)} \phi(v)dv =$$
$$= \int\int \mathcal{J}_s(I,J)\phi(g \cdot s_{I,J})\omega(g)dIdJ,$$

  y esto es, por invarianza de $\omega$,

$$\int\int \mathcal{J}_s(I,J)\phi(gg_{I,J} \cdot s_{I,J})\omega(g)dIdJ = \int\int \mathcal{J}_s(I,J)\phi(g \cdot s'_{I,J})\omega(g)dIdJ.$$

  Como $s'$ es localmente analítica, por el teorema de cambio de variable usual debe ser que $\mathcal{J}_{s'}(I,J) = \mathcal{J}_s(I,J)$.

- Independencia de $(I,J)$: esto lo haremos en dos partes. Primero notar que ahora la elección de $s$ es arbitraria. En particular, tomando una $s$ tal que $s_{I,J}$ tiene por coeficientes polinomios racionales en $I, J$ (como por ejemplo $s_{I,J} = x^3y - \frac{I}{3}xy^3 - \frac{J}{24}y^4$), tenemos que $\mathcal{J}(I,J)$ se calcula como un determinante con entradas en $\mathbb{Q}[I,J]$, así que $\mathcal{J}(I,J) \in \mathbb{Q}[I,J]$. Notar que no es cero, tomando $\phi \equiv 1$ en (12).
  Para ver que $\mathcal{J}(I,J) \in \mathbb{Q}$, tomemos $G_0 \subseteq PGL_2(\mathbb{C})$ acotado, con $Vol(G_0) = 1$. Sea $R_0$ acotado medible en $\mathbb{C}^2$. Entonces,

$$Vol(G_0 \cdot s(R_0)) = \int\limits_{G_0 \cdot s(R_0)} dv = \int\limits_{G_0}\int\limits_{R_0} \mathcal{J}(I,J)dIdJ.$$

  Si $c \in \mathbb{C}$,

$$\int\limits_{cG_0 \cdot s(R_0)} dv = |c|^5 \int\limits_{G_0 \cdot s(R_0)} = |c|^5 \int\limits_{R_0} \mathcal{J}(I,J)dIdJ,$$

  pues $V_{\mathbb{C}}$ es 5-dimensional. Asimismo,

$$\int\limits_{cG_0 \cdot s(R_0)} dv = \int\limits_{G_0 \cdot cs(R_0)} dv = \int\limits_{(c^{-2}I, c^{-3}J)} \mathcal{J}(I,J)dIdJ =$$
$$= \int\limits_{(I',J')} |c^5|\mathcal{J}(c^2I, c^3J)dIdJ.$$

Entonces, para todo $c \neq 0$,

$$|c|^5 \int\limits_{(I,J)\in R_0} \mathcal{J}(I,J) = \int\limits_{(I,J)\in R_0} |c^5|\mathcal{J}(c^2 I, c^3 J).$$

Esto es imposible para un polinomio racional, salvo que sea constante.
Finalmente, concluimos usando Stone-Weierstrass.

□

En general, el teorema vale cambiando $\mathbb{C}$ por $\mathbb{R}, \mathbb{Z}_p$ y tomando el valor absoluto correcto para $J$. Respecto a dicho valor, nos resta calcularlo y eso es el motivo de la siguiente sección.

## 4.5. Cálculo de $J$

Vamos a calcular el valor de $J$, el jacobiano constante del cambio de variable previo. La estrategia es calcularlo en cada lugar $p$-ádico, para luego recuperarlo en la parte arquimediana vía la fórmula del producto. Más específicamente, en cada lugar $p$ vamos a tomar un conjunto $S_p$ y despejar $|J|_p$ usando el teorema de cambio de variable. Esto se logra con el siguiente lema:

**Lema: 4.25.** *Sea $p$ un primo y sea $S \subseteq V_{\mathbb{Z}_p}$ un conjunto definido por condiciones de congruencia módulo $p$. Sea $T \subseteq V_{\mathbb{F}_p}$ la proyección de $S$ módulo $p$. Supongamos que si $\pi$ es tal que $\pi(f) = (I(f), J(f))$, luego $S = \pi^{-1}\pi(S)$. Tenemos que:*

$$|J|_p = \frac{\#PGL_2(\mathbb{F}_p) \cdot \left( \sum\limits_{f \in PGL_2(\mathbb{F}_p)\backslash T} \frac{1}{\#Aut_{\mathbb{F}_p}(f)} \right) dIdJ}{p^5 \cdot Vol(PGL_2(\mathbb{Z}_p)) \left( \int\limits_{(I,\ J)\in\pi(S)} \sum\limits_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{PGL_2(\mathbb{Z}_p)}} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} dIdJ \right)}. \quad (13)$$

*Demostración.* Usando el teorema de cambio de variable para la indicadora

de $S$, $\chi_S$, se tiene que

$$Vol(S) = |J|_p Vol(PGL_2(\mathbb{Z}_p)) \left( \int\limits_{(I,J)\in\pi(S)} \sum_{f\in\frac{V_{\mathbb{Z}_p}(I,J)}{PGL_2(\mathbb{Z}_p)}} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} dIdJ \right).$$

Observar que $S$ está definido por condiciones de congruencia módulo $p$, así que también

$$Vol(S) = \frac{\#T}{p^5}.$$

Por la ecuación de clases para $T$ actuando sobre $PGL_2(\mathbb{F}_p)$, obtenemos que

$$\#T = \#PGL_2(\mathbb{F}_p) \left( \sum_{f\in PGL_2(\mathbb{F}_p)\backslash T} \frac{1}{\#Aut_{\mathbb{F}_p}(f)} \right),$$

completando la demostración del lema. □

Sólo queda elegir ahora los conjuntos $S = S_p$ para cada $p$. Necesitamos un lema acerca de la elegibilidad de pares $(I, J)$, es decir, *qué pares pueden ser invariantes de formas*. Lo probaremos en la sección 5.3.4.

**Lema: 4.26** (Elegibilidad)**.** *Los $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ elegibles son unión de coclases de $9\mathbb{Z} \times 27\mathbb{Z}$. Más específicamente, $(I, J)$ ocurre como los invariantes de una forma cuártica entera si y solo si cumple alguna de las siguientes condiciones de congruencia:*

1. $I \equiv 0(3)$ *y* $J \equiv 0(27)$;
2. $I \equiv 1(9)$ *y* $J \equiv \pm 2(27)$;
3. $I \equiv 4(9)$ *y* $J \equiv \pm 16(27)$;
4. $I \equiv 0(3)$ *y* $J \equiv \pm 7(27)$.

Usando esto, procedemos a describir los $S$ que usaremos:

- $(p \neq 3)$: Tomamos $(I_0, J_0) \in \mathbb{F}_p^2 \backslash \{\Delta(I,J) = 0\}$. Si $f$ es una forma, sea $f_p$ su reducción mód $p$; definamos:

$$S = \{f : (I(f_p), J(f_p)) = (I_0, J_0)\}.$$

Para el cálculo de los términos entre paréntesis en (13), tenemos la proposición siguiente, cuya prueba puede leerse en [BS15a], Lema 3.15, y es un cálculo utilizando los resultados de [BSD63], el paper [SC02] y el Teorema 6.29.

**Proposición: 4.27.** *1. Sea $p$ un primo y $(I,J) \in \pi(V_{\mathbb{Z}_p})$ tal que $p^2 \nmid \Delta(I,J)$. Luego,*

$$\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{PGL_2(\mathbb{Z}_p)}} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} = 1;$$

*2. Si $p \neq 3$, fijemos $(I,J)$ em $\mathbb{F}_p^2$ con $\Delta(I,J) \neq 0$. Luego,*

$$\sum_{f \in \frac{V_{\mathbb{F}_p}(I,J)}{PGL_2(\mathbb{F}p)}} \frac{1}{\#Aut_{\mathbb{F}_p}(f)} = 1.$$

Por el lema y la proposición anteriores,

$$|J|_p = \frac{\frac{p(p-1)(p^2-1)}{p-1}}{p^5(1-p^{-2})\frac{1}{p^2}} = \frac{p(p^2-1)}{p^3\frac{p^2-1}{p^2}} = 1;$$

- Para $p = 3$, tomamos

$$S = \{f : I(f) \equiv 3(9)\}.$$

Dado $f \in S$, $J(f) \equiv 0(27)$ por elegibilidad. Luego, $\Delta(f) \not\equiv 0(3)$. Por la proposición, y por el hecho de que la congruencia en $I$ dice que $c \equiv 0(3)$ y $ae - bd \equiv 1(3)$, obtenemos que:

$$|J|_3 = \frac{3 \cdot (3^2-1)}{3^5\left(1-\frac{1}{9}\right) Vol(\pi(S))} = \frac{24}{3^5 \cdot \frac{8}{9} \cdot 3^{-5}} = 27.$$

Por la fórmula del producto, ahora se sigue:

$$|J| = \prod_p |J|_p = \frac{1}{27}.$$

## 4.6. Cálculo del volumen II

Usando el teorema de cambio de variables, tenemos que

$$Vol(R_X(L^i)) = \int_{\pi(\mathcal{F})R^i(X)} dv = \frac{1}{27}\int_{\pi(\mathcal{F})}\int_{R^i(X)} dIdJ\ \omega.$$

Como $\pi(\mathcal{F})$ es un dominio fundamental para la acción de $PGL_2(\mathbb{Z})$ sobre $PGL_2(\mathbb{R})$, esto es el volumen del cociente $PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R})$. Del cálculo de volumen se encarga la siguiente proposición (ver [Pla23], observaciones previas a la sección 4.7):

**Proposición: 4.28.** *El volumen del cociente $PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R})$ es igual a $2\zeta(2)$.*

Por otro lado, el volumen de $R^i(X)$ se obtiene integrando sobre una región elemental de $\mathbb{R}^2$. Calculemos estas integrales para finalizar la demostración del teorema.

Sea $i \in \{0, 2-, 2+\}$. Tenemos que integrar sobre la región

$$R = \left\{(I,J) : I^3 - \frac{J^2}{4} > 0,\ \text{máx}\left(|I|^3, \frac{J^2}{4}\right) < X\right\}.$$

Observar que en este caso $|I| \leq \sqrt[3]{X}$ y $|J| \leq 2\sqrt{X}$. Despejando $J$ en función de $I$ en la ecuación de $R$, obtenemos que hay que calcular:

$$\int_0^{\sqrt[3]{X}}\int_{-2I^{3/2}}^{2I^{3/2}} dJdI = 4\int_0^{\sqrt[3]{X}} I^{3/2}dI = \frac{8}{5}X^{5/6}.$$

Por otro lado, si $i = 1$, tenemos que integrar en la región

$$R = \left\{(I,J) : I^3 - \frac{J^2}{4} < 0,\ \text{máx}\left(|I|^3, \frac{J^2}{4}\right) < X\right\}.$$

Esto es una región que, pensada en $(I,J)$, se halla contenida en la caja $B = [-\sqrt[3]{X}, \sqrt[3]{X}] \times [-2\sqrt{X}, 2\sqrt{X}]$, y está delimitada por la curva $I = 4^{-1/3}J^{2/3}$ (en particular, queremos la región que encierra el eje de ordenadas con esta curva). Entonces, observando que los límites de esta última región coinciden con la integral que calculamos antes, se obtiene que:

$$Vol(R_1(X)) = Vol(B) - Vol(R_0(X)) = 8X^{5/6} - \frac{8}{5}X^{5/6} = \frac{32}{5}X^{5/6}.$$

Finalmente obtenemos:

**Teorema: 4.29** ( [BS15a], Teorema 2.1)**.**

$$N(V_{\mathbb{Z}}^i, X) = \begin{cases} \frac{4}{135}\zeta(2)X^{\frac{5}{6}} + O(X^{\frac{3}{4}+\varepsilon}) & i = 0, \\ \frac{32}{135}\zeta(2)X^{\frac{5}{6}} + O(X^{\frac{3}{4}+\varepsilon}) & i = 1, \\ \frac{8}{135}\zeta(2)X^{\frac{5}{6}} + O(X^{\frac{3}{4}+\varepsilon}) & i = 2. \end{cases}$$

## 4.7. Conteo con congruencias

Tenemos una versión del teorema de conteo usando congruencias. Sea $S \subseteq V_{\mathbb{Z}}$ definido por finitas condiciones de congruencia módulo potencias de primos $p^k$. Por el teorema chino del resto, podemos suponer que dicha congruencia se expresa como una congruencia módulo un entero $m$, y que, por ende, $S$ es una unión de $k$ reticulados $L_i$ con $L_i = m \cdot V_{\mathbb{Z}} + u_i$. Por el Teorema 4.19 aplicado a cada $L_i$, usando que los reticulados son disjuntos, tenemos que para cada $j$ podemos calcular $N(L_i \cap V_{\mathbb{Z}}^j, X)$, donde al usar el lema de Davenport tomamos en consideración que los volúmenes de dimensión menor se escalan por $\frac{1}{m^D}$, con $D$ la dimensión de la proyección, pues $V_{\mathbb{Z}}$ se escaló por $m$. Obtenemos al sumar sobre $i$ que:

$$N(S \cap V_{\mathbb{Z}}^j, X) = \frac{kVol(R_X(L^j))}{n_j m^5} + O(X^{3/4+\varepsilon}). \tag{14}$$

Sea $\mu_p(S)$ el volumen en $\mathbb{Z}_p$ de la clausura $p$-ádica de $S$ calculado con la medida de Haar aditiva normalizada de $V_{\mathbb{Z}_p}$. Tenemos el siguiente teorema de conteo con finitas congruencias, que los autores notan que se sigue de insertar la identidad

$$\frac{k}{m^5} = \prod_p \mu_p(S)$$

en la ecuación (14).

**Teorema: 4.30** (Conteo con finitas congruencias)**.** *Si $S$ está definido por condiciones de congruencia módulo finitos primos $p_1, \cdots, p_k$, entonces*

$$N(S \cap V_{\mathbb{Z}}^i, X) = N(V_{\mathbb{Z}}^i, X) \prod_p \mu_p(S) + O(X^{\frac{3}{4}+\varepsilon}).$$

Agregando pesos al teorema anterior, se consigue el teorema siguiente, cuya derivación es análoga:

**Teorema: 4.31.** *Sean $p_1, \cdots, p_k$ primos distintos y sean $\phi_{p_i} : V_{\mathbb{Z}} \to \mathbb{R}$ pesos, es decir, funciones definidas en $V_{\mathbb{Z}}$ tales que su valor en $f$ depende de la clase de congruencia de $f$ módulo alguna potencia de un primo $p_i$, y tal que son $GL_2(\mathbb{Z})$-invariantes. Sea $N_\phi(V^j_{\mathbb{Z}}, X)$ la cantidad de $GL_2(\mathbb{Z})$-clases de equivalencia de formas irreducibles en $V^j_{\mathbb{Z}}$ con altura acotada por $X$, tal que cada órbita está pesada por:*

$$\phi(f) = \prod_{i=1}^{k} \phi_{p_i}(f).$$

*Luego, se tiene que:*

$$N_\phi(V^j_{\mathbb{Z}}, X) = N(V^j_{\mathbb{Z}}, X) \prod_{i=1}^{k} \int_{f \in V_{\mathbb{Z}_{p_i}}} \psi_{p_j}(f)\, df + O_{\phi_{p_1}, \cdots, \phi_{p_k}, \varepsilon}(X^{3/4+\varepsilon}),$$

*donde $\psi_{p_j}$ extiende de manera natural la función $\phi_{p_j}$ a $V_{\mathbb{Z}_{p_j}}$.*

Conlcluimos esta sección con un teorema que describe "el promedio" de las formas con invariantes prescriptos:

**Teorema: 4.32.** *Sea $h^i(I, J)$ el número de $GL_2(\mathbb{Z})$-clases de equivalencia de formas cuárticas irreducibles enteras con $4 - 2i$ raíces reales e invariantes $I$, $J$. Luego,*

$$\lim_{X \to \infty} \frac{\sum_{H(I,J)<X} h^i(I, J)}{\sum_{\substack{(I,J)\ elegible,\\ (-1)^i \Delta(I,J)>0,\\ H(I,J)<X}} 1} = \frac{2\zeta(2)}{n_i}.$$

Lo único que nos falta para probar esto es complementar el cálculo de los volúmenes de los $R_X(L^i)$ con un cálculo de la cantidad de invariantes elegibles.

**Lema: 4.33.** *Sea $N^+_{I,J}(X)$ la cantidad de pares elegibles $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ con $H(I, J) < X$ y $\Delta(I, J) > 0$. Sea $N^-_{I,J}(X)$ el análogo para discriminante negativo. Luego:*

$$N^+_{I,J}(X) = \frac{8}{135} X^{5/6} + O(X^{1/2}),$$
$$N^-_{I,J}(X) = \frac{32}{135} X^{5/6} + O(X^{1/2}).$$

*Demostración.* Sean

$$R^{+}_{I,J}(X) = \{(i,j) \in \mathbb{R}^2 : |i| < X^{1/3},\ |j| < 2X^{1/2},\ 4i^3 - j^2 > 0\}$$

y

$$R^{-}_{I,J}(X) = \{(i,j) \in \mathbb{R}^2 : |i| < X^{1/3},\ |j| < 2X^{1/2}, -4i^3 + j^2 > 0\},$$

conjuntos que parametrizan en $\mathbb{R}^2$ el espacio donde queremos buscar los puntos enteros $(I,J)$. Observar que geométricamente esto es la intersección de la caja $[-X^{1/3}, X^{1/3}] \times [-2X^{1/2}, 2X^{1/2}]$ con una región delimitada por una función que proviene de la ecuación $\pm(4i^3 - j^2) > 0$. Observar que las proyecciones a los ejes están dominadas una $O(X^{1/2})$. Por el lema de Davenport, la cantidad de puntos enteros (considerando la elegibilidad) en $R^{\pm}_{I,J}(X)$ es

$$N^{\pm}_{I,J} = \frac{3^2}{3 \cdot 9^2} Vol(R^{\pm}_{I,J}) + O(X^{1/2}).$$

□

# 5. Obteniendo cotas uniformes: argumento *embedding sieve*

Para obtener cotas uniformes es preciso utilizar un argumento que embeba la representación que tenemos en un espacio con "más simetrías". Este tipo de argumento fue bautizado en [Bha14] como **embedding sieve**. A nivel estructural se compone de lo siguiente: sea $(G, V, f)$ una representación de un grupo algebraico lineal definido sobre $\mathbb{Z}$ con un polinomio invariante entero $f$ y supongamos que queremos contar órbitas bajo ciertas condiciones, pero que tenemos poco control sobre la simetría de $V$ (donde esto puede manifestarse de varias formas). Consideramos una representación $(G', V')$ que verifique las siguientes tres condiciones:

1. Hay un polinomio invariante $f'$ para la acción de $G'$ en $V'$;
2. Hay un mapa $\phi : G(\mathbb{Z})\backslash V(\mathbb{Z}) \to G'(\mathbb{Z})\backslash V'(\mathbb{Z})$ de órbitas y una constante uniforme $M$ tal que la fibra de cada vector $v$ en $V$ está acotada por $M$;
3. El polinomio invariante de $G$ es enviado al de $G'$: $f' \circ \phi = f$.

Luego, si $(G', V')$ *tiene más simetrías*, se puede "embeber" $G$ en $G'$ vía un mapa de fibra finita, lo cual permite controlar los problemas de conteo sobre $G$ vía los de $G'$.

## 5.1. El caso $GL_2(\mathbb{Z})$ actuando sobre $V_{\mathbb{Z}}$

Consideremos $V' := \mathbb{Z}^2 \otimes Sym^2(\mathbb{Z}^3)$ el espacio de formas cuadráticas ternarias enteras, que identificamos con el espacio de pares de matrices simétricas con coeficientes en $\frac{1}{2}\mathbb{Z}$ de $3 \times 3$. Podemos ver $V_{\mathbb{Z}}$ en $V'$ vía

$$\phi : (a, b, c, d, e) \to (A, B),$$

con $A$ la matriz fija

$$A = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 0, \end{pmatrix}$$

y $B$ dada por la matriz

$$\begin{pmatrix} a & \frac{b}{2} & 0 \\ \frac{b}{2} & c & \frac{d}{2} \\ 0 & \frac{d}{2} & e, \end{pmatrix}$$

es decir, con las formas

$$(xz - y^2, ax^2 + bxy + dyz).$$

Sea $V'_A$ el espacio de pares cuya primera coordenada es $A$. Hay una acción de $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ en $V'$, donde una matriz

$$C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

actúa por

$$(C, D) \to (aC + bD, cC + dD),$$

mientras que un elemento de $SL_3(\mathbb{Z})$ actúa por conjugación simultánea. Ambas acciones conmutan, así que esto define una acción del producto.

**Lema: 5.1** ( [Bha04b, 3.1]). *La acción de $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ sobre $V'$ tiene un único invariante, llamado discriminante.*

Más aún, tenemos que

**Proposición: 5.2.** *Sea $f \in V_{\mathbb{Z}}$. Luego, $\phi$ preserva el discriminante de $f$;*

*Demostración.* La forma cúbica binaria asociada a $f = (a, b, c, d, e)$ es

$$x^3 - (ad^2 + b^2e - 4ace)y^3 + cx^2y - 4axy^2e.$$

Un cálculo (que puede hacerse en una computadora) demuestra que el discriminante de esta forma coincide con el de $f$. □

Vamos a restringir aún más el espacio. Sea $SO(A)$ el grupo ortogonal especial de la forma cuadrática $A$, y sea $U \subseteq GL_2(\mathbb{Z})$ el grupo de matrices triangulares inferiores unipotentes. Notar que este grupo preserva $V_A$. Vamos a considerar la composición:

$$\Phi : V_{\mathbb{Z}} \to V'_A \to U \backslash V'_A.$$

Observar que este mapa es biyectivo, pues en cada clase de equivalencia hay una sola matriz con la entrada $b_{13} = 0$, y la imagen de una forma de $V_{\mathbb{Z}}$ a lo largo del mapa siempre tiene un cero en dicha entrada. Por otro lado, falta entender cómo se manifiesta la acción de $GL_2(\mathbb{Z})$ en $V_{\mathbb{Z}}$, para así tener una inyección del cociente en un grupo de órbitas más tratable. Esto se logra con un resultado de Wood (ver [Woo09]):

**Lema: 5.3.**

1. *Hay un mapa*
$$\rho : PGL_2(\mathbb{Z}) \to SL_3(\mathbb{Z})$$
*inducido por la acción de $GL_2(\mathbb{Z})$ en las formas cuadráticas $px^2 - 2qxy + ry^2$ vía*
$$\gamma \cdot f(x,y) = \frac{f((x,y)\gamma)}{det\gamma};$$

2. *Tenemos que $Im\rho = SO(A,\mathbb{Z})$;*

3. *Las órbitas de $GL_2(\mathbb{Z})$ en $V_{\mathbb{Z}}$ coinciden con las órbitas de la acción de $PGL_2(\mathbb{Z})$ en $V_{\mathbb{Z}}$ vía*
$$\gamma \cdot f(x,y) = \frac{f((x,y)\gamma)}{det^2\gamma};$$

4. *$\Phi(\gamma \cdot f) = \rho(\gamma) \cdot \Phi(f)$ en $U\backslash V'_A$.*

Esto induce un mapa biyectivo entre $PGL_2(\mathbb{Z})\backslash V_{\mathbb{Z}}$ y $(U \times SO(A,\mathbb{Z}))\backslash V_A$, y por ende un mapa

$$\Psi : PGL_2(\mathbb{Z})\backslash V_{\mathbb{Z}} \to (GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}))\backslash V'.$$

Acorde al esquema planteado previamente, nos interesa encontrar una constante $M$ que controle el cardinal de las pre-imágenes de $\Psi$. Observar que nos basta con acotar la cantidad de pre-imágenes del mapa

$$(U \times SO(A,\mathbb{Z}))\backslash V'_A \to (GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}))\backslash V',$$

dado que

$$PGL_2(\mathbb{Z})\backslash V_{\mathbb{Z}} \to (U \times SO(A,\mathbb{Z}))\backslash V_A$$

es una inyección. Observar que si $(A, B_k)_{k\in K} \to z$ es un conjunto completo de representantes para las pre-imágenes de $x$, los determinantes asociados $D_k = 4det(Ax - B_k y)$ son mónicos en $x$ y $GL_2(\mathbb{Z})$-equivalentes; en efecto, si $(A, B_i) = \gamma \cdot g \cdot (A, B_j)$, con

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

la matriz

$$\tau = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$$

actúa sobre $D_i$ de la siguiente forma:

$$\begin{aligned} &\tau \cdot D_i(x, y) = det(A(ax - cy) - B_i(bx - dy)) = \\ &= det(g(aAx + bB_i x)g^t - g(cAy + dB_i y)g^t) = \\ &= det((agAg^t + bgB_i g^t)x - (cgAg^t + dgB_i g^t)y) = det(Ax - B_j y). \end{aligned}$$

Como las $(A, B_k)$ no son $U \times SO(A, \mathbb{Z})$ equivalentes, las formas $D_k$ no son $U$-equivalentes. Llamemos $D$ a un representante común de $D_k$ módulo $GL_2$-equivalencia. Hay una inyección:

$$K \to D^{-1}(\{1\}) :$$

para cada $k$, $D_k$ es mónico, así que la forma $D_k$ representa al 1 vía $(1, 0)$. Si $\gamma_k$ realiza la equivalencia de $D_k$ con $D$, el vector $u_k = \gamma_k \cdot (1, 0)$ verifica que $D(u_k) = 1$. Por otro lado, si $i \neq j$, del hecho de que $D_i = \gamma_i \cdot D$ y que $D_j = \gamma_j \cdot D$ se desprende que

$$D_i = \gamma_i \gamma_j^{-1} \cdot D_j,$$

con lo cual $\gamma := \gamma_i \gamma_j^{-1}$ no puede estar en $U$. En particular, si tuviéramos que $\gamma_i \cdot (1, 0) = \gamma_j \cdot (1, 0)$, tendríamos que

$$(1, 0)\gamma = (1, 0),$$

lo cual quiere decir que la primera fila de $\gamma$ es $(1, 0)$. Como $|det\gamma| = 1$, $\gamma$ es unipotente triangular inferior, lo cual es absurdo. Esto dice que la función es inyectiva.

Con esto, nos alcanza acotar la cantidad de veces que una forma cúbica entera representa al 1 en $\mathbb{Z} \times \mathbb{Z}$ (a menos de equivalencia). Afirmamos que $M = 12$ alcanza: esto es el contenido de los teoremas de Delone (usualmente escrito como Delaunay) - para discriminante negativo - y Evertsé - para discriminante positivo - (respectivamente, [Del30], [Eve83]). Exponemos a continuación parte del primer resultado, siguiendo el libro de Delone y Faddeev ( [DF64], capítulo VI). El segundo resultado es más difícil, involucrando un delicado tratamiento de series hipergeométricas, y escapa a los contenidos de esta tesis.

## 5.2. Formas cúbicas con discriminante negativo representando a 1

Nuestro objetivo es estimar, a menos de equivalencia, la cantidad de veces que una forma cúbica representa al 1, es decir, la cantidad de soluciones enteras a la ecuación

$$f(X, Y) = 1$$

donde $f$ es una forma cúbica irreducible, con discriminante no nulo y entera. Observar que tenemos la igualdad, para una forma cúbica mónica en $Y$,

$$nX^3 + sX^2Y - qXY^2 + Y^3 = (X\rho + Y)(X\rho' + Y)(\rho'' + Y),$$

con $\rho$, $\rho'$, $\rho''$ las raíces de la des-homogeneización $X = 1$ del polinomio. En particular, a cada solución de la ecuación representando al 1 podemos asignarle una unidad en $\mathbb{Q}(\rho)$, de norma positiva. Esto sugiere que, estudiando este tipo de unidades, podemos estimar la cantidad de veces que una forma cúbica representa al 1.

A menos de una transformación modular, podemos suponer que la forma es mónica en $Y$, y se escribe como

$$f(X, Y) = nX^3 - qX^2Y + sXY^2 + Y^3.$$

Des-homogeneizando con $X = 1$, identificamos las formas con los polinomios de grado $\leq 3$ en $Y$ y podemos asignarle a cada una su conjunto de raíces. En el caso en que su discriminante es negativo, tendrá una raíz real y dos complejas conjugadas. En el caso en que su discriminante es positivo, se partirá completamente en $\mathbb{R}$. Nos concentraremos en el caso de

discriminante negativo.

Sea $K$ un cuerpo cúbico con embeddings complejos. Tiene entonces un embedding real y dos complejos conjugados, que llamaremos $\varrho$ y $\sigma$, $\overline{\sigma}$, respectivamente. Por teoría de Minkowski, si notamos la parte real de un complejo $z$ como $\Re\, z$ y la imaginaria como $\Im\, z$, el anillo de enteros de $K$ es un reticulado de rango 3 y que se puede embeber en $\mathbb{R}^3$ vía

$$x \to (\rho(x), \Re\, \sigma(x), \Im\, \sigma(x)).$$

Notar que si $x \in K$, la norma de $x$ es

$$\rho(x)\sigma(x)\overline{\sigma}(x) = \rho(x)|\sigma(x)|^2 = \rho(x)(\Re\, \sigma(x))^2 + (\Im\, \sigma(x))^2),$$

así que las unidades del anillo de enteros $\mathcal{O}_K$ están en la unión de las superficies $x(y^2+z^2) = 1$ y $x(y^2+z^2) = -1$. Supongamos que podemos escribir $K = \mathbb{Q}(\rho)$, con $\rho$ real verificando una ecuación cúbica irreducible sobre $\mathbb{Q}$. Nuestro reticulado tiene base entera $\{1, \rho, \rho^2\}$ y llamamos a un elemento **binomial** si es lineal en $\rho$, es decir, si es combinación lineal (entera) de 1 y $\rho$. En particular, los elementos binomiales se encuentran en el plano generado por $(1,1,0)$ y $(\rho, \Re\, \omega, \Im\, \omega)$, con $\omega$ un conjugado de $\rho$. Este plano tiene ecuación $x - y + Hz = 0$, con $H = \frac{\Re\, \omega - \rho}{\Im\, \omega}$. En particular, observar que cualquier elemento $(x,y,z)$ en la intersección de las superficies de números con norma 1 y números binomiales verifica que:

$$x^3 = \frac{x^2}{y^2+z^2} = \frac{y^2 - 2Hyz + H^2z^2}{y^2+z^2}.$$

Como $(y+Hz)^2 \geq 0$, obtenemos que $x^3 \leq H^2 + 1$. En particular,

$$x \leq \sqrt[3]{H^2+1}.$$

Por otro lado, por el teorema de unidades de Dirichlet, el grupo de unidades de $\mathcal{O}_K$ tiene un generador libre y todas las unidades se obtienen como $\pm\eta^m$, con $\eta$ el generador y $m$ un entero. Observar además que podemos suponer que $0 < \eta < 1$, a menos de cambiarlo de signo o cambiarlo por $1/\eta$. Llamamos a la unidad fundamental que está en el intervalo $(0,1)$, **unidad fundamental directa** y la notamos $\eta$, mientras que a su inverso lo llamamos **unidad fundamental inversa**, y lo notamos $\eta_*$. Podemos suponer que, al considerar las potencias de la unidad fundamental, tenemos

exponentes $m \geq 0$, usando en lugar de la unidad directa, la unidad inversa. Como la unidad inversa verifica que $\eta_* > 1$, elevarla a la $m$ la hará crecer; en particular, como hemos acotado uniformemente la coordenada $x$ de los puntos binomiales, se sigue que:

**Teorema: 5.4.** *Hay finitas potencias no-negativas de la unidad inversa que son unidades binomiales.*

Falta estudiar las potencias de la unidad directa. Primero observaremos de qué manera una transformación matricial afecta las soluciones en términos de $\eta$. Esto permitirá suponer que no hay soluciones que son potencia de la unidad inversa en nuestra forma cúbica.

**Teorema: 5.5** ( [DF64, VI.5]). *Sean $\eta^{m_i}$, $m_1 < m_2 < \cdots$, donde permitimos que $m_i < 0$, las soluciones de la forma $nX^3 - qX^2Y + sXY^2 + Y^3$. Si transformamos por una matriz*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

*entonces $(d, c)$ es una solución de la primera forma y, si $(d, c) = \eta^m$, las soluciones de la forma transformada son de la forma $\left\{ \frac{\eta^{m_i}}{\eta^m} \right\}_i$.*

En particular, como sabemos que las soluciones que son potencia de la unidad inversa son finitas, podemos transformar por una potencia lo suficientemente grande para que las nuevas soluciones sean todas de la forma $\eta^m$, con $m > 0$. Es decir, a menos de equivalencia, nos alcanza con probar que hay finitas unidades binomiales que son potencia positiva de la unidad directa.
Observar que si $\eta$ ya fuera binomial, terminamos:

**Teorema: 5.6.** *Si $A\rho + B$ es una unidad binomial y $|A| \neq 1$, ninguna potencia de $A\rho + B$ puede ser binomial.*

*Demostración.* Sea $m > 0$. Expandiendo el binomio de Newton, tenemos que si $(A\rho + B)^m$ fuera binomial,

$$\binom{m}{2} A^2 B^{m-2} + \binom{m}{2} A^3 B^{m-3} s + \binom{m}{4} A^4 B^{m-4} (q + s^2) + \cdots = 0.$$

Notar que $A$ y $B$ son coprimos, pues $A\rho + B$ es una unidad, y que no puede ser que un primo $p \geq 5$ divida a $A$, pues sino, si la valuación $p$-ádica

del primer término es $\nu$, la valuación $p$-ádica de todos los términos restantes sería $\geq \nu + 1$, lo cual es absurdo pues la suma está igualada a cero. Si $9|A$, y la valuación 3-ádica de $\frac{m(m-1)}{2\cdot 3}$ es $k$, a partir del segundo término la aparición de potencias de $A$ indica que la valuación 3-ádica es $\geq k+1$. Esto también es absurdo. El caso $2|A$ se prueba análogamente.

Supongamos entonces que $A = 3$. La unidad binomial se corresponde con una solución de la forma $B^3 = sA^2B - qA^2B + A^3n$. Es decir

$$B^3 = 9sB - 3qB^2 + 27n,$$

lo cual es cero módulo 3. Por el pequeño teorema de Fermat, $B$ es cero módulo 3. Sacando un 3 de todos lados, vemos que $s \equiv 0 \,\text{mód}\, 3$. Esta congruencia permite mirar, como antes, la valuación 3-ádica de $\frac{m(m-1)}{2}$ y compararla con la de los términos restantes para arribar a otro absurdo. □

Para concluir, sólo falta una técnica llamada *algoritmo del ascenso*, debida a Delone. Sea $\eta = A\rho^2 + B\rho + C$ y pongamos $\eta^{m_i}$ las soluciones binomiales a la forma cúbica representando al 1. Escribamos $\eta^{m_i} = P_i\rho + Q_i$. Recordar que $\rho$ es solución de

$$X^3 - sX^2 - qX - n = 0,$$

tal que si $\rho', \rho''$ son los conjugados de $\rho$ (y seguimos la misma convención para $\eta$ y $\eta^{m_i}$),

$$s - \rho = \rho' + \rho''.$$

Por otro lado,

$$P_i = \frac{\eta'^{\,m_i} - \eta''^{\,m_i}}{\rho' - \rho''}.$$

Notar que podemos calcular

$$\eta' - \eta'' = A\rho'^{\,2} + B\rho' + C - A\rho''^{\,2} - B\rho'' - C = A(\rho'^{\,2} - \rho''^{\,2}) + B(\rho' - \rho''),$$

con lo cual

$$P_i = \frac{\eta' - \eta''}{\rho' - \rho''} \sum_{i=1}^{n-1} \eta'^{\,m_i i} \eta''^{\,m_i (n-i)} = (A(s-\rho) + B) \left( \sum_{i=1}^{n-1} \eta'^{\,m_i i} \eta''^{\,m_i (n-i)} \right).$$

La última expresión es una expresión simétrica, racional en $\eta', \eta''$. Podemos entonces escribir

$$P_i = (A(s-\rho)+B)(\alpha_i\rho^2+\beta_i\rho+\gamma_i),$$

con $\alpha_i, \beta_i, \gamma_i$ en $\mathbb{Q}$. Desarrollando la ecuación e igualando en $\mathbb{Q}(\rho)$, tenemos que:

$$\begin{aligned}\alpha_i &= \frac{A^2P_i}{N(-A\rho+As+B)},\\ \beta_i &= \frac{ABP_i}{N(-A\rho+As+B)},\\ \gamma_i &= \frac{(B^2+ABs+A^2q)}{N(-A\rho+As+B)}.\end{aligned}$$

Luego, si llamamos $\delta^2 := (A^2 : AB : B^2+ABs+A^2q) = (A : B)^2$, el máximo común divisor de los numeradores de los coeficientes de la forma derecha verifica que $\delta \cdot N(-A'\rho+A's+B')|P_i$ para todo $i$, con $A' = A/\delta$, $B' = B/\delta$. Sea $\kappa := |\delta \cdot N(-A'\rho+A's+B')|$. Si $\kappa > 1$, las soluciones viven en un orden $\mathcal{O}_{\kappa\rho}$. Podemos ahora repetir el argumento para este nuevo anillo y construir una sucesión de anillos, cada uno "más alto"que el otro. El proceso termina cuando $\kappa = 1$, si es que esto ocurre. En particular, la norma previa debe ser un miembro de $\mathbb{Q}$ o una unidad de $\mathbb{Q}(\rho)$. Cada paso en el que vamos hacia un orden superior se llama *ascenso*.
El teorema fundamental del algoritmo del ascenso es el siguiente:

**Lema: 5.7.** *Sea $\tau = -A\rho+As+B$. Luego, $\tau$ no es una unidad no racional de ningún anillo producido a partir del primer ascenso.*

*Demostración.* Hemos de probar que la única forma de que esta cantidad sea una unidad es que lo sea de $\mathbb{Q}(\rho)$. Supongamos que las soluciones asociadas a la unidad fundamental inversa han sido "normalizadas", es decir, que todas las soluciones están dadas por potencias de la unidad fundamental directa. Si $\tau$ es una unidad en $\mathbb{Q}(\rho)$, es binomial, y luego es potencia no-negativa de la unidad fundamental directa $\eta$, posiblemente multiplicada por $-1$. Es fácil ver (igualando la ecuación) que $\tau \neq \eta$. Luego, la potencia debe ser positiva y $> 1$. Notar que si $\tau = \pm\eta^l$,

$$\pm\eta_*^l = \frac{1}{\tau} = A\eta + (ABs+B^2-A^2q-AC).$$

Luego,

$$\pm\eta_*^{l+1} = (ABs + B^2 - A^2q - AC)\eta_* + A.$$

Si hemos realizado un ascenso, el mismo argumento muestra que, llamando al nuevo elemento $\rho' := \kappa\rho + r$, con $\kappa > 1$ y $r \in \mathbb{Q}$, se tiene

$$\eta_* = (ABS + B^2 - A^2q - AC)\rho'^2 + b\rho' + c,$$

para coeficientes análogos al primero $b$, $c$. Esto se puede escribir como $\kappa\theta + c'$, con $\theta$ un entero del orden y $c''$ un racional. Luego,

$$\begin{aligned}\pm\eta_*^{l+1} &= \pm(\kappa\theta + c')^{l+1} = (ABS + B^2 - A^2q - AC)\eta_* + A \\ &= (ABS + B^2 - A^2q - AC)\kappa\theta + (ABS + B^2 - A^2q - AC)c' + A),\end{aligned}$$

lo cual contradice el Teorema 5.6, salvo $\kappa = 1$, es decir, si no hubo ascensos. □

Con esto en mente, veamos el desarrollo del algoritmo del ascenso con exhaustividad. Si $\tau$ no es una unidad ni un entero algebraico, realizamos al menos un ascenso. Denotemos $\tau'$ al $\tau$ ascendido.

- Si $\tau$ no se vuelve unidad al ascender, $P_i$ es infinitamente divisible por los ascensos suscesivos $\kappa, \kappa', \kappa'', \cdots$, lo cual es absurdo y no hay soluciones;
- Si ascendemos y $\tau$ se vuelve una unidad, por el lema no puede ser distinta de $\pm 1$. Luego, $A' = 0, B' = \pm 1$, y $\eta' = \pm\rho + C'$. Denotemos $\rho' = \kappa\rho$, con $\kappa > 1$. Luego, tenemos que $(\pm\kappa\rho + c)^m = P_k'\rho + Q$, lo cual es absurdo por el Teorema 5.6, a menos que $m = 1$. Por ende, además de la "solución infinita" $(0, 1)$, tenemos la solución $\pm\kappa\rho + C'$;
- Decimos que una forma $f$ es **reversible** si es mónica y $f(1, 0) = 1$. El caso donde el algoritmo no asciende nunca se desprende de un tratamiento de las formas reversibles. Este escenario se da cuando $\tau$ ya era una unidad. Si es una unidad trivial $\pm 1$, como antes se tiene que $\eta = \pm\rho + C'$. Como $\rho$ tiene grado 3 sobre $\mathbb{Q}$ y $\eta$ es una unidad, $\eta$ será raíz de una forma reversible; si $\tau$ es una unidad no racional,

definiendo

$$\begin{aligned} a &= \pm(ABs + B^2 - A^2q - AC), \\ b &= \pm(ACs + BC - A^2n), \\ c &= \pm(-A), \\ d &= \pm(B + As), \end{aligned}$$

vemos que

$$\eta = \frac{a\rho + b}{c\rho + d}.$$

Podemos elegirlos de manera tal que $N(c\rho + d) = 1$. Luego, la forma $(n, -q, s, 1)$ es equivalente a una reversible vía la matriz $(a, b, c, d)$, que tiene determinante de módulo 1.

Esto dice que podemos resumirnos al tratado de las formas reversibles. El mismo se realiza mediante un largo cálculo (ver [DF64], páginas 389-395). Resumimos la conclusión de este análisis, en conjunto con el anterior, en el siguiente teorema:

**Teorema: 5.8** (Representación del 1 por formas cúbicas)**.** *Sea $f$ una forma cúbica entera con discriminante negativo. Luego, la cantidad de veces que $f$ representa al 1 es $\leq 5$. En específico, si la forma no es reversible, hay $\leq 2$ representaciones. Si la forma es equivalente a una reversible, hay 3, o 4 representaciones. La única forma con 5 soluciones tiene discriminante $-23$ y está dada en coeficientes por $g = (1, 0, -1, 1)$.*

## 5.3. Cribas libres de cuadrados

Sea $W_p(V) \subseteq V_{\mathbb{Z}}$ el conjunto de las formas tales que su discriminante es divisible por $p^2$. Notar que esto puede ocurrir por dos razones: razones de naturaleza "mód $p$", es decir, $p^2|\Delta(f + pg)$ para toda $g$, en cuyo caso decimos que $f$ es **fuertemente divisible por** $p$; y razones de naturaleza "mód $p^2$", es decir, que existe $g \in V_{\mathbb{Z}}$ tal que $p^2 \nmid \Delta(f + pg)$, en cuyo caso decimos que es **débilmente divisible por** $p$. Sea $W_p^1(V)$ el conjunto de las formas fuertemente divisibles, resp. $W_p^2(V)$ el conjunto de las formas débilmemente divisibles. La idea usada en [BS15a] consiste en observar que el fenómeno fuerte puede atacarse de manera geométrica, con una criba, mientras que el fenómeno débil precisa de técnicas de teoría de

anillos asociadas a la parametrización previa.

### 5.3.1. Múltiplos fuertes

Tenemos la siguiente forma cuantitativa de un teorema de Ekedahl ( [Eke91]), que fue probada por Bhargava en [Bha14].

**Teorema: 5.9.** *Sea $Y$ un subesquema cerrado de $\mathbb{A}^n_{\mathbb{Z}}$ de codimensión mayor o igual a 2. Suponer que las proyecciones de $Y$ a las primeras $n-k+j$ coordenadas tienen clausura Zariski de codimensión $j$ en $\mathbb{A}^{n-k+j}$, para $0 \leq j \leq k$. Sea $B$ una región compacta de $\mathbb{R}^n$ de medida finita. Sean $M$, $r > 0$. Sean $t_1, \cdots, t_n$ reales positivos tales que $\prod_i t_i = 1$, y supongamos que existe una constante $\kappa > 0$ tal que $rt_i > \kappa \; \forall i$ y $t_i > \kappa$ para $i > n-k$. Luego, si $\Omega := B \cap Y \cap \mathbb{Z}^n$,*

$$\#\{a \in \Omega : \exists\, p > M \text{ primo, } a \text{ mód } p \in Y(\mathbb{F}_p)\} = O\left(\frac{r^n}{M^{k-1} log\ M} + r^{n-k+1}\right),$$

*con la constante dependiendo de $B, Y$ y $\kappa$.*

Una vez que tenemos esto, podemos truncar la región $\mathcal{F}_{PGL_2}$, que definimos como mirar a $\mathcal{F}$ módulo $PGL_2(\mathbb{R})$ (que es un dominio fundamental para $PGL_2(\mathbb{Z})$ sobre $PGL_2(\mathbb{R})$) para tener una dominio que se expande homogéneamente: sea $0 < \varepsilon < 1$ tal que si $\mathcal{F}^{\varepsilon}_{PGL_2}$ corresponde a los elementos de $\mathcal{F}_{PGL_2}$ donde $t = O_{\varepsilon}(1)$, se cumple

$$Vol(\mathcal{F}^{\varepsilon}_{PGL_2}) = (1-\varepsilon) Vol(\mathcal{F}_{PGL_2}).$$

Con este truncamiento, podemos aplicar la criba a $\mathcal{F}_{PGL_2} \cdot R^i(X)$ al tomar: $n = 5$, $k = 2$, $r = X^{\frac{1}{6}}$, donde podemos tomar $k = 2$ puesto que, suponiendo que $f$ es fuertemente divisible por $p$, y suponiendo sin pérdida de generalidad que $\Delta = \Delta(f)$ posee término en $e$, debe ser que $Y = V(\Delta, \frac{\partial \delta}{\partial e})$ es un subesquema cerrado de $\mathbb{A}^5_{\mathbb{Z}}$, de codimensión 2, que contiene a $W$. Se sigue que:

$$W = \left\{ \mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \bigcap \bigcup_{p>M} W^1_p(V) \right\} = O_{\varepsilon}\left(\frac{X^{\frac{5}{6}}}{M \cdot logM} + X^{\frac{2}{3}}\right).$$

### 5.3.2. Múltiplos débiles

Para los múltiplos débiles es mas conveniente usar el mapa $\Psi$, definido en la sección 5.1. Usaremos que conocemos cómo se comportan los múltiplos débiles en $V'$ y que el mapa tiene fibras uniformemente acotadas. Primero necesitamos un teorema de Bhargava, probado en [Bha05]. La moral de la prueba es interpretar el problema de las formas cuárticas como un problema sobre anillos cuárticos, y utilizar técnicas de teoría de cuerpos para realizar el conteo.

**Teorema: 5.10** (Bhargava)**.** *Sea $W_p^2(V')$ el conjunto de elementos de $V'$ que es débilemente divisible por $p$. Luego, la cantidad de órbitas bajo $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ en $W_p^2(V')$, con discriminante acotado por $X$, es $O(X/p^2)$, con la $O$ independiente de $p$.*

Usando esto, observar que tenemos el siguiente teorema:

**Teorema: 5.11.**

$$\#\{f \in W_p^2(V) : H(f) < X\} = O(X/p^2),$$

*con la $O$ independiente de $p$ y $X$.*

*Demostración.* El mapa $\Psi$ preserva discriminante y la pre-imagen de cada elemento tiene como mucho 12 elementos (módulo $(GL_2(\mathbb{Z})) \times SL_3(\mathbb{Z})$), así que cada $v$ de $V'$ que cumple la cota produce $\leq 12$ elementos con altura acotada en $V'$ (módulo $PGL_2$). □

Con esto, obtenemos una cota uniforme para el caso débil también, que, en conjunción con la cota para el caso fuerte, implicarán el teorema de conteo uniforme.

**Teorema: 5.12.** *Sea $0 < \varepsilon < 1$. Tenemos que*

$$\#\left\{\mathcal{F}_{PGL_2}^{\varepsilon} \cdot R^i(X) \bigcap \bigcup_{p>M} W_p^2(V)\right\} = O_\varepsilon\left(\frac{X^{5/6}}{logM}\right),$$

*con la $O$ independiente de $X$ y $M$.*

*Demostración.* Si $f \in \mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X)$, $\frac{\partial \Delta}{\partial e} \not\equiv 0(p)$. Notar que $\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X)$ es una región que se expande de manera homogénea y sus lados están acotados por $X^{1/6}$, así que, una vez fijado $e$, la cantidad de opciones para $(a, b, c, d)$ es $O(X^{4/6})$, si pedimos que $f \in \mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \cap V_{\mathbb{Z}}$. Más aún, como $\Delta$ es cúbico en $e$, una vez fijados $(a_0, b_0, c_0, d_0, e_0)$ como antes, hay como mucho 3 elecciones para el resto de $e_0$ módulo $p$, para que $p|\Delta$. Como $p \nmid \frac{\partial \Delta}{\partial e}$, por el lema de Hensel, hay un levantado módulo $p^2$ único, para cada una de esas 3 elecciones, tal que $p^2|\Delta$. Luego,

$$\#\{\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \cap W_p^2(V)\} = \begin{cases} O(\frac{X^{5/6}}{p^2}) & p \leq X^{1/12}, \\ O(X^{4/6}), & \end{cases}$$

pues si $p \leq X^{1/12}$, $p^2 \leq X^{1/6}$ y $X^{4/6} \leq X^{5/6}/p^2$. Esto nos da una cota puntual en función de $p$ para cada $\#\{\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \cap W_p^2(V)\}$. Para combinarlas, debemos estimar

$$\#(\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X)) \bigcap \bigcup_{p>M} W_p^2(V) = \#\bigcup_{p} (\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \cap W_p^2(V)).$$

Esto es

$$O\left(\sum_{p>M} \#(\mathcal{F}^{\varepsilon}_{PGL_2} \cdot R^i(X) \cap W_p^2(V))\right).$$

Para el rango $1 < p < X^{1/6}$, podemos acotar por la cantidad de sumandos y la cota previa: la función contadora de primos $\pi(X^{1/6})$ se comporta como $O\left(\frac{X^{1/6}}{\log(X)}\right)$, así que en este rango estamos acotados por un factor de orden $O(X^{4/6})O\left(\frac{X^{1/6}}{\log(X)}\right) = O(X^{5/6}/\log(X))$. Como $p < X^{1/6}$ y $p > M$, obtenemos que en el rango $1 < p < X^{1/6}$ podemos acotar por $O(X^{5/6}/\log M)$. Por otro lado, para $p > X^{1/6}$,

$$\sum_{p>X^{1/6}} \frac{1}{p^2} = O\left(\frac{1}{X^{1/6}\log(X)}\right),$$

pues, integrando por partes,

$$\sum_{p} \frac{1}{p^2} - \sum_{p \leq X} \frac{1}{p^2} \sim \frac{1}{X\log(X)}.$$

Finalmente, utilizando el Teorema 5.11, podemos acotar por $O(\frac{X^{5/6}}{logM})$ también en el rango $p > X^{1/6}$. □

Juntando las cotas se obtiene:

**Teorema: 5.13** (Criba uniforme, Teorema 2.13 de [BS15a]). *Sea $p$ un primo. Para cada $M > 0$,*

$$\lim_{X\to\infty} \frac{N\left(\bigcup_{p>M} W_p(V); X\right)}{X^{5/6}} = O\left(\frac{1}{logM}\right),$$

*con la $O$ independiente de $M$.*

### 5.3.3. La criba

Hasta ahora, sabemos controlar de manera uniforme el agregado de (infinitas) condiciones de congruencia para nuestro conteo. En esta sección, consideraremos un teorema de conteo que permita detectar discriminantes que son divisibles por el cuadrado de algún primo, para luego aplicarlo para calcular la cantidad de formas según la "suavidad"de su discriminante.

**Definición: 5.14.** Sea $\phi : V_{\mathbb{Z}} \to [0,1]$. Decimos que **está definida por condiciones de congruencia** si existen funciones locales $\phi_p : V_{\mathbb{Z}_p} \to [0,1]$ tal que:

- $\prod_p \phi_p \to \phi(f)$ puntualmente;
- Para cada $p$, $\phi_p$ es localmente constante fuera de un conjunto $S_p$ cerrado de medida cero.

Decimos además que $\phi$ es **aceptable** si, para $p \gg 1$,

$$p^2 \nmid \Delta(f) \quad \Longrightarrow \quad \phi_p(f) = 1.$$

Un ejemplo de función aceptable es el siguiente:

**Teorema: 5.15.** *Sea $S$ el conjunto de formas cuárticas con discriminante libre de cuadrados. Luego, $\chi_S$ es una función aceptable.*

*Demostración.* Sean

$$\chi_p(f) = \begin{cases} 1 & p^2 \nmid \Delta(f), \\ 0 & p^2 | \Delta(f). \end{cases}$$

Notar que el producto de las $\chi_p$ da cero, salvo que para todo $p$, $\Delta(f)$ sea libre de cuadrados, lo cual dice que le producto $\prod \chi_p(f)$ converge a $\chi_S(p)$. Por otro lado, las funciones $\chi_p$ son localmente constantes y la condición de aceptabilidad se satisface trivialmente. □

El teorema central de esta parte es el teorema de conteo siguiente, en el cual no sólo podemos poner pesos, sino que estos detectan infinitas condiciones de congruencia:

**Teorema: 5.16.** *Sea $\phi : V_{\mathbb{Z}} \to [0,1]$ aceptable. Luego,*

$$N_\phi(V^i_{\mathbb{Z}}, X) = N(V^i_{\mathbb{Z}}, X) \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f) df + o(X^{5/6}).$$

*Demostración.* La estrategia de la prueba es reducirla al teorema que ya conocemos para finitas condiciones de congruencia vía truncamientos, para luego acotar el error que esto introduce con la criba uniforme.
Para cada $\phi_p$, como son localmente constantes fuera de $S_p$, podemos tomar una sucesión de funciones acotadas que convergen puntual y crecientemente a $\phi_p$, llámense $\psi_{pi}$, a la par que una sucesión decreciente $\psi'_{pi}$, todas ellas definidas por congruencias módulo $p^i$, para cada $i$. Suponer que si $i = 0$, el valor de las funciones es 1. Tenemos que

$$\int_{V_{\mathbb{Z}_p}} \psi_{pn} \underset{n\to\infty}{\to} \int_{V_{\mathbb{Z}_p}} \phi_p,$$

y que

$$\int_{V_{\mathbb{Z}_p}} \psi'_{pn} \underset{n\to\infty}{\to} \int_{V_{\mathbb{Z}_p}} \phi_p.$$

Por aceptabilidad, si $p \gg 1$, usando el teorema chino del resto y el argumento geométrico de [Poo03] (Teorema 3.2),

$$1 - \int_{V_{\mathbb{P}}} \phi_p(f) df \leq \int_{f \in V_{\mathbb{Z}_p}, p^2 | \Delta(f)} \ll \frac{1}{p^2}.$$

Consideremos ahora truncamientos de los pesos: si $Y \in \mathbb{Z}$, sea $N_\psi^Y(V_{\mathbb{Z}}^i, X)$ el número de $GL_2(\mathbb{Z})$-órbitas de formas irreducibles con altura acotada por $X$, pesadas por $\prod_p \psi_{p,\lfloor \frac{Y}{p} \rfloor(f)}(f)$. Análogamente definimos las nociones para $\psi'$. Por el teorema de conteo para finitas condiciones de congruencia, que se puede aplicar dados los truncamientos, tenemos que:

$$\limsup_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}, X)}{X^{5/6}} \leq \limsup_{X\to\infty} \frac{N_{\psi'}(V_{\mathbb{Z}}, X)}{X^{5/6}} =$$
$$= \lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}, X)}{X^{5/6}} \prod_p \int_{f\in V_{\mathbb{Z}_p}} \psi'_{p,\lfloor \frac{Y}{p} \rfloor(f)} df.$$

Por aceptabilidad, el producto cumple que

$$\prod_p \int_{f\in V_{\mathbb{Z}_p}} \phi_p(f) df < \infty,$$

así que si $Y \to \infty$, con $p$ fijo,

$$\prod_p \int_{f\in V_{\mathbb{Z}_p}} \psi'_{p,\lfloor \frac{Y}{p} \rfloor(f)}(f) df \underset{Y\to\infty}{\to} \prod_p \int_{f\in V_{\mathbb{Z}_p}} \phi_p(f) df.$$

En particular, tenemos la cota superior:

$$\limsup_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}, X)}{X^{5/6}} \leq \prod_p \int_{f\in V_{\mathbb{Z}_p}} \phi_p(f) df.$$

Falta la cota inferior. Por aceptabilidad, nuevamente los pesos darán 1 siempre y cuando primos suficientemente grandes no dividan al discriminante. Observar que si $p \gg 1$ - $p > Y$ en particular - la única condición que rompe que $\phi \geq \psi_{p,n}$ es si $n = 0$ y $p^2|\Delta(f)$. Por ende, salvo en los puntos tales que $p > Y$, $p^2|\Delta(f)$ y $H(f) < X$, tenemos que $\psi \geq \psi_{pn}$, así que a menos de una constante se estima:

$$N_\phi(V_{\mathbb{Z}}^i, X) \geq N_\psi^Y(V_{\mathbb{Z}}^i, X) - O\left(N\left(\bigcup_{p>Y} W_p(V)\right), X\right),$$

siguiendo la notación de la sección anterior. Dividiendo por $X^{5/6}$, tomando límite cuando $X \to \infty$,

$$\liminf_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}^i, X)}{X^{5/6}} \geq \liminf_{X\to\infty} \left( \frac{N_\psi^Y(V_{\mathbb{Z}}^i, X) - O(N(\bigcup_{p>Y} W_p(V)), X)}{X^{5/6}} \right),$$

y usando la criba uniforme se deduce que:

$$\liminf_{X\to\infty} \frac{N_\phi(V^i_{\mathbb{Z}}, X)}{X^{5/6}} \geq \liminf_{X\to\infty} \frac{N(V^i_{\mathbb{Z}}, X)}{X^{5/6}} \prod_p \int_{f\in V_{\mathbb{Z}_p}} \psi_{p,\lfloor \frac{Y}{p} \rfloor(f)}(f)df - O\left(\frac{1}{logY}\right).$$

La demostración concluye enviando $Y \to \infty$, donde los límites y productos conmutan por convergencia dominada y por el hecho de que el producto converge. □

### 5.3.4. Formas con estabilizador grande

En esta sección probaremos los Lemas 4.11, 4.18 y 4.26. Estos lemas se interpretan como fenómenos de la teoría de invariantes, correspondientes a resolventes cúbicas de formas cuárticas. Utilizamos la notación de la sección 5. Una forma cúbica se dice **mónica** si vista como forma en $x$ es mónica. Sea $R_{\mathbb{Z}}$ el espacio de formas cúbicas enteras y $R_{\mathbb{Z},1}$ el subespacio de formas mónicas. Si $(A, B) \in V'$, $4det\ (Ax - By) \in V'_A$. Tenemos que $U$ actúa sobre $R_{\mathbb{Z},1}$ por cambio de variables. Si $g = (1, r, s, t) \in R_{\mathbb{Z},1}$, $I(g) = r^2 - 3s$, $J(g) = -2r^3 + 9rs - 27t$ son invariantes para $U$. El discriminante $\Delta(g)$ se debe poder escribir en base a $I,\ J$. En particular, vale que

$$27\Delta(g) = 4I(g)^3 - J(g)^2.$$

La altura de $g$ es $H(g) = \max(|I(g)|^3, \frac{J(g)^2}{4})$. Sea $U_{\mathbb{Q}}$ el grupo de unipotentes triangulares inferiores con entradas racionales. Mirando la acción por cambio lineal de variables de $U_{\mathbb{Q}}$ sobre $R_{\mathbb{Z},1}$ vemos que toda forma $g = (1, r, s, t)$ es equivalente a $h(x, y) = x^3 - \frac{I(g)}{3}xy^2 - \frac{J(f)}{27}y^3$.

Si $f \in V_{\mathbb{Z}}$ y $\phi(f) = (A, B)$ su **cúbica resolvente** es la forma cúbica mónica $g(x, y) = 4det(Ax - By)$. Tenemos que $I(f) = I(g)$ y $J(f) = J(g)$. Como ya hemos mencionado, la curva elíptica $z = g(x, 1)$ es la jacobiana de la curva de género 1, $z^2 = f$. Usaremos un lema de conteo básico:

**Lema: 5.17.** *La cantidad de $U$-órbitas de formas cúbicas binarias mónicas enteras $g$, con $g$ $\mathbb{Q}$-reducible y de altura $H(g) < X$, es una $O(X^{1/2+\varepsilon})$.*

*Demostración.* A menos de $U$-equivalencia, dada la forma $g = (1, r, s, t)$, podemos suponer que $|r| \leq 1$. Si $H(g) < X$, $|I(g)| \leq \sqrt[3]{H(g)} \leq X^{1/3}$. Más aún, $3|s| \leq |r^2 - 3s| + |r^2| \leq |I| + 1 = O(X^{1/3})$, así que $|s| = O(X^{1/3})$.

Análogamente, como $\frac{|J(g)|^2}{4} \leq H(g) \leq X$, $t = O(X^{1/2})$. Consideremos ahora la condición de reducibilidad para $g$. Si $t = 0$, $g = (1, r, s)$, así que hay $O(1)O(X^{1/3}) = O(X^{1/3})$ opciones para $g$. Podemos entonces suponer que $t \neq 0$. Como $g$ es reducible, debe tener un factor racional. Sea $x - my$ un tal factor. Luego,

$$g(x,y) = x^3 + rx^2y + sxy^2 + ty^3 = (x - my)l(x,y).$$

Observar que de esta igualdad se deduce que $m|t$. Como $t = O(X^{1/2})$, $m = O(X^{\varepsilon})$. Observar que al fijar $r$, $t$, $m$, como $g(m,1) = 0$, tenemos que $s$ queda determinado. Luego, hay $O(1)O(X^{1/2})O(X^{\varepsilon}) = O(X^{1/2+\varepsilon})$ elecciones para $g$. □

Ahora procedemos con la demostración del Lema 4.11.

*Demostración del Lema 4.11.* Primero consideremos la acción de $PGL_2(\mathbb{Z})$ como en el Lema 5.3, inciso 3. Si $\Delta(f) \neq 0$, por el isomorfismo de (3.18), $\#Stab_{PGL_2(\mathbb{R})}(f) =$

$$\begin{cases} 2 & \Delta(f) < 0, \\ 4 & \Delta(f) > 0. \end{cases}$$

Ahora consideremos la acción de $GL_2(\mathbb{R})$ por cambio lineal. Si $\gamma \in Stab_{\mathbb{R}}(f)$, usando que $I$, $J$ se transforman por potencias del determinante, vemos que $|det\ \gamma| = 1$. Luego, $\gamma$ mod $PGL_2(\mathbb{R})$ estabiliza $f$. Como $\#Stab_{\mathbb{R}}(f) \cap \lambda I = 2$, hay que multiplicar por 2 a los valores anteriores. Luego,

$$\begin{cases} \#Stab_{\mathbb{R}}(f) = 8 & f \in V^0_{\mathbb{R}}, V^{2-}_{\mathbb{R}}, V^{2+}_{\mathbb{R}}, \\ \#Stab_{\mathbb{R}}(f) = 4 & f \in V^1_{\mathbb{R}}. \end{cases}$$

□

Ahora, armados con el Lema 5.17 y el Lema 4.11, damos una demostración del Lema 4.18.

*Demostración del Lema 4.18.* Sea $f$ una forma entera cuyo estabilizador tiene más de un elemento. Luego, la curva $E_f$ inducida por el Corolario 3.18 admite 2-torsión racional no trivial. Por la observación del comienzo, si $g$ es la cúbica mónica resolvente de $f$, $g$ es reducible. Si $H(f) < X$, como $g$ tiene la misma altura, $H(g) < X$, y estamos en las condiciones del Lema 5.17. Podemos afirmar luego que hay a lo sumo $O(X^{1/2+\varepsilon})$ elecciones para

la $U$-órbita de $g$.

Si fijamos ahora la $GL_2(\mathbb{Z})$-órbita de $g$, donde $g$ es una forma cúbica, entera, reducible y $H(g) < X$, nuevamente usando los resultados de [Bha05] (ver Lema 12 y su demostración), las $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$-órbitas de (pares de) formas en $V'$ con $g$ como cúbica resolvente es como mucho $O(X^{1/4})$. Por lo hecho en la sección 5.1, tenemos que el número de $PGL_2(\mathbb{Z})$-órbitas en $V_{\mathbb{Z}}$ con $g$ como cúbica resolvente es a lo sumo $O(X^{1/4})$. Luego, la cantidad de $PGL_2(\mathbb{Z})$-órbitas de formas en $V_{\mathbb{Z}}$ con estabilizador no trivial en $PGL_2(\mathbb{Q})$ y altura menor a $X$ se acota como las formas de elegir la órbita en $PGL_2(\mathbb{Z})$, y luego la órbita de $g$, lo cual hay a lo sumo $O(X^{1/4}X^{1/2+\varepsilon}) = O(X^{3/4+\varepsilon})$ opciones. □

Por último, demostramos el Lema 4.26.

*Demostración del Lema 4.26.* Podemos reducir el problema a las formas cúbicas, pues dada una $f$, su forma cúbica resolvente tiene los mismos invariantes, y, dada cualquier $g = (1, r, s, t)$, construimos la forma $f(x, y) = x^3y + rx^2y^2 + sxy^3 + ty^4$ y chequeamos que tiene a $g$ como cúbica resolvente.

Sea $g \in R_{\mathbb{Z},1}$. Podemos suponer que $r = -1, 0, 1$, sin cambiar los invariantes. Si $I \equiv 0(3)$, $r^2 \equiv I + 3s \equiv 0(3)$. Luego, $J \equiv -2 \cdot 27 + 27s - 27t \equiv 0(27)$. Suponer que $I \not\equiv 0(3)$. Luego, $r \neq 0$, tal que $r = \pm 1$. Luego, $I \equiv r^2 \equiv 1(3)$. Mirando módulo 9, hay 4 opciones para el resto de $I$. Cada una de ellas induce una congruencia módulo 3 para $s$, y, como $J$ se determina módulo 27 en base a $r, s$, que ya tenemos determinado $J$. Esquematizamos con la siguiente tabla.

| $s$ | $I \equiv 1 - 3s(9)$ | $J \equiv -2r + 9rs(27) \equiv r(9s - 2)$ |
|---|---|---|
| 0 | 1 | $\pm 2$ |
| 1 | 7 | $\pm 7$ |
| 2 | 4 | $\pm 16$ |

Cuadro 1: Tabla con conguencias de elegibilidad

□

# 6. El rango promedio de las curvas elípticas

Sea $E/\mathbb{Q}$ una curva elíptica. Recordar que podemos escribirla como

$$E : y^2 = x^3 + Ax + B, \tag{15}$$

donde $A$ y $B$ son enteros, vía cambiar variables. En particular, imponiendo la condición de minimalidad siguiente:

$$\text{si un primo } p \text{ verifica } p^6|B, \text{ luego } p^4 \nmid A,$$

el conjunto de las ecuaciones de la forma anterior conforma un conjunto de representantes para las curvas elípticas sobre $\mathbb{Q}$ módulo isomorfismo. Sean $I = -3A$, $J = -27B$ y consideremos la altura

$$H(E) = H(I, J) = \text{máx}\left(|I|^3, \frac{J^2}{4}\right),$$

que es $\frac{4}{27}$ veces la altura usual. Nuestro interés es usar la parametrización de los elementos del grupo de Selmer para estimar el rango de las curvas elípticas en familias **grandes**. En específico, nos interesa la cantidad

$$\frac{\sum_{E\in\mathcal{E}_X}(\#Sel^2(E) - 1)}{\sum_{E\in\mathcal{E}_X} 1},$$

donde $\mathcal{E}_X$ es el conjunto de curvas elípticas a menos de isomorfismo y de altura acotada por $X$, que podemos pensar como la familia de curvas de altura menor a $X$ dadas por ecuaciones de la forma (15) (y que veremos que se puede reemplazar por familias grandes $F$). Para realizar estos conteos vamos a usar consideraciones locales. Notar que ya hemos contado las formas cuárticas a menos de equivalencia por $GL_2(\mathbb{Z})$. Como $-Id$ actúa trivialmente, estas clases de equivalencia coinciden con las clases de $PGL_2(\mathbb{Z})$. Para pasar de $PGL_2(\mathbb{Z})$ a $PGL_2(\mathbb{Q})$, debemos pesar por cuantas órbitas por $PGL_2(\mathbb{Z})$ hay en una sola clase de $PGL_2(\mathbb{Q})$-equivalencia. Sea $n(f)$ el número de tales órbitas. Sea

$$m(f) = \sum_{f'\in B(f)} \frac{\#Aut_{\mathbb{Q}}(f')}{\#Aut_{\mathbb{Z}}(f')},$$

donde $B(f)$ es un conjunto completo de representantes para $PGL_2(\mathbb{Z})$ actuando sobre $PGL_2(\mathbb{Q}) \cdot f$ y $Aut_R$ denota estabilizadores cuando estamos considerando las acciones de los grupos generales proyectivos sobre un anillo $R$ - a diferencia de los estabilizadores usuales que denotábamos como $Stab_R$. Por el mismo argumento hecho en el conteo para probar el Corolario 4.15, podemos usar $m(f)$ en lugar de $n(f)$ como multiplicidad de nuestros representantes, salvo una cantidad de orden asintótico fijo.

En [BS15a], se prueba el teorema para curvas elípticas en familias grandes. Vamos a definir estas nociones.
Para cada primo $p$, sea $\Sigma_p$ un cerrado de $\mathbb{Z}_p$, donde $\Sigma_p \cap \{\Delta = 0\} = \emptyset$ y $\partial\Sigma_p$ es medida cero. Sea $F_\Sigma$ el conjunto de curvas elípticas sobre $\mathbb{Q}$ cuyos invariantes están en $\Sigma_p$ para cada primo $p$. Agregamos condiciones de congruencia en infinito a $F_\Sigma$ pidiendo que las curvas cumplan que sus invariantes $(I, J)$ estén en $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) > 0\}$, o bien en $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) < 0\}$ o bien en $\{(I, J) \in \mathbb{R}^2 : \Delta(I, J) \neq 0\}$. Decimos que $F_\Sigma$ **está definida por condiciones de congruencia**. Sea $F$ una familia de curvas elípticas sobre $\mathbb{Q}$ no vacía. Supongamos que está definida por condiciones de congruencia. Denotamos $Inv(F)$ a los pares de enteros que son invariantes de curvas en $F$. Denotamos $Inv_p(F)$ a la clausura $p$-ádica de $Inv(F)$ en $\mathbb{Z}_p$, sacando aquellos elementos donde $\Delta(I, J) = 0$. Denotamos $Inv_\infty(F)$ al conjunto:

$$\begin{cases} \{(I, J) \in \mathbb{R}^2 : \Delta(I, J) > 0\}, & \text{si } F \text{ contiene solamente curvas con } \Delta > 0 \\ \{(I, J) \in \mathbb{R}^2 : \Delta(I, J) < 0\}, & \text{si } F \text{ contiene solamente curvas con } \Delta < 0 \\ \{(I, J) \in \mathbb{R}^2 : \Delta(I, J) \neq 0\} & \text{si } F \text{ contiene curvas con } \Delta > 0 \text{ y } \Delta < 0. \end{cases}$$

Una familia $F$ se dice **grande** si para todos salvo finitos $p$, $Inv_p(F)$ contiene todos los pares $(I, J)$ de $\mathbb{Z}_p \times \mathbb{Z}_p$ tal que $p^2 \nmid \Delta(I, J)$.

Sea $F$ una familia grande de curvas elípticas, sea $Inv(F)$ el conjunto de invariantes de formas en $F$ y sea $S(F)$ el conjunto de formas localmente solubles enteras con invariantes $2^4 I$, $2^6 J$, $(I, J) \in Inv(F)$. Si pesamos $S(F)$ por $\frac{1}{m(f)}$, estamos considerando todas las formas localmente solubles con invariantes prescriptos iguales a los invariantes de las curvas en $F$. Por ende, **la cantidad de órbitas pesadas de formas en $S(F)$ de altura acotada por $X$ coincide asintóticamente con la cantidad de elementos no identi-**

**dad del Grupo de Selmer de las curvas $E$ en $F$ de altura acotada**.

El hecho de pesar con $m(f)$ es lo que permite la aparición de las consideraciones locales. Sea, para cada $p$, $m_p(f)$ el peso definido análogamente a $m(f)$ reemplazando $\mathbb{Q}$ por $\mathbb{Q}_p$, $\mathbb{Z}$ por $\mathbb{Z}_p$. Luego tenemos el siguiente lema:

**Lema: 6.1.** *Si $f$ tiene discriminante no nulo,*

$$m(f) = \prod_p m_p(f).$$

Este lema será probado en la siguiente subsección.

## 6.1. Números de clase de grupos algebraicos

En esta sección probaremos el lema previo, usando que $PGL_2(\mathbb{Q})$ tiene número de clase 1. Para ello, daremos suficiente background en grupos algebraicos, adeles y números de clase para enunciar la definición general del número de clase y probaremos en el camino algunos resultados interesantes acerca de casos elementales de teoría de reducción. Luego, probaremos la proposición. En general, el número de clase de un grupo algebraico controla el tamaño del grupo en base a "medirlo" utilizando los puntos $K$-racionales, así como el grupo de adeles enteros. Esta construcción abarca diversas construcciones aritméticas, como la asociada a formas cuadráticas y anillos de enteros.

### 6.1.1. Grupos algebraicos lineales

En esta sección tomamos la siguiente convención para nuestra geometría (que es acorde a [Pla23]): nuestras variedades están consideradas sobre un cuerpo de trascendencia infinita sobre $K$, algebraicamente cerrado, y usamos la noción de "estar definido sobre $K$" para significar que las ecuaciones del ideal que definen la variedad tienen coeficientes en $K$. En general, nuestros grupos algebraicos lineales los consideraremos como subgrupos de $GL_n$, pero damos por completitud una definición general.

**Definición: 6.2.** Un **grupo algebraico lineal** es una variedad afín $X$ equipada con dos mapas $\mu : X \times X \to X$, $i : X \to X$ algebraicos tal que $(X, \mu, i)$ es un grupo.

Por ejemplo, los subgrupos del grupo de matrices $GL_2$ que están dados por condiciones cerradas (es decir, cuyos puntos son soluciones a ecuaciones polinomiales, por ejemplo: $SL_2$). Otro (no-)ejemplo son las curvas elípticas: si bien son grupos algebraicos, no son lineales, en tanto no son variedades afines. Son un ejemplo de lo que se conoce como variedad abeliana.
La ley de grupo impone condiciones geométricas en la variedad. Por ejemplo, tenemos la siguiente proposición:

**Proposición: 6.3.** *Un grupo algebraico lineal es una variedad suave.*

*Demostración.* Por [Har08] (capítulo 1, Teorema 5.3) hay al menos un punto no singular. Como $\mu$ e $i$ son algebraicos, hay un isomorfismo, para cada $x \in X$, que envía $y \to yx$. Esto dice que $X$ es *homogénea*, en particular, se ve localmente igual en todos lados. Como ya tenemos un punto de suavidad, todo otro punto debe ser suave. □

### 6.1.2. Adeles e ideles

Sea $K$ un cuerpo de números. Sea $M = M_K$ su conjunto de lugares a menos de equivalencia. Notemos $M^\infty$ a los lugares infinitos o arquimedianos, y $M^f$ a los lugares finitos, asociados a primos.

**Definición: 6.4.** El **grupo de adeles de** $K$ es el producto restringido

$$A_K = \prod_{v \in M}{}' K_v,$$

a lo largo de los subanillos $\mathcal{O}_v$. Esto quiere decir que, dada una tupla $(x_v)$ en el anillo de adeles, salvo finitos $v$, $x_v \in \mathcal{O}_v$. A $A_K$ lo dotamos de las operaciones coordenada a coordenada, pero no de la topología producto, sino de la **topología adélica**: una base de abiertos es de la forma: si

$$M^\infty \subseteq S \subseteq M,\ \#S < \infty,$$

elegimos $W_v \subseteq K_v$ abiertos para los lugares $v \in S$ y un abierto básico es

$$A_K(S) = \prod_{v \in S} W_v \times \prod_{v \notin S} \mathcal{O}_v.$$

Como cada $K_v$ es localmente compacto, salvo los lugares infinitos, y contiene un subgrupo compacto $\mathcal{O}_v$, $A_K(S)$ es localmente compacto, tal que $A_K$ es localmente compacto. Esta teoría tiene su contraparte multiplicativa:

**Definición: 6.5.** El producto restringido de los grupos $K_v^*$ respecto $\mathcal{O}_K^*$ se denomina **grupo de ideles de** $K$. Lo notamos $J_K$.

Lo dotamos de una topología análoga a la de los adeles, pero debemos observar que esta topología no coincide con la subespacio. Podemos embeber $K$ en $A_K$ y $K^*$ en $J_K$ vía el embedding diagonal

$$x \to (x, x, x, \cdots).$$

**Proposición: 6.6.** *$K$ es discreto en $A_K$.*

*Demostración.* Sin pérdida de generalidad, veamos que $0 = (0)_v$ es un punto aislado en $A_K$. Sea $x$ tal que $x$ está en un entorno de cero, suficientemente chico. Entonces, está en un entorno básico de 0 y esto se traduce en que hay un número finito de lugares $v_i$, cada uno asociado a un abierto $U_v \subseteq K_v$, que contienen al 0, tal que

$$\begin{cases} |x|_v \ll 1 & v = v_i, \\ |x|_v \leq 1 & . \end{cases}$$

Por la fórmula del producto,

$$1 = \prod_v |x|_v < 1,$$

lo cual es absurdo, salvo $x = 0$. □

De la misma manera se obtiene que

**Proposición: 6.7.** *$K^*$ es discreto en el grupo de ideles.*

**Moraleja: 6.8.** *Con la multiplicación coordenada los adeles son un anillo topológico.*

Veremos ahora que $K$ es compacto en $A_K$. Esto indica que podemos tratar de estudiar una teoría de reducción para $A_K$ relativo a $K$, bajo la acción por translación. Seguimos ( [Lan10], capítulo VII).

**Lema: 6.9.** *El cociente $K\backslash A_K$ es compacto.*

*Demostración.* Primero observemos que

$$K + A_\infty = A_K,$$

donde $A_\infty = A_K(S)$ con $S = M^\infty$. Sea $x \in A_K$. Basta hallar un $t \in K$ tal que $x - t$ tiene componentes enteras fuera de los lugares infinitos. Como $x$ es entero salvo en finitos lugares, podemos tomar un entero en $\mathbb{Z}$, $m$, suficientemente grande tal que $mx$ es entero para todos los lugares finitos. Ahora buscamos un $t$ tal que $x - t$ sea entero en cada lugar. Notar que si encontramos un entero muy divisible por $m$, tendremos que en los lugares donde $x$ ya era entero, tenemos una resta de enteros, así que tendremos un entero; en los lugares donde "había denominadores", que $m$ corrigió, la resta $mx - t$ será muy divisible por $m$, así que $x - \frac{t}{m}$ será entero allí. Esto sugiere considerar un elemento $t$ tal que, para cada $\mathfrak{P}|m$,

$$xm - t \equiv 0(\mathfrak{P}^l),$$

donde el $l$ es suficientemente grande para garantizar lo anterior. Entonces, hallando $t \in \mathcal{O}_K$ por el teorema chino del resto y pasando $t$ por el embedding diagonal, tenemos que $t/m \in K$ y $x - t/m \in A_\infty$.

Con esto, tomemos $x \in A_k$. A menos de $K$-equivalencia, podemos suponer que está en $A_\infty$. Embebiendo $\mathcal{O}_K \hookrightarrow \mathbb{R}^{r+2s}$, sabemos que el anillo de enteros es un reticulado, y podemos trasladar $x$ por un entero tal que sus componentes finitas están acotadas. Esto indica que todo elemento de $K\backslash A_K$ tiene un representante en un compacto de $A_\infty$, probando la proposición. □

Un importante paso que hicimos en la demostración merece ser resaltado aparte.

**Teorema: 6.10** (Aproximación fuerte adélica)**.** *Tenemos la descomposición*

$$A_K = K + A_\infty.$$

**Teorema: 6.11** (Teoría de reducción para $K\backslash A_K$)**.** *Hay un dominio fundamental para la acción de $K$ en $A_K$. Explícitamente, sea $w_1, \cdots, w_n$ una base de $\mathcal{O}_K$. Sea $F_\infty$ el paralelogramo fundamental para $\mathcal{O}_K$, visto en los adeles vía considerar el subconjunto $F$ de $\prod_{v\in M^\infty} K_v$ que generan los vectores $\sum_i t_i w_i$, $0 \leq t_i < 1$. Luego, un dominio fundamental para $K$ sobre $A_K$ es*

$$F' = \prod_{v\in M^f} \mathcal{O}_v \times F.$$

Notar que esta proposición dice que para hallar representantes de la acción basta controlar las componentes arquimedianas, entendidas como el látiz en $\mathbb{R}^{r+2s}$ que define el anillo de enteros.

*Demostración.* Dado $x \in A_K$, lo llevamos vía $t$ a $A_\infty$. Este elemento ahora está en todos los $\mathcal{O}_v$, así que es entero, y podemos hallar, módulo un único elemento de $\mathcal{O}_K$, un representante en el paralelogramo fundamental. □

La teoría de la reducción está relacionada con la teoría de aproximación en grupos, de la cual el fenómeno que usaremos es el de aproximación fuerte. En esencia, la aproximación fuerte es una vasta generalización del teorema chino del resto. Damos ahora las definiciones pertinentes, que usaremos en la subsección siguiente.

**Definición: 6.12.** Sea $S$ un subconjunto arbitrario no vacío de lugares de $K$. El anillo de $S$**-adeles** es el truncamiento de $A_K$ en los lugares que no están en $S$, es decir, la imagen de la proyección de $A_K$ a

$$\prod_{v\notin S}{}' K_v.$$

Lo denotamos $A_S$. Los puntos de $G$ en este anillo se denotan $G_{A_S}$.

La noción de aproximación fuerte pide que el embedding de los puntos $K$-racionales, una vez que restringimos suficientes lugares, se vuelva denso.

**Definición: 6.13.** $G$ tiene **aproximación fuerte respecto a** $S$ si

$$G_K \hookrightarrow G_{A_S}$$

es denso. Si $G$ tiene aproximación fuerte respecto a $S = M^\infty$, decimos que tiene **aproximación fuerte absoluta**.

Notar que esto dice que $G_K \prod_{v\in S} G_v$ es denso en $G_{A_K}$.

### 6.1.3. Puntos adélicos en grupos algebraicos lineales

Sea $G$ un grupo algebraico lineal definido sobre $K$. Lo consideramos embebido en $GL_n$, y por ende en un espacio afín suficientemente grande $\mathbb{A}^n$, del cual es una subvariedad cerrada. Los puntos adélicos de $G$ son $G_A := G(A_K)$, es decir, el conjunto de puntos de adeles tales que verifican las ecuaciones que definen a $G$. Siguiendo el capítulo $V$ de [Pla23], podemos ver que las definiciones de puntos adélicos y $S$-adélicos no dependen del embedding, y, más aún, que los puntos $G_A$ se recuperan de los puntos $GL_{n,A}$ vía intersecar con $\prod_v G_v$, con $G_v := G(K_v)$, los puntos que $G$ ve en $K_v$.

En paralelo con lo hecho para $K$ (es decir, para el grupo algebraico aditivo $G_a$), tenemos que $G_A$ es el producto restringido de los grupos $G_v$ respecto los subgrupos $G_{\mathcal{O}_v}$. El embedding $G_K \to G_A$ es discreto, y, si

$$M^\infty \subseteq S \subseteq M,\ \#S < \infty,$$

podemos definir

$$G_{A_K(S)} = \prod_{v \in S} G_v \times \prod_{v \notin S} G_{\mathcal{O}_v},$$

el grupo de adeles de $G$, $S$-enteros. Dada la topología adélica, estos subconjuntos son abiertos de $G_A$. Si $S = M^\infty$, $G_{A_K(S)} := G_{(\infty)}$.

**Definición: 6.14.** Sea $G$ como antes. El **número de clase** de $G$ se define como el mínimo entero $h$ tal que

$$G_A = \bigcup_{i=1}^{h} G_{(\infty)} x_i G_K,$$

donde la descomposición de la derecha es en doble-cosets.

En general, el hecho más importante a este respecto es el siguiente:

**Teorema: 6.15** ( [Pla23], Teorema 5.1)**.** *El número de clase de $G$ es finito.*

Solamente necesitaremos que el número de clase de $PGL_2$ lo es (más precisamente, que es 1). Basta con demostrar que esto vale para $GL_2$. A continuación lo probaremos para $n$ arbitrario (pero siempre manteniendo

el cuerpo base como $\mathbb{Q}$. En general, si $GL_n$ lo consideramos sobre un cuerpo de números $K$, $cl(GL_n) = cl(K)$). Lo haremos en dos pasos: primero veremos que podemos deducirlo de $SL_2$ (resp. $SL_n$) y $G_m = \mathbb{R}^*$ el toro de dimensión 1. Luego, usando aproximación fuerte para $SL_n$, concluiremos efectivamente el resultado.

**Proposición: 6.16.** *Sea $G = HN$ un producto semidirecto, donde $N$ es normal en $G$ y tiene aproximación fuerte absoluta. Luego:*

1. *$N_A$ es normal en $G_A$;*
2. *Se tiene $c(G) \leq C(H)$.*

*Demostración.*

1. El subgrupo $N_A$ es normal pues sus entradas, al igual que las entradas de $G_A$ tienen elementos de $K_v$, y estamos suponiendo que $N$ es normal en $G$. Por otro lado, hay un isomorfismo $G \cong H \times N$, con lo cual, tomando puntos adélicos, obtenemos un isomorfismo $G_A \cong H_A \times N_A$, que induce la descomposición $G_A = H_A N_A$;

2. Como $N_{(\infty)} \subseteq N$ es abierto, también lo es $x^{-1}N_{(\infty)}x$ para cualquier $x$ en $G_A$. Como $N$ tiene aproximación fuerte absoluta, $N_{A_{M^\infty}} = N_\infty$ verifica que $N_K$ es denso en $N_A$. Afirmamos que

$$N_A = (x^{-1}N_{(\infty)}x)N_K.$$

En efecto, si $y \in N_A$, $x^{-1}N_{(\infty)}x$ corta a $N_\infty N_K y^{-1}$, así que
$y \in (x^{-1}N_{(\infty)}x)N_\infty N_K$. Notando que $N_\infty$ se contiene en $N_{(\infty)}$ y, más aún, que es normal allí, pues en $N_{(\infty)}$ los lugares no-arquimedianos tienen elementos enteros, deducimos que

$$N_A = (x^{-1}N_\infty x)N_K.$$

Poniendo $x = 1$, $N_A = N_{(\infty)}N_K$, así que

$$xN_{(\infty)}N_K = xN_A = N_{(\infty)}xN_K.$$

Usando esto,

$$G_A = H_A N_A = H_A N_{(\infty)} N_K = N_{(\infty)} H_A N_K,$$

donde el primer igual vale por el inciso previo, el segundo por lo ya probado, y el tercero por el hecho de que para todo $x \in G_A$, $xN_{(\infty)}N_K = N_{(\infty)}xN_K$. Finalmente, cualquier descomposición en doble cosets de $H_A$ se traslada a una descomposición de $G_A$, lo cual implica la cota de los números de clase.

□

Nuestro objetivo es demostrar el siguiente teorema:

**Teorema: 6.17.** *El número de clase de $GL_n$, definido sobre $\mathbb{Q}$, es 1.*

La estrategia será usar la Proposición 6.16 para la descomposición $GL_n = HN$, con $H = G_m$, $N = SL_2$. Utilizaremos algunos resultados previos para ver que estamos en las hipótesis de la proposición.

**Lema: 6.18.** *El grupo afín $G_a^n \cong \mathbb{A}^n$ tiene aproximación fuerte.*

*Demostración.* Esto es una consecuencia del teorema de aproximación fuerte para adeles probado en 6.10 y 6.11. □

**Teorema: 6.19** ( [Sch23], Prop. 4.8.4)**.** *El grupo $SL_n$ definido sobre $\mathbb{Q}$ tiene aproximación fuerte para cualquier conjunto finito $S$ con $M_{\mathbb{Q}}^{\infty} \subseteq S \subseteq M_{\mathbb{Q}}$.*

*Demostración.* Como esto funciona para cualquier cuerpo de números (o cualquier cuerpo global), probaremos ese resultado más general.
Tenemos que $SL_n =< U_{ij} >_{i \neq j}$, con $U_{ij}(a)$ la matriz elemental dada por $I + aE^{ij}$, $a \neq 0$, $i \neq j$. Para cada $(i, j)$ fuera de la diagonal, podemos considerar los subgrupos

$$\begin{cases} U_{ij}^{+} = \{U_{ij}(a) : a \in \mathbb{Q}\} & i < j, \\ U_{ij}^{-} = \{U_{ij}(a) : a \in \mathbb{Q}\} & i > j. \end{cases}$$

Tenemos que $U_{ij}^{\pm} \cong G_a$ y que

$$< U_{ij}^{+}, U_{ij}^{-} > \cong SL_2.$$

En particular, si probamos la aproximación fuerte para $SL_2$, la obtendremos para $SL_n$.

Sea $v_0$ un lugar fuera de $S$. Tenemos un embedding coordenado

$$SL_{2,K_{v_0}} \hookrightarrow SL_{2,A_S}.$$

Por otro lado, los grupos $U_{ij}^{\pm}$ también están embebidos en $SL_{2,v}$.
Sea $(i,j) = (1,2)$. Tenemos que

$$U_{12}^{+} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in K, \right\} \cong K,$$

$$U_{12}^{-} = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} : a \in K, \right\} \cong K.$$

Por aproximación fuerte para $K$, el embedding $U_{12}^{\pm} \to A_S$ es denso, así que pasando por los isomorfismos, tenemos que

$$\overline{U}_{ij}^{+} = \left\{ \left( \begin{pmatrix} 1 & a_v \\ 0 & 1 \end{pmatrix} \right)_v : v \notin S,\ a_v \in \mathcal{O}_v \text{ salvo finitos} \right\},$$

mientras que:

$$\overline{U}_{ij}^{-} = \left\{ \left( \begin{pmatrix} 1 & 0 \\ a_v & 1 \end{pmatrix} \right)_v : v \notin S,\ a_v \in \mathcal{O}_v \text{ salvo finitos} \right\}.$$

Poniendo en todos los lugares 0 salvo en el de $v_0$, vemos que $U_{ij}^{\pm}(K_{v_0}) \subseteq \overline{SL_{2,K}}$. En particular, iterando esto sobre todo $v \notin S$, hallamos que la clausura de $SL_{2,K}$ contiene a todos los $SL_{2,K_v}$. Esto es suficiente: la clausura contiene a todos los productos finitos de $SL_{2,K_v}$, y por ende a los abiertos básicos. □

Ya estamos en posición de demostrar que el número de clase de $GL_2$ sobre $\mathbb{Q}$ es 1.

*Demostración del Teorema 6.17.* Sea $G = GL_n$ y consideremos $f = det$ el mapa determinante, que induce una sucesión exacta corta

$$1 \to SL_n \to G \to G_m \to 1,$$

con $G_m$ el toro de dimensión 1. Luego, $GL_n = SL_n G_m$. Observar que $G_{m,A}$ se identifica con los ideles de $\mathbb{Q}$, $J_{\mathbb{Q}}$, puesto que son los adeles invertibles.

Por ende, $G_{m(\infty)}$ es $J_{\mathbb{Q},(\infty)}$, y afirmamos que $J_{\mathbb{Q}} = J_{\mathbb{Q}}(\infty)\mathbb{Q}^*$ (notar que los puntos $\mathbb{Q}$-racionales de $G_m$ son $\mathbb{Q}^*$). Consideremos el mapa

$$J_{\mathbb{Q}} \twoheadrightarrow I_{\mathbb{Q}},\ (x_p)_{p<\infty} \to \prod_{p<\infty} (p)^{v_p(x)},$$

donde el codominio es el conjunto de ideales fraccionarios de $\mathbb{Q}$. Como $x$ es un idele, las valuaciones en cada lugar de $x$ dan 0, salvo en finitos, así que el producto está bien definido. El mapa es suryectivo, y su kernel es el conjunto de todos aquellos ideles con coordenada entera en los lugares finitos, es decir, $J_{\mathbb{Q}(\infty)}$. En particular, se induce un isomorfismo

$$J_{\mathbb{Q}}/J_{\mathbb{Q}(\infty)} \cong I_{\mathbb{Q}}.$$

Notando que los ideales principales de $\mathbb{Q}$, $P_{\mathbb{Q}}$, coinciden con la imagen de $\mathbb{Q}^*$ por el isomorfismo, obtenemos que

$$\frac{J_{\mathbb{Q}}}{J_{\mathbb{Q}(\infty)}\mathbb{Q}^*} \cong Cl(\mathbb{Q}).$$

Ahora bien, $\mathbb{Q}$ tiene class number 1, así que este mapa debe ser el único mapa al grupo 0. En particular, $J_{\mathbb{Q}} = J_{\mathbb{Q}(\infty)}\mathbb{Q}^*$. Esto dice que $C(G_m) = 1$ (definido sobre $\mathbb{Q}$).

Por el Lema 6.1.3, sabemos que $SL_n$ tiene aproximación fuerte (absoluta). En particular, se sigue de la Proposición 6.16 que $GL_n$ cumple que:

$$C(G) \leq C(G_m) = 1.$$

□

Usando que $GL_2$ tiene número de clase 1, ya podemos probar el Lema 6.1.

*Demostración del Lema 6.1.* Sea $PGL_2(\mathbb{Q})_f$ el conjunto de elementos $\gamma \in PGL_2(\mathbb{Q})$ tal que $\gamma \cdot f \in V_{\mathbb{Z}}$. Análogamente definimos $PGL_2(\mathbb{Q}_p)_f$, cambiando $\mathbb{Q}$ por $\mathbb{Q}_p$ y $\mathbb{Z}$ por $\mathbb{Z}_p$. Hay un mapa natural de los elementos de $PGL_2(\mathbb{Q})_f$ a las $PGL_2(\mathbb{Z})$-órbitas dentro de la $PGL_2(\mathbb{Q})$-clase de una $f \in V_{\mathbb{Z}}$, el cual tiene la forma $\gamma \to [\gamma]_\sim \cdot f$. Imitando la prueba

del Lema 4.14, tenemos que dos elementos de $PGL_2(\mathbb{Q})_f$ van a la misma órbita si y solo si van al mismo elemento del espacio de doble coclases $PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{Q})_f / Aut_{\mathbb{Q}}(f)$. En particular, el número de elementos de $PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{Q})_f$ que van a la misma órbita $PGL_2(\mathbb{Z}) \cdot f'$ es igual a $\frac{\#Aut_{\mathbb{Q}}(f)}{\#Aut_{\mathbb{Z}}(f')}$. Se deduce que:

$$\#[PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{Q})_f] = \sum_{f' \in B(f)} \frac{\#Aut_{\mathbb{Q}}(f)}{\#Aut_{\mathbb{Z}}(f')} = m(f).$$

Análogamente,

$$\#[PGL_2(\mathbb{Z}_p)\backslash PGL_2(\mathbb{Q}_p)_f] = \sum_{f' \in B(f)} \frac{\#Aut_{\mathbb{Q}_p}(f)}{\#Aut_{\mathbb{Z}_p}(f')} = m_p(f).$$

Sea $\tau$ el embedding diagonal

$$\tau : PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{Q})_f \to \prod_p PGL_2(\mathbb{Z}_p)\backslash PGL_2(\mathbb{Q}_p)_f,$$

y notar que si $p \nmid \Delta(f)$, $PGL_2(\mathbb{Q})_f = PGL_2(\mathbb{Z}_p)$ (pues $p$ no puede dividir a $I$ y a $J$ a la vez). Luego, el producto es finito y $\tau$ está bien definido. Afirmamos que $\tau$ es una biyección - esto alcanza para probar el lema. Es inyectiva pues si $\tau(\gamma) = \tau(\eta)$, $\gamma\eta^{-1} \in PGL_2(\mathbb{Q}) \cap \bigcap_p PGL_2(\mathbb{Z}_p) = PGL_2(\mathbb{Z})$. Por otro lado, para la suryectividad, si $\sigma \in \prod_p PGL_2(\mathbb{Z}_p)\backslash PGL_2(\mathbb{Q}_p)_f$, como $PGL_2(\mathbb{Q})$ tiene número de clase 1, debe haber un $\gamma \in PGL_2(\mathbb{Q})$ tal que $\tau(\gamma) = \sigma$. Como $\gamma \cdot f \in V_{\mathbb{Z}_p} \forall p$, $\gamma \cdot f \in V_{\mathbb{Z}}$. □

## 6.2. Cálculo de las masas locales

Procedamos con las masas locales. Recordemos el teorema del cambio de variable de la sección 4.4 (y recordar que ya hemos calculado la constante $\mathcal{J}$):

**Teorema: 6.20.** *Sea $R \subseteq \mathbb{C}^2$ un abierto y $s : R \to V_{\mathbb{C}}$ tal que es continua y, para cada $(I_0, J_0)$, $I(s_{I_0,J_0}) = I_0$, $J(s_{I_0,J_0}) = J_0$. Luego, existe $\mathcal{J} \in \mathbb{Q}$, no nulo, tal que para toda $\phi : V_{\mathbb{C}} \to \mathbb{R}$ medible,*

$$\int_{v \in PGL_2(\mathbb{C}) \cdot s(R)} \phi(v)dv = |\mathcal{J}| \int_R \int_{PGL_2\mathbb{C}} \phi(g \cdot s_{I,J})\omega(g)dIdJ,$$

*donde consideramos a $PGL_2(\mathbb{C}) \cdot s(R)$ como multiset.*

Queremos ver que esto implica el siguiente resultado, que en [BS15a] aparece como la Proposición 3.7:

**Proposición: 6.21.** *Para cualquier función continua $\phi : V_{\mathbb{Z}_p} \to \mathbb{R}$,*

$$\int_{V_{\mathbb{Z}_p}} \phi(f)df = |27^{-1}|_p \int_{\Delta(I,J)\neq 0} \left( \sum_{f\in V_{\mathbb{Z}_p}^{\sim}} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} \int_{g\in PGL_2(\mathbb{Z}_p)} \phi(g\cdot f)\omega \right) dIdJ,$$

*donde $V_{\mathbb{Z}_p}(I,J)^{\sim}$ es un conjunto de representantes para la acción de $PGL_2(\mathbb{Z}_p)$ en los elementos de $V_{\mathbb{Z}_p}$ de invariantes $I, J$, y $\omega = \omega(g)$ es la forma de volumen que aparece en el teorema de cambio de variables.*

*Demostración.* Alcanza con probarlo localmente, pues toda función continua en $V_{\mathbb{Z}_p}$ es localmente constante en casi todo punto. En particular, podemos suponer que tenemos un $f_0$, de discriminante no nulo, fijo, y debemos construir un entorno $B$ de $f_0$ donde el teorema vale para $\phi = \chi_B$ la indicadora de $B$. El teorema en este caso se transforma en:

$$\int_B df = |27^{-1}|_p \int_{\Delta(I,J)\neq 0} \left( \sum_{f\in V_{\mathbb{Z}_p}^{\sim}} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} \int_{g\in PGL_2(\mathbb{Z}_p)} \chi_B(g\cdot f)\omega \right) dIdJ.$$

La idea es la siguiente: como la acción de $PGL_2(\mathbb{Z}_p)$ viene dada por un mapa $\psi_p : PGL_2(\mathbb{Z}_p) \times (I,J) \to V_{\mathbb{Z}_p}$ que es polinomial y suave, al irnos "cerca" de $f_0$, podemos invertir y hallar un homeomorfismo a un entorno $B$. Allí, hay un sólo elemento de invariantes $(I,J)$ para cada $(I,J)$ que aparece en las formas de $B$, y, a menos de achicar el entorno, los estabilizadores se mantienen constantes, lo cual simplifica la proposición a:

$$\int_B df = |J|_p \int_{Inv(P)} \frac{1}{\#Aut_{\mathbb{Z}_p}(f)} \int_{g\in PGL_2(\mathbb{Z}_p)} \chi_B(g\cdot f)\omega(g)dIdJ,$$

donde $P$ es algún entorno correspondiente a los invariantes. Vamos a construir ese entorno. Sea $P$ un 2-plano genérico que pasa por $f_0$, definido sobre $\mathbb{Q}$. Tenemos el siguiente teorema de la teoría de espacios de Banach sobre cuerpos locales, que extraemos de [Sch11]:

**Teorema: 6.22** ( [Sch11], Proposición 4.3). *Sean $V$ y $W$ espacios de Banach sobre un cuerpo local $K$. Sea $U \subset V$ un abierto y $f : U \to W$ un mapa estrictamente diferenciable en un $v_0 \in U$. Suponer que la diferencial $D_{v_0} f : V \cong W$ es un isomorphismo topológico. Luego, existen $v_0 \in U_0 \subseteq U$, $f(v_0) \in U_1 \subseteq W$ tal que:*

- *$f : U_0 \to U_1$ es un homemorfismo;*
- *El mapa inverso es estrictamente diferenciable en $f(v_0)$;*
- *$D_{f(v_0)} g = (D_{v_0} f)^{-1}$.*

Por ende, podemos hallar en $P$ un entorno $P_0$ de $f_0$ al cual $\Psi_p|_{PGL_2(\mathbb{Z}_p)\times P}$ se restringe como homeomorfismo. Sea $B = PGL_2(\mathbb{Z}_p) \cdot P_0$, considerado como un conjunto, en lugar de un multiset. Usando el teorema de cambio de variables se tiene:

$$\int_B dv = |J|_p \int_{Inv(P_0)} \int_{PGL_2(\mathbb{Z}_p)} \chi_B(g \cdot s_{I,J}) \omega(g) dI dJ,$$

donde $Inv(P_0)$ es el conjunto de invariantes que aparecen en formas de $P_0$. Como $B$ no es un multiset, el lado izquierdo es

$$Vol(B) \cdot \#Aut_{\mathbb{Z}_p}(f).$$

Como hemos invertido y hay un homemorfismo $B \cong PGL_2(\mathbb{Z}_p) \times P_0$, el lado derecho es

$$|J|_p \cdot Vol(PGL_2(\mathbb{Z}_p)) \cdot \int_{Inv(P_0)} dI dJ.$$

En particular, para $B$, $P$, $P_0$ como los dados, esto es equivalente a la ecuación previa, lo cual implica el teorema. □

A modo de corolario, obtenemos:

**Proposición: 6.23.** *Sea $p$ un primo, $\phi$ un mapa continuo en $V_{\mathbb{Z}_p}$ que es $PGL_2(\mathbb{Q}_p)$-invariante. Supongamos que si $f \in Sopp\ \phi$, $\Delta(f) \neq 0$, $f$ es localmente soluble y $2^4 \cdot 3 | I(f)$, $2^6 \cdot 3^3 | J(f)$. Sea, para cada $\sigma \in \frac{E^{I,J}(\mathbb{Q}_p)}{2E^{I,J}(\mathbb{Q}_p)}$, una forma $f_\sigma \in V_{\mathbb{Z}_p}$*

*asociada vía la biyección entre elementos del grupo cociente de la imagen de* $[2]$ *de* $E^{I,J}$ *y formas binarias (ver Teorema 3.18). Luego,*

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df =$$

$$= |27^{-1}|_p Vol(PGL_2(\mathbb{Z}_p)) \int_{\Delta(I,J)\neq 0} \frac{1}{\#E^{I,J}[2](\mathbb{Q}_p)} \sum_{\sigma \in \frac{E^{I,J}(\mathbb{Q}_p)}{2E^{I,J}(\mathbb{Q}_p)}} \phi(f_\sigma) dI dJ.$$

**Observación: 6.24.** Podemos suponer que $f_\sigma \in V_{\mathbb{Z}_p}$ usando los Lemas 3.20, 3.21 y 3.22.

*Demostración.* Por la proposición previa,

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df =$$

$$= |27^{-1}|_p Vol(PGL_2(\mathbb{Z}_p)) \int_{\Delta(I,J)\neq 0} \left( \sum_{f \in V_{\mathbb{Z}_p}(I,J)^\sim} \frac{\phi(f)}{m_p(f) \# Aut_{\mathbb{Z}_p}(f)} \right) dI dJ,$$

donde usamos la $PGL_2(\mathbb{Z}_p)$-invarianza de $\phi$ y $m_p$. Nos interesa tener información asociada a $\mathbb{Q}_p$, pues sabemos que la biyección se pasa bien por ellos, pero tenemos $Aut_{\mathbb{Z}_p}$. Para remediar esto, hacemos el siguiente truco. Sean $f_1, \cdots, f_n$ los elementos de $V_{\mathbb{Z}_p}(I,J)^\sim$ que están en la clase $PGL_2(\mathbb{Q}_p) \cdot f$. Usando $PGL_2(\mathbb{Q}_p)$-invarianza:

$$\sum_{i=1}^{n} \frac{\phi(f_i)}{m_p(f_i) \# Aut_{\mathbb{Z}_p}} (f_i) = \frac{\phi(f)}{m_p(f)} \sum_{i=1}^{k} \frac{1}{\# Aut_{\mathbb{Z}_p}} (f_i) = \frac{\phi(f)}{\# Aut_{\mathbb{Q}_p}(f)}.$$

Con esto, si $V_{\mathbb{Z}_p}(I,J)^{\mathbb{Q}_p\sim}$ se define análogamente a $V_{\mathbb{Z}_p}(I,J)^\sim$, pero cambiando $PGL_2(\mathbb{Z}_p)$ por $PGL_2(\mathbb{Q}_p)$, tenemos que

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df =$$

$$= |27^{-1}|_p Vol(PGL_2(\mathbb{Z}_p)) \int_{\Delta(I,J)\neq 0} \left( \sum_{f \in V_{\mathbb{Z}_p}(I,J)^{\mathbb{Q}_p\sim}} \frac{\phi(f)}{\# Aut_{\mathbb{Q}_p}(f)} \right) dI dJ.$$

Como tenemos una biyección

$$E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p) \xrightarrow{\sim} \{f \in V_{\mathbb{Z}_p}(I,J)^{\mathbb{Q}_p\sim} : f \text{ soluble}\}$$

y un isomorfismo $Aut_{\mathbb{Q}_p}(f) \cong E^{I,J}[2](\mathbb{Q}_p)$, terminamos. □

Esta proposición es clave para calcular la integral de las multiplicidades locales.

**Corolario: 6.25.**

$$\int\limits_{S_p(F)} \frac{1}{m_p(f)} df =$$
$$= \left|\frac{2^{10}}{27}\right|_p Vol(PGL_2(\mathbb{Z}_p)) \int\limits_{(I,J)\in Inv_p(F)} \frac{\#(E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p))}{E^{I,J}[2](\mathbb{Q}_p)} dIdJ.$$

*Demostración.* Tomar $\phi = 1$ en la proposición previa y notar que

$$E^{I,J}(\mathbb{Q}_p) \cong E^{2^4 I, 2^6 J}(\mathbb{Q}_p).$$

□

## 6.3. Conclusión de la prueba

Para finalizar la prueba del teorema de Bhargava–Shankar hemos de obtener cotas para aquellas curvas tales que su discriminante es divisible por un primo $p$ al cuadrado. Esto permitirá usar la fuerza de las técnicas anteriores para la función indicadora de las curvas elípticas con discriminante libre de cuadrados, y así obtener un estimativo para la cantidad de elementos de Selmer. Comencemos con un lema que controla la cantidad de curvas elípticas con altura acotada y discriminante divisible por cierto $p^2$:

**Teorema: 6.26.** *La cantidad de curvas elípticas $E/\mathbb{Q}$ con altura acotada por $X$, tal que $p^2|\Delta(E)$, es $O(X^{5/6}/p^{3/2})$, con la $O$ sin depender de $p$.*

*Demostración.* Esta demostración es similar a la de la *embedding sieve*, en tanto incluiremos el conjunto que nos interesa en otro y usaremos conteos

para el más grande. Consideremos $U_{\mathbb{Z}}$ el conjunto de formas cúbicas en $\mathbb{Z}$, $L$ el subconjunto de formas de la forma $\{x^3 + Ax + B\}$ y el mapa

$$L \to U_{\mathbb{Z}} \to GL_2(\mathbb{Z})\backslash U_{\mathbb{Z}},$$

donde la acción es la usual por cambio de variable lineal, y $L \to U_{\mathbb{Z}}$ es homogeneizar. Sea $u = (A, B, C, D) \in U_{\mathbb{Z}}$. Si $f$ está en la pre-imagen de $GL_2(\mathbb{Z}) \cdot u$, entonces existe una matriz

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

tal que $f = \gamma \cdot u$. En particular, puesto que $f$ es mónica y que

$$\gamma \cdot v = (a^3A + a^2bB + ab^2C + b^3D)x^3 + \cdots,$$

cada $f$ induce una solución $(a, b) = (1, 0)\gamma$ de la ecuación

$$u(x, y) = 1.$$

Al igual que antes, esta asignación es inyectiva, así que por los resultados de Delaunay y Evertsé, las fibras del mapa tienen cardinal uniformemente acotado por 12. Por otro lado, en su trabajo sobre conteo de formas cúbicas [HH71], Davenport y Heilbronn demuestran que la cantidad de $GL_2(\mathbb{Z})$-órbitas en $U_{\mathbb{Z}}$ con $p^2|\Delta$ es $O(X/p^2)$. Combinando esto con el hecho de que $\Delta(u) = \Delta(u(x, 1)) = \Delta(E)$, la cantidad de curvas elípticas que deseamos contar es $O(X/p^2)$. Esto da una primera cota.

En lo que sigue, usaremos varias veces la Proposición 5.1 del libro de Silverman [Sil09], que caracteriza en base a la forma corta de Weierstrass cuándo tenemos reducción mala aditiva o multiplicativa. Para mejorar la cota, consideremos dos subconjuntos dentro del conjunto de curvas elípticas con $p^2|\Delta$. Supongamos primero que $p > 3$ y que la reducción de $E$ en $p$ es aditiva. Luego, debe ser que $p|A$ y que $p|B$, con lo cual hemos de acotar los pares $(A, B)$ que verifican $p|A$, $p|B$, $H(E) < X$. Esto está acotado por $O(X^{5/6}/p^2 + X^{1/2}/p + 1)$. Para $p \geq \sqrt{X}$, podemos usar la cota de $O(X/p^2)$; para $p \leq \sqrt{X}$, podemos usar la cota de $O(X^{5/6}/p^2 + X^{1/2}/p + 1)$; estas dos acotaciones dicen que la cantidad de curvas, en el caso aditivo, es $O(X^{5/6}/p^{5/3})$.

Para el caso multiplicativo, supongamos que $p > 3$. Luego, $p \nmid A$. Debido a que $H(E) < X$, hay $O(X^{1/3})$ opciones para $A$ y $O(X^{1/2})$ opciones para $B$. Una vez fijado el $A$, las reducciones de $B$ módulo $p^2$ quedan determinadas por la divisibilidad, lo cual da $O(1)$ opciones. Entonces, tenemos $O(X^{1/3}(X^{1/2})/p^2 + 1) = O(X^{5/6}/p^2 + X^{1/3})$ elecciones para la cantidad de curvas buscada. Al igual que antes, usando una cota para un intervalo, y otra para otro, obtenemos que la cantidad de curvas, en el caso multiplicativo, está acotada por $O(X^{5/6}/p^{3/2})$. □

Tenemos un análogo al teorema de conteo uniforme, que se sigue, con el mismo error, del lema previo. Si $F$ es una familia grande de curvas elípticas, sean

$$M_p(V, F) = \int\limits_{Inv_p(F)} \frac{\#(E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p))}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ,$$

$$M_p(F) = \int\limits_{Inv_p(F)} dIdJ,$$

$$M_\infty(F, X) = \int\limits_{(I,J)\in Inv_\infty(F), H(I,J)<X} dIdJ,$$

$$M_\infty(V, F, X) = \int\limits_{(I,J)\in Inv_\infty(F), H(I,J)<X} \frac{\#(E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}))}{\#E^{I,J}(\mathbb{R})[2]} dIdJ.$$

Notar que estas cantidades capturan las masas locales, al igual que el tamaño de los invariantes de la familia en cuestión.

**Teorema: 6.27.** *Sea $N(F, X)$ la cantidad de curvas elípticas en $F$ de altura $H(E) < X$. Luego,*

$$N(F, X) = M_\infty(F, X) \prod_p M_p(F) + o(X^{5/6}).$$

Para usar el teorema de conteo libre de cuadrados, debemos cribar las formas con discriminante no libre de cuadrados. En general, decimos que una forma es *mala en $p$*, para un primo $p$, si $f$ no es $\mathbb{Q}_p$-soluble o $m_p(f) \neq 1$. El siguiente teorema afirma que las formas malas en $p$ se encuentran ya contempladas en aquellas las cuales $p^2|\Delta$:

**Teorema: 6.28.** *Si $f$ es mala en $p > 2$, $p^2|\Delta(f)$.*

*Demostración.* Si la multiplicidad local es mayor a 1, por definición existe algún elemento $\gamma \in PGL_2(\mathbb{Q}_p)$, que no está en $PGL_2(\mathbb{Z}_p)$, con $\gamma \cdot f \in V_{\mathbb{Z}_p}$. Triangulando, a menos de reemplazar $f$ por otro elemento de la órbita $PGL_2(\mathbb{Z}_p) \cdot f$ (agregando $p$'s, y como el estabilizador no cambia para formas equivalentes), podemos suponer que $\gamma$ es triangular superior y de la forma

$$\gamma = \begin{pmatrix} p^k & 0 \\ 0 & 1 \end{pmatrix}, \ k > 0.$$

Luego, $p^2|a$, $p|b$, tal que $p^2|\Delta$.

Ahora bien, resta ver el caso en que $f$ no es localmente soluble en $p$. Afirmamos que en este caso, los únicos posibles tipos de descomposición de $f$ en $\mathbb{F}_p$ son $(1^2 1^2)$, $(2^2)$, $(1^4)$ (es decir, dos factores lineales al cuadrado, un factor cuadrático al cuadrado o un factor lineal a la cuarta). Observar que, una vez probado esto, como todas esas formas tienen al menos dos raíces repetidas, $\Delta(f \bmod p) = 0$, y $p^2|\Delta(f)$. Lo haremos en casos:

- Notar que si $p \nmid \Delta(f)$, $f$ es $\mathbb{Q}_p$-soluble ( [Cre92], capítulo 3.6, pág. 80), así que la descomposición de $f$ debe tener cuadrados, para que $f$ tenga una raíz doble en $\mathbb{F}_p$ y luego $p|\Delta(f)$;
- Si $f$ tiene un factor lineal separable en $\mathbb{F}_p$, por el lema de Hensel es $\mathbb{Q}_p$-soluble. Esto cubre las reducciones $(1^2 11)$, $(1^3 1)$;
- Si $f$ tiene tipo de descomposición $(1^2 2)$, podemos suponer que su reducción módulo $p$ tiene a cero como raíz, tal que

  $$\overline{f} = \overline{a}x^2(x^2 - \overline{n}y^2),$$

  con $\overline{n}$ residuo que no es cuadrático. Podemos levantar a $\mathbb{Z}_p$:

  $$f = a(x^2 - kpy^2)(x^2 - ny^2),$$

  $p \nmid a$. Si $a$ es un cuadrado en $\mathbb{Q}_p$, $f(1,0)$ es un cuadrado en $\mathbb{Q}_p$, y $f$ es localmente soluble pues podemos tomar $z = a$, $(x,y) = (1,0)$.
  Podemos suponer que $a$ no es un cuadrado. Si $p \nmid x_0$, $x_0^2 - kp$ es un cuadrado en $\mathbb{Q}_p$, así que basta probar que existe una reducción $\overline{x_0}$ tal

que es no nula y $\overline{x_0}^2 - \overline{n}$ es un residuo no cuadrático módulo $p$. Para ello, considerar la lista $\overline{n}, 2\overline{n}, \cdots, (p-1)\overline{n}$. Tiene $p-1$ elementos, así que podemos elegir $x_0^2 = (c+1)\overline{n}$ el primer residuo cuadrático que aparece. Observar ahora que $c\overline{n}$ no es un residuo, así que

$$x_0^2 - \overline{n} = (c+1)\overline{n} - \overline{n} = c\overline{n}$$

tampoco.

□

Consideremos ahora $S_p(F)$ la clausura $p$-ádica de $S(F)$ en $V_{\mathbb{Z}_p}$ y el análogo en infinito de $S_p(F)$, $S_\infty(F)$, el conjunto de formas cuárticas $\mathbb{R}$-solubles de $V_{\mathbb{R}}$ con invariantes en $Inv_\infty(F)$. Siguiendo la demostración del teorema de conteo y usando que el integrando de $M_\infty(V,F,X)$ es $\frac{1}{2}$ (ver Teorema 6.29), tenemos que, si $Vol(PGL_2(\mathbb{R})) := Vol(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))$,

$$N(V_{\mathbb{Z}} \cap S_\infty(F), X) = \frac{1}{27} Vol(PGL_2(\mathbb{R})) M_\infty(V,F,X) + O(X^{3/4+\varepsilon}). \quad (16)$$

Nos resta calcular cómo son asintóticamente las siguientes sumas:

$$S_1 := \sum_{E \in F_{\leq X}} (\#Sel^2(E) - 1),$$

$$S_2 := \sum_{E \in F_{\leq X}} 1.$$

Para $S_1$, recordar que en la subsección del comienzo notamos que la cantidad de órbitas pesadas de formas en $S(F)$ de altura acotada por $X$ coincide asintóticamente con la cantidad de elementos no identidad del Grupo de Selmer de las curvas $E$ en $F$ de altura acotada. En particular, recordando la biyección de los elementos de Selmer, la altura de las formas en este caso debe estar acotada por $2^{12}X$. Por el teorema de conteo uniforme aplicado a la indicadora de las formas con discriminante libre de cuadrados,

$$S_1 = N(V_{\mathbb{Z}} \cap S_\infty(F), 2^{12}X) \prod_p \int_{S_p(F)} \frac{1}{m_p(f)} df + o(X^{5/6}).$$

Por (16), el término de infinito es

$$\frac{2^{10}}{27} Vol(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R})) M_\infty(V,F,X) + O(X^{3/4+\varepsilon}),$$

mientras que por el cómputo de las masas en la Proposición 6.30,

$$\int_{S_p(F)} \frac{1}{m_p(f)} df = \prod_p \left|\frac{2^{10}}{27}\right|_p Vol(PGL_2(\mathbb{Z}_p)) M_p(V,F) + o(X^{5/6}).$$

Juntando ambas igualdades, se tiene que, siguiendo la notación de (16),

$$S_2 = Vol(PGL_2(\mathbb{R})) M_\infty(V,F,X) \prod_p Vol(PGL_2(\mathbb{Z}_p)) M_p(V,F) + o(X^{5/6}).$$

Por otro lado, el teorema de conteo de curvas en $F$ nos dice que

$$S_2 = M_\infty(F,X) \prod_p M_p(F) + o(X^{5/6}).$$

En particular,

$$\frac{S_1}{S_2} = \frac{N(V_{\mathbb{Z}} \cap S_\infty(X)) \prod_p \int_{S_p(F)} \frac{1}{m_p(f)} df + o(X^{5/6})}{M_\infty(F,X) \prod_p M_p(F) + o(X^{5/6})},$$

así que obtenemos que si $X \to \infty$, $\lim_{X\to\infty} S_1/S_2$ coincide con

$$Vol(PGL_2(\mathbb{Z}) \backslash PGL_2(\mathbb{R})) \prod_p Vol(PGL_2(\mathbb{Z}_p)) \frac{M_\infty(V,F,X)}{M_\infty(F,X)} \frac{M_p(V,F,X)}{M_p(F,X)}.$$

Para el cálculo de los últimos dos términos, usamos la siguiente proposición, en la cual el primer ítem se deduce de [Hus04, sección 7 de la introducción] (ver también [Sil94, Corolario 2.3.1]), y el segundo de [BK77].

**Proposición: 6.29.** *Tenemos que:*

1. $$\frac{M_\infty(V,F,X)}{M_\infty(F,X)} = \frac{1}{2};$$

2. $$\frac{M_p(V,F,X)}{M_p(F,X)} = \begin{cases} 1 & p \neq 2 \\ 2 & p = 2. \end{cases}$$

Una consecuencia inmediata de la proposición previa es el siguiente corolario:

**Corolario: 6.30.** *Tenemos que*

$$\frac{M_\infty(V,F,X)}{M_\infty(F,X)}\prod_p \frac{M_p(V,F,X)}{M_p(F,X)} = \frac{1}{2}\frac{M_2(V,F,X)}{M_2(F,X)} = 1.$$

Usando esto y observando que

$$\prod_p Vol(PGL_2(\mathbb{Z}_p)\backslash PGL_2) = \prod_p \left(1-\frac{1}{p^2}\right),$$

arribamos al importante

**Teorema: 6.31** (Bhargava–Shankar)**.** *El tamaño promedio del grupo de Selmer en cualquier familia grande de curvas elípticas sobre* $\mathbb{Q}$*, cuando las mismas son ordenadas por su altura, es* 3*. En particular, el rango promedio de las curvas elípticas sobre* $\mathbb{Q}$ *es* $\leq \frac{3}{2}$*.*

*Demostración.* Usando el Corolario 6.30,

$$\lim_{X\to\infty}\frac{S_1}{S_2} = Vol(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))\prod_p Vol(PGL_2(\mathbb{Z}_p)),$$

así que

$$\lim_{X\to\infty}\frac{S_1}{S_2} = Vol(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))\prod_p \left(1-\frac{1}{p^2}\right) = 2\zeta(2)\zeta(2)^{-1} = 2.$$

□

## 6.4. Heurísticas y conjeturas para los rangos

Concluida la prueba del teorema central de [BS15a], veremos en esta sección un posible marco teórico en el cual situar al resultado, así como diversas conjeturas que buscan predecir la distribución del rango y el grupo de Selmer ante la imposibilidad de controlar el rango de forma general.

Antes de exponer algunas de estas heurísticas, cabe mencionar que existe un algortimo, **mwrank**, que calcula, para muchas clases de curvas, el rango al generar elementos de orden infinito. En realidad, este algoritmo utiliza sucesivos descensos vía (si se puede) 2-isogenías para calcular $E(\mathbb{Q})/2E(\mathbb{Q})$. Esto nos da ciertos generadores del rango, que en principio podrían no ser todos. Para terminar de calcular todos los generadores, en caso de que sea posible el algoritmo calcula una cota superior para el tamaño de los puntos faltantes (tal tamaño se cuantifica con una noción llamada **altura**), y busca entre los finitos puntos de altura menor a tal cota - en lo que se conoce como algoritmo de *saturación* (lo cual es en esencia la demostración del teorema de Mordell-Weil). En particular, usa formas cuárticas para buscar en los espacios homogéneos de $E$ puntos que provengan de $E$. Sin embargo, de ningún método para calcular el rango de una curva elíptica arbitraria se sabe que termine en tiempo finito.

Sea ahora $E/\mathbb{Q}$ una curva elíptica y tomemos un *modelo minimal* de $E$ (ver [Sil09], VII). Para todo $p \nmid \Delta(E)$, podemos reducir módulo $p$, y obtener una curva elíptica sobre $\mathbb{F}_p$. Sea $a_p := p + 1 - \#E(\mathbb{F}_p)$, donde el cardinal se toma sobre la reducción de $E$. A estos lugares los llamamos lugares de **buena reducción**. Si $p|\Delta(E)$, la reducción será **mala** y, dentro de este caso, **multiplicativa** si tenemos una singularidad nodal, **aditiva** si tenemos una singularidad de cúspide. Definimos $a_p$ para los lugares malos como $a_p = 0$ si la reducción es mala aditiva y $a_p = -1$ si la reducción es mala multiplicativa. La $L$-función de $E$ es ( ver [Dar04], sección 2.4):

$$L(E,s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p p^{s})^{-1}.$$

Esta $L$-función converge de manera holomorfa en $Re\ s > \frac{3}{2}$ vía métodos elementales. Del trabajo sobre la modularidad de Wiles, Taylor, Breuil, Conrad, Diamond sabemos que se extiende de manera holomorfa a todo el plano complejo. Tenemos la famosa:

**Conjetura: 6.32** (Conjetura de Birch y Swinnerton-Dyer)**.** *El rango analítico de $E$ es igual al rango algebraico de $E$. Más precisamente,*

$$ord_{s=1} L(E,s) = r_E,$$

*donde $ord_{s=1}$ indica el orden de $s$ como cero de $L$. En particular, $\#E(\mathbb{Q}) < \infty$ si y solo si $L(E,s) \neq 0$.*

La conjetura de Birch y Swinnerton-Dyer está probada en los casos $r = 0, 1$ por el trabajo de Coates, Wiles, Kolyvagin, Gross y Zagier. En el proceso de probar la conjetura, demuestran que el grupo de Tate-Shafarevich es finito. La conjetura también tiene evidencia estadística: Bhargava–Skinner–Wang prueban que $> 66\,\%$ curvas sobre $\mathbb{Q}$ satisfacen la conjetura de Birch y Swinnerton - Dyer en [BSZ14].

A nivel folklore (siguiendo el trabajo de Goldfeld), la conjetura que se tiene es la siguiente:

**Conjetura: 6.33.** *De las curvas elípticas sobre $\mathbb{Q}$, 50 % tiene rango 0 y 50 % tiene rango 1, acorde a los ordenamientos naturales (por altura, por discriminante, por conductor).*

Como mencionamos en la introducción, trabajos de Brumer y Heath-Brown muestran cotas condicionales para el rango en promedio. El paper [BS15a] es el primero en romper la condicionalidad de estas cotas. En trabajos subsiguientes, los autores logran utilizar grupos de Selmer superiores para acotar el rango en promedio al ordenar por altura. Utilizando el 5-grupo de Selmer, prueban que el rango en promedio está acotado por $\frac{177}{200} < 1$. Por otra parte, utilizando geometría de números, son capaces de también acotar el segundo momento del 2-grupo de Selmer ( [BSS21]), y la distribución de estos grupos en diversas familias de curvas (ver, por ejemplo, el trabajo de Bhargava y Ho [BH22]). En cuanto al promedio sobre cuerpos de funciones, tenemos el siguiente resultado de de Jong ( [dJ02]):

**Teorema: 6.34.** *Cuando ordenamos las curvas elípticas sobre $\mathbb{F}_q(t)$ por su altura, el rango promedio es $\leq \frac{3}{2} + O\left(\frac{1}{q}\right)$.*

Tenemos también heurísticas para grupos y rangos de Selmer, cuyo interés proviene, por ejemplo, de usar estos invariantes para arrojar luz sobre el rango. Unas de las heurísticas más importantes en este respecto son

las heurísticas de Poonen-Rains. En su paper [PR11], los autores dan un modelo para tratar de predecir el comportamiento del grupo de Selmer asociado a las isogenías $[p]$. El trabajo requiere varios prerrequisitos de cohomología y variedades abelianas. Como tal, una exposición exhaustiva del mismo se halla fuera de los límites de esta tesis, así que nos limitamos a enunciar las conjeturas que conciernen a los grupos de Selmer. En cuanto al método, la idea principal de [PR11] es interpretar el grupo de Selmer como la intersección de dos subespacios aleatorios en un espacio cuadrático infinito-dimensional, los cuales son isotrópicos para la forma cuadrática y maximales, y modelar la distribución inducida.

La conjetura que obtienen es la siguiente:

**Conjetura: 6.35** ( [PR11, Conjetura 1.1b]). *El tamaño promedio del grupo de Selmer $Sel^p(E)$ es $p+1$.*

Los autores extienden la heurística a números compuestos de la siguiente forma:

**Conjetura: 6.36** ( [PR11, Conjetura 1.4b]). *El tamaño promedio del grupo de Selmer $Sel^n(E)$ es $\sigma(n)$, la suma de divisores de $n$.*

En vista del Teorema 6.31, el trabajo de Bhargava y Shankar puede verse como una **confirmación de las heurísticas de Poonen-Rains** para el caso $p = 2$. En general, se ha logrado progreso en los casos $p = 3$ ( [BS15b]), $p = 5$ ( [BS13b]) y $n = 4$ ( [BS13a]). Cada uno de estos trabajos permite utilizar grupos de Selmer superiores para obtener una correspondiente cota para el rango promedio de las curvas elípticas. En general, la posible iteración de este método para grupos de orden cada vez más alto requiere una estrategia de parametrización análoga en el nuevo contexto. Por una generalización de un resultado de Birch y Swinnerton-Dyer debida a Cassels ( [Cas62]), los $n$-cubrimientos de $E$ inducen divisores racionales de grado $n-1$, que a su vez inducen embeddings proyectivos. En el caso que nos concierne, esto se manifiesta vía la aparición de las formas cuárticas, que dan ecuaciones homogéneas de hipersuperficies en $\mathbb{P}^1$. En el caso general, si bien el lado geométrico aparece vía dichos embeddings, la parametrización no es tan clara. Por ejemplo, en el caso $p = 3$ ( [BS15b]), se prueba que se pueden utilizar formas enteras cúbicas ternarias.

Otra heurística que mencionamos en la introducción es la heurística de Park, Poonen, Voight y Wood, desarrollada en [PPVW19]. En este trabajo, los autores construyen un modelo estadístico asociando a cada curva elíptica $E$ una matriz aleatoria con entradas pertenecientes a $\{-1, 0, 1\}$. Usando un teorema de conteo para tales matrices arriban a su conjetura principal:

**Conjetura: 6.37** ( [PPVW19, 8.2]). *Todas las curvas elípticas sobre* $\mathbb{Q}$*, salvo finitas, verifican que* $r_E \leq 21$.

# 7. Torsión en estadística aritmética

## 7.1. La conjetura de la torsión

En la introducción mencionamos que hay varios problemas que podrían considerarse "de conteo" o "de distribución" para objetos aritméticos, y que podríamos enmarcar estos problemas en el campo de la estadística aritmética. Prosiguiendo en ese espíritu, y ya habiendo terminado con la exposición del teorema de Bhargava–Shankar, el objetivo de esta sección es exponer recientes avances en un problema central de la estadística aritmética, la conjetura de la torsión. Esta conjetura describe el tamaño de los grupos de torsión de cuerpos de números. Sea $K$ un cuerpo de números. Sea $n$ el grado de $K$ y sea $\mathcal{C} := Cl(K)$. Tenemos la siguiente conjetura ( [BST+20], [HB25]):

**Conjetura: 7.1** (Conjetura de la $\ell$-torsión)**.** *Sea $K$ un cuerpo de números de grado $n$ y $\mathcal{C}[\ell]$ el subgrupo de $\ell$-torsión de $Cl(K)$, el grupo de clases de $K$. Luego, para todo $\varepsilon > 0$,*

$$\#\mathcal{C}[l] \ll_{n,\ell,\varepsilon} |\Delta_K|^{\varepsilon}.$$

La conjetura, entonces, afirma que la torsión en los grupos de clase de los cuerpos de números crece más lento que cualquier potencia positiva del determinante. Actualmente, los resultados que se tienen son para casos particulares, restringiendo o bien el grado o bien el nivel de torsión. Denotemos $(n, l)$ a los pares grado-torsión. Se conocen resultados para $(2, 2)$ (caso en el cual, por teoría del género, se conoce la conjetura), $(2, 3)$, $(3, 3)$, $(4, 3)$ ( [EV07], [Pie06], [HV06]), $(n, 2)$ ( [BST+20]). Pre-prints recientes de Lemke-Oliver ( [OZ25]) y Heath-Brown ( [HB25]) producen nuevos resultados. En esta sección exponemos parte de los resultados de Ellenberg–Venkatesh y Bhargava–Shankar–Taniguchi–Thorne–Tsimerman–Zhao. En particular, el primero de ellos da una nueva estrategia para conseguir mejores cotas, al producir y usar primos pequeños no inertes y el principio de reflexión de Scholz, mientras que el segundo usa geometría de números y el método del determinante para transformar el problema en un problema de conteo de generadores de ideales de $m$-torsión.

## 7.2. Los resultados de Ellenberg–Venkatesh

En esta subsección exponemos el siguiente teorema:

**Teorema: 7.2** ( [EV07], Proposición 2)**.** *Sea $D$ libre de cuadrados. Sea $K = \mathbb{Q}(\sqrt{D})$. La 3-torsión del grupo de clases de $K$ es $O_\varepsilon(|D|^{\frac{1}{3}+\varepsilon})$.*

Es importante aclarar, antes de proceder a su demostración, que siempre tenemos una cota "trivial" para la torsión de cualquier grupo de clase, que proviene de acotar todo el grupo. Una tal cota es la **cota de Landau** (que, según afirma Heath-Brown en [HB25], se suele atribuir a Brauer-Siegel, y no es el caso), y fue probada en [Lan18]:

**Lema: 7.3** (Landau)**.** *Sea $K$ un cuerpo de números de grado $n$. Luego,*

$$h(K) \ll |\Delta_K|^{\frac{1}{2}}(log|\Delta_K|)^{n-1}.$$

Esto produce la cota trivial

$$\#Cl(K)[\ell] \ll |\Delta_K|^{\frac{1}{2}+\varepsilon}.$$

En los trabajos [EV07] y [BST+20] se utiliza esta cota en diversas partes, siendo siempre el objetivo final vencerla.

Respecto el Teorema 7.2, su demostración conlleva dos ingredientes: el primero es un resultado acerca del efecto de tomar primos pequeños en la extensión, y el segundo es el principio de reflexión de Scholz. El primero requiere del uso de grupos de clase de Arakelov y nos limitamos a citarlo, refiriendo a [EV07], Lema 3 para su demostración, y a [Sch08] para teoría de grupos de clase de Arakelov.

**Lema: 7.4.** *Sea $L/K$ una extensión de cuerpos de números. Sea $[L : K] = d$. Sea $\ell > 0$ un entero y $\delta < (2\ell(d-1))^{-1}$. Sean $\mathfrak{P}_i$, $1 \leq i \leq M$ ideales primos tal que:*

- *Tienen norma a lo sumo $N_{L/K}(\Delta_{L/K})^\delta$;*
- *Son no ramificados;*
- *No son extensiones de ideales primos de subcuerpos propios que contienen a $K$,*

*donde $\Delta_{L/K}$ es el discriminante relativo de la extensión $L/K$. Luego,*

$$\#Cl(K)[\ell] \ll_{[L:\mathbb{Q}],\varepsilon,\ell} M^{-1}(|\Delta_L|^{\frac{1}{2}+\varepsilon}).$$

Prosigamos demostrando el principio de reflexión de Scholz, que relaciona los 3-rangos de los grupos de clase de $\mathbb{Q}(\sqrt{m})$ y $\mathbb{Q}(\sqrt{-3m})$, y por ende permite "retroalimentar las cotas" que se obtienen para cuerpos cuadráticos. Seguimos esencialmente el paper de Scholz [Sch32].

Para comenzar, expongamos un poco de teoría de Kummer. Sea $G$ un grupo. Su **exponente** es el menor entero $k$ tal que $x^k = 1$ para todo $x \in G$. Sea $K/F$ una extensión de cuerpos de números, finita y Galois. Sea $p$ un primo que no divide a 2. La extensión se dice $N$**-Kummer** si $\xi_p \in F$ y el grupo de Galois de $K/F$ es abeliano de exponente $N$, donde $\xi_p$ es una raíz primitiva $p$-ésima. La teoría de Kummer describe las extensiones $N$-kummer de un cuerpo. Precisamos algo de notación para describir el teorema fundamental. Sea $K/F$ $N$-kummer y $G = Gal(K/F)$. El **dual de Pontryagin** de $G$ es el grupo de caracteres $\hat{G} = Hom(G, \mathbb{C}^*)$. Recordemos que $\hat{G} \cong G$ de manera no-canónica, mientras que $\hat{\hat{G}} \cong G$ de manera canónica. Sea $G'$ definido por

$$G' := \frac{F^* \cap K^{*N}}{F^{*N}} \subseteq \frac{F^*}{F^{*N}}.$$

El **pairing de Kummer** es el pairing $B$,

$$B : G \times G' \to \mathcal{U}_N(F), \quad < \sigma, [a] >= \frac{\sigma(\sqrt[N]{a})}{\sqrt[N]{a}}.$$

Un resultado clásico (ver [Gui18], Teorema 1.22) indica que el pairing de Kummer es un pairing bilineal no degenrado. Con esta terminología, tenemos el teorema fundamental de la teoría de Kummer:

**Teorema: 7.5** ( [Gui18], Teorema 1.25)**.** *Sea $F$ un cuerpo que contiene una raíz primitiva $N$-ésima. Hay una biyección entre las extensiones algebraicas de $N$-kummer de $F$ y los subgrupos finitos de $F^*/F^{*N}$, dada por tomar*

$$K/F \to \frac{F^* \cap K^{*N}}{F^{*N}},$$
$$A \subseteq \frac{F^*}{F^{*N}} \to F(\sqrt[N]{A}).$$

*Además, si $K/F$ corresponde a $A$, el pairing de Kummer induce un isomorfismo de grupos*

$$Gal(K/F) \cong A.$$

Ahora recordemos los teoremas pricipales de la teoría de cuerpos de clase global, siguiendo a Milne [Mil20b]. Sea $K$ un cuerpo de números. Consideremos $I_K$ su grupo de ideales fraccionarios y $S \subseteq K$ un conjunto de primos de $K$, que se supone finito. Sea $I^S :=< \mathfrak{P} : \mathfrak{P} \notin S >\subseteq I_K$ y definamos también $K^S := \{a \in K^* : (a) \in I^S\}$, e $i : K \to I_K$ el mapa que toma clase de ideales a los elementos del cuerpo.

**Definición: 7.6.** Un **módulo** para $K$ es una función

$$\mathfrak{m} :< \mathfrak{P} \in K >\to \mathbb{N}_0,$$

tal que $\mathfrak{m}$ tiene soporte finito, vale 0 en los lugares complejos y vale $\leq 1$ en los lugares reales. Notamos

$$\mathfrak{m} = \prod_{\mathfrak{P}} \mathfrak{P}^{m(\mathfrak{P})}.$$

Observar que podemos separar un módulo en su parte finita e infinita, $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, con $\mathfrak{m}_0 \in K$.

Para cada módulo $\mathfrak{m}$, sea $S(\mathfrak{m})$ el conjunto de primos que dividen a $\mathfrak{m}_0$. Definimos

$$K_{\mathfrak{m},\,1} := \{a \in K^* : v_{\mathfrak{P}}(a-1) \geq m(\mathfrak{P}) \forall \mathfrak{P} | \mathfrak{m}_0,\ \rho(a) > 0 \forall \rho \text{ real } | \mathfrak{m}_\infty\}.$$

Notar que si $a \in K_{\mathfrak{m},\,1}$, $i(a) \in I^{S(\mathfrak{m})}$.

**Definición: 7.7.** El **grupo de rayos de clases módulo** $\mathfrak{m}$ es

$$\mathcal{C}_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},\,1}).$$

Ahora sí, tenemos el llamado teorema de existencia de la teoría de cuerpos de clases:

**Teorema: 7.8** (Existencia)**.** *Sea $H$ un* ***subgrupo de congruencias para el módulo*** $\mathfrak{m}$*, es decir, un subgrupo tal que*

$$K_{\mathfrak{m},\,1} \subseteq H \subseteq I^{S(\mathfrak{m})}.$$

*Luego, existe un extensión abeliana finita $L/K$ tal que:*

- *$L/K$ no ramifica en los primos $\mathfrak{P}$ que no dividen a $\mathfrak{m}$;*
- *El grupo de Galois es $Gal(L/K) \cong \frac{C_{\mathfrak{m}}}{H}$.*

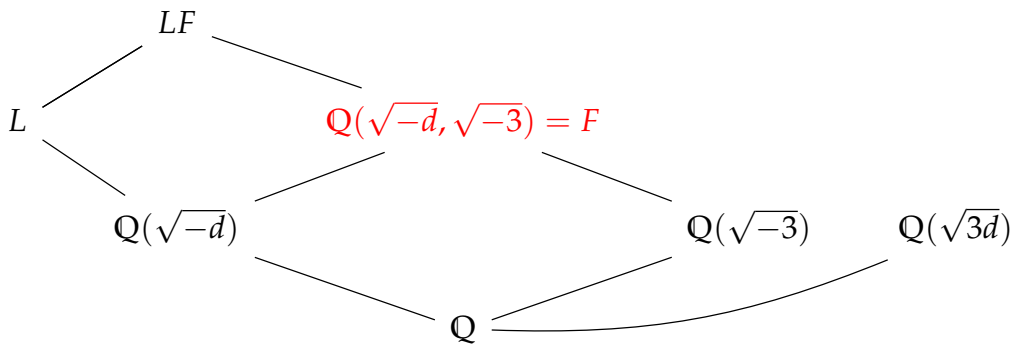
Tomando $\mathfrak{m} = 1$, tenemos que el grupo de clases de rayos módulo $\mathfrak{m}$ es el grupo de clases de $K$. En particular, si $H = P_K$ el grupo de clases de ideales principales fraccionarios de $K$, obtenemos una extensión abeliana no ramificada con grupo de Galois isomorfo al grupo de clases de $K$, el **cuerpo de clases de Hilbert**. Sin embargo, cualquier elección de un $H$ para el módulo trivial devuelve extensiones abelianas no ramificadas con grupos de Galois de índice más grande.
Utilizando la teoría de cuerpos de clase expuesta, probaremos el principio de reflexión de Scholz. Dado un grupo abeliano finito $G$, denotemos $r_3\ G$ a su 3-rango, es decir, al máximo $n$ tal que $G$ admite un 3-subgrupo elemental de orden $3^n$.

**Teorema: 7.9** (Principio de reflexión de Scholz)**.** *Sea $d > 0$ tal que $-d$ es un discriminante diferente de $-3$. Tenemos que:*

$$r_3\ Cl(\mathbb{Q}(\sqrt{3d})) \leq r_3\ Cl(\mathbb{Q}(\sqrt{-d})) \leq r_3\ Cl(\mathbb{Q}(\sqrt{3d})) + 1.$$

*Demostración.* Sean $K = \mathbb{Q}(\sqrt{-d})$, $E = \mathbb{Q}(\sqrt{3d})$, $C = Cl(K)$, $r$ el 3-rango de $\mathbb{Q}(\sqrt{-d})$ y $s$ el 3-rango de $\mathbb{Q}(\sqrt{3d})$. Por teoría de cuerpos de clases, tomando el módulo trivial, las extensiones abelianas cúbicas (y por ende cíclias) no ramificadas de $K$ se obtienen de todos los subgrupos (independientes entre sí) de índice 3 en el grupo de clases de $K$. La cantidad de subgrupos de índice 3 coincide con la cantidad de subgrupos de orden 3, con lo cual hay exactamente $r$ tales extensiones. Por teoría de Kummer (o, como indica Scholz, por un resultado de Hasse - ver [Has30]), sabemos que $L$ se obtiene extendiendo a un número de la forma $v = \sqrt[3]{a + b\sqrt{3d}}$ (o bien con un $-$, o bien la suma de ambos). Sea $\alpha = a + b\sqrt{3d}$ y consideremos el

siguiente diagrama:




donde estamos considerando $F = \mathbb{Q}(\sqrt{-d},\sqrt{3d})$, y $L$ es una extensión cúbica no ramificada de $K$. Al adjuntar $\sqrt{-3}$, volvemos al cuerpo $L$ en una extensión abeliana no ramificada de $K(\sqrt{-3}) = F$. Luego, $L(\sqrt{-3})/F$ tiene grado 3 (por el diagrama) y no ramifica. Se sigue por ( [Gui18], ejercicio 9.1) que, como $v$ genera $L(\sqrt{-3})$ sobre $F$ (notar que $\sqrt{-3} = \frac{\sqrt{3d}}{\sqrt{-d}}$ ya está en $F$), $\alpha$ debe ser el cubo de un ideal $I$ de $F$. Como $v$ ya está en $\mathbb{Q}(\sqrt{3d})$, tomando mapa norma vemos que *$\alpha$ ya es el cubo de un ideal* en $E$ (notar que $F/K$ es de grado 2). Entonces, hemos establecido un mapa de ideales de índice 3 a ideales que son cubo de algún ideal, y además generan los cuerpos de clases descritos antes. Notar que las imágenes de estos cuerpos, $\alpha_i$, no admiten ninguna relación de la forma $\prod_i \alpha_i^{t_i} = \gamma^3$, $\gamma \in F$, salvo que $t_i$ sea múltiplo de 3 para todo $i$, pues cada $\alpha_i$ induce un $v_i$ que genera el cuerpo de clases del ideal correspondiente.

Sean ahora $I_E$ el grupo de ideales fraccionarios de $E$, $I_3$ los ideales que son un cubo, $E^3$ los elementos de $E$ que son un cubo, y análogamente definimos $C^3$ y $W^3$, donde $W$ es el grupo de unidades de $E$. Luego, se tiene que:

$$[I_E^3 : E^3] = [C : C^3][W : W^3].$$

Notar que hemos producido $r$ elementos independientes que son cubos de ideales, así que $[I_E : E^3] \geq 3^r$. Por otro lado, como $3d > 0$, $\mathbb{Q}(\sqrt{3d})$ es un cuerpo cuadrático real y admite dos embeddings a $\mathbb{C}$, ambos reales. Por el teorema de unidades de Dirichlet, $W =< \eta >$ es un grupo isomorfo a $\mathbb{Z}$, así que su cociente por los cubos es isomorfo a $\mathbb{Z}/3\mathbb{Z}$ y tiene orden 3. Por

otro lado, por definición, $[C : C^3] = 3^s$. Luego, $[I_E : E^3] = 3^{s+1}$. Se sigue que

$$3^r \leq 3^{s+1},$$

de lo cual

$$r \leq s + 1.$$

El mismo argumento, pero hecho para permutando los roles de $K$ y $E$, nos lleva a que

$$s \leq r,$$

pues el cuerpo cuadrático imaginario no tiene parte libre en las unidades. Esto prueba el teorema. □

Ahora probemos el Teorema 7.2.

**Teorema: .** *Sea $D$ libre de cuadrados. Sea $K = \mathbb{Q}(\sqrt{D})$. La 3-torsión del grupo de clases de $K$ es $O_\varepsilon(|D|^{\frac{1}{3}+\varepsilon})$.*

*Demostración.* Notar que un primo $p \in \mathbb{Z}$ coprimo con $6D$, e inerte en $\mathbb{Q}(\sqrt{-3})$, se parte en $\mathbb{Q}(\sqrt{D})$ o bien $\mathbb{Q}(\sqrt{-3D})$, pues

$$\left(\frac{-3D}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{D}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{D}{p}\right),$$

por reciprocidad cuadrática, donde $\left(\frac{a}{b}\right)$ es el símbolo de Legendre. Ahora bien, como $p$ es inerte en $\mathbb{Q}(\sqrt{-3})$, $\left(\frac{-3}{p}\right) = -1$. Luego,

$$\left(\frac{-3D}{p}\right) = -\left(\frac{D}{p}\right),$$

así que si uno es 1, el otro es $-1$, y viceversa.

Luego, para algún $d$ entre $\{-3D, D\}$, afirmamos que hay $\gg |d|^{\frac{1}{6}-2\varepsilon}$ primos $p$, con $|d|^{\frac{1}{6}-\varepsilon} \leq p \leq 2|d|^{\frac{1}{6}-\varepsilon}$ que se parten en $\mathbb{Q}(\sqrt{d})$. En efecto, esto se sigue viendo que hay tal cantidad de primos en ese intervalo, inertes en $\mathbb{Q}(\sqrt{-3})$. Esto equivale a que $p$ no sea un residuo cuadrático módulo 3, es decir, que $p \equiv 2(3)$. Por el teorema de densidad de Dirichlet, esto es aproximadamente contar la mitad de los primos en $[|d|^{\frac{1}{6}-\varepsilon}, 2|d|^{\frac{1}{6}-\varepsilon}]$.

Tal cantidad de primos es una resta de las funciones contadoras de primos en $2|d|^{\frac{1}{6}-\varepsilon}$ y $|d|^{\frac{1}{6}-\varepsilon}$. Por el teorema de los números primos, esto es $\gg_\varepsilon \left(\frac{|d|^{\frac{1}{6}-\varepsilon}}{\log|d|}\right)$. Usando que $\log(x) = O(x^\varepsilon)$ para todo $\varepsilon > 0$, tenemos que hay $\gg_\varepsilon |d|^{\frac{1}{6}-2\varepsilon}$ en ese intervalo, inertes en $\mathbb{Q}(\sqrt{-3})$. Por el lema del inicio,

$$\#Cl(\mathbb{Q}(\sqrt{d}))[3] \ll_\varepsilon |d|^{\frac{1}{3}+\varepsilon}.$$

Por el principio de reflexión de Scholz, es inmaterial si $d \neq D$, pues

$$r_3Cl(\mathbb{Q}(\sqrt{-3D})) \leq r_3Cl(\mathbb{Q}(\sqrt{D})),$$

lo cual completa el teorema. □

## 7.3. Los resultados para $(n,2)$

Ahora nos abocamos al paper [BST+20]. Lo que los autores prueban es lo siguiente:

**Teorema: 7.10.** *Sea $K$ un cuerpo de números de orden $n$. Existe una constante $\delta_n$ que depende de $n$ tal que el tamaño de la 2-torsión del grupo de clases de $K$ es $O(|\Delta_K|^{\frac{1}{2}-\delta_n+\varepsilon})$.*

Procedamos a probar este resultado. Recordemos que la teoría de Minkowski nos provee de un embedding $K \to \prod_\sigma \mathbb{C} =: K_\mathbb{C}$, donde el producto está hecho sobre todos los embeddings de $K$ en $\mathbb{C}$, y el mapa envía $x$ a $(\sigma x)$. El espacio de Minkowski $K_\mathbb{C}$ tiene un producto interno dado por el producto interno conjugado. Sea $f : \mathbb{C} \to \mathbb{C}$ la conjugación. El generado por $f$, es decir, es Galois de $\mathbb{C}/\mathbb{R}$, actúa sobre las entradas de $K_\mathbb{C}$, así como sobre $Hom_\mathbb{Q}(K,\mathbb{C})$. En particular, hay una involución $F : K_\mathbb{C} \to K_\mathbb{C}$, $F(x_\tau) = (\overline{x}_{\overline{\tau}})$. Sea $K_\mathbb{R}$ el espacio de elementos invariantes por $F$. La restricción del producto interno vuelve a $K_\mathbb{R}$ un espacio con producto interno e induce una medida de Haar en $K_\mathbb{R}$, $\mu$. Tenemos el teorema de Minkowski (ver [Neu99], cap. 1, sección 5):

**Teorema: 7.11.** *Sea $K_\mathbb{R}$ el espacio de Minkowski real definido previamente.*

1. *Tenemos que hay un isomorfismo $K_\mathbb{R} \cong \mathbb{R}^{r+2s}$, donde $r$ es la cantidad de embeddings reales y $s$ la cantidad de embeddings imaginarios a menos de conjugación, dado por*
$$(z_\tau) \to (x_\tau),$$

*donde si $\tau$ es real, $x_\tau = z_\tau$, y si $\tau$ es complejo, $x_\tau = Re\ z_\tau$, $x_{\overline{\tau}} = Im\ z_\tau$;*

2. *Este isomorfismo transforma la métrica de Minkowski, es decir, la restricción del producto escalar de $K_{\mathbb{C}}$ a $K_{\mathbb{R}}$, al producto escalar pesado*

$$< x, y >= \sum_{\tau} \alpha_\tau x_\tau y_\tau,$$

*donde $\alpha_\tau$ es 1 para los lugares reales y 2 para los complejos;*

3. *Equipemos a $\mathbb{R}^n$ con la medida de Lebesgue, $Vol$, y sea $A \subseteq K_{\mathbb{R}}$ un medible. Luego,*

$$\mu(A) = 2^s Vol(A).$$

4. *Tenemos que $\mu(\mathcal{O}_K)| = \sqrt{|\Delta|}$;*

5. *Para cada ideal fraccionario $I$, $u(I) = N(I)\sqrt{|\Delta|}$.*

La estrategia para acotar el tamaño del grupo de 2-torsión de $Cl(K)$ es obtener cotas directas de la geometría de números para representantes de ideales de 2-torsión, así como control sobre la degeneración de la forma de los latices fraccionarios de $K$. Esto permite transformar el problema en uno más atacable, y las cotas provendrán o bien de la teoría del género, o bien del método de Bombieri-Pila, o bien de la geometría de números. Las dependencias que permitimos a la notación asintótica son en base a $n$.

Para comenzar, tenemos el siguiente teorema:

**Teorema: 7.12.** *Sea $K$ un cuerpo de números de grado $n$. Luego, toda clase de ideales de $m$-torsión admite un representante $I$ que es entero y verifica que existe un $\beta$ con $I^m = (\beta)$, y $|\beta|_v \leq |\Delta_K|^{\frac{m}{2n}}$, para cada $v$ lugar infinito, donde $\Delta_K$ es el discriminante de $K$.*

Recordar que el valor absoluto que induce $v$ es

$$|x|_v = \begin{cases} |\rho(x)| & \text{si } v = \rho \text{ es real,} \\ \sqrt{\sigma(x)\overline{\sigma(x)}} & \text{si } v = \sigma \text{ es complejo .} \end{cases}$$

*Demostración.* Sea $I$ cualquier representante y sea $\alpha$ tal que $I^m = (\alpha)$. Vamos a usar el teorema de Minkowski sobre cuerpos convexos para alterar $\alpha$ y obtener $\beta$. Sean $l_v := |\Delta_K|^{1/2n}|\alpha^{-1/m}|$, $v$ recorriendo los lugares. Vía el isomorfismo del teorema, podemos ver a $J$ como un látiz en $\mathbb{R}^n \cong \mathbb{R}^r \times \mathbb{R}^{2s} \cong \mathbb{R}^r \times \mathbb{C}^s$, y allí su volumen es

$$Vol(I^{-1}) = 2^{-s}\mu(I^{-1}) = 2^{-s}N(I)^{-1}|\Delta|^{1/2}.$$

Ahora, consideramos la caja en $\mathbb{R}^r \times \mathbb{C}^s$ de lados $l_v$. Tenemos que su volumen en los lugares reales es el producto de los $2l_\rho$, mientras que (observando que si $z = x + iy$ es complejo, $|z| < R$ equivale a que $\sqrt{x^2+y^2} < R$) en los lugares complejos es $\pi l_\sigma^2$, es decir, que este paralelepípedo tiene volumen

$$\prod_\rho (2l_\rho)\prod_\sigma \pi l_\sigma^2 \geq 2^r 2^s l^n = 2^{n-s}|\Delta_K|^{n/2n}\prod_v |\alpha|_v^{-1/m}.$$

Notar que esto es

$$2^n(2^{-s}|\Delta_K|^{1/2}N(I)^{-1}) = 2^n Vol(I^{-1}).$$

Por el teorema de Minkowski, existe un punto no trivial de $I^{-1}$ en la caja. Es decir, hay un $\kappa \in I^{-1}$ tal que para cada lugar infinito $v$,

$$|\kappa|_v \leq |\Delta_K|^{1/2}|\alpha|_v^{-1/m}.$$

En particular, si $\beta = \alpha\kappa^m$, $\beta$ cumple lo pedido (observar que, como $\kappa \in I^{-1}$ y $\alpha \in I^m \subseteq I$, $\beta$ es entero, mientras que $(\beta) \sim (\alpha)$ en el grupo de clases). □

El siguiente lema que prueban los autores da control acerca de los elementos de una base del anillo de enteros. Precisamos un resultado clásico de la geometría de números, que es la existencia una base distinguida, llamada **base de Minkowski**, (ver [Cas97], [Min91]) que verifica lo siquiente:

1. $B = \{1, v_1, \cdots, v_n\}$;
2. Si $v_0 = 1$, $|v_i| \leq |v_{i+1}|$ para todo $i$;
3. Si $1 \leq i \leq n-2$ y $v \notin < 1, \cdots, v_{i-1} >$, $|v_i| \ll |v|$;
4. $\prod_{i=1}^n |v_i| \gg\ll \sqrt{|\Delta_K|}$.

Ahora, la idea es acotar por arriba a $|v_{n-1}|$, y, para ello, hallar alguna permutación de la base que permita utilizar las cotas que induce la base de Minkowski. Hallar una tal permutación no nula equivale a que el determinante de la matriz cuyos coeficientes son las coordenadas en $v_{n-1}$ de los productos mixtos $v_i v_j$ no sea cero. Pero esto se puede garantizar; ejemplificamos en 3 dimensiones primero: si $1, v, w$ conforman una base entera de $K$, escribamos

$$vw = a_{12}^0 + a_{12}^1 v + a_{12}^2 w,$$
$$w^2 = a_{22}^0 + a_{22}^1 v + a_{22}^2 w.$$

Veamos que la no invertibilidad de la matriz nombrada previamente nos daría una contradicción. Supongamos que buscamos un $T$ no nulo en $< 1, v >$ tal que $Tw \in < 1, v >$. Escribiendo $T = a + bv + cw$, esto equivale a que la coordenada en $w$ de $Tw$ sea nula. Notar que

$$Tw = aw + bvw + cw^2 = aw + b(a_{12}^0 + a_{12}^1 v + a_{12}^2 w) + c(a_{22}^0 + a_{22}^1 v + a_{22}^2 w).$$

Por ende, la coordenada de $w$ tiene la forma $a + a_{12}^2 b + a_{22}^2 c$. La matriz de $v_{n-1}$-coordenadas tiene la forma

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{11}^2 & a_{12}^2 \\ 1 & a_{12}^2 & a_{22}^2 \end{pmatrix},$$

donde $v^2 = a_{11}^0 + a_{11}^1 v + a_{11}^2 w$. Por ende hallar un tal $T$ es equivalente a que esta matriz tenga núcleo no trivial. Pero, en tal caso, tendríamos que la transformación lineal $L_T : K \to K$ envía todo $K$ a un subespacio de dimensión 2, mientras que como $T \neq 0$, $T$ es inversible. Esto es absurdo. Generalicemos esto:

**Teorema: 7.13.** *Sea $1 = v_0, \cdots, v_{n-1}$ una base de Minkowski del anillo de enteros del cuerpo de números K de grado n. Luego, $|v_{n-1}| \ll |\Delta_K|^{1/n}$.*

*Demostración.* Sea $A$ la matriz que tiene las coordenadas en el lugar de $v_{n-1}$ de los productos mixtos $v_i v_j$. $A$ es simétrica e inversible, puesto que sino procedemos análogo a antes. Se deduce que hay una permutación que aparece en la fórmula de Leibniz, llamémosla $\pi$, tal que $a_{i,\pi(i)} \neq 0$

para cada $i$. Dado $i$, $v_{n-1}$ y $v_{i,\pi(i)}$ pueden usarse para completar la base $\{1, \cdots, v_{n-1}\}$. Por la condición de Minkowski,

$$|v_{n-1}| = \sqrt[n]{|v_{n-1}|^n} \leq \sqrt[n]{\prod_i |v_{i,\pi(i)}|} \ll |\Delta_K|^{1/n}.$$

□

Con estos dos lemas procedemos a acotar el tamaño de la 2-torsión de grupos de clase de cuerpos de números. En principio, notar que el último resultado permite obtener una base de $\mathcal{O}_K$ donde todos los elementos tienen tamaño acotado por $O(|\Delta_K|^{1/n})$ (para $1 \leq i \leq n-2$ esto es consecuencia de las condiciones de Minkowski, y para $v_{n-1}$ lo acabamos de probar) y en tanto podemos, utilizando un caso básico del lema de Davenport (ver [Dav51], [BW13]), acotar la cantidad de generadores $\beta$, como en el teorema 2: si $B$ es un cubo de lado $|\Delta_K|^{1/n}$ donde podemos hallar los $\beta$ del teorema 2 y $L$ el látiz que induce $\mathcal{O}_K$ vía la base de Minkowski en $\mathbb{R}^n$, podemos hallar $C$ dependiendo de $n$ tal que $L \subseteq C \cdot B$. Luego, la cantidad de $\beta$ que queremos contar está acotada por $O(Vol(C \cdot B)/Vol(L)) = O(|\Delta_K|^{1/2})$. Para hallar un exponente más chico, contamos en un lugar más chico,

$$B' = \{x \in B : N_{K/\mathbb{Q}}(x) \text{ es un cuadrado}\}.$$

Aquí los autores separan dos casos, uno que es tratado por teoría de género y otro que es tratado utilizando el método del determinante.

### 7.3.1. Género

Debemos utilizar algo de teoría de género. En general, este es un concepto que data de Gauss, y que busca distinguir formas cuadráticas en base a los números que representan, o bien módulo $n$, o bien en $\mathbb{Q}_p$ y $\mathbb{R}$ (dependiendo del autor). No obstante, no nos vamos a enfocar en las importantes minucias de esta teoría, sino que vamos a utilizar la llamada *fórmula ambigua del número de clase*, siguiendo el paper de Lemmermeyer [Lem13]. Sea $K$ un cuerpo de números y supongamos que $L/K$ es cíclica de orden $l$. Sea $Gal(L/K) =< \sigma >$ y recordemos que el Galois actúa sobre $Cl(L)$ vía $[I]^\sigma = \sigma \cdot [I] = [\sigma(I)]$. Una clase de ideales $[\mathfrak{a}]$ se dice **ambigua** si $[\mathfrak{a}]^\sigma = [\mathfrak{a}]$, es decir, si está fija por el grupo de Galois. En particular, especializando a

$l = 2$, vemos que, dado que el Galois actúa transitivamente en los ideales primos que se sientan sobre otro primo, tenemos que

$$[\mathfrak{a}][\mathfrak{a}]^{\sigma} = [\mathfrak{a}\sigma(\mathfrak{a})] = [N(\mathfrak{a})],$$

donde $N$ es la norma relativa de la extensión.
En particular, $[\mathfrak{a}]^{\sigma} = [\mathfrak{a}]^{-1}$, y un ideal es ambiguo si y solo si es 2-torsión. Ante esto, tenemos la importante:

**Teorema: 7.14** (Fórmula ambigua del número de clases, [Lem13], Teorema 1)**.** *Sea $C_a$ el conjunto de clases ambiguas. Luego,*

$$|C_a| = \frac{h_K \cdot 2^{t-1}}{(\mathcal{O}_K^* : \mathcal{O}_K^* \cap N(L^*))},$$

*donde $h_K$ es el número de clases de $K$, $N(L)$ son los elementos de $K$ que son normas y $t$ es la cantidad de primos ramificados en $L/K$.*

Usando esto, supongamos que $L$ contiene un subcuerpo $K$ de índice 2, y vemos que podemos acotar la 2-torsión en $Cl(L)$ por

$$h_K O(2^t).$$

Por la cota de Landau en el primer factor, mientras que usando que los ramificados están acotados por los divisores de $|\Delta_L|$ - lo cual es una $O(|\Delta_L|^{\varepsilon})$ para cada $\varepsilon > 0$, obtenemos que:

$$\#Cl(L)[2] = O(|\Delta_K|)|\Delta_L|^{1/2+\varepsilon} = O(|\Delta_L|^{1/4+\varepsilon}),$$

donde usamos que $|\Delta_K|^2 \leq |\Delta_L|$ por la fórmula discriminante-diferente. Esto da una cota de orden $1/4 + \varepsilon$ que rompe tanto la cota de Landau de $1/2 + \varepsilon$, como la cota previa de $1/2$.

### 7.3.2. El método de Bombieri-Pila

El método de Bombieri-Pila, también llamado método del determinante, permite dar cotas uniformes en el grado para la cantidad de puntos enteros que pertencen a una curva algebraica, restringiendo a cajas de lado $N$. En esta subsección enunciamos el teorema y lo usamos para tratar el caso en que $L$ no admite subcuerpos de índice 2. La forma que utilizaremos es la que aparece en [BP89] como Teorema 5:

**Teorema: 7.15.** *Sea $C$ una curva absolutamente irreducible de grado $d \geq 2$. Sea $N \geq e^{d^6}$. Luego, la cantidad de puntos enteros en $S := C \cap [0, N]^2$ cumple:*

$$\#S \leq N^{\frac{1}{d}} e^{12\sqrt{d \log N \log\log N}}.$$

Sea $\beta \in B \cap \mathcal{O}_K$, donde mantenemos la notación del inicio. Sea $f_\beta(X) = N_{K/\mathbb{Q}}(\beta - X)$. Ahora probemos el Lema 4.1 de [BST+20]:

**Teorema: 7.16.** *Si $K$ no contiene subcuerpos de índice 2, la cantidad de $\beta$ en $B \cap \mathcal{O}_K$ tal que $f_\beta$ es un cuadrado en $\mathbb{Q}[X]$ es $\ll |\Delta_K|^{1/4}$.*

Notar que las raíces de $f_\beta$ se dan cuando aparece un factor nulo en el producto de los $\sigma(\beta) - \sigma(x)$, sobre $\sigma$ los embeddings de $K$. En particular, las raíces son los conjugados de $\beta$. Si $f_\beta$ tuviera raíces dobles, tendríamos que hay un morfismo que fija algún conjugado de Galois, y por ende $\beta$ está en un subcuerpo de $K$ propio. Por ende, $f_\beta$ es libre de cuadrados salvo cuando $\beta \in F \subsetneq K$ y $[K : F] > 1$. Por la hipótesis, sabemos que debe ser $[K : F] > 2$, mientras que $f_\beta$ es un cuadrado si el grado es par. Por la fórmula discriminante-diferente, dado un $F$ que verifica esas condiciones, $|\Delta_F| \leq |\Delta_K|^{1/[K:F]}$. Ahora usemos geometría de números como antes. El anillo de enteros de $F$ tiene volumen proporcional a $|\Delta_F|$ y, tomando una base de Minkowski, sabemos que el mayor elemento tiene norma $\ll |\Delta_F|^{1/[F:\mathbb{Q}]}$. Como $|\Delta_F| \leq |\Delta_K|^{1/[K:F]}$, concluimos que los elementos de la base se contienen en un cubo $R$ de lado $\ll |\Delta_K|^{1/([F:\mathbb{Q}][K:F])} = |\Delta_K|^{1/n}$, así que la cantidad de $\beta$'s está dominada por

$$Vol(R)/Vol(\mathcal{O}_F) \ll \frac{|\Delta_K|^{[F:\mathbb{Q}]/n}}{|\Delta_F|^{1/2}} = \frac{|\Delta_K|^{1/[K:F]}}{|\Delta_F|^{1/2}} \leq |\Delta_K|^{1/[K:F]}.$$

Como $[K : F]$ es par y mayor a 2, $[K : F] \geq 4$, con lo cual $\frac{1}{[K:F]} \leq \frac{1}{4}$, y podemos finalizar de acotar la cantidad de $\beta$'s por

$$Vol(R)/Vol(\mathcal{O}_F) \ll |\Delta_K|^{1/4}.$$

La cantidad de subcuerpos de índice mayor a 2 y grado par es una $O_n(1)$ (por ejemplo, podemos pasar a una clausura de Galois y acotar la cantidad de subcuerpos por la cantidad de subgrupos, y esta a su vez por el cardinal del conjunto de partes). Por ende, el resultado se sigue sumando sobre

las $O(1)$ elecciones.

Ahora bien, falta ocuparnos del caso en el que $f_\beta$ no es un cuadrado, y acá entran las consideraciones geométricas. Si $f_\beta$ no es un cuadrado, la cantidad de enteros $m \in R$ con $f_\beta(m)$ un cuadrado es la cantidad de puntos enteros en la curva irreducible $y^2 = f_{sq}(X)$, con $f_{sq}$ la parte libre de cuadrados de $f_\beta$, en la caja $|x| \ll |\Delta_K|^{1/n}$, $|y| \ll |\Delta|^{1/2}$. Por el teorema de Bombieri-Pila, la cantidad de tales puntos es $O_\varepsilon(|\Delta_K|^{1/2n+\varepsilon})$. Sumando sobre los $O(|\Delta_K|^{\frac{1}{2}-\frac{1}{n}})$ representantes de $\beta$ en $\mathcal{O}_K \cap B/\mathbb{Z}$, obtenemos una cota de $O(|\Delta_K|^{\frac{1}{2}-\frac{1}{n}})O(|\Delta_K|^{\frac{1}{2n}+\varepsilon}) = O(|\Delta_K|^{\frac{1}{2}-\frac{1}{2n}+\varepsilon})$. En particular, con $n > 4$, podemos tomar $\delta_n = \frac{1}{2n}$.

# 8. Bibliografía

[BG12] Manjul Bhargava and Benedict H. Gross. Arithmetic invariant theory, 2012.

[BH22] Manjul Bhargava and Wei Ho. On average sizes of selmer groups and ranks in families of elliptic curves having marked points, 2022.

[Bha04a] Manjul Bhargava. Higher composition laws I: A new view on gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159(1):217–250, 2004.

[Bha04b] Manjul Bhargava. Higher composition laws III: The parametrization of quartic rings. *Annals of Mathematics*, 159(3):1329–1360, May 2004.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, 162(2):1031–1063, 2005.

[Bha14] Manjul Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials, 2014.

[BK77] A. Brumer and K. Kramer. The rank of elliptic curves. *Duke Mathematical Journal*, 44(4), 1977.

[BP89] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Mathematical Journal*, 59(2), 1989.

[Bru92] Armand Brumer. The average rank of elliptic curves I. *Inventiones Mathematicae*, 109(1):445–472, 1992.

[BS13a] Manjul Bhargava and Arul Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7, 2013.

[BS13b] Manjul Bhargava and Arul Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1, 2013.

[BS15a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average

rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[BS15b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, March 2015.

[BSD63] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. i. *Journal für die reine und angewandte Mathematik*, 1963(212):7–25, 1963.

[BSS21] Manjul Bhargava, Arul Shankar, and Ashvin Swaminathan. The second moment of the size of the 2-selmer group of elliptic curves, 2021.

[BST+20] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *Journal of the American Mathematical Society*, 33(4):1087–1099, August 2020.

[BSZ14] Manjul Bhargava, Christopher Skinner, and Wei Zhang. A majority of elliptic curves over  satisfy the birch and swinnerton-dyer conjecture, 2014.

[BW13] Fabrizio Barroero and Martin Widmer. Counting lattice points and O-minimal structures. *International Mathematics Research Notices*, 2014(18):4932–4957, 2013.

[Cas62] J.W.S. Cassels. Arithmetic on curves of genus 1. iv. proof of the hauptvermutung. *Journal für die reine und angewandte Mathematik*, 1962(211):95–112, 1962.

[Cas91] John W. S. Cassels. *Lectures on elliptic curves*. Number 24 in London Mathematical Society student texts. Cambridge University Press, Cambridge, 1991.

[Cas97] John W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer eBook Collection. Springer Berlin Heidelberg, Berlin, Heidelberg, 1997.

[CF09] J.E. Cremona and T.A. Fisher. On the equivalence of binary quartics. *Journal of Symbolic Computation*, 44(6):673–682, June 2009.

[CL84] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. pages 33–62, 1984.

[Coh03] Henri Cohen. Constructing and counting number fields. *arXiv: Number Theory*, 2003.

[Coh10] Donald L. Cohn. *Measure Theory*. Birkhäuser, 2010.

[Cre92] John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge Univ. Press, 1. publ. edition, 1992.

[Cre01] J. E. Cremona. Reduction of binary cubic and quartic forms. *LMS Journal of Computation and Mathematics*, 4:73–73, 2001.

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*. Number Number 101 in CBMS Regional Conference Series in Mathematics. Published for the Conference Board of the Mathematical Sciences by the American Mathematical Society, 2004.

[Dav51] H. Davenport. On a principle of lipschitz. *Journal of the London Mathematical Society*, s1-26(3):179–183, 1951.

[Del30] Boris Delaunay. Über die darstellung der zahlen durch die binären kubischen formen von negativer diskriminante. *Mathematische Zeitschrift*, 31(1):1–26, 1930.

[DF64] B. N. Delone and D. K. Faddeev. *The Theory of Irrationalities of the Third Degree*, volume 10. American Mathematical Society, 1964.

[dJ02] J. de Jong. Counting elliptic surfaces over finite fields. *Moscow Mathematical Journal*, 2(2):281–311, 2002.

[Duj] Infinite families of elliptic curves with high rank and prescribed torsion. Available at http://web.math.pmf.unizg.hr/ duje/tors/generic.html.

[DY24] Ratko Darda and Takehiko Yasuda. The Batyrev–Manin conjecture for DM stacks. *Journal of the European Mathematical Society*, 2024.

[Eke91] T. Ekedahl. An infinite version of the chinese remainder theorem. *Comment. Math. Univ. St. Paul.*, 40, 1991.

[Elk] Trivial torsion group, rank $\geq$ 29. Available at https://web.math.pmf.unizg.hr/

[ESZB23] Jordan S. Ellenberg, Matthew Satriano, and David Zureick-Brown. Heights on stacks and a generalized Batyrev–Manin–Malle conjecture. *Forum of Mathematics, Sigma*, 11, 2023.

[EV06] Jordan Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Annals of Mathematics*, 163(2):723–741, March 2006.

[EV07] Jordan S. Ellenberg and Akshay Venkatesh. Reflection principles and bounds for class group torsion. *International Mathematics Research Notices*, 2007, January 2007.

[Eve83] J. H. Evertse. On the representation of integers by binary cubic forms of positive discriminant. *Inventiones Mathematicae*, 73(1):117–138, 1983.

[Gui18] Pierre Guillot. *A Gentle Course in Local Class Field Theory*. Cambridge University Press, New York, NY, 1st ed. edition, 2018.

[Har08] Robin Hartshorne. *Algebraic geometry*. Number 52 in Graduate texts in mathematics. Springer, New York, NY, 14 edition, 2008. Literaturverz. S. 459 - 469.

[Has30] Helmut Hasse. Arithmetische theorie der kubischen zahlkörper auf klassenkörpertheoretischer grundlage. *Mathematische Zeitschrift*, 31(1):565–582, 1930.

[HB04] D. R. Heath-Brown. The average analytic rank of elliptic curves. *Duke Mathematical Journal*, 122(3), 2004.

[HB25] D. R. Heath-Brown. $\ell$-torsion in class groups via dirichlet $L$-functions, 2025.

[HH71] Davenport. H and H. A. Heilbronn. On the density of discriminants of cubic fields. II. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 322(1551):405–420, 1971.

[Hil06] David Hilbert. *Theory of algebraic invariants*. Cambridge mathematical library. Cambridge Univ. Press, Cambridge, 2006.

[Hus04] Dale Husemöller. *Elliptic Curves*. Springer eBook Collection. Springer-Verlag New York, Inc, 2004.

[HV06] H. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *Journal of the American Mathematical Society*, 19(3):527–550, 2006.

[JHS15] J. T. Tate J. H. Silverman. *Rational Points on Elliptic Curves*. Springer International Publishing, 2nd ed. 2015 edition, 2015.

[Kl5] Jürgen Klüners. A counter example to Malle's conjecture on the asymptotics of discriminants. *Comptes Rendus. Mathématique*, 340(6):411–414, 2005.

[Lan18] E. Landau. Abschätzungen von charaktersummen, einheit und klassenzahlen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1918:79–97, 1918.

[Lan10] Serge Lang. *Algebraic number theory*. Number 110 in Graduate texts in mathematics. Springer, New York, 2010.

[Lan20] Aaron Landesman. Notes on counting extensions of degree 2 and 3 following bhargava, 2020. Available at https://people.math.harvard.edu/ landesman/notes.html.

[Lem13] Franz Lemmermeyer. The ambiguous class number formula revisited, 2013.

[Mal02] Gunter Malle. On the distribution of galois groups. *Journal of Number Theory*, 92(2):315–329, 2002.

[Mal04] Gunter Malle. On the distribution of galois groups, II. *Experimental Mathematics*, 13(2):129–135, 2004.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Publications mathématiques de l'IHÉS*, 47(1):33–186, 1977.

[Mil20a] James S Milne. *Elliptic Curves*. World Scientific, 2020.

[Mil20b] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Min91] Hermann Minkowski. Ueber die positiven quadratischen formen und über kettenbruchähnliche algorithmen. *Journal für die reine und angewandte Mathematik*, 107:278–297, 1891.

[Mor15] David Witte Morris. *Introduction to arithmetic groups*. Deductive Press, version 1.0 of april 2015 edition, 2015.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften Ser. Springer Berlin / Heidelberg, Berlin, Heidelberg, 1999.

[OZ25] Robert J. Lemke Oliver and Asif Zaman. Improving the trivial bound for $\ell$-torsion in class groups, 2025.

[Pie06] Lillian B Pierce. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Mathematicum*, 18(4):677–698, 2006.

[Pie22] Lillian B. Pierce. Counting problems: class groups, primes, and number fields, 2022.

[Pla23] Vladimir P. Platonov. *Algebraic Groups and Number Theory*. Cambridge University Press, 2nd ed. edition, 2023.

[Poo03] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Mathematical Journal*, 118(2), 2003.

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *Journal of the European Mathematical Society*, 21(9):2859–2903, 2019.

[PR11] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, July 2011.

[RT20] Beth Romano and Jack A. Thorne. E8 and the average size of the 3-selmer group of the jacobian of a pointed genus-2 curve. *Proceedings of the London Mathematical Society*, 122(5):678–723, 2020.

[SC02] Michael Stoll and John E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS Journal of Computation and Mathematics*, 5:220–243, 2002.

[Sch32] Arnold Scholz. Über die beziehung der klassenzahlen quadratischer körper zueinander. *Journal für die reine und angewandte Mathematik*, 166:201–203, 1932.

[Sch95] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. In *Columbia university number theory seminar - New-York, 1992*, number 228 in Astérisque, pages 189–195. Société mathématique de France, 1995.

[Sch08] Rene Schoof. Computing arakelov class groups, 2008.

[Sch11] Peter Schneider. *P-adic Lie groups*. Number 344 in Grundlehren der mathematischen Wissenschaften. Springer, Heidelberg, 2011.

[Sch23] Joachim Schwermer. *Reduction theory and arithmetic groups*. Number 45 in New mathematical monographs. Cambridge University Press, Cambridge ; New York, NY, 2023.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Springer New York, 1973.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer New York, 1979.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer New York, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.

[Tho13] Jack Thorne. Vinberg's representations and arithmetic invariant theory. *Algebra amp; Number Theory*, 7(9):2331–2368, 2013.

[Ulm02] Douglas Ulmer. Elliptic curves with large rank over function fields. *The Annals of Mathematics*, 155(1):295, 2002.

[Woo09] Melanie Matchett Wood. Moduli spaces for rings and ideals. 2009.