Métodos explícitos de Chabauty: un punto de vista computacional a los puntos racionales

Jerson Caro Reyes
jl.caro10@uniandes.edu.co
Universidad de los Andes

Juanita Duque Rosero
j.duque.rosero@rug.nl
Universidad de Groningen

Última versión: 7 de agosto de 2026

Introducción

Este curso estudia la geometría aritmética de curvas algebraicas y variedades abelianas, con énfasis en la descripción de puntos racionales mediante métodos clásicos y modernos, especialmente las técnicas de Chabauty.

Motivación

La teoría de puntos racionales sobre curvas algebraicas constituye uno de los temas centrales de la geometría aritmética moderna. Su objetivo principal es comprender las soluciones de ecuaciones dadas por polinomios cuando las coordenadas pertenecen a un cuerpo aritméticamente significativo, como $\mathbb{Q}$ o los campos de números. Problemas clásicos de la teoría de números, desde las ecuaciones diofánticas hasta las curvas elípticas asociadas al teorema de modularidad, pueden reformularse en este lenguaje geométrico.

Una idea fundamental de la geometría algebraica es que la complejidad aritmética de una curva está relacionada con su geometría. El invariante que gobierna esta relación es el género. Las curvas de género 0 poseen una estructura racional y, cuando tienen un punto racional, admiten parametrizaciones explícitas. Las curvas de género 1, presentan una rica estructura algebraica: sus puntos racionales (si tiene) forman un grupo abeliano finitamente generado, según el teorema de Mordell–Weil. Finalmente, las curvas de género al menos 2 exhiben un comportamiento radicalmente distinto: el teorema de Faltings afirma que poseen solamente un número finito de puntos racionales.

El problema de determinar efectivamente estos puntos racionales continúa siendo uno de los grandes desafíos de la matemática contemporánea. Aunque el teorema de Faltings garantiza finitud, su demostración no proporciona un procedimiento explícito para calcular los puntos. Esto ha motivado el desarrollo de métodos explícitos capaces de describir efectivamente el conjunto de soluciones racionales.

Entre estos métodos destaca el método de Chabauty–Coleman, basado en integración p-ádica y en la geometría de la variedad jacobiana de la curva. La idea esencial consiste en estudiar la intersección entre el cierre p-ádico del grupo de Mordell–Weil y la imagen de la curva dentro de su jacobiano. Cuando el rango del jacobiano es estrictamente menor que el género, el método permite demostrar la finitud de los puntos racionales y, en numerosos casos, calcularlos explícitamente.

En las últimas décadas, estas técnicas han evolucionado considerablemente. El desarrollo de alturas p-ádicas, métodos cuadráticos y enfoques no abelianos ha permitido extender el alcance del método clásico de Chabauty a nuevas situaciones donde las herramientas tradicionales resultaban insuficientes.

Objetivo

El curso tiene como objetivo introducir las bases geométricas y aritméticas necesarias para comprender estos métodos modernos. Se comienza con el estudio de curvas algebraicas y de sus puntos racionales, seguido por la teoría de divisores y jacobianos. Posteriormente se desarrolla el método de Chabauty–Coleman y sus refinamientos recientes, incluyendo alturas p-ádicas y Chabauty

cuadrático. Posteriormente consideraremos generalizaciones a variedades de dimensión mayor a 1. Todo esto irá de la mano con ejemplos computacionales explícitos.

Prerequisitos

Intentaremos que las charlas sean autocontenidas y las notas del curso contendrán todos los detalles necesarios. Este curso está dirigido a estudiantes que tengan experiencia con temas básicos de teoría de números y geometría algebraica: curvas elípticas, análisis p-ádico, y teoría algebraica de números (clásica).

Computaciones explícitas

La forma ideal de seguir este curso es intentar ejemplos en su sistema de álgebra favorito. Nosotros usamos Magma y muchas computaciones para Chabauty cuadrático están escritas en ese lenguaje. Otras opciones son: (SageMath, PARI/GP, Oscar, etc.). Ejemplos de Magma pueden ser encontrados aquí. También, aquí hay una lista de trucos que una de las autoras ha compilado y aquí hay un ejercicio para familiarizarse con las funcionalidades de Magma para teoría de números.

Agradecimientos

Nuestro sincero agradecimiento por leer cuidadosamente las notas y proponer ejercicios a Matías Alvarado, Wilmar Bolaños, Alex Junior Gomez Saltachin, Esteban Saldarriaga Marín, quienes fueron asistentes de cursos dados con estas notas.

También queremos agradecer a la coordinadora de nuestro curso, Cecília Salgado Guimares da Silva. Igualmente, agradecemos a Steffen Müler por sus valiosa ayuda describiendo el método de Chabauty cuadrático.

Finalmente, queremos agradecer al comité organizador de la escuela: Jhon J. Bravo, John H. Castillo, Maria de Los Angeles Chara, Elisa Lorenzo García, Harald Helfgott, Gonzalo Tornaría Lopez, Ariel Pacetti, Cecília Salgado Guimaraes da Silva, Carlos Alberto Trujillo Solarte, Lola Thompson, Fernando Rodriguez Villegas, and Emanuel Carneiro.

Índice general

Clase 1: Curvas afines y proyectivas y puntos racionales

Las curvas son estructuras algebraicas que aparecen en muchos problemas clásicos de la geometría, empezando por las ternas pitagóricas. El estudio de sus puntos racionales surge de manera natural al preguntarse cuándo una ecuación polinómica admite soluciones en un cuerpo dado y cómo describirlas explícitamente. Problemas tan elementales como determinar todas las soluciones de una ecuación diofántica conducen de manera natural al estudio de curvas algebraicas y revelan conexiones entre la geometría y la aritmética.

En la actualidad las curvas tienen aplicaciones en criptografía (las curvas elípticas, por ejemplo) y se estudian como objetos que parametrizan otras estructuras algebraicas (las curvas modulares, por ejemplo). Las curvas son las variedades algebraicas más simples, pero, como veremos a continuación, su estructura aritmética es muy rica: preguntas aparentemente sencillas sobre la existencia, cantidad o distribución de sus puntos racionales han motivado algunos de los desarrollos más importantes de la teoría de números y la geometría algebraica. Por ello, siguen siendo un tema central y fascinante de estudio en las matemáticas contemporáneas.

En esta clase seguiremos [Sil09] y [Ser97], junto con [Mir95] para una visión más geométrica.

Para empezar, consideremos el siguiente problema clásico de geometría:

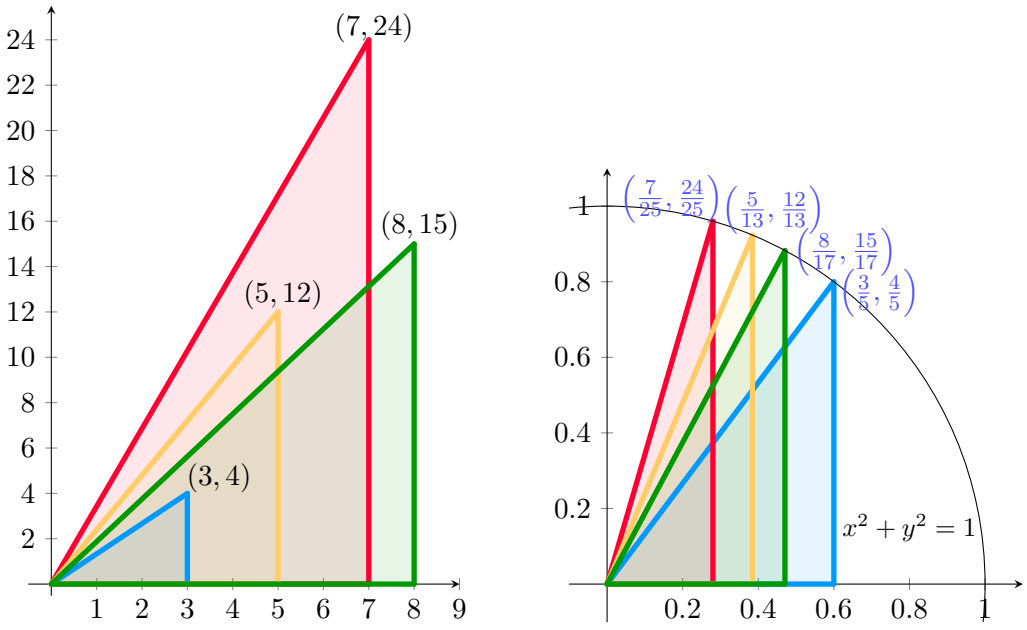
Pregunta 1.1. Hay alguna forma de describir todas las ternas Pitagóricas (x, y, z) donde

$$x^2 + y^2 = z^2.$$

Una de las dificultades de este problema es que si (x, y, z) es una terna Pitagórica, entonces para cualquier $\lambda \in \mathbb{Z}_{>0}$, $(\lambda x, \lambda y, \lambda z)$ es otra terna. Para evitar esto, podemos dividir la ecuación por z^2 y parametrizar las soluciones racionales a la ecuación

$$\tilde{x}^2 + \tilde{y}^2 = 1,$$

donde $\tilde{x} = x/z$ y $\tilde{y} = y/z$.



Note que todos los pares racionales tales que $x^2 + y^2 = 1$ son los puntos con coordenadas racionales en el círculo unitario.

Proyección estereográfica: Vamos a tomar todas las rectas que pasan por el punto $(-1, 0)$ con pendiente racional t, definida por la ecuación

$$y = t(1 + x), \tag{1.2}$$

es decir, la recta que pasa por los puntos $(-1, 0)$ y $(0, t)$. Esta recta intersecta al circulo en $(-1, 0)$ y un punto (x_0, y_0), el cuál tiene coordenadas racionales. Para ver esto, note que $x_0 \neq -1$ es una solución a la ecuación

$$1 - x^2 = y^2 = t^2(1 + x)^2.$$

Resolviendo para x, obtenemos que $x_0 = \dfrac{1 - t^2}{1 + t^2}$. En particular, x_0 es racional y (1.2) implica que $y_0 = \dfrac{2t}{1 + t^2}$ también es racional.

Note que esta función es biyectiva: para todo punto $(x_0, y_0) \neq (-1, 0)$ con coordenadas racionales en el círculo, la pendiente $t = \dfrac{y_0}{1 + x_0}$ recupera este punto.

Este método se puede aplicar para cualquier ecuación cuadrática, obteniendo así el siguiente teorema:

✎ **Ejercicio 1.3.** En este ejercicio, describiremos las ternas (x, y, z) que satisfacen

$$x^2 + 2y^2 = z^2. \tag{1.4}$$

Note que si (x, y, z) es una terna satisface (1.4), entonces para cualquier $\lambda \in \mathbb{Z}_{\geq 0}$, $(\lambda x, \lambda y, \lambda z)$ también satisface(1.4).

1. Defina una biyección entre ternas que satisfacen (1.4) (salvo multiplicar por un entero positivo) y soluciones racionales a la ecuación $x^2 + 2y^2 = 1$.

2. Use una proyección estereográfica para parametrizar todas las soluciones racionales a $x^2+2y^2 = 1$. Esto es,

   a) Encuentre la ecuación de la recta por el punto $(-1, 0)$ con pendiente racional t.

   b) Encuentre el otro punto de intersección de la recta con la elipse $x^2 + 2y^2 = 1$ (en términos de t).

   c) Justifique por qué la función que asigna a cada t racional el punto del ítem anterior es una biyección de racionales t con soluciones racionales a $x^2 + 2y^2 = 1$ diferentes de $(-1, 0)$.

Teorema 1.5. *Si una ecuación cuadrática*

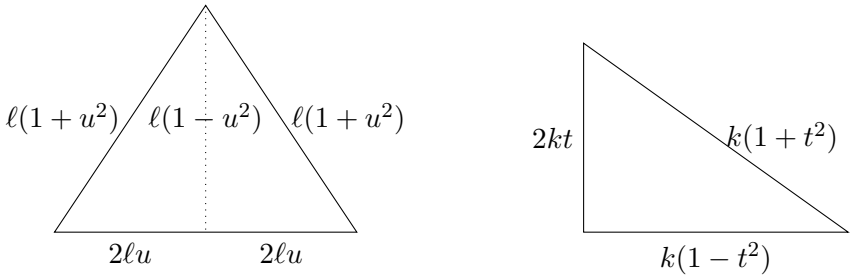
$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

tiene una solución (no trivial) con coordenadas racionales, entonces tiene infinitas.

Idea de la prueba. El método para parametrizar los puntos racionales en el círculo unitario se puede generalizar a cualquier ecuación cuadrática. La idea es proyectar desde un punto racional en la curva y parametrizar las rectas que pasan por este punto. Cada recta intersecta a la curva en otro punto, el cuál tiene coordenadas racionales. Para una demostración más detallada, el lector puede consultar [Sil09]. □

✎ **Ejercicio 1.6** (Un Problema de la geometría clásica)**.** Existen un triángulo rectángulo y uno isósceles ambos con lados racionales que tengan la misma área y mismo perímetro?

(a) Pruebe que es lo mismo que tener triángulos con las siguientes dimensiones:



Sin perdida de generalidad, asuma que $\ell = 1$, también que $k, t, u \in \mathbb{Q}$, $0 < t$, $u, 1$ y $k > 0$.

(b) Sea $x = 1 + u$. Pruebe que si tales triángulos existen, existen $x \in \mathbb{Q} \cap (1, 2)$ y $y \in \mathbb{Q}$ tales que:

$$y^2 = (-3x^3 - 2x^2 + 6x - 4)^2 - 4(2x)x^5.$$

1.1. Curvas

En esta sección, presentaremos algunos resultados importantes de la teoría de curvas. Solo presentaremos lo que será relevante en las secciones posteriores. Para un tratamiento mas a fondo de este tema, el lector puede consultar [Ser97]. Las referencias que más usamos para esta sección fueron [Sil09] y [Mir95].

1.1.1. Curvas afines y planas

Sea k un campo. Denotaremos por $\bar{k}$ a una clausura algebraica del campo k.

Definición 1.7. Una curva afín y plana definida sobre k es el conjunto C de ceros en $\bar{k}^2$ de un polinomio $f(x, y) \in k[x, y]$ que es irreducible en $k[x, y]$. El polinomio $f(x, y)$ es suave en un punto $P \in \bar{k}^2$ si las derivadas parciales $\partial f/\partial x$ y $\partial f/\partial y$ no son cero al tiempo en P. La curva plana afín C es suave, si esta es suave en cualquier punto P de C.

Remark 1.8. Si el polinomio $f(x, y)$ es irreducible en $\bar{k}[x, y]$ decimos que la curva es geometricamente irreducible.

En general, escribiremos C/k para una curva C definida sobre el campo k. A veces también obviaremos escribir el campo de definición cuando este sea claro.

Ejemplo 1.9. La curva afín plana definida como los ceros de $y^2 + x^2 - 1 = 0$ es una curva interesante, pues soluciones racionales a esta ecuación parametriza ternas pitagóricas salvo múltiplos comunes.

Definición 1.10. El anillo de coordenadas de C/k es definido por

$$k[C] := \frac{k[x,y]}{\langle f(x,y)\rangle}.$$

Dado que el polinomio f es irreducible en $k[x,y]$, $k[C]$ es un dominio integral. Su campo cociente (campo de fracciones) es denotado por $k(C)$ y es llamado campo de funciones de C/k. Similarmente, $\bar{k}[C]$ y $\bar{k}(C)$ son definidos reemplazando k por $\bar{k}$.

1.1.2. El plano proyectivo $\mathbb{P}^2$

Definición 1.11. El plano proyectivo $\mathbb{P}^2$ es el conjunto de espacios unidimensionales de $\bar{k}^3$.

Si (x,y,z) es un vector diferente de cero en $\bar{k}^3$, entonces el espacio que genera se denota por $[x:y:z]$. Note que para todo $\lambda \in \bar{k}^\times$,

$$[x,y,z] = [\lambda x : \lambda y : \lambda z].$$

Las entradas en $[x:y:z]$ se llaman las coordenadas homogéneas del punto.

De hecho, el plano proyectivo $\mathbb{P}^2$ se puede ver como el espacio cociente de $\bar{k}^3 \setminus \{0\}$ por la acción multiplicativa de $\bar{k}^*$. De este modo, $\mathbb{P}^2$ recibe la topología cociente desde $\bar{k}^3$ (que es de Hausdorff).

El espacio proyectivo $\mathbb{P}^2$ puede ser recubierto por los tres conjuntos abiertos

$$U_0 := \{[x:y:z] \ : \ x \neq 0\}, \ \ U_1 := \{[x:y:z] \ : \ y \neq 0\}, \ \ U_2 := \{[x:y:z] \ : \ z \neq 0\}.$$

Cada conjunto es homeomorfo a $\bar{k}^2$. Por ejemplo, el homeomorfismo desde U_0 esta dado por $[x:y:z] \mapsto (y/x, z/x)$. Note que el plano proyectivo no es compacto, pero esta cubierto por los tres compactos U_0, U_1 y U_2.

1.1.3. Curvas planas, suaves y proyectivas

Un polinomio F es homogéneo si cada monomio tiene el mismo grado en las variables; dicho grado es el grado del polinomio homogéneo. Por ejemplo $y^2z - x^3 + z^3$ es un polinomio homogéneo de grado 3 en las variables x, y y z. Sea $F(x,y,z)$ un polinomio homogéneo de grado d. No es posible evaluar el polinomio F en un punto del plano proyectivo, ya que si asumimos que $[x_0:y_0:z_0] = [\lambda x_0 : \lambda y_0 : \lambda z_0]$ para $\lambda \in \bar{k}$, al evaluar a F tendríamos que

$$F(\lambda x_0, \lambda y_0, \lambda z_0) = \lambda^d F(x_0, y_0, z_0), \tag{1.12}$$

lo que puede ser distinto a $F(x_0,y_0,z_0)$. Es decir, evaluar el polinomio en un punto del plano proyectivo no está bien definido. Sin embargo, por (1.12), si F se anula en un punto $(x_0,y_0,z_0) \in \bar{k}^3$ se anulará en todo el espacio $[x_0:y_0:z_0]$.

De aquí que el conjunto de ceros

$$V(F) := \{[x:y:z] \in \mathbb{P}^2 \ : \ F(x,y,z) = 0\}$$

está bien definido. Más aún este es un conjunto cerrado de $\mathbb{P}^2$. La intersección de $V(F)$ y el conjunto abierto U_i es una curva afín en $\bar{k}^2$.

Por ejemplo, en U_0 donde $x \neq 0$, nosotros tenemos la curva afín en $\bar{k}^2$

$$C_0 := C \cap U_0 = \{(a,b) \in \bar{k}^2 \ : \ F(1,a,b) = 0\}.$$

la cuál es una curva afín descrita por el polinomio $f(a,b)=0$, donde $f(a,b)=F(1,a,b)$.

Definición 1.13. Una curva plana proyectiva es el conjunto de ceros de un polinomio homogéneo e iireducible $F(x,y,z)$.

Definición 1.14. Un polinomio homogéneo $F(x,y,z)$ es suave si no existen soluciones comunes al sistema de ecuaciones

$$F=\frac{\partial F}{\partial x}=\frac{\partial F}{\partial y}=\frac{\partial F}{\partial z}=0$$

en el plano proyectivo $\mathbb{P}^2$. Una curva plana proyectiva $C\colon F(z,y,z)$ es suave si $F(x,y,z)$ es suave.

Ejemplo 1.15. La curva de Fermat $F_2\colon x^2+y^2-z^2$, proveniente de la Pregunta 1.1, es suave.

Ejemplo 1.16. Similar al plano proyectivo $\mathbb{P}^2$, podemos definir la curva proyectiva $\mathbb{P}^1$ como el conjunto de espacios unidimensionales de $\bar{k}^2$. En nuestro lenguaje de curvas, $\mathbb{P}^1$ puede ser definida por la ecuación $z=0$.

✎ **Ejercicio 1.17.** Pruebe que un polinomio homogéneo $F(x,y,z)$ de grado d que define una línea proyectiva C es suave si y solo si cada $C_i:=C\cap U_i$ is una curva suave, afín y plana.

Definición 1.18. El campo de funciones de una curva plana proyectiva C, es el campo de funciones de $C_i:=C\cap U_i$ para cualquier $i\in\{0,1,2\}$.

Remark 1.19. Una curva plana, suave, y proyectiva (definida sobre $\mathbb{C}$) resulta ser una superficie compacta de Riemann (ver el Ejercicio 1.20). Estas superficies están clasificadas por un invariante geométrico llamado el *género*. El género de una curva es su género como superficie compacta de Riemann. Más adelante (en el Teorema 2.16), vamos a ver una forma más aritmética de calcular el género de una curva y como extender esta definición a cualquier campo.

La frase más importante para nosotros con respecto al género es:

"El género controla la aritmética".

Antes de darle sentido, necesitaremos algunas definiciones más.

✎ **Ejercicio 1.20.** En este ejercicio, probará que una curva suave plana proyectiva definida sobre $\mathbb{C}$ es una superficie compacta de Riemann. Supongamos que $F(x,y,z)$ es un polinomio homogéneo de grado d.

1. Probar que $F(x,y,z)$ es no-singular si y solo si cada C_i es una curva suave afín y plana en $\mathbb{C}^2$.
2. Probar que un polinomio homogéneo no-singular es irreducible. *Hint:* usar la regla del producto para derivadas.
3. Probar que las funciones de transición entre las cartas C_i son holomorfas.

1.1.4. Morfismos

Ahora que hemos visto la definición de curvas, entenderemos como interactúan entre sí por medio de morfismos. En esta sección, seguiremos [Sil09].

Definición 1.21. Sea C/k una curva y P un punto de C. El anillo local de C en P, denotado por $\bar{k}[C]_P$, es la localización de $\bar{k}[C]$ en el ideal primo

$$M_P = \{f \in \bar{k}[C] \,:\, f(P) = 0\}. \tag{1.22}$$

Esto es,

$$\bar{k}[C]_P := \{F \in \bar{k}(C) \,:\, F = f/g \text{ para } f, g \in \bar{k}[C] \text{ con } g(P) \neq 0\}.$$

Las funciones en $\bar{k}[C]_P$ son llamadas funciones regulares en P.

Remark 1.23. Cuando $k = \mathbb{C}$, la curva $C(\mathbb{C})$ posee naturalmente estructura de superficie de Riemann compacta. En este caso, las funciones racionales sobre C coinciden exactamente con las funciones meromorfas sobre la superficie de Riemann $C(\mathbb{C})$.

Definición 1.24. Un mapa $\varphi\colon C \to C'$ entre curvas planas suaves y proyectivas es un morfismo si es una función racional regular en todos los puntos.

Ejemplo 1.25. Considere las curvas $C\colon y^2z = x^3 + x^2z$ y $\mathbb{P}^1 = \{[s : t]\}$ sobre cualquier campo k. Definimos las funciones

$$\begin{aligned} \varphi\colon \mathbb{P}^1 &\to C, & \varphi([s,t]) &= [(s^2 - t^2)t, (s^2 - t^2)s, t^3]] \\ \psi\colon C &\to \mathbb{P}^1, & \psi([x,y,z]) &= [y, x]. \end{aligned}$$

Tenemos que φ es un morfismo, mientras que ψ no es regular en $[0, 0, 1]$.

✎ **Ejercicio 1.26.** Considere las curvas $F_3\colon x^3 + y^3 = z^3$ y $E\colon y^2z = x^3 - 314928z^3$. Considere la función $\varphi\colon F_3 \to E$ dada por

$$[x : y : z] \mapsto [108x, -972(y + z) : -y + z].$$

Probar que φ es un isomorfismo.

Definición 1.27. Sea $\varphi\colon C_1 \to C_2$ un morfismo de curvas definido sobre un campo K. Si φ es constante, entonces decimos que su grado es 0. De otro modo, el grado de φ es

$$\deg(\varphi) := [K(C_1) : \varphi^* K(C_2)].$$

Morfismos entre curvas planas suaves y proyectivas nos dan una importante relación entre el género de las curvas.

Teorema 1.28 (Formula de Riemann–Hurwitz)**.** *Sea $\varphi\colon C \to C'$ un morfismo no constante entre dos curvas suaves planas y proyectivas de género g_C y $g_{C'}$, respectivamente. Entonces se tiene que*

$$2g_C - 2 = \deg \varphi \cdot (2g_{C'} - 2) + \sum_{P \in C} [\mathrm{mult}_P(\varphi) - 1].$$

Demostración. Este es un teorema acerca de superficies compactas de Riemann, entonces saltaremos la prueba. El lector interesado puede consultar [Mir95, Theorem 4.16]. □

✎ **Ejercicio 1.29.** Use el morfismo φ del Ejemplo 1.25 para encontrar el género de C. En este ejercicio, puede usar que el género de $\mathbb{P}^1$ es 0.

Una consecuencia importante de la formula de Riemann–Hurwitz es la siguiente.

Proposición 1.30 (Fórmula de Plücker)**.** *Sea C una curva suave proyectiva plana de grado d. Entonces el género de C es*

$$g = \frac{(d-1)(d-2)}{2}.$$

Demostración. Vea el Ejercicio 1.31. □

✎ **Ejercicio 1.31.** En este ejercicio probaremos la Fórmula de Plücker de la Proposición 1.30. Sea $C\colon F(x,y,z)$ una curva suave plana y proyectiva. Considere el mapa $\pi\colon C \to \mathbb{P}^1$ dado por $\pi([x:y:z]) \to [x:z]$.

1. Probar que π es un morfismo bien definido.
2. Calcular el grado de π.
3. Describa los puntos de C para los que π tiene multiplicidad distinta a 1. *Sugerencia: considere $\partial F/\partial y$.*
4. Use la formula de Riemann–Hurwitz (Teorema 1.28) para concluir que el género de C es $(d-1)(d-2)/2$.

✎ **Ejercicio 1.32.** Sea $n \geq 2$ un entero y defina $F_n\colon x^n + y^n = z^n$. Estas curvas son conocidas como curvas de Fermat. Use la Fórmula de Plücker para encontrar el género de F_n.

✎ **Ejercicio 1.33.** Probar que si $\varphi\colon C \to C'$ es un isomorfismo de curvas definido sobre un campo k, entonces la función $\varphi\colon C(k) \to C'(k)$ está bien definida y es una biyección entre los conjuntos de puntos k-racionales de C y C'.

1.2. Puntos racionales

Desde el punto de vista aritmético, dada una curva C definida sobre un campo k una de las cosas de más interés para la geometría aritmética es encontrar los *puntos racionales* de la curva. Esta noción difiere un poco para curvas afines o proyectivas.

Definición 1.34 (Puntos K-racionales en una curva)**.** Sea K/k una extensión algebraica de campos (posiblemente trivial). Tenemos lo siguiente

- Si $C\colon f(x,y)$ es una curva afín sobre k, el conjunto de puntos K-racionales de C, denotado por $C(K)$, es el conjunto de $(x,y) \in K^2$ tales que $f(x,y) = 0$.
- Sea $C : F(x,y,z)$ una curva proyectiva plana sobre k. Los puntos K-racionales de C, denotados por $C(K)$ son el conjunto de $[x:y:z] \in C$ tales que $x,y,z \in K$.

En particular, si $k = \mathbb{Q}$, llamamos a los puntos $C(\mathbb{Q})$ los puntos racionales de C.

Ejemplo 1.35. La curva $\mathbb{P}^1$ tiene infinitos puntos racionales:

$$\mathbb{P}^1(\mathbb{Q}) = \{[x:y] \,:\, x,y \in \mathbb{Q}\}.$$

Por ejemplo, los puntos $[x:1]$ con $x \in \mathbb{Q}$, son todos distintos y son puntos de $\mathbb{P}^1$.

Ejemplo 1.36. Consideremos la curva proyectiva dada por ecuación de Fermat $F_3\colon x^3+y^3=z^3$. El Ejercicio 1.37 da una forma de probar que no hay solución racional no trivial (con alguna de las coordenadas 0) a esta ecuación. Por tanto tenemos que

$$F_3(\mathbb{Q}) = \{[1:0:1],[0:1:1],[1:-1:0]\}.$$

✎ **Ejercicio 1.37.** El objetivo de este ejercicio es demostrar mediante descenso infinito, que la ecuación $x^3+y^3=z^3$ no tiene soluciones enteras positivas no triviales. Supongamos, hacia una contradicción, que existe una solución no trivial en enteros positivos. Entre todas ellas, elijamos una con z mínimo y, dividiendo por el máximo común divisor si es necesario, supongamos además que $\gcd(x,y,z)=1$.

1. **Factorización en los enteros de Eisenstein.** Sea ζ_3 una raíz tercera primitiva de la unidad. En el anillo $\mathbf{Z}[\zeta_3]$ se tiene la factorización

   $$x^3+y^3=(x+y)(x+\omega y)(x+\omega^2 y).$$

   Como $x^3+y^3=z^3$, el producto de estos tres factores es un cubo. Utilizando que $\mathbf{Z}[\zeta_3]$ es un DFU y que los factores son coprimos salvo por el primo asociado a 3, se concluye que $x+\zeta_3 y$ es, salvo una unidad y un factor de $1-\zeta_3$, un cubo en $\mathbf{Z}[\zeta_3]$.

2. **Parametrización.** Por lo anterior, existen enteros a, b tales que

   $$x+\zeta_3 y = u(1-\zeta_3)(a+b\zeta_3)^3,$$

   donde u es una unidad de $\mathbf{Z}[\zeta_3]$. Al desarrollar el cubo y comparar coeficientes, se obtiene una nueva solución $X^3+Y^3=Z^3$ en enteros positivos.

3. **Descenso infinito.** La construcción anterior verifica además que $0<Z<z$. Por tanto, a partir de una solución con valor mínimo de z, hemos construido otra solución con una tercera coordenada estrictamente menor, lo cual contradice la minimalidad de z.

Ejemplo 1.38. La curva dada por la ecuación

$$\begin{aligned} y^2 = {} & 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 \\ & + 567207969x^2 - 985905640x + 247747600 \end{aligned}$$

tiene al menos 642 puntos racionales. Este ejemplo viene de aquí.

Ahora estamos listos para ir de vuelta a nuestra fase: "El género controla la aritmética". Vamos a estudiar qué ocurre con los puntos racionales de una curva proyectiva, dependiendo de su género.

1.2.1. Género 0

En el Ejemplo 1.16, vimos que $\mathbb{P}^1$ es una curva proyectiva de género 0 y en el Ejemplo 1.35 vimos que el conjunto de puntos racionales $\mathbb{P}^1(\mathbb{Q})$ es infinito. Resulta que esto es lo único que puede ocurrir para curvas de género 0.

El siguiente teorema clasifica las curvas suaves y proyectivas de género 0.

Teorema 1.39. *Si una curva suave y proyectiva C de género 0 tiene un punto, entonces es isomorfa a $\mathbb{P}^1$.*

Demostración. Esta prueba esta basada en [HS00, § A.4.3]. Más adelante, vamos a ver que cualquier curva suave y proyectiva de género 0 puede ser inmersa en el plano proyectivo $\mathbb{P}^2$ como una curva suave de grado 2 (ver § 2.2.1). Dada esta curva en $\mathbb{P}^2$, la idea es identificar $\mathbb{P}^1$ como el espacio de lineas en $\mathbb{P}^2$ que pasan por un punto. Sea P_0 un punto en la curva C de género 0. Para todo punto P en C, definimos $L(P, P_0)$ como la línea entre P y P_0, si $P \neq P_0$ o como la línea tangente a C en P_0, si $P = P_0$. Además, dada una línea L en P^2 pasando por P_0, sea P_L el punto en $\mathbb{P}^2$ tal que $L \cap C = \{P_0, P_L\}$. Entonces las funciones

$$\begin{array}{rccc} \phi\colon & C & \to & \mathbb{P}^1 \\ & P & \mapsto & L(P, P_0) \end{array} \qquad\qquad \begin{array}{rccc} \psi\colon & \mathbb{P}^1 & \to & C \\ & L & \mapsto & P_L \end{array}$$

son inversas y por lo tanto isomorfismos. □

Corolario 1.40. *Si C es una curva suave y proyectiva de género 0 que tiene un punto racional, entonces tiene infinitos.*

Demostración. Como C es una curva suave y proyectiva de género 0, entonces el Teorema 1.39 implica que C es isomorfa a $\mathbb{P}^1$, entonces tiene infinitos puntos racionales por el Ejercicio 1.33. □

1.2.2. Género 1

El siguiente teorema nos dice que las curvas de género 1 (con un punto racional) tiene una extructura algebraica adicional.

Teorema 1.41. *Si una curva suave y proyectiva de género 1 tiene un punto, entonces tiene una estructura de grupo abeliano (a partir de la geometría).*

No es difícil ver que si una curva definida sobre un campo k de género 1 tiene un punto R y la característica de k no es 2 ni 3, ella es isomorfa (sobre k) a una curva con ecuación de la forma

$$E\colon Y^2Z = X^3 + AXZ^2 + BZ^3,$$

donde $A, B \in k$. Dicho isomorfismo envía R a $\infty = [0 : 1 : 0]$. Definimos una función κ de los puntos de E a $\mathrm{Pic}^0(E)$, como $\kappa(P) = (P) - (\infty)$. Notemos que esta función es biyectiva:

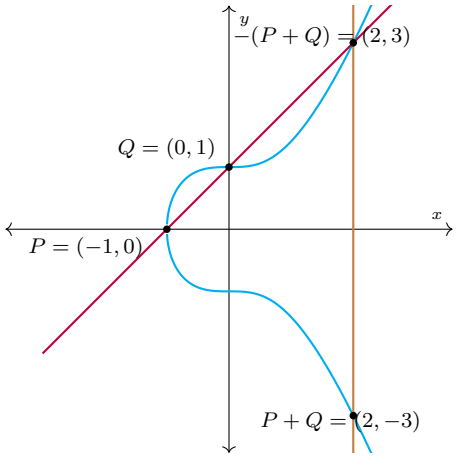
Inyectividad: Suponga que P y Q son puntos distintos en E y que $\kappa(P) = \kappa(Q)$. Entonces existe una función $f \in \overline{k}(E)$ cuyo divisor es $(P) - (Q)$. Entonces el morfismo $(f, 1)\colon E \to \mathbb{P}^1$ tiene grado 1. Luego E es isomorfa a $\mathbb{P}^1$, lo cuál es una contradicción a que $g = 2$.

Sobreyectividad: Sea $D \in \mathrm{Div}^0(E)$, el Teorema 2.16 implica que $\ell(D + (\infty)) = 1$. Por tanto el divisor $D + (\infty)$ es equivalente a un divisor efectivo, es decir, existe $P \in E$ tal que $(P) \sim D + (\infty)$, es decir, $\kappa(P) = [D]$.

Dada esta biyección podemos definir una operación en los puntos de la curva E, es decir $P + Q = \kappa^{-1}(\kappa(P) + \kappa(Q))$. Como ∞ es un punto de inflexión, la operación que definimos esta caracterizada por la siguiente regla:

$$P + Q + R = \infty \qquad \text{si y solo si} \qquad P, Q \text{ y } R \text{ son colineales.}$$

La siguiente gráfica representa la suma geométricamente:



Ejemplo 1.42. En el Ejemplo 1.36, vimos que la curva $F_3/\mathbb{Q}$ dada por la ecuación $x^3 + y^3 = z^3$ solo tiene tres puntos racionales: $[1 : 0 : 1]$, $[0 : 1 : 1]$, y $[1 : -1 : 0]$. Podemos usar la Fórmula de Plücker (Proposición 1.30) para probar que el género de F_3 es 1. Entonces este es un ejemplo de una curva de género 1 con finitos puntos racionales.

✎ **Ejercicio 1.43.** Use el isomorfismo del Ejercicio 1.26 para probar que el grupo $\mathbb{F}_3(\mathbb{Q})$ es isomorfo a $\mathbb{Z}/3\mathbb{Z}$ y generado por $[1 : -1 : 0]$. De hecho, tenemos que

$$2[1 : -1 : 0] = [1, 0, 1] \qquad \text{y} \qquad 3[1 : -1 : 0] = [0, 1, 1].$$

Definición 1.44. Sea K un campo. Una curva elíptica E sobre K es una curva definida sobre K, de género 1, y tal que $E(K) \neq \emptyset$.

Remark 1.45. La base de datos LMFDB incluye 3,824,372 curvas elípticas sobre $\mathbb{Q}$. Cada curva tiene una etiqueta única, dependiendo de algunos de sus invariantes.

Ejemplo 1.46. La curva $E/\mathbb{Q}$ dada por la ecuación $y^2 = x^3 + x^2 - 228x + 1252$ es una curva elíptica con infinitos puntos racionales. Esto se probará en el Ejercicio 3.26 una vez tengamos todas las herramientas necesarias. Más aún, se tiene que

$$E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

La etiqueta de LMFDB de esta curva es 1108.a1. Haciendo clic, usted podrá encontrar información de la curva.

1.2.3. Género ≥ 2

El siguiente es un ejemplo de una curva de género 3, a la que le podemos hallar sus puntos racionales.

Ejemplo 1.47. Considere la curva de Fermat dada por la ecuación $F_4 \colon x^4 + y^4 = z^4$. Esta curva tiene género 3, por la Proposición 1.30. Con un método análogo al caso $n = 3$ como en el Ejemplo 1.36 se puede probar que todo punto racional $[a : b : c]$ de F_4 satisface que $abc = 0$. Para una prueba rigurosa ver estas notas.

Recordemos que si una curva tiene género cero, ella no tiene puntos racionales o tiene infinitos puntos. En el caso de género uno, en el Ejemplo 1.36 vimos una curva con solo finitos puntos y en el Ejemplo 1.46 vimos que también hay curvas de género uno con infinitos puntos. Pero, ¿Qué pasa cuando una curva tiene género mas grande? Mordell en 1922, conjeturó que estas curvas siempre tienen solo finitos puntos. Este resultado fue demostrado por Gerd Faltings en 1983.

Teorema 1.48 (Teorema de Faltings)**.** *Una curva de género 2 tiene finitos puntos racionales.*

La prueba se basa en resultados profundos sobre variedades abelianas, incluyendo el teorema de finitud de Shafarevich, y constituye uno de los hitos de la geometría aritmética moderna. Tras el trabajo de Faltings, surgieron nuevas demostraciones y simplificaciones parciales de distintos componentes de la teoría. En particular, las ideas de alturas aritméticas, la teoría de Arakelov y los métodos diofánticos desarrollados por numerosos autores permitieron obtener enfoques más conceptuales de algunos pasos de la prueba y extender sus consecuencias a otros problemas. Sin embargo, la demostración original de Faltings sigue siendo la base de todas las pruebas conocidas del teorema.

Antes de que Faltings probara la conjetura de Mordell en toda generalidad, Chabauty comprobó que se puede verificar en casos en los que el género satisfaga una condición numérica (que depende de la aritmética de la curva). Posteriormente, Coleman aplicó este resultado para encontrar cotas para puntos racionales.

Teorema 1.49 (Teorema de Chabauty-Coleman)**.** *Sea C una curva de genero g y J su Jacobiano. Sea p un primo de buena reducción para C satisfaciendo $p > 2g$. Si $g > \operatorname{rank}(J(\mathbb{Q}))$, entonces*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

Remark 1.50. LMFDB también contiene una base de datos de curvas de género 2 definidas sobre $\mathbb{Q}$ aquí.

Curvas hiperelípticas.

Terminaremos esta sección con la definición de un tipo de curvas que son muy importantes computacionalmente por la simpleza de su construcción.

Definición 1.51. Una curva de género $g \geq 2$ es llamada una curva hiperelíptica si es un cubrimiento doble de una linea proyectiva.

En particular, se puede probar que toda curva hiperelíptica (en un abierto) definida sobre un campo K de caracteríistica diferente de 2 se puede definir por la ecuación $y^2 = f(x)$, en donde $f \in K[x]$ es un polinomio sin raíces repetidas. Más precisamente, sea K un campo con $\operatorname{Char}(K) \neq 2$ $f(x) \in K[x]$ un polinomio de grado $d \geq 1$ de discriminante diferente de cero, sea C_0/K la curva afín definida por la ecuación

$$C_0 : y^2 = f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d,$$

y sea g es el único entero que satisface

$$d - 3 \leq 2g \leq d - 1.$$

Sea C la clausura de la imagen de C_0 via el morfismo

$$[1, x, x^2, \ldots, x^{g-1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}.$$

✎ **Ejercicio 1.52.** Pruebe que C es una curva asuave y que la intersección es $C \cap \{X_0 \neq 0\}$ es isomorfa a C_0.

Sea

$$f^*(v) = v^{2g+2} f(1/v) = \begin{cases} a_0 + a_1 v + \cdots + a_{d-1} v^{d-1} + a_d v^d & \text{si } d \text{ es par,} \\ a_0 v + a_1 v^2 + \cdots + a_{d-1} v^d + a_d v^{d+1} & \text{si } d \text{ es impar.} \end{cases}$$

✎ **Ejercicio 1.53.** Muestre que C consiste de los abiertos afines

$$C_0 \colon y^2 = f(x) \qquad \text{y} \qquad C_1 \colon w^2 = f^*(v),$$

"pegadas" por los morfismos

$$\begin{aligned} C_0 &\longrightarrow C_1, \\ (x, y) &\longmapsto (1/x, y/x^{g+1}), \end{aligned} \qquad \begin{aligned} C_1 &\longrightarrow C_0, \\ (v, w) &\longmapsto (1/v, w/v^{g+1}). \end{aligned}$$

Más adelante veremos que el género de la una curva hiperelíptica es precisamente g. Note que la curva en el Ejemplo 1.38 es hiperelíptica de género 2.

✎ **Ejercicio 1.54.** ¿Cuándo se tiene que $\binom{x}{2} = \binom{y}{5}$ para enteros x y y?

Clase 2: Una pincelada a la geometría de curvas y al análisis p-ádico

En esta sección, recordaremos algunas nociones básicas de la geometría de curvas algebraicas que utilizaremos a lo largo de estas notas. Introduciremos el cuerpo de funciones racionales de una curva, la teoría de divisores, los sistemas lineales y el teorema de Riemann–Roch, herramientas fundamentales para el estudio de los puntos racionales. Finalmente revisaremos la definición de números p-ádicos y algunas propiedades fundamentales.

A lo largo de esta sección, C denotará una curva suave, proyectiva y geométricamente irreducible definida sobre un campo k.

2.1. Funciones racionales

Recordemos la definición del campo de funciones de C en Definición 1.10. Una función racional sobre C es un elemento del campo de funciones $k(C)$. Equivalentemente, una función racional es una función regular definida sobre un abierto denso de C. En particular, una función racional únicamente puede dejar de estar definida en un número finito de puntos.

Proposición 2.1. *Sea C una curva y $P \in C$ un punto suave. Entonces $\bar{k}[C]_P$ es un anillo de valoración discreta.*

Demostración. Ver [Sil09, Proposition 1.1.]. □

En particular, la Proposición anterior nos dice que existe un único ideal maximal M_P en $\bar{k}[C]_P$ (ver (1.22)). Además, para cada punto $P \in C$, existe un parámetro local $t \in \bar{k}[C]_P$ tal que todo elemento de $\bar{k}[C]_P$ puede escribirse como ut^n, donde u es una unidad en $\bar{k}[C]_P$ y $n \in \mathbb{Z}$. En otras palabras, $\bar{k}[C]_P$ es un anillo local con ideal maximal generado por t.

De esta forma, podemos definir el orden de una función racional en un punto de la curva.

Definición 2.2. Sea C una curva y $P \in C$ un punto suave. La valuación (normalizada) en $\bar{k}[C]_P$ esta dada por

$$\begin{array}{rccc} \mathrm{ord}_P\colon & \bar{k}[C]_P & \to & \mathbb{Z}_{\geq 0} \cup \{\infty\} \\ & f & \mapsto & \sup\{d \in \mathbb{Z} \,:\, f \in M_P^d\} \end{array}$$

Definiendo $\mathrm{ord}_P(f/g) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ podemos extender ord_P a $\bar{k}(C)$. Un uniformizador para C en P es cualquier función $t \in \bar{k}(C)$ con $\mathrm{ord}_P(t) = 1$, es decir, un generador del ideal M_P.

Ejemplo 2.3. Consideremos la curva $\mathbb{P}^1$ sobre k, con campo de funciones $k[x,y]/\langle xy-1\rangle$. Sea $P = [0:1]$. Entonces tenemos que el ideal maximal es $M_P = \langle x \rangle$. De esta forma,

$$\begin{aligned} \mathrm{ord}_P(x) &= 1 \\ \mathrm{ord}_P(y) &= \mathrm{ord}_P\left(\frac{1}{x}\right) = -1. \end{aligned}$$

✎ **Ejercicio 2.4.** Consideremos la curva elíptica

$$E\colon y^2 = x^3 - x + 1$$

y el punto $P = (1,1) \in E$.

1. Pruebe que $M_P = \langle x - 1 \rangle$
2. Demuestre que $\mathrm{ord}_P\left(\frac{x+1}{y+2}\right) = 0$.
3. Demuestre que $\mathrm{ord}_P\left(\frac{x+y-2}{y+2}\right) = 1$.

Con esta noción de orden podemos definir los ceros y polos de una función racional.

Definición 2.5. Sean C una curva y $P \in C$ un punto suave. Sea $f \in \bar{k}(C)$. El orden de f en P es $\mathrm{ord}_P(f)$. Si $\mathrm{ord}_P(f) > 0$, entonces f tiene un cero en P, y si $\mathrm{ord}_P(f) < 0$, entonces f tiene un polo en P. Si $\mathrm{ord}_P(f) \geq 0$, entonces f es regular (o definida) en P y podemos evaluar $f(P)$. De lo contrario, f tiene un polo en P y escribimos $f(P) = \infty$.

Ejemplo 2.6. Volviendo a nuestro ejemplo de $\mathbb{P}^1$, podemos probar que $[1:0]$ es un polo de x. Igualmente, para todo $P \in \mathbb{P}^1 \setminus \{[1:0], [0,1]\}$ tenemos que x no tiene polos ni ceros en esos puntos. Entonces x tiene un polo de orden 1 y un cero de orden 1.

Remark 2.7. Usando parámetros locales, también podemos definir el orden de una función racional en un punto de la curva de forma equivalente. Sea $P \in C$ y sea t un parámetro local en P. Entonces toda función racional $f \in k(C)$ admite un desarrollo de Laurent de la forma

$$f = \sum_{n \geq N} a_n t^n,$$

donde $a_N \neq 0$. El entero N no depende del parámetro local elegido. El orden de f en P es entonces el entero N tal que $a_N \neq 0$ y $a_n = 0$ para todo $n < N$.

2.2. Divisores

Sea C una curva, el grupo de divisores de C es el grupo libre generado por los puntos de C y se lo denota como $\mathrm{Div}(C)$. Entonces, los elementos de $\mathrm{Div}(C)$ son de la forma

$$D = \sum_{P \in C} n_P P, \qquad \text{donde } n_P \in \mathbb{Z} \text{ y } n_P \neq 0 \text{ para finitos } P \in C.$$

Dado un divisor D como arriba, el grado de D es el entero

$$\deg(D) := \sum_{\mathbb{P} \in C} n_P.$$

El subconjunto de divisores de grado 0,

$$\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C) \,:\, \deg(D) = 0\},$$

es un subgrupo de $\mathrm{Div}(C)$.

Otra forma de definir divisores es a partir de funciones racionales. Dada una función racional f en C, sean $P_1, \ldots, P_m$ sus ceros y $Q_1, \ldots, Q_n$ sus polos (contados con multiplicidad). Entonces el divisor de f, denotado como $\mathrm{div}(f)$ es $\mathrm{div}(f) := P_1 + \cdots P_m - Q_1 - \cdots - Q_n$. Si un divisor en C puede verse como el divisor de una función racional en C, entonces decimos que el divisor es principal. El subconjunto de divisores principales se denota como $\mathrm{PDiv}(C)$.

Lema 2.8. *Sean f y g funciones racionales en C. Entonces las siguientes propiedades se cumplen.*

1. $\operatorname{div}(f) \in \operatorname{Div}^0(C)$.
2. $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$.

En particular, $\operatorname{PDiv}(C)$ *es un subgrupo de* $\operatorname{Div}^0(C)$.

Ejemplo 2.9. Similarmente al Ejemplo 2.3 tenemos que:

$$\operatorname{div}(x) = ([0:1]) - ([1:0]).$$

✎ **Ejercicio 2.10.** Sea C una curva suave y proyectiva. Mostrar que si C tiene género 0, entonces $\operatorname{PDiv}(C) = \operatorname{Div}^0(C)$. Por otro lado, si el género de C es mayor que 0, entonces $\operatorname{PDiv}(C) \subsetneq \operatorname{Div}^0(C)$.

Definición 2.11. Sea C una curva plana y proyectiva. El grupo de Picard de C, denotado $\operatorname{Pic}(C)$ es el cociente de los divisores de C por los divisores principales de C. El subgrupo correspondiente a la imagen de los divisores de grado 0 bajo este cociente se denota $\operatorname{Pic}^0(C)$. En resumen,

$$\operatorname{Pic}(C) := \frac{\operatorname{Div}(C)}{\operatorname{PDiv}(C)} \qquad \text{y} \qquad \operatorname{Pic}^0(C) := \frac{\operatorname{Div}^0(C)}{\operatorname{PDiv}(C)}.$$

Definición 2.12. Dados dos divisores D y D' en C, decimos que son linealmente equivalentes si su clase en $\operatorname{Pic}(C)$ es la misma. Esto es,

$$D \sim D' \iff D - D' = \operatorname{div}(f) \text{ para alguna función racional } f.$$

2.2.1. Sistemas lineales

Ya hemos visto los subgrupos de divisores de grado 0 y de divisores principales de los divisores de una curva. Otro subconjunto esencial es el siguiente. Un divisor $D = \sum_{P \in C} n_P P \in \operatorname{Div}(C)$ es efectivo si $n_P \geq 0$ para todo $P \in C$. En este caso escribimos $D \geq 0$. Resulta que hay una gran cantidad de información geométrica asociada a estos divisores efectivos.

Definición 2.13. Dado un divisor D de una curva C, el sistema lineal asociado a D es el espacio vectorial

$$L(D) := \{f \text{ racional} : \operatorname{div}(f) + D \geq 0\} \cup \{0\}$$

y su dimensión se denota por $\ell(D)$.

Ejemplo 2.14. Dado un entero positivo r, el espacio $L(r\infty)$ es, por definición, el espacio de funciones racionales tales que $\operatorname{div}(f) + r\infty$ no tiene polos. Entonces, corresponde al espacio de funciones racionales cuyo único polo es en infinito y es de grado menor o igual a r.

Remark 2.15. El conjunto $L(D)$ está naturalmente parametrizado por el espacio proyectivo $\mathbb{P}^{\ell(D)-1}$. La parametrización está dada por

$$\begin{array}{ccc} \mathbb{P}(L(D)) & \to & \{D' : D' \geq 0 \text{ y } D' \sim D\} \\ f \text{ mód } k^* & \mapsto & D + \operatorname{div}(f) \end{array}$$

La noción de divisor efectivo también nos permite darle un orden parcial a los divisores de una curva. Dados divisores D_1 y D_2, definimos $D_1 \leq D_2$ si $D_2 - D_1 \geq 0$. De esta forma, si $D_1 \leq D_2$, entonces $L(D_1) \subseteq L(D_2)$.

Ahora estamos listos para entender uno de los resultados esenciales de este tema.

Teorema 2.16 (Riemann-Roch)**.** *Sea C una curva suave y proyectiva de género g. Si D es un divisor de C de grado* $\deg(D) > 2g-2$*, entonces la dimensión de $L(D)$, es*

$$\ell(D) = 1 - g + \deg(D).$$

Demostración. Para una prueba elegante usando dualidad de Serre, ver [Har13, IV,§1]. Una prueba más elemental, debida a Weil, esta en [Lan12, Capítulo 1] □

Ejemplo: Curvas elípticas

Sea E una curva elíptica con un punto marcado P_∞. Consideremos el divisor $D := rP_\infty$ para cualquier entero positivo r. Entonces $\deg(D) > 0 = 2g-2$. Aplicando Riemann-Roch (Teorema 2.16), obtenemos que

$$\dim(L(rP_\infty)) = 1 - 1 + r = r.$$

Ahora observamos que las siete funciones 1, x, y, x^2, xy, x^3, y^2 pertenecen al espacio $L(6P_\infty)$, que tiene dimensión 6. Entonces, las funciones deben ser linealmente dependientes. Así, obtenemos que los puntos de E satisfacen una ecuación en esas variables y como esto reduce la dimensión del espacio por 1, esta relación define la curva elíptica.

2.3. Diferenciales

Sea C una curva suave, proyectiva y geométricamente irreducible definida sobre un campo k de característica cero. En esta sección introducimos las distintas clases de diferenciales que aparecen en la teoría de integración p-ádica y de alturas, así como la cohomología de de Rham asociada a la curva.

Definición 2.17. Sea C una curva. El espacio de formas diferenciales (meromorfas) sobre C, denotado por Ω_C, es el $\bar{k}(C)$-espacio vectorial generado por símbolos de la forma $\mathrm{d}x$ para $x \in k(C)$, sujeto a las siguientes relaciones usuales:

(i) $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$ para todo $x, y \in k(C)$.

(ii) $\mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x$ para todo $x, y \in k(C)$.

(iii) $\mathrm{d}a = 0$ para todo $a \in k$.

Una diferencial racional sobre C puede escribirse localmente en la forma

$$\omega = f\, dt, \tag{2.18}$$

donde $f \in k(C)$ y t es un parámetro local [Sil09, Proposición 4.3]. El conjunto de todas las diferenciales racionales forma un espacio vectorial sobre $k(C)$ de dimensión 1 [Sil09, Proposición 4.2].

Sea $P \in C$ un punto y sea t un parámetro local en P. Escribiendo f en 2.18 en términos de t, también podemos escribir ω de forma única como

$$\omega = \left(\sum_{n \geq N} a_n t^n \right) \mathrm{d}t, \tag{2.19}$$

con $a_N \neq 0$. En este caso, el orden de ω en P es $\mathrm{ord}_P(\omega) := N$. Si $\mathrm{ord}_P(\omega) \geq 0$, la diferencial es regular en P. Si $\mathrm{ord}_P(\omega) < 0$, la diferencial posee un polo en P.

Escribiendo ω como en (2.19), el residuo de ω en P es

$$\mathrm{Res}_P(\omega) := a_{-1}.$$

✎ **Ejercicio 2.20.** Probar que la definición del residuo es independiente de la elección del parámetro local t.

Uno de los resultados fundamentales en este tema es el teorema de los residuos.

Teorema 2.21 (Teorema de los residuos)**.** *Para toda diferencial racional ω sobre una curva proyectiva suave C, se tiene que*

$$\sum_{P \in C} \mathrm{Res}_P(\omega) = 0.$$

Como consecuencia, el divisor de residuos de una diferencial siempre tiene grado cero.

De la misma manera en la que definimos divisores de funciones, podemos definir divisores de formas diferenciales.

Definición 2.22. Dada una forma diferencial $\omega \in \Omega^1_C$, definimos

$$\mathrm{div}(\omega) := \sum_P \mathrm{ord}_P(\omega) P \in \mathrm{Div}(C).$$

Ejemplo 2.23. En $\mathbb{P}^1$, la forma $\omega = \mathrm{d}x$ tiene divisor $\mathrm{div}(\omega) = -2\infty$, puesto que el parámetro local cuando $Y \neq 0$ es x.

✎ **Ejercicio 2.24.** Sean α_1, α_2 y $\alpha_3 \in \mathbb{Q}$, tres números distintos. Considere la curva elíptica $E\colon y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Calcule el divisor asociado al diferencial dx.

La importancia de los divisores canónicos de una curva viene de su relación con el Teorema de Riemann-Roch. Ya hemos visto una versión específica de este teorema en el Teorema 2.16.

Teorema 2.25 (Riemann–Roch, versión geométrica)**.** *Sea C una curva algebraica de género g. Para todo divisor D y cualquier divisor canónico K tenemos*

$$\ell(D) - \ell(K - D) = 1 - g + \deg(D).$$

✎ **Ejercicio 2.26.** Use el Teorema 2.25 para probar el Teorema 2.16.

Remark 2.27. Tomando $D = 0$ obtenemos

$$\ell(0) - \ell(K) = 1 - g$$

Como $L(0)$ consiste de las funciones constantes $\ell(0) = 1$, de aquí que $\ell(K) = g$. Observemos que

$$L(K) = \{f \in k(C) \colon \operatorname{div}(f) + K \geq 0\},$$

como K es un divisor canónico $K = \operatorname{div}(\omega)$, por lo que $\operatorname{div}(f) + \operatorname{div}(\omega) = \operatorname{div}(f\omega)$. Por lo que $L(K)$ esta en biyección con el espación de diferenciales holomorfos, denotado por $H^0(C, \Omega^1_C)$, entonces $h^0(C, \Omega^1) := \dim H^0(C, \Omega^1) = g$.

Corolario 2.28. *Sea C una curva algebraica de género g y K un divisor canónico. Entonces* $\deg(K) = 2g - 2$.

Demostración. Usando Riemann–Roch, tenemos que

$$\ell(K) - \ell(0) = 1 - g + \deg(K),$$

pero $\ell(K) = g$ (haciendo $D = 0$) y $\ell(0) = 1$. □

✎ **Ejercicio 2.29.** Sea C una curva hiperelíptica, como en § 1.2.3. Calcule el divisor del diferencial dx/y sobre C y use este resultado para demostrar que su género es $g = \lfloor \frac{d-1}{2} \rfloor$.

2.3.1. Tipos de diferenciales

Existen varios tipos de diferenciales racionales, dependiendo de su comportamiento para residuos y sus ordenes.

Definición 2.30 (Tipos de dirferenciales)**.** Sea ω un diferencial racional. Entonces decimos que ω es:

- exacta si $\omega = \mathrm{d}f$ para alguna función $f \in k(C)$;
- del primer tipo si es regular en todos los puntos de C;
- del segundo tipo si todos sus residuos son cero;
- del tercer tipo si todos sus polos son simples.

Las formas diferenciales del primer tipo corresponden a las diferenciales holomorfas de la curva. El conjunto de estas diferenciales (módulo diferenciales exactas) se denota por $H^0(C, \Omega^1_C)$. El espacio de diferenciales del primer tipo tiene dimensión igual al género de la curva.

Los residuos de una diferencial del tercer tipo determinan completamente el divisor residual

$$\operatorname{Res}(\omega) := \sum_P \operatorname{Res}_P(\omega)\, P. \tag{2.31}$$

En §6.3.2, veremos como las diferenciales del tercer tipo aparecen de manera natural en la teoría de alturas de Coleman–Gross. Dado un divisor de grado cero $D = \sum_P n_P P$, se buscará una diferencial de tercera especie ω_D tal que $\operatorname{Res}(\omega_D) = D$.

2.3.2. Cohomología de de Rham

Notemos que toda diferencial exacta es automáticamente del segundo tipo, pues $\operatorname{Res}_P(\mathrm{d}f) = 0$ para todo punto P.

Definición 2.32. La primera cohomología de de Rham de C el el cociente de diferenciales del segundo tipo por diferenciales exactas y se denota por $\mathrm{H}^1_{\mathrm{dR}}(C/k)$.

Para curvas suaves proyectivas, se tiene que la dimensión de $\mathrm{H}^1_{\mathrm{dR}}(C/k)$ es $2g$, donde g es el género de C.

Igualmente, la cohomología de de Rham posee una filtración natural

$$0 \subset \mathrm{H}^0(C, \Omega^1) \subset \mathrm{H}^1_{\mathrm{dR}}(C/k),$$

conocida como la filtración de Hodge. En muchas aplicaciones aritméticas se fija un complemento $W \subset \mathrm{H}^1_{\mathrm{dR}}(C/K)$ tal que

$$\mathrm{H}^1_{\mathrm{dR}}(C/k) = \mathrm{H}^0(C, \Omega^1) \oplus W. \tag{2.33}$$

Finalmente, $\mathrm{H}^1_{\mathrm{dR}}(C/K)$ viene equipado con un producto cup dado por

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(C/K) \times \mathrm{H}^1_{\mathrm{dR}}(C/K) &\to \mathbb{Q}_p \\ ([\mu_1], [\mu_2]) &\mapsto [\mu_1 \cup \mu_2] := \sum_{P \in C(\mathbb{C}_p)} \mathrm{Res}_P \left(\mu_2 \int \mu_1 \right). \end{aligned}$$

Notemos que la imagen del producto cup debería ser la segunda cohomología de Rham. Sin embargo, este espacio tiene dimensión 1 y por eso la imagen es únicamente $\mathbb{Q}_p$.

2.4. Análisis p-ádico

Una herramienta importante en el estudio de puntos racionales en curvas es el análisis sobre los números p-ádicos. Antes de concentrarnos en las definiciones y propiedades de los números p-ádicos, estudiaremos un primer ejemplo en el que son de gran utilidad.

Ejemplo 2.34. Aquí vamos a estudiar la ecuación diofántica

$$x^3 + y^3 + z^3 = 4.$$

Si existe una solución entera (x_0, y_0, z_0), entonces tendriamos que para todo primo p y para todo entero $k \geq 1$, $x_0^3 + y_0^3 + z_0^3 \equiv 4 \pmod{p^k}$. Por ejemplo, tomando $p = 3$, tendríamos una solución para

$$x^3 + y^3 + z^3 \equiv 1 \pmod 3.$$

Que es posible ya que, por ejemplo, $1 \equiv 1^3 \pmod 3$. Sin embargo, si tomamos $k = 2$, tendríamos que

$$x_0^3 + y_0^3 + z_0^3 \equiv 4 \pmod 9.$$

Sin embargo, los cubos módulo 9 son $0, 1$ y 8. Por lo tanto, la suma de tres cubos módulo 9 puede ser $0, 1, 2, 7$ u 8, pero nunca 4. Por lo tanto, no existen soluciones enteras a la ecuación.

La idea de este ejemplo es que, para estudiar la existencia de soluciones enteras a una ecuación diofántica, podemos estudiar la existencia de soluciones módulo p^k para todo primo p y todo entero $k \geq 1$. Esto nos lleva a estudiar el concepto más a fondo.

2.4.1. El campo $\mathbb{Q}_p$

Ahora nos centraremos en los valores absolutos sobre cuerpos de números y en el concepto de sus completaciones. El objetivo es extender la construcción familiar de los números reales como clases de equivalencia de sucesiones de Cauchy de números racionales a un contexto más general, que permita desarrollar nuevas herramientas para estudiar campos de números. Antes de introducir las definiciones formales, presentamos el ejemplo fundamental de una completación distinta de $\mathbb{R}$: el campo $\mathbb{Q}_p$ de los números p-ádicos.

Definición del valor absoluto p-ádico

Sea p un número primo. Para todo entero no nulo $x \in \mathbb{Z}$, definimos la valoración p-ádica $v_p(x)$ como el mayor exponente de p que divide a x. Esta valoración se extiende naturalmente a $\mathbb{Q}$ mediante

$$v_p\left(\frac{x}{y}\right) := v_p(x) - v_p(y),$$

donde $x, y \in \mathbb{Z}$ y $y \neq 0$. Por convenio, definimos $v_p(0) = +\infty$. Para $x \in \mathbb{Q}$, el valor absoluto p-ádico se define por

$$|x|_p = p^{-v_p(x)},$$

y por definición $|0|_p = 0$. Este valor absoluto tiene la propiedad fundamental de definir una métrica no arquimediana. Más precisamente:

1. $|x|_p = 0$ si y sólo si $x = 0$.
2. $|xy|_p = |x|_p \cdot |y|_p$.
3. $|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\}$, propiedad conocida como desigualdad ultramétrica.

Para la desigualdad ultramétrica, si $|x|_P \neq |y|_P$, entonces la desigualdad se convierte en una igualdad.

Construcción de $\mathbb{Q}_p$

Recordemos que una sucesión x_n en un espacio métrico es una *sucesión de Cauchy* respecto de una métrica $|\cdot|$ si, dado $\varepsilon > 0$, existe N tal que $|x_m - x_n| < \varepsilon$ para todo $m, n \geq N$. Definimos una relación de equivalencia sobre el conjunto de sucesiones de Cauchy declarando que $\{x_n\} \sim \{y_n\}$ si

$$\lim_{n\to\infty} |x_n - y_n| = 0.$$

La completación de un espacio métrico X respecto de $|\cdot|$ se define como el conjunto de clases de equivalencia de sucesiones de Cauchy en X. Denotaremos por $\mathbb{Q}_p$ la completación de $\mathbb{Q}$ respecto del valor absoluto $|\cdot|_p$. $\mathbb{Q}_p$ satisface las siguientes propiedades fundamentales:

(a) $\mathbb{Q}_p$ es un campo. Lo llamaremos el *campo de los números p-ádicos.*

(b) El valor absoluto $|\cdot|_p$ se extiende naturalmente a $\mathbb{Q}_p$, y esta extensión sigue satisfaciendo las propiedades anteriores.

(c) $\mathbb{Q}_p$ es completo; es decir, toda sucesión de Cauchy en $\mathbb{Q}_p$ converge.

Dentro de $\mathbb{Q}_p$ aparece el subanillo $\mathbb{Z}_p$ de los enteros p-ádicos. Este puede definirse como la completación de $\mathbb{Z}$ respecto de $|\cdot|_p$, o equivalentemente como

$$\{x \in \mathbb{Q}_p \colon |x|_p \leq 1\}.$$

El anillo $\mathbb{Z}_p$ es un anillo local cuyo único ideal maximal es

$$p\mathbb{Z}_p \coloneqq \{x \in \mathbb{Z}_p \colon |x|_p < 1\}.$$

✎ **Ejercicio 2.35.** Use la topología de $\mathbb{Q}_p$ dada por el valor absoluto $|\cdot|_p$ para probar las siguientes propiedades.

1. Todo triángulo en $\mathbb{Q}_p^2$ es isósceles.
2. Todo punto en una bola abierta en $\mathbb{Q}_p$ es su centro.
3. Las bolas en $\mathbb{Q}_p$ son abiertas y cerradas al tiempo.
4. Dos bolas del mismo radio son disjuntas o iguales.

2.4.2. Una construcción alternativa de $\mathbb{Q}_p$

Para cada entero $n \geq 1$, supongamos que se nos da un elemento $a_n \in \mathbb{Z}$ tal que $0 \leq a_n \leq p^n - 1$ y además $a_n \equiv a_{n-1} \pmod{p^{n-1}}$. Una sucesión $\{a_n\}$ con esta propiedad se denomina una *sucesión coherente* (o sucesión p-ádica coherente). Por ejemplo, si $p = 3$, entonces $\{1, 4, 22, \ldots\}$ es el comienzo de una sucesión coherente, ya que $4 \equiv 1 \pmod 3$ y $22 \equiv 4 \pmod 9$.

Afirmamos que existe una biyección entre las sucesiones coherentes y los elementos de $\mathbb{Z}_p$. Por una parte, es fácil comprobar que toda sucesión coherente es una sucesión de Cauchy respecto de $|\cdot|_p$, por lo que determina un elemento de $\mathbb{Z}_p$. Recíprocamente, dado un elemento $x \in \mathbb{Z}_p$, puede demostrarse que existe una única sucesión coherente que converge a x. Como consecuencia obtenemos el siguiente resultado.

Teorema 2.36. *Todo entero p-ádico $x \in \mathbb{Z}_p$ puede escribirse de manera única en la forma*

$$x = b_0 + b_1 p + \cdots + b_n p^n + \cdots,$$

donde $b_n \in \{0, 1, \ldots, p-1\}$ para todo n. De manera similar, todo elemento $x \in \mathbb{Q}_p$ puede escribirse de manera única en la forma

$$x = b_{-k} p^{-k} + b_{-k+1} p^{-k+1} + \cdots + b_0 + b_1 p + \cdots + b_n p^n + \cdots,$$

para algún entero k, donde $b_{-k} \neq 0$ y $0 \leq b_n \leq p-1$ para todo n. En este caso, $v_p(x) = -k$, y por tanto $|x|_p = p^k$.

Obsérvese que un entero p-ádico $b = b_0 + b_1 p + b_2 p^2 + \cdots$ es una unidad del anillo $\mathbb{Z}_p$ si y sólo si $|b|_p = 1$. Por el Teorema 2.36, esto equivale a la condición $b_0 \neq 0$. Además, esta construcción proporciona un isomorfismo canónico

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

para todo $n \geq 1$.

Las operaciones aritméticas en $\mathbb{Q}_p$ se realizan de la manera esperada, utilizando las expansiones p-ádicas. Por ejemplo, si $p = 3$ y

$$x = 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^4 + O(3^5),$$
$$y = 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^4 + O(3^5),$$

donde $O(3^5)$ indica que todos los términos restantes son divisibles por 3^5, y por tanto son 3-ádicamente pequeños. Entonces

$$x + y = 1 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + O(3^5).$$

Esta expresión se obtiene sumando coeficiente a coeficiente y transportando los acarreamientos hacia las potencias superiores de 3. Por ejemplo,

$$2 \cdot 3^2 + 2 \cdot 3^2 = 4 \cdot 3^2 = (1 + 3) \cdot 3^2 = 1 \cdot 3^2 + 1 \cdot 3^3.$$

✎ **Ejercicio 2.37.** Verifique las siguientes identidades en $\mathbb{Z}_p$:

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots + p^n + \cdots,$$
$$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots.$$

Una propiedad fundamental de los números p-ádicos está descrita por el siguiente resultado.

Proposición 2.38. *Sea $F(x) \in \mathbb{Z}_p[x]$ un polinomio y suponga que existe $\alpha \in \mathbb{Z}_p$ tal que*

$$F(\alpha) \equiv 0 \pmod{p} \qquad y \qquad F'(\alpha) \not\equiv 0 \pmod{p}.$$

Entonces F tiene una única raíz α_0 en $\mathbb{Z}_p$ con la condición que $\alpha \equiv \alpha_0 \pmod{p}$.

Demostración. Supongamos primero que $F(x)$ tiene una raíz en $\mathbb{Z}_p$. La aplicación natural

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

envía dicha raíz a una raíz de $F(x)$ módulo p^n. Por tanto, $F(x)$ tiene una raíz módulo p^n para todo $n \geq 1$. Recíprocamente, supongamos que $F(x)$ tiene una raíz módulo p^n para todo $n \geq 1$. Para cada n, elijamos un entero x_n tal que

$$F(x_n) \equiv 0 \pmod{p^n}.$$

Como $\mathbb{Z}/p\mathbb{Z}$ es finito, existen infinitos términos de la sucesión (x_n) que tienen la misma reducción módulo p. Denotemos esta clase por $y_1 \in \mathbb{Z}/p\mathbb{Z}$.

Extrayendo una subsucesión adecuada, obtenemos una sucesión $x_n^{(1)}$ tal que

$$x_n^{(1)} \equiv y_1 \pmod{p} \qquad \text{y} \qquad F(x_n^{(1)}) \equiv 0 \pmod{p}$$

para todo n. Repitiendo este argumento inductivamente, para cada $k \geq 1$ obtenemos una subsucesión $x_n^{(k)}$ y un elemento $y_k \in \mathbb{Z}/p^k\mathbb{Z}$ tales que

$$x_n^{(k)} \equiv y_k \pmod{p^k} \qquad \text{y} \qquad F(x_n^{(k)}) \equiv 0 \pmod{p^k}$$

para todo n. Además,

$$y_k \equiv y_{k-1} \pmod{p^{k-1}}.$$

Por tanto, $(y_k)_{k \geq 1}$ forma una sucesión coherente y determina un elemento $y \in \mathbb{Z}_p$. Como $F(y_k) \equiv 0 \pmod{p^k}$ para todo k, se sigue que $F(y) = 0$. Por lo tanto, F tiene una raíz en $\mathbb{Z}_p$. □

✎ **Ejercicio 2.39.** Estudie la ecuación $x^2 = -1$ en los anillos $\mathbb{Z}_3$ y $\mathbb{Z}_5$.

1. Determine cuáles son los cuadrados módulo 3, y concluya que la ecuación no tiene soluciones en $\mathbb{Z}_3$.
2. Demuestre que $x^2 = -1$ tiene soluciones en $\mathbb{Z}_5$.
   a) Muestre que -1 es un cuadrado módulo 5.
   b) Suponga que para algún $n \geq 0$ se ha construido un entero
   $$c_n = 2 + a_1 5 + a_2 5^2 + \cdots + a_n 5^n$$
   tal que $c_n^2 + 1 \equiv 0 \pmod{5^{n+1}}$. Busque un coeficiente a_{n+1} tal que
   $$c_{n+1} = c_n + a_{n+1} 5^{n+1}$$
   satisfaga $c_{n+1}^2 + 1 \equiv 0 \pmod{5^{n+2}}$. Concluya que existe una única elección de $a_{n+1} \pmod 5$ que satisface
   $$a_{n+1} \equiv \frac{1 + c_n^2}{5^{n+1}} \pmod 5.$$
   c) Explique por qué esto permite construir inductivamente una sucesión
   $$c_0, c_1, c_2, \ldots$$
   que converge en $\mathbb{Z}_5$ a una solución de $x^2 + 1 = 0$.

Remark 2.40. Igual que como en los números racionales, cualquier número en $\mathbb{Q}_p$ tiene una aproximación p-ádica con potencias de p. Para ver ejemplos de este proceso, puede revisar estas notas. Si el lector usa Magma, para tener las expansiones p-ádicas de estos números, después de definir el campo p-ádico `Qp`, se debe cambiar el atributo `Qp`‘`SeriesPrinting := true;`.

2.4.3. Trabajando con p-ádicos en Magma

A continuación tenemos código en Magmapara definir los números p-ádicos y trabajar con ellos.

```
// Podemos definir los enteros p-adicos
p := 5;
prec := 4;
Zp := pAdicRing(p,prec);
Zp‘SeriesPrinting := true;
Zp!2;

// Ahora polinomios sobre los enteros p-adicos y raices de polinomios
_<x> := PolynomialRing(Zp);
f := x^2 + 1;
roots := Roots(f);
roots[1][1];
roots[2][1];

// Otro ejemplo similar
```

```
p := 7;
Zp := pAdicRing(p);
Zp`SeriesPrinting := true;
_<x> := PolynomialRing(Zp);
f := x^2 + 1;
roots := Roots(f);
roots;

// Ahora podemos definir los numeros p-adicos y curvas sobre ellos
Qp := pAdicField(p, 4);
Qp`SeriesPrinting := true;
_<x> := PolynomialRing(Qp);
E := EllipticCurve(x^3+x+1);
P := E![0, 1];
2*P;
3*P;

// Otro punto y sumamos
Q := E![2,Roots(x^2-Evaluate(x^3+x+1,2))[1][1]];
Q;
P+Q;
```

Clase 3: La variedad jacobiana

En el caso de una curva elíptica, los puntos racionales poseen naturalmente una estructura de grupo. Cuando el género es mayor que uno ya no es posible definir una ley de grupo sobre la curva, pero sí existe una variedad abeliana asociada a ella, llamada el jacobiano. Esta variedad permite trasladar problemas sobre puntos racionales de la curva a problemas sobre variedades abelianas.

Una primera descripción del jacobiano puede darse en términos del grupo de Picard y aplica para curvas sobre cualquier campo. Igualmente, si trabajamos sobre $\mathbb{C}$, podemos definir el jacobiano de una forma más geométrica usando la estructura de superficie de Riemann de la curva. Ambas construcciones son equivalentes (ver Teorema 3.13), aunque la que más usaremos será la primera.

3.1. La variedad Jacobiana de una curva como grupo de Picard

Definición 3.1. Sea C una curva suave y proyectiva. El jacobiano de C es la variedad abeliana cuya variedad de puntos es

$$J(C) = \mathrm{Pic}^0(C).$$

En otras palabras, sus puntos corresponden a clases de equivalencia lineales de divisores de grado cero.

Esta descripción es puramente algebraica y tiene sentido sobre cualquier campo. En particular, si C está definida sobre un campo de números o sobre un campo p-ádico, el jacobiano también lo está.

Existe una relación importante entre la curva y su Jacobiano.

Definición 3.2. Sea C una curva suave y proyectiva con un punto $P_0 \in C$. El mapa de Abel–Jacobi es

$$\begin{array}{rccc} \mathrm{AJ}_{P_0}: & C & \to & \mathrm{Pic}^0(C) \\ & P & \mapsto & [P - P_0] \end{array} \tag{3.3}$$

En la siguiente sección, probaremos que este es un morfismo de variedades y además es inyectivo cuando el género de C es $g \geq 1$ (ver Corolario 3.14).

3.2. La variedad Jacobiana de una curva como superficie de Riemann

La variedad jacobiana de una superficie de Riemann compacta C puede construirse como un cociente del espacio dual de las 1-formas holomorfas sobre C. Esta construcción permite ver al jacobiano como un cociente de $\mathbb{C}^g$, donde g es el género de la superficie. Más precisamente, al elegir una base de $\Omega^1(C)$, el espacio dual $\Omega^1(C)^*$ se identifica con $\mathbb{C}^g$, y el subgrupo de periodos da lugar al cociente correspondiente. En esta sección mostramos dicha construcción.

Recordemos el Teorema de Stokes [Mir95, Theorem VII.3.16], que afirma que si B es un conjunto

cerrado triangulable en C y ω es una 1-forma de clase $\mathcal{C}^\infty$ sobre C, entonces

$$\int_{\partial B} \omega = \iint_B d\omega.$$

Sea $[c] \in H_1(C, \mathbb{Z})$. Para todo 1-ciclo d tal que $[d] = [c]$, se tiene $d = c + \partial b$ para alguna 2-cadena b. Usando el Teorema de Stokes con $B = b$, obtenemos que para toda 1-forma cerrada y de clase $\mathcal{C}^\infty$, ω,

$$\int_d \omega = \int_c \omega + \int_{\partial b} \omega = \int_c \omega + \iint_b d\omega = \int_c \omega.$$

En particular, si ω es una 1-forma holomorfa, entonces también es cerrada [Mir95, Lemma IV.2.4], lo cual implica que el siguiente mapa está bien definido:

$$\begin{array}{rccc} \displaystyle\int_{[c]}: & \Omega^1(C) & \to & \mathbb{C} \\ & \omega & \mapsto & \displaystyle\int_c \omega \end{array}$$

donde $[c] \in H_1(C, \mathbb{Z})$.

Decimos que un funcional lineal $\lambda\colon \Omega^1(C) \to \mathbb{C}$ es un *periodo* si $\lambda = \int_{[c]}$ para algún $[c] \in H_1(C, \mathbb{Z})$. El conjunto de periodos es un subgrupo de $\Omega^1(C)^*$. En efecto, dados $[c], [d] \in H_1(C, \mathbb{Z})$,

$$\int_{[c]} \omega + \int_{[d]} \omega = \int_{[c]+[d]} \omega,$$

donde $[c]+[d]$ es la suma en homología, inducida por la suma de ciclos. Denotamos por Λ al conjunto de periodos y, como es un subgrupo de $\Omega^1(C)^*$, podemos considerar el cociente $\Omega^1(C)^*/\Lambda$.

Definición 3.4. El jacobiano de una superficie de Riemann compacta C es el cociente del espacio de funcionales lineales sobre las 1-formas holomorfas de C por el conjunto de periodos; es decir,

$$\mathrm{J}(C) := \frac{\Omega^1(C)^*}{\Lambda}.$$

Remark 3.5. Como $\Omega^1(C)^*$ es un grupo abeliano, $\mathrm{J}(C)$ también lo es. Además, si C es una superficie de Riemann compacta de género g, entonces $\Omega^1(C)$ tiene una base $\omega_1, \ldots, \omega_g$. Todo $\lambda \in \Omega^1(C)^*$ queda completamente determinado por el vector

$$v_\lambda := (\lambda(\omega_1), \ldots, \lambda(\omega_g)).$$

Esto implica que $\Omega^1(C)^*$ es isomorfo a $\mathbb{C}^g$, al identificar λ con v_λ. Bajo este isomorfismo, Λ corresponde al conjunto de elementos de la forma

$$\left(\int_c \omega_1, \ldots, \int_c \omega_g \right), \qquad [c] \in H_1(C, \mathbb{Z}).$$

Ejemplo 3.6. El género de $\mathbb{P}^1$ es 0, lo que implica que el espacio de formas holomorfas es trivial; por lo tanto, $\mathrm{J}(C) = 0$.

Ejemplo 3.7. Si C es el toro complejo $\mathbb{C}/L$, entonces $\mathrm{J}(C) \cong C$. En efecto, el género del toro es 1, así que $\Omega^1(C)$ está generado por dz, y por tanto $\Omega^1(C)^* \cong \mathbb{C}$. Por consiguiente, basta demostrar que $\Lambda \cong L$.

Supongamos que $L = z_1\mathbb{Z} \oplus z_2\mathbb{Z}$ y que $\pi\colon \mathbb{C} \to \mathbb{C}/L$ es el mapa cociente. Definamos además los caminos

$$\begin{array}{rccc} \gamma_1\colon & [0,1] & \to & \mathbb{C} \\ & t & \mapsto & tz_1 \end{array} \qquad \begin{array}{rccc} \gamma_2\colon & [0,1] & \to & \mathbb{C} \\ & t & \mapsto & tz_2. \end{array}$$

Nótese que las composiciones $\pi \circ \gamma_1$ y $\pi \circ \gamma_2$ son lazos en C basados en 0. Como z_1 y z_2 son linealmente independientes sobre $\mathbb{R}$, las clases de estos lazos son linealmente independientes en homología. Puesto que $H_1(C, \mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}$, concluimos que $[\pi \circ \gamma_1]$ y $[\pi \circ \gamma_2]$ generan $H_1(C, \mathbb{Z})$. En particular, Λ es una red en $\Omega^1(C)^* \cong \mathbb{C}$.

Además,

$$\int_{\pi\circ\gamma_1} dz = \int_{\gamma_1} \pi^*(dz) = \int_{\gamma_1} dz = \int_0^1 z_1\, dt = z_1,$$

y de manera análoga,

$$\int_{\pi\circ\gamma_2} dz = z_2.$$

Por lo tanto,

$$\Lambda \cong z_1\mathbb{Z} \oplus z_2\mathbb{Z} = L,$$

y en consecuencia

$$\mathrm{J}(C) \cong \mathbb{C}/L \cong C.$$

3.2.1. El mapa de Abel–Jacobi

Una propiedad importante del jacobiano de una superficie de Riemann compacta y suave C es que C puede encajarse en $\mathrm{J}(C)$. En esta sección estudiamos el mapa que proporciona dicho encaje, llamado mapa de Abel–Jacobi. Además, damos la generalización del mapa de Abel–Jacobi a un mapa cuyo dominio es el conjunto de divisores de C. Finalmente, enunciamos el Teorema de Abel–Jacobi, un resultado importante que caracteriza al jacobiano de otra manera.

Primero, sea C una superficie de Riemann compacta. Fijemos $P_0 \in C$ y, para cada $P \in C$, sea γ_P un camino de P_0 a P. Quisiéramos definir un mapa

$$\begin{array}{ccc} C & \to & \Omega^1(C)^* \\ P & \mapsto & \displaystyle\int_{\gamma_P}. \end{array} \tag{3.8}$$

Sin embargo, este mapa no está bien definido porque depende del camino elegido. Si γ'_P es otro camino de P_0 a P, entonces

$$\int_{\gamma_P} \omega = \int_{\gamma'_P} \omega + \int_{\gamma_P - \gamma'_P} \omega.$$

Observamos que $\gamma_P - \gamma'_P$ es un lazo cerrado basado en P_0, de modo que define una clase de homología, y por tanto $\int_{\gamma_P-\gamma'_P}$ es un periodo. Esto implica que el mapa en (3.8) está bien definido módulo el conjunto de periodos de C.

Definición 3.9. El mapa de Abel–Jacobi de C es el mapa

$$\mathrm{AJ}_{P_0}\colon \quad C \quad \to \quad \mathrm{J}(C)$$

dado por

$$\mathrm{AJ}_{P_0}(P) = \int_{\gamma_P} \quad (\text{mód } \Lambda).$$

Esta definición depende del punto base P_0. Para definir un mapa independiente de la elección de P_0, es necesario extender la definición al grupo de divisores de C.

Definición 3.10. El mapa de Abel–Jacobi sobre $\mathrm{Div}(C)$ es el mapa

$$\begin{array}{rccc} \mathrm{AJ}_{P_0}: & \mathrm{Div}(C) & \to & \mathrm{J}(C) \\ & \sum n_i P_i & \mapsto & \sum n_i \,\mathrm{AJ}_{P_0}(P_i). \end{array}$$

Si restringimos AJ_{P_0} a divisores de grado 0, obtenemos un mapa

$$\mathrm{AJ}^0 : \mathrm{Div}^0(C) \to \mathrm{J}(C),$$

el cual es independiente del punto base, como afirma el siguiente lema.

Lema 3.11. *El mapa* $\mathrm{AJ}^0 : \mathrm{Div}^0(C) \to \mathrm{J}(C)$ *definido por*

$$\mathrm{AJ}^0\left(\sum n_i P_i\right) = \sum n_i \,\mathrm{AJ}_{P_0}(P_i)$$

es independiente de la elección del punto base P_0.

Demostración. Supongamos que P_0 y P_0' son dos puntos base distintos, y sea γ un camino de P_0' a P_0. Sea $P \in C$ y sea γ_P un camino de P_0 a P. Evaluando AJ_{P_0} obtenemos

$$\mathrm{AJ}_{P_0}(P) = \left(\int_{\gamma_P} \omega_1, \ldots, \int_{\gamma_P} \omega_g\right) + \Lambda.$$

En cambio, si usamos el punto base P_0', tenemos

$$\mathrm{AJ}_{P_0'}(P) = \left(\int_{\gamma+\gamma_P} \omega_1, \ldots, \int_{\gamma+\gamma_P} \omega_g\right) + \Lambda = \left(\int_{\gamma_P} \omega_1, \ldots, \int_{\gamma_P} \omega_g\right) + \left(\int_{\gamma} \omega_1, \ldots, \int_{\gamma} \omega_g\right) + \Lambda. \quad (3.12)$$

Tomando $j := \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g\right)$, (3.12) muestra que $\mathrm{AJ}_{P_0}(P) - \mathrm{AJ}_{P_0'}(P) = j$. Entonces, para un divisor de grado cero $\sum n_i P_i$, el valor $\mathrm{AJ}^0\left(\sum n_i P_i\right)$ cambia en

$$\sum n_i j = j \sum n_i = 0,$$

pues $\sum n_i = 0$. □

Teorema 3.13 (Teorema de Abel–Jacobi)**.** *El mapa de Abel–Jacobi es sobreyectivo y su núcleo es el grupo de divisores principales de* C. *Es decir,*

$$\mathrm{Pic}^0(C) = \frac{\mathrm{Div}^0(C)}{\mathrm{PDiv}(C)} \cong \mathrm{J}(C).$$

Explicaremos una demostración de este teorema en la siguiente sección. Antes, presentamos un corolario que prueba que el mapa de Abel–Jacobi define un encaje de C en su jacobiano.

Corolario 3.14. *Si* C *una curva suave y proyectiva con un punto* P_0, *entonces el mapa de Abel–Jacobi en* (3.3) *es inyectivo.*

Demostración. Supongamos, buscando una contradicción, que $\mathrm{AJ}(P) = \mathrm{AJ}(Q)$ para $P \neq Q$ en C. Entonces

$$\mathrm{AJ}^0(P - Q) = 0,$$

y por el Teorema de Abel–Jacobi se sigue que $P - Q$ es un divisor principal. Por lo tanto, existe una función meromorfa f sobre C con un único cero en P y un único polo en Q. Usando f, se puede definir la función holomorfa

$$F\colon C \to \mathbb{P}^1$$

por

$$F(x) = \begin{cases} f(x), & \text{si } x \text{ no es un polo de } f; \\ \infty, & \text{si } x \text{ es un polo de } f. \end{cases}$$

La función F no es constante porque f tiene un cero y un polo. Además, F tiene grado 1, pues posee exactamente un polo simple y un cero simple. Por consiguiente, F define un isomorfismo entre C y $\mathbb{P}^1$. Sin embargo, el género de $\mathbb{P}^1$ es 0, mientras que $g \geq 1$, lo cual es una contradicción. □

3.2.2. Prueba del Teorema de Abel–Jacobi

Presentamos un bosquejo de la demostración del Teorema de Abel–Jacobi, enunciado en el Teorema 3.13. La demostración consta de dos teoremas, que muestran respectivamente que el mapa de Abel–Jacobi tiene el núcleo deseado y que es sobreyectivo.

Teorema 3.15 (Teorema de Abel)**.** *Un divisor de grado* 0 *es principal si y sólo si su imagen bajo el mapa de Abel–Jacobi es cero.*

Demostración (bosquejo). Para la implicación directa, sea f una función meromorfa y sea $D = \mathrm{Div}(f)$ su divisor. Definamos $F\colon C \to \mathbb{P}^1$ como el mapa correspondiente, que es el mismo que se definió en el Corolario 3.14. Sea γ un camino de ∞ a 0 en $\mathbb{P}^1$ que no pase por valores críticos de F. Entonces

$$F^*\gamma = \sum_{i=1}^{d} \gamma_i,$$

donde cada γ_i es un camino de un polo a un cero de f, contando multiplicidades. Definamos $P_i = \gamma_i(1)$ y $Q_i = \gamma_i(0)$. Entonces podemos escribir

$$D = \sum_{i=1}^{d} (P_i - Q_i).$$

Ahora escojamos un punto base $P_0 \in C$, un camino α_i de P_0 a P_i y un camino β_i de P_0 a Q_i. Si $\{\omega_1, \ldots, \omega_g\}$ es una base de $\Omega^1(C)$, entonces

$$\mathrm{AJ}^0(D) = \sum_{i=1}^{d} \left(\int_{\alpha_i} \omega_1, \ldots, \int_{\alpha_i} \omega_g \right) - \left(\int_{\beta_i} \omega_1, \ldots, \int_{\beta_i} \omega_g \right) + \Lambda.$$

Si η_i es el camino cerrado $\alpha_i - \gamma_i - \beta_i$, entonces el vector

$$\left(\int_{\eta_i} \omega_1, \ldots, \int_{\eta_i} \omega_g \right)$$

es un periodo para todo $i \in \{1, \dots, d\}$. Por lo tanto, podemos restar estos vectores a $\mathrm{AJ}^0(D)$ sin cambiar su clase en el cociente:

$$\begin{aligned}\mathrm{AJ}^0(D) &= \sum_{i=1}^{d} \left(\int_{\alpha_i} \omega_1, \dots, \int_{\alpha_i} \omega_g \right) - \left(\int_{\beta_i} \omega_1, \dots, \int_{\beta_i} \omega_g \right) - \left(\int_{\eta_i} \omega_1, \dots, \int_{\eta_i} \omega_g \right) + \Lambda \\ &= \left(\sum_{i=1}^{d} \int_{\gamma_i} \omega_1, \dots, \sum_{i=1}^{d} \int_{\gamma_i} \omega_g \right) + \Lambda \\ &= \left(\int_{F^*\gamma} \omega_1, \dots, \int_{F^*\gamma} \omega_g \right) + \Lambda.\end{aligned}$$

Además,

$$\int_{F^*\gamma} \omega_i = \int_{\gamma} \mathrm{Tr}(\omega_i) \qquad \text{[Mir95, Lemma VIII.3.4]},$$

donde $\mathrm{Tr}(\omega_i)$ es holomorfa porque ω_i lo es [Mir95, VIII.3]. Sin embargo, la única 1-forma holomorfa sobre $\mathbb{P}^1$ es 0, ya que su género es cero. En consecuencia,

$$\mathrm{AJ}^0(D) = 0.$$

Recíprocamente, sea $D \in \mathrm{Div}^0(C)$ un divisor en el núcleo de AJ^0. Por [Mir95, Lemma VIII.4.6], existe una 1-forma meromorfa ω tal que:

- ω tiene polos simples en los puntos donde $D(P) \neq 0$, y no tiene otros polos;
- $\mathrm{Res}_P(\omega) = D(P)$ para todo $P \in C$, donde $D(P)$ es el coeficiente de P en la suma formal D;
- los a-periodos y los b-periodos de ω son múltiplos enteros de $2\pi i$.

Aquí, los a-periodos y b-periodos se definen usando una estructura CW de C con 1-celdas $\{a_i, b_i\}_{i=1}^{g}$. Para cualquier 1-forma σ definimos

$$A_i(\sigma) := \int_{a_i} \sigma \qquad \text{y} \qquad B_i(\sigma) := \int_{b_i} \sigma.$$

Los a-periodos de σ son los números $A_i(\sigma)$, y los b-periodos son los números $B_i(\sigma)$.

Fijemos un punto $P_0 \in C$ y definamos una función $f \colon C \to \mathbb{C}$ por

$$f(P) = \exp\left(\int_{P_0}^{p} \omega \right).$$

Esta función es holomorfa donde ω es holomorfa, es decir, en el conjunto de puntos cuyo coeficiente en D es 0. Además, como los periodos son múltiplos de $2\pi i$ y los residuos de ω son enteros, el valor de f no depende del camino elegido de P_0 a P. Nuestro objetivo es mostrar que f es meromorfa y que $\mathrm{Div}(f) = D$.

Sea $P \in C$ tal que $D(P) = n \neq 0$. Por la construcción de ω, esto implica que en una vecindad de P puede escribirse

$$\omega = \left(\frac{n}{z} + g(z) \right) dz,$$

donde z es una coordenada local centrada en P y $g(z)$ es holomorfa. Para z en esa vecindad,

$$f(z) = \exp\left(\int_{P_0}^{z} \omega \right) = \exp\left(n \log z + h(z) \right) = z^n e^{h(z)},$$

donde $h(z)$ es una función holomorfa. Esto implica que f es meromorfa en una vecindad de P y que $\mathrm{ord}_P(f) = n$. En conclusión, $\mathrm{Div}(f) = D$. □

Teorema 3.16 (Teorema de inversión de Jacobi)**.** *El mapa de Abel–Jacobi de divisores de grado cero al jacobiano es sobreyectivo.*

Demostración. Elijamos un punto base P_0 y definamos el mapa

$$\begin{array}{rccc} \varphi\colon & C^g & \to & \mathrm{J}(C) \\ & (P_1,\dots,P_g) & \mapsto & \left(\displaystyle\sum_{i=1}^{g}\int_{P_0}^{P_i}\omega_1,\dots,\sum_{i=1}^{g}\int_{P_0}^{P_i}\omega_g\right)+\Lambda, \end{array}$$

donde $\{\omega_1,\dots,\omega_g\}$ es una base de $\Omega^1(C)$. Es posible demostrar que existe una g-tupla $\vec{P} := (P_1,\dots,P_g)$ tal que el determinante jacobiano de φ en $\vec{P}$ es no nulo [Nar92, Lemma 15.1]. El teorema de la función implícita implica que existe una vecindad abierta de P sobre la cual φ induce un biholomorfismo local sobre una vecindad V de $\varphi(P)$.

Sea ahora $\lambda = (\lambda_1,\dots,\lambda_g) \in \Omega^1(C)^* \cong \mathbb{C}^g$. Como V es abierta, existe un entero $n \geq 1$ tal que

$$\varphi(P) + \frac{\lambda}{n} \in V.$$

Dado que φ es biyectiva sobre V, existe $\vec{Q} := (Q_1,\dots,Q_g) \in C^g$ tal que

$$\varphi(\vec{Q}) = \varphi(P) + \frac{\lambda}{n}. \tag{3.17}$$

Definamos ahora el divisor

$$D' := n\sum_{i=1}^{g} Q_i - n\sum_{i=1}^{g} P_i + gP_0.$$

El grado de D' es g, y por el Teorema de Riemann–Roch,

$$h^0(D') = 1 + h^0(K - D') \geq 1,$$

donde K es el divisor de una 1-forma meromorfa no nula. Esto implica que D' es linealmente equivalente a un divisor efectivo $D = \sum_{i=1}^{g} r_i$. Por tanto,

$$\mathrm{AJ}^0(D' - gP_0) = \mathrm{AJ}^0(D - gP_0).$$

Por la definición de φ,

$$\mathrm{AJ}^0(D - gP_0) = \mathrm{AJ}^0\left(\sum_{i=1}^{g}(r_i - P_0)\right) = \varphi(r_1,\dots,r_g).$$

Además,

$$\begin{array}{rcl} \mathrm{AJ}^0(D' - gP_0) & = & \mathrm{AJ}^0\left(n\displaystyle\sum_{i=1}^{g}(Q_i - P_0) - n\sum_{i=1}^{g}(P_i - P_0)\right) \\ & = & n\big(\varphi(Q) - \varphi(P)\big) \\ & = & \lambda, \end{array}$$

donde en la última igualdad usamos (3.17). En consecuencia, λ pertenece a la imagen de AJ^0, y así AJ^0 es sobreyectivo. □

3.3. Teorema de Mordell-Weil

Sabemos desde el Teorema 1.41 que los puntos racionales de una curva elíptica forman un grupo abeliano. El siguiente teorema nos dice además que los puntos K-racionales, con K un campo de números, forman un grupo abeliano finitamente generado.

Teorema 3.18 (Teorema de Mordell para curvas elípticas, [Mor22])**.** *Dada una curva elíptica E sobre un campo de números K, el grupo de puntos $E(K)$ es un grupo abeliano finitamente generado. En otras palabras,*

$$E(K) \cong \mathbb{Z}^r \times E(K)_{\text{tors}}.$$

A lo largo de esta sección daremos la idea de la prueba de este importante teorema. Vale la pena resaltar que hay una versión más general de este resultado para variedades abelianas de mayor dimensión. Este resultado será importante cuando hablemos de curvas de género ≥ 2.

Teorema 3.19 (Teorema de Mordell-Weil, [Wei29])**.** *Dada una variedad abeliana A sobre un campo de números K, el grupo de puntos $A(K)$ es un grupo abeliano finitamente generado. En otras palabras,*

$$A(K) \cong \mathbb{Z}^r \times A(K)_{\text{tors}}.$$

Siempre que tenemos un grupo abeliano finitamente generado Γ, tenemos que para todo entero positivo m, $\Gamma/m\Gamma$ es un grupo finito. Un paso importante para demostrar el Teorema de Mordell-Weil es probar $E(K)$ satisface esta condición.

Teorema 3.20 (Teorema débil de Mordell-Weil)**.** *Sea K un campo de números y E/K una curva elíptica y sea $m \geq 2$ un entero. Entonces $E(K)/mE(K)$ es un grupo finito.*

La demostración se basa en el método de descenso. El homomorfismo $[m]$ de multiplicación por m, permite asociar a cada clase de $E(K)/mE(K)$ ciertos datos aritméticos que pueden estudiarse mediante teoría de Galois. Estos datos forman un subconjunto del llamado grupo de Selmer. Utilizando propiedades fundamentales de los campos de números y el hecho de que el subgrupo de torsión $E[m]$ es finito, se demuestra que el grupo de Selmer es finito. Como $E(K)/mE(K)$ se inyecta en dicho grupo, se concluye que $E(K)/mE(K)$ también es finito. En la siguiente sección, hablaremos más profundamente del método de descenso.

En el resto de esta sección vamos a fijar una curva elíptica con forma de Weierstrass

$$E\colon y^2 = x^3 + Ax + B, \text{ con } A, B \in K. \tag{3.21}$$

Definición 3.22. Sea $t \in \mathbb{Q} \setminus \{0\}$, y escriba $t = p/q$ de forma minimal. La altura de t, denotada por $H(t)$, es definida por

$$H(t) = \max\{|p|, |q|\}.$$

Esta función se puede extender a cualquier campo de números K. Esto nos permite definir la siguiente función en los puntos K-racionales de una curva elíptica.

Definición 3.23. La altura logarítmica de $E(K)$ (con ecuación de Weierstrass como en (3.21)) es la función

$$h_x\colon E(K) \to \mathbb{R}, \qquad h_x(P) = \begin{cases} \log H(x(P)) & \text{si } P \neq O; \\ 0 & \text{si } P = O. \end{cases}$$

Proposición 3.24. *Sea E/K una curva elíptica como en (3.21), entonces la altura logarítmica de E satisface las siguientes propiedades.*

1. *Sea $P_0 \in E(K)$. Entonces existe una constante C_1 que depende de P_0, A y B y tal que*

$$h_x(P + P_0) \leq 2h_x(P) + C_1$$

   para todo $P \in E(K)$.

2. *Existe una constante C_2 que depende de A y B tal que*

$$h_x([2]P) \geq 4h_x(P) - C_2$$

   para todo $P \in E(K)$.

3. *Para cada constante C_3, el conjunto*

$$\{P \in E(K) \colon h_x(P) \leq C_3\}$$

   es finito.

Demostración. Para una prueba general de este resultado ver [Sil09, Capítulo VIII, §6] □

Demostración del Teorema 3.18. Por el Teorema 3.20, aplicado con $m = 2$, el cociente $E(K)/2E(K)$ es finito. Por tanto, existen puntos

$$Q_1, \ldots, Q_r \in E(K)$$

tales que todo punto $P \in E(K)$ puede escribirse en la forma

$$P = Q_i + [2]P'$$

para algún $i \in 1, \ldots, r$ y algún $P' \in E(K)$. Sea

$$C = \max_i h_x(Q_i).$$

Usando las propiedades de la altura, mostraremos que todo punto de $E(K)$ puede generarse a partir de una suma puntos en un conjunto finito. Por la Proposición 3.24(1), para cada representante Q_i existe una constante $C_{1,i}$ tal que

$$h_x(P' + Q_i) \leq 2h_x(P') + C_{1,i}.$$

Tomando el máximo de estas constantes, obtenemos una constante C_1 válida para todos los Q_i. Es decir, si $P = Q_i + 2P'$, tenemos que

$$h_x(P) = h_x([2]P' + Q_i) \leq 2h_x([2]P') + C_1.$$

Por otro lado, por la Proposición 3.24(2), existe una constante C_2 tal que:

$$h_x([2]P') \geq 4h_x(P') - C_2.$$

Equivalente tenemos que

$$h_x(P') \leq \frac{1}{4}h_x([2]P') + \frac{C_2}{4}.$$

La idea del descenso es que, al pasar de P a P', la altura disminuye esencialmente por un factor de 4. Más precisamente, combinando las estimaciones de altura se obtiene una constante C_4 tal que, siempre que $P = Q_i + 2P'$, se tiene

$$h_x(P') \leq \frac{1}{2}h_x(P) + C_4.$$

Elegimos ahora una constante M suficientemente grande, por ejemplo tal que $M \geq 2C_4$. Entonces, si $h_x(P) > M$, de la desigualdad anterior se sigue que

$$h_x(P') < h_x(P).$$

Por lo tanto, cualquier punto $P \in E(K)$ con altura mayor que M puede escribirse como

$$P = Q_i + 2P'$$

donde P' tiene altura estrictamente menor que la de P. Repitiendo este proceso, obtenemos una sucesión de puntos de alturas estrictamente decrecientes hasta llegar a un punto $R \in E(K)$ tal que $h_x(R) \leq M$. Por la Proposición 3.24(3), el conjunto

$$S = \{R \in E(K) : h_x(R) \leq M\}$$

es finito. Además, el conjunto de representantes $\{Q_1, \ldots, Q_r\}$ también es finito. Así, todo punto de $E(K)$ se obtiene a partir de los puntos de S y de los representantes $Q_1, \ldots, Q_r$ mediante sumas y duplicaciones. En consecuencia, $E(K)$ está generado por el conjunto finito

$$S \cup \{Q_1, \ldots, Q_r\}.$$

Por lo tanto, $E(K)$ es un grupo abeliano finitamente generado. □

3.4. Torsión de una curva elíptica

El teorema de Mordell nos dice que para conocer la estructura de $E(\mathbb{Q})$, es suficiente con conocer su rango y su torsión. El siguiente teorema, nos da una forma de conocer la torsión de $E(\mathbb{Q})$.

Teorema 3.25 (Nagell–Lutz)**.** *Sea E una curva elíptica dada por la ecuación*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

donde a, b, c son enteros. Sea D el discriminante de f, es decir, $-4a^3c+a^2b^2+18abc-4b^3-27c^2$. Entonces cada punto racional (x, y) de orden finito en E satisface las siguientes propiedades:

(1) Ambos x y y son enteros.

(2) La coordenada es y es 0 o un divisor de D Más aún, si $y \mid D$, entonces $y^2 \mid D$.

✎ **Ejercicio 3.26.** Considere la curva elíptica $E/\mathbb{Q}$ definida por la ecuación $y^2 = x^3+x^2-228x+1252$ Calcule los puntos de torsión de $E(\mathbb{Q})$ y demuestre que $E(\mathbb{Q})$ es un grupo infinito. *Sugerencia:* Muestre que $(-4, 46)$ es un punto racional de E.

3.5. Rango de una curva elíptica

Calcular el rango de una curva elíptica es un problema muy complejo. En la sección siguiente veremos un método para calcular cotas superiores para este número. Al ser un invariante tan complicado de calcular, hay conjeturas muy importantes en geometría aritmética. A continuación listamos algunas de las más importantes:

- **Conjetura de Birch y Swinnerton-Dyer (BSD).** Sea $E/\mathbb{Q}$ una curva elíptica y sea $L(E,s)$ su L-función. Entonces
$$\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s).$$
Es decir, el rango algebraico coincide con el orden de anulación de la L-función en $s=1$. Esta es considerada una de las conjeturas centrales de la teoría de curvas elípticas y uno de los siete Problemas del Milenio.

- **Conjetura del rango promedio** Más generalmente, al ordenar curvas elípticas por altura, se espera que el rango promedio sea $1/2$. Más aún, se espera que el $50\,\%$ de las curvas elípticas tienen rango 0, que $50\,\%$ tienen rango 1, por consiguiente, la proporción de curvas elípticas con rango ≥ 2 es 0. Los mejores resultados actuales muestran que el rango promedio es finito y acotado, pero el valor exacto sigue abierto.

- **Conjetura de uniformidad del rango.** Pregunta si existe una constante absoluta B tal que
$$\operatorname{rank} E(Q) \leq B$$
para toda curva elíptica sobre $\mathbb{Q}$. Actualmente no se sabe si los rangos están uniformemente acotados o si pueden crecer arbitrariamente.

Clase 4: El método de Chabauty para curvas

Esta clase esta basada en el artículo de McCallum y Poonen [MP12]. El objetivo es entender la idea del método de Chabauty para acotar el número de puntos racionales en curvas usando herramientas p-ádicas. El método de Chabauty solo aplica para curvas cuyo Jacobiano es de rango de Mordell-Weil menor que el género de la curva y por tanto primero debemos acotar dicho rango.

4.1. Cotas para el rango

Existen diferentes métodos para acotar el rango del jacobiano de una curva. Aquí nos enfocaremos en el caso de curvas de género 1, es decir, curvas elípticas. Para este caso, el método de 2-descenso proporciona una cota superior para el rango del grupo de Mordell-Weil.

4.1.1. El método de descenso y el grupo de Selmer

El objetivo del método de descenso es obtener una cota superior para r. La idea consiste en estudiar el cociente $E(\mathbb{Q})/2E(\mathbb{Q})$.

Por el Teorema 3.18 se obtiene

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong E(\mathbb{Q})[2] \oplus (\mathbb{Z}/2\mathbb{Z})^r.$$

Tomando la dimensión de estos $\mathbb{F}_2$ espacio vectoriales obtenemos:

$$r = \dim_{\mathbb{F}_2}(E(\mathbb{Q})/2E(\mathbb{Q})) - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2].$$

Si pudiéramos calcular $E(\mathbb{Q})/2E(\mathbb{Q})$, entonces podríamos determinar el rango. Sin embargo, este grupo suele ser difícil de describir directamente. Para superar esta dificultad se introducen los espacios homogéneos y el grupo de Selmer.

4.1.2. Espacios homogéneos

Un espacio homogéneo principal (o torsor) para E es una curva $C/\mathbb{Q}$ equipada con una acción de E tal que, sobre $\overline{\mathbb{Q}}$, la curva C es isomorfa a E. Geométricamente, un espacio homogéneo es una copia torcida de la curva elíptica. La diferencia fundamental es que C puede no tener puntos racionales. Si $C(\mathbb{Q}) \neq \varnothing$, entonces al escoger un punto racional $P \in C(\mathbb{Q})$ se obtiene un isomorfismo $C \simeq E$ definido sobre $\mathbb{Q}$. Por tanto, los espacios homogéneos miden la obstrucción a la existencia de puntos racionales. La teoría de Galois muestra que los espacios homogéneos asociados al 2-descenso están parametrizados por

$$H^1(\mathbb{Q}, E[2]).$$

Cada elemento de este grupo puede representarse mediante una curva auxiliar que localmente se parece a E.

4.1.3. El grupo de Selmer

No todos los elementos de $H^1(\mathbb{Q}, E[2])$ son relevantes para el estudio de $E(\mathbb{Q})$. Se consideran únicamente aquellos que poseen puntos en todas las completaciones de $\mathbb{Q}$. Esto conduce al grupo de Selmer:

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) = \left\{\xi \in H^1(\mathbb{Q}, E[2]) : \xi \text{ es localmente soluble en todo lugar}\right\}.$$

Equivalentemente, $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$ parametriza los espacios homogéneos de 2-descenso que tienen puntos sobre $\mathbb{Q}_p$ para todo primo p y sobre $\mathbb{R}$. Existe una sucesión exacta fundamental

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[2] \longrightarrow 0.$$

En particular,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathrm{Sel}^{(2)}(E/\mathbb{Q}).$$

Por tanto,

$$\dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E/\mathbb{Q}).$$

Combinando esta desigualdad con la descomposición anterior obtenemos

$$r \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2].$$

Esta es la cota superior para el rango que proporciona el 2-descenso.

4.1.4. Ejemplo: la curva $y^2 = x^3 - x$

Consideremos la curva elíptica

$$E: \quad y^2 = x^3 - x = x(x-1)(x+1).$$

Los puntos de orden 2 son $\{(0,0),(1,0),(-1,0)\}$ junto con el punto al infinito. Por tanto,

$$E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

es decir $\dim_{\mathbb{F}_2} E(\mathbb{Q})[2] = 2$. En el 2-descenso se asocia a un punto racional $P = (x, y)$ la información cuadrática contenida en las clases de $\{x, x-1, x+1\}$ en $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

La ecuación $y^2 = x(x-1)(x+1)$ impone relaciones entre estas clases. Posteriormente se estudia qué combinaciones satisfacen las condiciones de solubilidad local en todos los cuerpos $\mathbb{Q}_p$ y en $\mathbb{R}$. El resultado del cálculo es

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Por tanto, $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E/\mathbb{Q}) = 2$. Aplicando la desigualdad obtenida anteriormente,

$$0 \leq \operatorname{rank} E(\mathbb{Q}) \leq 2 - 2 = 0.$$

En consecuencia,

$$E(\mathbb{Q}) = \{O, (0,0), (1,0), (-1,0)\},$$

y todos los puntos racionales de E son de torsión. Este ejemplo ilustra la filosofía general del descenso: sustituir el difícil problema de estudiar $E(\mathbb{Q})$ por el problema más accesible de calcular un grupo de Selmer finito, cuya dimensión proporciona una cota superior para el rango de la curva elíptica.

✎ **Ejercicio 4.1.** Reinterpretar la curva en el Ejemplo 1.36 mediante el cambio de variables $x \to x - y$. Calcular el rango y los puntos de torsión y demostrar que las únicas soluciones son tales que $xyz = 0$.

✎ **Ejercicio 4.2.** Considere ahora la curva dada por $F_4\colon x^4 + y^4 = z^4$. Note que existe un automorfismo de la curva dado por $\iota\colon [x : y : z] \mapsto [x : y : -z]$. Considere F_4/ι, el cociente de F_4 por ι.

1. Determine cuales son las imágenes de puntos racionales de F_4 en el cociente $F_4/\iota =: C$.

2. Verifique que la deshomogenización del cociente F_4/ι con $x = 1$ tiene como ecuación $w^2 = y^4+1$. Esta es una una curva de género 1. Usando Magma, verifique que el rango del jacobiano de esta curva es 0.

3. Usando el cambio de variable

$$X = \frac{2(w+1)}{y^2}, \qquad Y = \frac{4(w+1)}{y^3},$$

pruebe que la curva elíptica $E\colon Y^2 = X^3 - 4X$ es isomorfa a C.

4. Usando el Teorema de Nagell–Lutz y el ítem anterior, encuentre todos los puntos racionales de E.

5. Concluya que los únicos puntos racionales de F_4 son triviales.

4.2. Conjetura de Mordell

Como vimos en §1.2.3, la Conjetura de Mordell establece que cualquier curva de género mayor a 1 definida sobre $\mathbb{Q}$ tiene finitos puntos racionales. Esta conjetura permaneció abierta por casi 60 años, hasta que Faltings la demostró en 1983.

4.2.1. Desarrollo histórico

A continuación, un poco de historia sobre la conjetura de Mordell.

- En 1922, L. Mordell conjeturó que:

  $$C(\mathbb{Q}) \text{ es finito para } g \geq 2.$$

  Esta conjetura fue establecida en el mismo artículo en el que se demuestra que los puntos racionales de curvas elípticas forman un grupo abeliano finitamente generado. Mordell desde ese entonces pensaba que $C \cap J_C(\mathbb{Q})$ era un conjunto finito (aquí J_C es el Jacobiano de C), sin embargo, no tenía herramientas suficientes para probarlo.

- En 1941, se dio el primer avance parcial de esta conjetura. Asumiendo que $\operatorname{rank}(J_C(\mathbb{Q})) < g$, C. Chabauty demostró que se cumple la conjetura de Mordell. Consideramos las siguientes inclusiones:

  $$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \subset J_C(\mathbb{Q}_p)$$

  Usando análisis p-ádico, se puede demostrar que la hipótesis de Chabauty implica que la clausura p-adica de $J(\mathbb{Q})$ es pequeña y por eso debe intersectar a $C(\mathbb{Q}_p)$, lo que implica que $C(\mathbb{Q}) = C(\mathbb{Q}_p) \cap J_C(\mathbb{Q})$ es finito.

- Finalmente, en 1983, se dio una prueba completa de esta conjetura por parte de G. Faltings. Faltings reduce el problema a estudiar puntos racionales en subvariedades de variedades abelianas y usa teoría de alturas para demostrar que estos puntos no pueden ser infinitos. En esencia, muestra que la estructura aritmética impone restricciones tan fuertes que solo pueden existir finitos puntos racionales.

Hay nuevas pruebas de la conjetura de Mordell con métodos más modernos. Por ejemplo, Vojta, usando aproximación diofantina, teoría de Nevanlinna, alturas, entre otras herramientas, reprobó el ahora teorema de Faltings [Voj91].

Siguiendo las ideas de Vojta, Faltings demostró la conjetura de Mordell-Lang:

Teorema 4.3 ([Fal91a]). *Sea A una variedad abeliana sobre un campo de números K y sea X una subvariedad geometricamente irreducible de A la cuál no es el trasladado de una subvariedad sobre $\bar{K}$. Entonces $X \cap A(K)$ no es Zariski denso en X.*

4.3. La idea de Chabauty

La idea principal de Chabauty es estudiar los puntos racionales de una curva no sobre los números reales, sino sobre los números p-ádicos. Sea X una curva de género $g \geq 2$ definida sobre $\mathbb{Q}$, y sea J su jacobiano. El objetivo es entender el conjunto de puntos racionales $X(\mathbb{Q})$ mediante la inclusión

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p).$$

Si consideramos $J(\mathbb{Q}) \subset J(\mathbb{R})$, tenemos que su clausura es un grupo abierto y cerrado por tanto la dimensión de la clausura de $J(\mathbb{Q})$ es $g = \dim(J(\mathbb{R}))$. A diferencia del caso real, la clausura de $J(\mathbb{Q})$ dentro de $J(\mathbb{Q}_p)$ puede tener dimensión menor.

Si denotamos por $r = \operatorname{rank} J(\mathbb{Q})$ y por $r_0 = \dim \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$, entonces se tiene $r_0 \leq r$, pues la función logaritmo $\log\colon A(J(\mathbb{Q}_p)) \to J(\mathbb{Q}_p)$ es un difeomorfismo local, donde $A(J(\mathbb{Q}_p))$ es el álgebra de Lie del grupo de Lie $J(\mathbb{Q}_p)$.

El punto clave es que, si $r_0 < g$, entonces la intersección

$$X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

es finita. En particular, esto implica que $X(\mathbb{Q})$ también es finito.

En §5.1, vamos a ver cómo Chabauty hizo esta idea explícita para que además de probar que la intersección es finita, la podamos calcular computacionalmente.

Clase 5: El método de Chabauty–Coleman

En esta sección, estudiaremos el método de Coleman para calcular puntos racionales en curvas en donde $r < g$. Primero definiremos el método y posteriormente estudiaremos un ejemplo detalladamente.

5.1. La idea de Coleman

En 1985, R. Coleman hizo efectiva la idea de Chabauty usando integración p-ádica. La idea es construir integrales de formas diferenciales que se anulan sobre los puntos racionales.

Primero, se considera una forma diferencial ω en la curva C. A partir de esta forma se define una función p-ádica

$$\eta(P) = \int_O^P \omega,$$

donde O es un punto base racional.

La forma ω se escoge de tal manera que

$$\eta(P) = 0$$

para todos los puntos racionales $P \in C(\mathbb{Q})$. Dicha forma existe debido a la condición de $r_0 < g$. Por lo tanto, los puntos racionales están contenidos en el conjunto de ceros de una función analítica p-ádica. Ahora usamos la reducción de la curva módulo p:

$$C(\mathbb{Q}_p) \to C(\mathbb{F}_p).$$

Las fibras de esta aplicación se llaman clases residuales. En cada clase residual se puede usar un parámetro local t, y la integral se escribe como una serie de potencias

$$I(t) \in \mathbb{Q}_p[[t]].$$

El problema de contar puntos racionales se reduce entonces a contar ceros de una serie de potencias p-ádica. Para ello usamos el siguiente lema:

Lema 5.1 ([MP12, Lemma 5.1.]). *Suponga que $f(t) \in \mathbb{Q}_p[\![t]\!]$ es una serie de potencias tal que $f'(t) \in \mathbb{Z}_p[\![t]\!]$. Sea $m = \mathrm{ord}_{t=0}(f'(t) \pmod p)$. Si $m < p-2$, entonces f tiene a lo más $m+1$ ceros en $p\mathbb{Z}_p$.*

Coleman demuestra el siguiente teorema:

Teorema 5.2 ([Col85]). *Sea C una curva de genero g y J su Jacobiano. Sea p un primo de buena reducción para C satisfaciendo $p > 2g$. Si $g > \mathrm{rank}(J(\mathbb{Q}))$, entonces*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

Idea de la prueba. Para cada punto $\widetilde{Q} \in C(\mathbb{F}_p)$, sea $\widetilde{m}_Q := \operatorname{ord}_{\widetilde{Q}}(\widetilde{\omega})$. Por el teorema de Riemann–Roch, el número total de ceros de $\widetilde{\omega}$ sobre $C(\mathbb{F}_p)$ es $2g-2$. Por tanto,

$$\sum_{\widetilde{Q} \in C(\mathbb{F}_p)} \widetilde{m}_Q \leq 2g-2.$$

En particular, $\widetilde{m}_Q \leq 2g-2 < p-2$ para todo $\widetilde{Q} \in C(\mathbb{F}_p)$, por lo que podemos aplicar el Lema 5.1. Sumando sobre todos los puntos de $C(\mathbb{F}_p)$ y aplicando el Lema 5.1, obtenemos

$$\#C(\mathbb{Q}) \leq \sum_{\widetilde{Q} \in C(\mathbb{F}_p)} (\widetilde{m}_Q + 1) = \#C(\mathbb{F}_p) + \sum_{\widetilde{Q} \in C(\mathbb{F}_p)} \widetilde{m}_Q.$$

Finalmente,

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + (2g-2),$$

lo que nos da el resultado deseado. □

5.2. Ejemplo computacional

Consideremos la curva hiperelíptica C de género 2 definida por la ecuación:

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

Usando una calculadora podemos encontrar algunos de los puntos racionales de esta curva

$$C(\mathbb{Q}) \supset \{(0,0),(1,0),(2,0),(5,0),(6,0),(3,6),(3,-6),(10,120),(10,-120),\infty\}. \tag{5.3}$$

Es muy difícil saber si estos son todos los puntos racionales. Sin embargo, resolver este problema en un campo finito es un problema muy sencillo. Por ejemplo, reduciendo módulo 7 podemos encontrar todos los $\mathbb{F}_7$-puntos racionales.

$$C(\mathbb{F}_7) = \{(0,0),(1,0),(2,0),(5,0),(6,0),(3,6),(3,1),\infty\}. \tag{5.4}$$

Aplicando el método del 2-descenso al Jacobiano de C, Gordon & Grant mostraron el siguiente teorema:

Teorema 5.5 ([GG93, Teorema 2])**.** *Sea C la curva*

$$y^2 = x(x-1)(x-2)(x-5)(x-6)$$

y J su Jacobiano. Entonces $J(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4$.

Idea de la prueba. Denotemos por J al Jacobiano de la curva C. Además, sus cinco puntos de Weierstrass afines son racionales:

$$(0,0), \quad (1,0), \quad (2,0), \quad (5,0), \quad (6,0).$$

Junto con el punto al infinito ∞, estos puntos determinan toda la torsión de orden 2 de J. En particular,

$$J[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

El objetivo es calcular el rango de $J(\mathbb{Q})$. Para ello se usa el 2-descenso. Recordemos que

$$J(\mathbb{Q})/2J(\mathbb{Q}) \cong J(\mathbb{Q})[2] \oplus (\mathbb{Z}/2\mathbb{Z})^r,$$

donde $r = \operatorname{rank} J(\mathbb{Q})$. Por tanto,

$$\dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) = 4 + r.$$

Así, una cota superior para $J(\mathbb{Q})/2J(\mathbb{Q})$ nos da una cota superior para el rango.

El 2-descenso no calcula directamente $J(\mathbb{Q})/2J(\mathbb{Q})$, sino que lo inyecta en el grupo de Selmer:

$$J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow \mathrm{Sel}^{(2)}(J/\mathbb{Q}).$$

Por consiguiente,

$$r \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(J/\mathbb{Q}) - 4.$$

En esta curva, los primos de mala reducción son $\{2, 3, 5\}$. Por tanto, en el descenso sólo aparecen clases cuadráticas no ramificadas fuera del conjunto

$$S = \{\infty, 2, 3, 5\}.$$

Esto quiere decir que sólo se deben considerar elementos de

$$D = \{d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : \mathrm{ord}_v(d) \equiv 0 \pmod 2 \text{ para todo } v \notin S\}.$$

En este caso, D está generado por las clases de $\{-1, 2, 3, 5\}$, por lo que $\#D = 16$. Como $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$, el cálculo del 2-Selmer se reduce a estudiar elementos de D^4. Por tanto, inicialmente hay $16^4 = 65536$ espacios homogéneos que deben ser examinados.

A cada elemento $d = (d_1, d_2, d_3, d_4) \in D^4$ se le asocia un espacio homogéneo $H(d)$ para el jacobiano J. La clase d pertenece al grupo de Selmer si y sólo si $H(d)$ tiene puntos localmente en todas partes, es decir, si

$$H(d)(\mathbb{R}) \neq \varnothing \qquad y \qquad H(d)(\mathbb{Q}_p) \neq \varnothing$$

para todo primo p. Por la construcción del descenso, basta verificar esta condición en los lugares de S, es decir, en

$$\mathbb{R}, \quad \mathbb{Q}_2, \quad \mathbb{Q}_3, \quad \mathbb{Q}_5.$$

Gordon y Grant realizan estas verificaciones locales de manera explícita. Primero, el test sobre $\mathbb{R}$ reduce los 65536 espacios homogéneos a 16384. Luego, los tests módulo 2 y módulo 4 reducen el número a 2048. Después, los tests módulo 9 dejan solamente 128 posibilidades. Finalmente, los tests módulo 25 eliminan todas salvo 32 clases.

Por tanto, el cálculo muestra que

$$\#\,\mathrm{Sel}^{(2)}(J/\mathbb{Q}) \leq 32.$$

Equivalentemente,

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(J/\mathbb{Q}) \leq 5.$$

Como $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 4$, obtenemos $r \leq 5 - 4 = 1$. Así, $\operatorname{rank} J(\mathbb{Q}) \leq 1$. Para probar que el rango es exactamente 1, basta exhibir un punto racional en $J(\mathbb{Q})$ que no sea de torsión. Gordon y Grant consideran el punto

$$P = (3, 6) - \infty \in J(\mathbb{Q}).$$

Bajo el mapa de descenso, este punto corresponde a la clase $(3, 2, 1, -2) \in D^4$. Esta clase no pertenece a la misma clase que los puntos de 2-torsión. Por tanto P no puede ser torsión de orden 2, y su imagen en $J(\mathbb{Q})/2J(\mathbb{Q})$ es no trivial fuera del subgrupo generado por $J[2]$. Combinando ambas desigualdades, $\operatorname{rank} J(\mathbb{Q}) = 1$.

Resta determinar la torsión de $J(\mathbb{Q})$. Para ello se usa reducción módulo primos de buena reducción. Si $p > 2$ es un primo de buena reducción, entonces la torsión racional se inyecta en $J(\mathbb{F}_p)$. En particular,

$$J(\mathbb{Q})_{\text{tors}} \hookrightarrow J(\mathbb{F}_p).$$

Gordon y Grant calculan $\#J(\mathbb{F}_7) = 48$ y $\#J(\mathbb{F}_{11}) = 176$. Por tanto, $\#J(\mathbb{Q})_{\text{tors}} \mid \gcd(48, 176) = 16$. Pero ya sabemos que $\#J[2](\mathbb{Q}) = 16$. Así, $J(\mathbb{Q})_{\text{tors}} = J[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$.

Como el rango es 1 y la torsión es exactamente $(\mathbb{Z}/2\mathbb{Z})^4$, obtenemos el resultado deseado. □

Para resumir, tenemos lo siguiente:

- El género $g(C)$ de la curva C es 2. En particular $2 = 2g(C) - 2$.
- $\#C(\mathbb{Q}) \geq 10$, pues encontramos 10 puntos racionales con una calculadora, ver (5.3).
- $\#C(\mathbb{F}_7) = 8$, ver (5.4).
- Por el Teorema 5.5 tenemos que $\operatorname{rank}(J(\mathbb{Q})) = 1$.

Por esta razón, dado que $g(C) = 2 > 1 = \operatorname{rank}(J(\mathbb{Q}))$ podemos aplicar el Teorema 5.2 para cualquier primo de buena reducción mayor a $2g(C) = 4$, en particular, para $p = 7$. Entonces tenemos que:

$$\begin{aligned} \#C(\mathbb{Q}) &\leq \#C(\mathbb{F}_7) + (2g(C) - 2) \\ &= 8 + 2 = 10. \end{aligned}$$

En conclusión, $\#C(\mathbb{Q}) = 10$, es decir, la lista (5.3) son los únicos puntos racionales de la curva C.

A continuación, vemos el la reducción de los puntos conocidos de la curva módulo 7.

$$C(\mathbb{Q}) \supset \{ (0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,-6), \infty, (10,-120), (10,120) \}$$

$$C(\mathbb{F}_7) = \{ (0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,1), \infty \}$$

Notamos que sobre cada uno de los puntos $(3,6), (3,1) \in C(\mathbb{F}_7)$ hay dos puntos racionales. Estos dos puntos (con las flechas rojas) son explicados por $2 = 2g(C) - 2$ como vimos en la prueba del Teorema 5.2. Este ejemplo es perfecto, pues sobre cada punto en $C(\mathbb{F}_7)$ hay al menos un punto racional, y el número de puntos "sobrantes" coincide con la cota del teorema.

Aquí tenemos un ejemplo de código en Magma que podemos usar para aplicar el método de Chabauty-Coleman.

```
// El metodo de Coleman
_<x> := PolynomialRing(Rationals());
C := HyperellipticCurve(x*(x-1)*(x-2)*(x-5)*(x-6));
Genus(C);
smallPoints := Points(C : Bound := 100);
#smallPoints;
smallPoints;
```

```
// Sobre campos finitos
BadPrimes(C);
// 7 Es un buen primo, por lo que podemos reducir modulo 7
CF7 := ChangeRing(C, GF(7));
#Points(CF7);
Points(CF7);

// Ahora acotamos el Rango del Jacobiano
J := Jacobian(C);
RankBound(J);

// Entonces tenemos r<g, por lo que podemos aplicar el metodo de Coleman.
SetVerbose("Chabauty", 3);
// Necesitamos un punto de orden infinito en el Jacobiano
G, m := MordellWeilGroupGenus2(J);
G;

P0 := m(G.5);
Order(P0);
Chabauty(P0,7);
// Esto nos dice que existe:
// a lo mas un par de puntos que se reducen (mod 7^4) al punto (10, 1) y
// a lo mas un par de puntos que se reducen (mod 7^4) al punto (3, 1).
// En total, tenemos 10 <= #C(Q) <= C(F_7)+2=10.
```

✎ **Ejercicio 5.6.** Recuerde que en Ejercicio 1.6 nos hicimos la pregunta: ¿Existen un triángulo rectángulo y uno isósceles ambos con lados racionales que tengan la misma área y mismo perímetro?

También demostramos en el mismo ejercicio que encontrar un par de triángulos es equivalente a encontrar $x \in \mathbb{Q} \cap (1,2)$ y $y \in \mathbb{Q}$ tales que

$$y^2 = (-3x^3 - 2x^2 + 6x - 4)^2 - 4(2x)x^5.$$

En este ejercicio, encontraremos todas las soluciones.

(a) Sea C la curva definida por la anterior ecuación. Calcule el género de C y rango del Jacobiano de C. Calcule el número de puntos módulo 5 y con ayuda de Magma busque en una caja suficientemente grande los puntos racionales de C hasta encontrar 10.

```
> R<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(x^6 + 12*x^5 - 32*x^4 + 52*x^2 - 48*x + 16);
> J := Jacobian(C);
> RankBounds(J);
> Points(C : Bound := 100);
```

(b) Utilice el Teorema 5.2 para encontrar todos los puntos racionales de C, y utilice esto para demostrar que los únicos pares de triángulos que responden a la preguntan inicial consiste de un triángulo rectángulo con lados $(377, 135, 352)$ y un triángulo isósceles con lados $(366, 366, 132)$.

✎ **Ejercicio 5.7.** El objetivo de este ejercicio es demostrar que las soluciones a $x^6 + y^6 = z^6$ satisfacen que $xyz = 0$.

1. Verifique que la curva de Fermat $F_6 \colon X^6 + Y^6 = Z^6$ admite un morfismo de grado 3 a la curva hiperelíptica definida por la ecuación

$$C \colon y^2 = x^6 + 1.$$

   En la carta $Y \neq 0$, el mapa racional está dado por

$$[X : Y : Z] \longmapsto \left(\frac{X}{Y}, \left(\frac{Z}{Y} \right)^3 \right).$$

   y se extiende a un morfismo entre los modelos suaves proyectivos.

2. Calcule computacionalmente el género de C y el rango de su jacobiano.

3. Usando Chabauty–Coleman, determine $C(\mathbb{Q})$ y deduzca que toda solución racional de la ecuación $x^6 + y^6 = z^6$ satisface $xyz = 0$.

Clase 6: Alturas

Las alturas en el espacio proyectivo constituyen una herramienta básica en geometría aritmética, ya que permiten medir la complejidad aritmética de los puntos racionales. Estas funciones también serán esenciales en el método de Chabauty cuadrático para calcular puntos racionales en curvas que estudiaremos en la Clase 7. Empezaremos estudiando ejemplos básicos de alturas y después nos concentraremos en las alturas p-ádicas, necesarias para ejecutar el método de Chabauty. Esta clase sigue de cerca [BM20].

6.1. Motivación

Recordemos que en la Clase 5, encontramos puntos racionales de coordenadas pequeñas en nuestra curva y después usamos el método de Chabauty–Coleman para demostrar que esos eran todos los puntos. Sin embargo, no es claro qué tan *grandes* son los puntos en una curva. Por ejemplo, la curva elíptica $y^2 + xy = x^3 - ax + b$, donde

$$\begin{aligned} a =& 270061832416309222184346521452974537847680546218363579547373 85 \\ b =& 552580585513423764757366995911181918215210670325350796083724047791494132777161 7 \\ & 3425636721497 \end{aligned}$$

tiene puntos racionales, pero el punto de coordenadas más *pequeñas* es

$$P = (28911954742285371894582555366 34, 11599307480961247064598359107273186795934252 83).$$

Remark 6.1. La curva anterior es un ejemplo encontrado por Elkies–Klagsbrun en 2024 de una curva elíptica de rango al menos 29. Se puede encontrar aquí.

La altura nos dará una noción de *complejidad* en las soluciones racionales.

De la misma forma, podemos pensar en un problema de aproximación de números reales. Por ejemplo, podemos aproximar el número $\sqrt{2} \approx 1.41421356237$ por números racionales:

$$\sqrt{2} \approx \frac{17}{12} = 1.41\bar{6} \qquad\qquad \sqrt{2} \approx \frac{109}{77} = 1.\overline{415584}.$$

Ambas aproximaciones son buenas, pero una es más complicada de escribir (como números racionales) que la otra. Para volver esta noción rigurosa, tenemos la siguiente definición.

Definición 6.2. La altura de un número racional a/b, escrito de forma minimal ($\gcd(|a|, |b|) = 1$), es

$$H(a/b) := \text{máx}(|a|, |b|).$$

La altura logarítmica de a/b es

$$h(a/b) := \log H(a/b).$$

Remark 6.3. Esta altura aparece naturalmente en el teorema de Thue–Siegel–Roth: controlar la altura del denominador permite cuantificar la calidad de aproximaciones racionales a números algebraicos.

Una propiedad fundamental de esta altura es la siguiente.

Lema 6.4 (Propiedad de Northcott)**.** *Existen finitos números racionales de altura acotada.*

Demostración. Si $H(a/b) \leq B$ para algún número real positivo B, entonces $|a|, |b| \leq B$ y $b \neq 0$. Hay solamente un número finito de pares enteros con estas propiedades. □

6.2. Ejemplo: Altura naive en $\mathbb{P}^n$

En la siguiente sección introducimos la definición de la altura en $\mathbb{P}^n$, su formulación global en campos de números y sus propiedades básicas. Estas nociones servirán como punto de partida para el estudio de alturas más refinadas en variedades algebraicas. Para concentrarnos en los ejemplos, obviaremos las pruebas en esta sección. Una buena referencia es [Ser97].

6.2.1. Altura de puntos racionales

Sea $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$. Podemos elegir coordenadas homogéneas $x_i \in \mathbb{Z}$ tales que $\gcd(x_0, x_1, \ldots, x_n) = 1$. La altura naive de P se define como

$$H(P) := \max\{|x_0|, |x_1|, \ldots, |x_n|\}.$$

Notamos que $H(P)$ está bien definida, es decir, no depende de la elección de coordenadas homogéneas primitivas.

Definición 6.5. La altura logarítmica de $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$ es

$$h(P) := \log H(P).$$

Esta última versión es más conveniente en aplicaciones analíticas y en estimaciones asintóticas.

✎ **Ejercicio 6.6** (Propiedades de $h(P)$)**.** Probar las siguientes propiedades elementales de la altura logarítmica en $\mathbb{P}^n$. Por simplicidad, puede asumir que $n = 2$.

1. Para todo $P \in \mathbb{P}^n(\mathbb{Q})$, se tiene que $h(P) \geq 0$.

2. Para cualquier número real $B \in \mathbb{R}_{\geq 0}$ existen finitos puntos $P \in \mathbb{P}^n(\mathbb{Q})$ con altura $h(P) \leq B$. Es decir, la altura $h(P)$ cumple la *Propiedad de Northcott*.

6.2.2. Generalización a campos de números

No solo podemos definir alturas para números racionales. En campos de números, también podemos usar la noción de valuación para definir una función de altura.

Definición 6.7. Sea K un campo de números y M_K el conjunto de sus lugares. Fijamos valores absolutos $|\cdot|_v$ normalizados de modo que satisfagan la fórmula del producto. Para $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$, definimos primero la altura relativa a K por

$$H_K(P) := \prod_{v \in M_K} \max(|x_0|_v, \ldots, |x_n|_v).$$

La altura absoluta y la altura logarítmica absoluta de P son, respectivamente,

$$H(P) := H_K(P)^{1/[K:\mathbb{Q}]}, \qquad h(P) := \log H(P).$$

Estas cantidades no dependen del campo de números K que contiene las coordenadas de P.

✎ **Ejercicio 6.8.** Pruebe que la definición anterior cuando $K = \mathbb{Q}$ coincide con la definición de altura para puntos en $\mathbb{P}^n(\mathbb{Q})$.

Ejemplo 6.9. Sea $K = \mathbb{Q}(\zeta_3)$, donde ζ_3 es una raíz del polinomio $x^2 + x + 1$. El anillo de enteros de K es $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$. Este campo tiene una pareja de inclusiones complejas $\sigma, \bar{\sigma} \colon \zeta_3 \mapsto -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. El primo 3 ramifica en K: $3\mathcal{O}_K = \mathfrak{P}_3^2$. Los primos $p \equiv 1 \pmod 3$ son split: $p\mathcal{O}_K = \mathfrak{P}_p\bar{\mathfrak{P}}_p$ y los primos $p \equiv 2 \pmod 3$ son inertes en $\mathcal{O}_K$. Para los primos de $\mathcal{O}_K$ tenemos que $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$. De esta forma tenemos, por ejemplo,

$$\begin{aligned} &|\zeta_3|_{\mathfrak{p}_3} = N(\mathfrak{p}_3)^{-2} = 1/9. \\ &|\zeta_3|_{\mathfrak{p}} = 1 \qquad\qquad \text{para todo } \mathfrak{p} \neq \mathfrak{p}_3 \end{aligned}$$

Igualmente $|\zeta_3|_\sigma = |\sigma(\zeta_3)| = 1$. En conclusión, $H([1 : \zeta_3]) = 1$ y $h([1 : \zeta_3]) = 0$.

Remark 6.10. Sea K un campo de número, para $\alpha \in K$, podemos definir $H(\alpha) := H([\alpha : 1])$.

✎ **Ejercicio 6.11.** Probar que para toda raíz n-ésima de la unidad ζ_n, tenemos que $h(\zeta_n) = 0$. Más aún, tenemos que para todo $\alpha \in \bar{\mathbb{Q}}$, $h(\alpha) = 0$ si y solo si α es una raíz de la unidad.

Proposición 6.12. *Las alturas $H(P)$ y $h(P)$ cumplen lo siguiente:*

(i) *$H(P)$ está bien definida: no depende de las coordenadas homogéneas ni del campo de números usado para calcularla;*

(ii) *$H(P) \geq 1$;*

(iii) *$h(P) \geq 0$;*

Demostración. Ver [Sil09, Proposition VIII.5.4]. □

Remark 6.13. Para toda curva C/K y una inmersión $C \hookrightarrow \mathbb{P}^n$ definida sobre K, la altura en $\mathbb{P}^n(K)$ nos permite definir una altura en puntos K-racionales de C. Más aún, por la propiedad de Northcott, si de alguna forma logramos acotar $h(P)$ para todo $P \in C(K)$, tendríamos un método para calcular todos los puntos $C(K)$. Esta es una idea fundamental del siguiente teorema.

Teorema 6.14 ([DGH21])**.** *Sea C una curva suave proyectiva y geométricamente irreducible de género $g \geq 2$ definida sobre un campo de números K de grado d sobre $\mathbb{Q}$. Sea r el rango de $J(K)$. Entonces existe una constante B, dependiendo únicamente de d y g tal que*

$$\#C(K) \leq B^{1+r}.$$

Volviendo a nuestra definición, tenemos que la propiedad de Northcott también se cumple para estas alturas.

Teorema 6.15 (Propiedad de Northcott)**.** *Sea K un campo de números. Entonces el conjunto de puntos*

$$\{P \in \mathbb{P}^n(K) \,:\, H(P) \leq B\}$$

es finito para todo $B > 0$.

Remark 6.16. La altura en $\mathbb{P}^n$ proporciona una medida global de la complejidad aritmética de los puntos racionales y constituye la base para el estudio de alturas más sofisticadas en variedades algebraicas, como las alturas de Néron–Tate y sus análogos p-ádicos.

Definición 6.17. Sea $E/\mathbb{Q}$ una curva elíptica. La altura logarítmica asociada a la coordenada x es la función

$$h_x \colon E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}, \qquad h_x(P) = \begin{cases} \log H(x(P)) & \text{si } P \neq O; \\ 0 & \text{si } P = O. \end{cases}$$

La misma fórmula, usando la altura absoluta de $[x(P) : 1]$, define una altura h_x en $E(K)$ para todo campo de números K; esta es la versión que se usará en el ejercicio siguiente.

✎ **Ejercicio 6.18.** Probar que h_x satisface la propiedad de Northcott.

✎ **Ejercicio 6.19.** En este ejercicio, usaremos la siguiente proposición:

Proposición 6.20 (Tate)**.** *Sea $E/\mathbb{Q}$ una curva elíptica y sea $P \in E(\mathbb{Q})$. Entonces el límite*

$$\hat{h}(P) \coloneqq \lim_{n\to\infty} \frac{h_x(2^n P)}{4^n}$$

existe.

Probar que si P es un punto de torsión de E, entonces $\hat{h}_x(P) = 0$.

✎ **Ejercicio 6.21.** El objetivo de este ejercicio es demostrar el teorema de Mordell-Weil asumiendo que para todo entero positivo m se tiene que $E(K)/mE(K)$ es finito y ciertas condiciones que satisface la altura logarítmica. A lo largo de este ejercicio asumiremos que la curva elíptica está definida por una ecuación de la forma:

$$E \colon y^2 = x^3 + Ax + B,$$

con $A, B \in K$.

Asuma sin demostrar que la altura logarítmica de E satisface las siguientes propiedades:

(i) Sea $P_0 \in E(K)$. Entonces existe una constante c_1 que depende de P_0, A y B y tal que

$$h_x(P + P_0) \leq 2h_x(P) + c_1$$

para todo $P \in E(K)$.

(ii) Existe una constante c_2 que depende de A y B tal que

$$h_x([2]P) \geq 4h_x(P) - c_2$$

para todo $P \in E(K)$.

(iii) Para cada constante c_3, el conjunto

$$\{P \in E(K) \colon h_x(P) \leq c_3\}$$

es finito.

1. Muestre que existen $Q_1, \ldots, Q_r \in E(K)$ tales que todo punto $P \in E(K)$ puede escribirse en la forma
$$P = Q_i + [2]P'$$
para algún $i \in \{1, \ldots, r\}$ y algún $P' \in E(K)$.

2. Muestre que existe una constante c_1 tal que para todo $P \in E(K)$
$$h_x([2]P') \leq 2h_x(P) + c_1,$$
para una descomposición $P = Q_i + [2]P'$ como en el inciso anterior.

3. Demuestre que existe una constante M suficientemente grande tal que si $h_x(P) > M$, entonces
$$h_x(P') < h_x(P).$$

4. Sea $S = \{R \in E(K) : h_x(R) \leq M\}$, demuestre que
$$S \cup \{Q_1, \ldots, Q_r\}$$
es un conjunto generador de $E(K)$, luego es finitamente generado.

6.3. Alturas p-ádicas en Jacobianos

Las alturas p-ádicas constituyen una herramienta fundamental en geometría aritmética. Mientras que la altura clásica toma valores reales y juega un papel central en el estudio de puntos racionales sobre variedades abelianas, las alturas p-ádicas permiten incorporar información local en el primo p, lo cual resulta especialmente útil en contextos donde intervienen métodos p-ádicos.

En esta sección introducimos la construcción de alturas p-ádicas en curvas elípticas y su generalización a jacobianos de curvas, siguiendo las ideas de Mazur–Stein–Tate y Coleman–Gross. En particular, veremos cómo estas alturas pueden describirse en términos de integrales de Coleman (ver §5.1) y cómo se descomponen en contribuciones locales. Estas ideas serán esenciales en aplicaciones posteriores, especialmente en el contexto del método de Chabauty cuadrático.

6.3.1. Alturas p-ádicas en curvas elípticas

Empezaremos por un ejemplo clásico: curvas elípticas. Sea $E/\mathbb{Q}$ una curva elíptica y sea p un primo de buena reducción ordinaria. La teoría de Mazur–Stein–Tate permite definir una altura p-ádica.

Teorema 6.22 (Mazur–Stein–Tate [MST06])**.** *Existe una altura p-ádica*

$$h : E(\mathbb{Q}) \longrightarrow \mathbb{Q}_p,$$

que es cuadrática, es decir, satisface que

$$\begin{array}{rccc} \langle \cdot, \cdot \rangle \colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \to & \mathbb{Q}_p \\ & \langle P, Q \rangle & \mapsto & h(P+Q) - h(P) - h(Q) \end{array}$$

es bilineal, y que admite una descomposición en contribuciones locales, donde el término en p puede describirse mediante funciones p-ádicas explícitas.

Remark 6.23. Esta función es análoga a la altura canónica de E o altura de Néron–Tate, que toma valores en $\mathbb{R}_{\geq 0}$ [Sil09, § VIII.9].

Tras fijar la rama usual de $\log_p$ y la normalización de la función sigma p-ádica, para puntos $P \in E(\mathbb{Q})$ en el grupo formal de un modelo de Weierstrass minimal se tiene una expresión explícita:

$$h(P) = \frac{2}{p} \log_p\left(\frac{\sigma_p(P)}{d(P)}\right),$$

donde, si $P = (a/d(P)^2, b/d(P)^3)$ está escrito en coordenadas minimales, $d(P)$ es su denominador y σ_p es la función sigma p-ádica. La fórmula depende de estas convenciones de normalización.

6.3.2. Alturas p-ádicas en jacobianos de curvas

Sea $C/\mathbb{Q}$ una curva suave, proyectiva y geométricamente conexa, y sea $J := \mathrm{Jac}(C)$ su jacobiano. La teoría de Coleman–Gross generaliza la construcción anterior a divisores de grado cero. Para fijar una altura global se debe elegir un carácter p-ádico global y, en el lugar p, un complemento de Hodge; para la altura ciclotómica hacemos las elecciones descritas a continuación.

Teorema 6.24 (Coleman–Gross)**.** *Fijemos el carácter ciclotómico y un complemento isotrópico W tal que*

$$\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) = \mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1) \oplus W.$$

Existe un emparejamiento de alturas p-ádicas

$$h : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p,$$

bilineal y simétrico. Para clases representadas por divisores $D_1, D_2 \in \mathrm{Div}^0(C)$ con soportes disjuntos, se descompone como suma de alturas locales

$$h([D_1], [D_2]) = h_p(D_1, D_2) + \sum_{\ell \neq p} h_\ell(D_1, D_2),$$

para todo par de representantes con soportes disjuntos. Con la elección del carácter ciclotómico, esta altura se llama la altura ciclotómica.

Para entender la altura ciclotómica debemos entender su descomposición en alturas locales. En ellas, existe una clara distinción entre la altura en el primo p y la altura en primos $\ell \neq p$.

Alturas para el primo p

El método para calcular explícitamente la altura ciclotómica en p para curvas hiperelípticas fue desarrollado por Balakrishnan y Besser en [BB12] y, incluyendo curvas con mala reducción, por Bianchi, Kaya y Müller en [BKM25]. Igualmente, Gajović y Müller [GM25] desarrollaron la teoría para curvas afines definidas sobre $\mathbb{Z}$. Finalmente, también es posible calcular estas alturas sobre campos de números [BBH+25].

Para la descripción mediante integrales de Coleman suponemos, por el momento, que p es impar y que C tiene buena reducción en p. Sea C una curva hiperelíptica definida por $y^2 = f(x)$. Tomamos una base $\{\omega_0, \dots, \omega_{2g-1}\}$ de $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ en la que $\{\omega_0, \dots, \omega_{g-1}\}$ es una base de $\mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1)$. También fijamos un lift de Frobenius ϕ.

Sea $T(\mathbb{Q}_p)$ el grupo de diferenciales del tercer tipo con residuos enteros. Consideraremos el subgrupo de diferenciales logarítmicos

$$T_{\log}(\mathbb{Q}_p) := \left\{ \frac{\mathrm{d}f}{f} \,:\, f \in \mathbb{Q}_p(C)^\times \right\}.$$

✎ **Ejercicio 6.25.** Pruebe que $T(\mathbb{Q}_p)$ y $T_{\log}(\mathbb{Q}_p)$ tienen las siguientes propiedades.

1. Existe una secuencia exacta corta
$$0 \to \mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1) \to T(\mathbb{Q}_p) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(C_{\mathbb{Q}_p}) \to 0$$
2. $T_{\log}(\mathbb{Q}_p) \cap \mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1) = 0$.
3. $\mathrm{Res}\, \frac{\mathrm{d}f}{f} = \mathrm{div}\, f$.
4. Existe una secuencia corta
$$0 \to \mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1) \to T(\mathbb{Q}_p)/T_{\log}(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \to 0. \tag{6.26}$$

Aquí, haremos uso del homomorfismo canónico

$$\Psi \colon T(\mathbb{Q}_p)/T_{\log}(\mathbb{Q}_p) \to \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$$

tal que Ψ es la identidad en diferenciales del primer tipo y envía diferenciales del tercer tipo a diferenciales del segundo tipo módulo diferenciales exactos [CG89]. Fijamos un complemento isotrópico W tal que

$$\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) = \mathrm{H}^0(C_{\mathbb{Q}_p}, \Omega^1) \oplus W.$$

Definición 6.27. Sean D_1 y D_2 dos divisores de $C_{\mathbb{Q}_p}$ de grado 0 y con soportes disjuntos. La altura p-ádica local es

$$h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}, \tag{6.28}$$

donde $\int_{D_2}$ denota la extensión lineal de la integral de Coleman a divisores y ω_{D_1} es la única diferencial que cumple:

- es una diferencial del tercer tipo con residuos enteros;
- $\mathrm{Res}(\omega_{D_1}) = D_1$;
- $\Psi([\omega_{D_1}]) \in W$.

Para la aplicación en el método de Chabauty, estaremos interesados en calcular la altura p-ádica local explícitamente. Para esto, es necesaria la siguiente información.

1. **El complemento W.** En la práctica, se fija un complemento isotrópico elegido.
2. **La aplicación Ψ.** Para determinar la componente de una diferencial en el complemento W es necesario calcular la imagen de una diferencial del tercer tipo en $H^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ mediante el homomorfismo canónico
$$\Psi : T(\mathbb{Q}_p)/T_{\log}(\mathbb{Q}_p) \longrightarrow H^1_{\mathrm{dR}}(C/\mathbb{Q}_p).$$
3. **La forma diferencial ω_{D_1}.** En general, se empieza construyendo una forma diferencial con los residuos prescritos. Posteriormente, usando 2, podemos modificar esta diferencial para asegurarnos de que satisfaga
$$\Psi([\omega_{D_1}]) \in W.$$
4. **Las integrales de Coleman.** Una vez obtenida ω_{D_1}, la altura local se calcula mediante la integral en (6.28). Por tanto, es necesario disponer de algoritmos efectivos para calcular integrales de Coleman entre puntos de la curva.

Alturas para primos $\ell \neq p$

Las contribuciones de alturas locales para primos $\ell \neq p$ se calculan de una forma completamente distinta a las alturas para el primo p. Nuestra estrategia en este caso será usar un modelo regular de la curva, combinado con números de intersecciones.

Definición 6.29. Sea R un anillo de valoración discreta con campo de fracciones K. Sea C una curva proyectiva definida sobre K. Un modelo regular propio de C es un R-esquema regular, propio y plano de dimensión relativa 1, cuya fibra genérica es isomorfa a C.

Sea $\mathcal{C}$ un modelo regular propio de $C_{\mathbb{Q}_\ell}$ sobre $\mathbb{Z}_\ell$. Dado un divisor D sobre $C_{\mathbb{Q}_\ell}$, denotaremos por $\mathcal{D}$ su clausura de Zariski en $\mathcal{C}$. La idea fundamental consiste en expresar la altura local en términos de números de intersección sobre $\mathcal{C}$. Sin embargo, las clausuras de dos divisores horizontales no suelen tener intersección nula con las componentes de la fibra especial. Por ello, es necesario corregirlas mediante divisores verticales adecuados. Más precisamente, para cada divisor D de grado 0 existe un divisor vertical $\Phi(D)$, único módulo múltiplos de la fibra especial, tal que
$$(\mathcal{D} + \Phi(D)) \cdot \Gamma = 0$$
para toda componente irreducible Γ de la fibra especial de $\mathcal{C}$.

Definición 6.30. Sean D_1 y D_2 dos divisores de $C_{\mathbb{Q}_\ell}$ de grado 0 y con soportes disjuntos. Sea $\mathcal{C}$ un modelo regular propio de $C_{\mathbb{Q}_\ell}$. Con la normalización ciclotómica y la convención de signo adoptada aquí, la altura local en ℓ está dada por
$$h_\ell(D_1, D_2) = \log_p(\ell)\,(\mathcal{D}_1 + \Phi(D_1)) \cdot \mathcal{D}_2, \tag{6.31}$$
donde $\cdot$ denota el emparejamiento de intersección sobre el modelo regular.

Por tanto, el cálculo efectivo de $h_\ell(D_1, D_2)$ se reduce a los siguientes pasos:

1. Construir un modelo regular propio $\mathcal{C}$ de la curva sobre $\mathbb{Z}_\ell$.

2. Determinar las componentes irreducibles de la fibra especial y la matriz de intersección asociada.

3. Calcular el divisor vertical $\Phi(D_1)$.

4. Calcular los números de intersección

$$\mathcal{D}_1 \cdot \mathcal{D}_2 \qquad \text{y} \qquad \Phi(D_1) \cdot \mathcal{D}_2.$$

5. Combinar estos datos mediante la fórmula anterior para obtener la contribución local en ℓ.

Remark 6.32. Si C tiene buena reducción en ℓ y las reducciones de los soportes de D_1 y D_2 son disjuntas, entonces la contribución local es nula. Por ello, para dos divisores globales fijos únicamente un número finito de primos contribuye a la altura global.

Remark 6.33. Para la aplicación de Chabauty cuadrático, aunque existen algoritmos para calcular las alturas locales dado un modelo regular de C sobre $\mathbb{Z}_\ell$, calcular la función de altura h_ℓ de esta manera parece ser poco práctico, dado que las ecuaciones que definen los divisores suelen tener un grado muy elevado. Existen formas alternativas para calcular estas alturas, que no necesitan un modelo regular (ver por ejemplo [BD20] y [BDHS25]).

6.4. El método de Chabauty no abeliano

El método de Chabauty–Coleman que discutimos en la Clase 5 constituye una de las herramientas más eficaces para determinar los puntos racionales de una curva cuando el rango de Mordell–Weil de su Jacobiano es estrictamente menor que el género. Sin embargo, esta hipótesis resulta muy restrictiva y falla en numerosas aplicaciones aritméticas. Con el objetivo de superar esta limitación, Kim introdujo una teoría no abeliana de Chabauty basada en grupos fundamentales unipotentes y teoría de Hodge p-ádica, conocida actualmente como el *programa de Kim* [Kim05, Kim09].

Para una curva hiperbólica $C/\mathbb{Q}$, un primo p de buena reducción y tras fijar un punto base racional (o tangencial), el punto de partida es la observación de que el método clásico de Chabauty puede interpretarse en términos del grupo fundamental étale abelianizado. Kim reemplaza esta información abeliana por aproximaciones sucesivamente más refinadas del grupo fundamental no abeliano. Siguiendo este proceso, se obtiene una sucesión decreciente de loci de Selmer

$$C(\mathbb{Q}) \subset \cdots \subset C(\mathbb{Q}_p)_2 \subset C(\mathbb{Q}_p)_1 \subset C(\mathbb{Q}_p), \tag{6.34}$$

en donde cada $C(\mathbb{Q}_p)_n$ viene de cocientes maximales n-unipotentes del grupo fundamental de la curva.

El conjunto $C(\mathbb{Q}_p)_1$ es el locus de Chabauty–Kim de profundidad 1, estrechamente relacionado con el locus de Chabauty lineal. En la Clase 7 estudiaremos $C(\mathbb{Q}_p)_2$. Por ahora, terminamos con la conjetura de Kim sobre el comportamiento de estos conjuntos.

Conjetura 6.35 (Conjetura de Kim)**.** *Sean $C(\mathbb{Q}_p)_n$, $n \geq 1$, los conjuntos descritos anteriormente. Entonces*

1. *Para $n \gg 0$, se tiene que $C(\mathbb{Q}) = C(\mathbb{Q}_p)_n$. En particular, $C(\mathbb{Q}_p)_n$ es finito.*

La conexión con Chabauty cuadrático es la siguiente. Fijado un punto base $b \in C(\mathbb{Q})$, la altura global evaluada en la imagen de $P \mapsto [P - b]$ en el jacobiano se expresa, sobre la clausura p-ádica

de $J(\mathbb{Q})$, como una función cuadrática de las integrales abelianas. Por la descomposición local de la altura, para $P \in C(\mathbb{Q})$ esta expresión se relaciona con la altura local en p y con las contribuciones en los primos $\ell \neq p$. Estas últimas toman solamente un número finito de valores en los puntos racionales. Cada valor posible produce una ecuación analítica p-ádica en $C(\mathbb{Q}_p)$; Chabauty cuadrático busca los ceros de la unión finita de estas ecuaciones.

Clase 7: Chabauty cuadrático

El método de Chabauty–Coleman permite demostrar la finitud de $C(\mathbb{Q})$ cuando $\operatorname{rank} J(\mathbb{Q}) < g$, donde $C/\mathbb{Q}$ es una curva suave proyectiva de género g y J es su jacobiano. Sin embargo, esta hipótesis falla en numerosos ejemplos de interés aritmético. El método de Chabauty cuadrático, introducido por Balakrishnan y Dogra [BD18, BD21], extiende el alcance del método clásico utilizando alturas p-ádicas e integrales iteradas de Coleman.

La idea fundamental consiste en sustituir las funciones lineales obtenidas mediante integración de formas diferenciales por funciones cuadráticas relacionadas con la altura p-ádica de Coleman–Gross. Estas funciones permiten obtener nuevas ecuaciones que satisfacen los puntos racionales y que, bajo hipótesis apropiadas, vuelven a definir un conjunto finito. En esta clase, seguiremos [BM20].

7.1. Introducción a Chabauty cuadrático

Como vimos en la clase anterior, el método clásico de Chabauty–Coleman proporciona una herramienta muy poderosa para abordar este problema cuando el rango del jacobiano es estrictamente menor que el género de la curva. Sin embargo, esta condición deja fuera una gran cantidad de casos de interés, particularmente aquellos en los que el rango coincide con el género.

Con el propósito de superar esta limitación, Minhyong Kim propuso un programa basado en grupos fundamentales unipotentes y teoría de Hodge p-ádica, el cual puede verse como una generalización del método de Chabauty–Coleman. Este programa produce una sucesión decreciente de subconjuntos

$$C(\mathbb{Q}_p) \supseteq C(\mathbb{Q}_p)_1 \supseteq C(\mathbb{Q}_p)_U \supseteq C(\mathbb{Q}_p)_2 \supseteq \cdots \supseteq C(\mathbb{Q}),$$

cuyos términos se espera aproximen cada vez mejor el conjunto de puntos racionales. El primer nivel coincide precisamente con el conjunto considerado por Chabauty–Coleman, mientras que el segundo nivel da origen al método conocido como *Quadratic Chabauty*.

En la práctica, una versión especialmente efectiva es *Skimmed Quadratic Chabauty*, introducida por Balakrishnan y Dogra. En lugar de trabajar con todo el segundo cociente del grupo fundamental unipotente, este método considera un cociente máximo sobre el cual el conmutador es isomorfo a una suma directa de copias de $\mathbb{Q}_p(1)$. Esta simplificación conserva suficiente información aritmética para obtener algoritmos computacionalmente viables, al tiempo que evita parte de la complejidad inherente al programa completo de Kim.

Un resultado importante es el siguiente lema. Aquí $\rho(J)$ denota el rango del grupo de Néron–Severi del jacobiano.

Teorema 7.1. *[BD18, Lemma 3.2] Suponga que* $\operatorname{rank} J(\mathbb{Q}) < g + \rho(J) - 1$. *Entonces* $C(\mathbb{Q}_p)_2$ *es finito.*

En estas notas nos concentraremos en la situación en la que se satisfacen las siguientes hipótesis:

1. El rango del jacobiano satisface $\operatorname{rk}(J(\mathbb{Q})) = g$, donde g es el género de la curva.
2. El grupo de Néron–Severi del jacobiano verifica $\operatorname{rk} \mathrm{NS}(J) > 1$.

3. La función logaritmo, restringida a $J(\mathbb{Q}) \otimes \mathbb{Q}_p$,

$$\log : J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee$$

es un isomorfismo.

Mientras que el método de Chabauty–Coleman explota relaciones lineales satisfechas por la imagen del logaritmo p-ádico, Quadratic Chabauty reemplaza estas relaciones por relaciones cuadráticas obtenidas a partir del emparejamiento de alturas p-ádicas que dependen de una correspondencia.

7.1.1. Correspondencias

En esta sección, seguimos [Smi23]. La idea de la teoría de correspondencias entre dos curvas es relacionar divisores del producto de las curvas con homomorfismos entre los Jacobianos de las curvas.

Definición 7.2. Sean C_1 y C_2 dos curvas proyectivas no singulares irreducibles. Una correspondencia en $C_1 \times C_2$ es un divisor en $C_1 \times C_2$.

Remark 7.3. Como C_1 y C_2 son curvas, obtenemos que $C_1 \times C_2$ es una superficie. La teoría de divisores en superficies se asemeja a la de curvas, pero no consiste en tomar sumas formales de puntos. De hecho, un divisor en $C_1 \times C_2$ es una suma formal (finita) de curvas irreducibles en $C_1 \times C_2$.

Ejemplo 7.4. Consideremos el producto $C_1 \times C_2$ con proyecciones π_1 y π_2 en cada componente. Entonces $\pi_1^{-1}(C_1)$ y $\pi_2^{-1}(C_2)$ son correspondencias.

Decimos que una correspondencia es prima si es un divisor primo: una curva reducida irreducible en el producto. Dada una correspondencia prima Z, definimos $d_1(Z) := \deg(\pi_1 Z)$ y $d_2(Z) := \deg(\pi_2 Z)$ como los grados de Z. Aquí notemos que $\pi_i Z$ es un divisor de C_i, entonces podemos tomar su grado.

✎ **Ejercicio 7.5.** Sea $f\colon C_1 \to C_2$ un morfismo de curvas. Pruebe que si grafo

$$\Gamma_f := (\mathrm{Id}_{C_1} \times f)(C_1) \subseteq C_1 \times C_2,$$

es una correspondencia. Mas aún, calcule su grado.

Ahora estamos listos para relacionar las correspondencias con morfismos entre Jacobianos. Sea Z una correspondencia prima en $C_1 \times C_2$. Notemos que las proyecciones $\pi_i\colon Z \to C_i$ pueden ser vistas como cubrimientos de curvas. Entonces obtenemos las funciones

$$\begin{array}{rccc} {\pi_1}^{*Z}\colon & \mathrm{Div}(C_1) & \to & \mathrm{Div}(Z) \\ & \sum n_P P & \mapsto & \sum n_P \sum_{Q \in \pi_1^{-1}(P)} \mathrm{ord}_Q(t_P) Q \end{array} \qquad \begin{array}{rccc} {\pi_2}_*^{Z}\colon & \mathrm{Div}(Z) & \to & \mathrm{Div}(C_2) \\ & \sum n_P P & \mapsto & \sum n_P \pi_2(P), \end{array}$$

donde t_P es un parámetro local.

Lo anterior nos da un homomorfismo $\mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$, dado por la composición ${\pi_2}_*^{Z} \circ {\pi_1}^{*Z}$, que se extiende a un morfismo de jacobianos $J_1 \to J_2$. Podemos extender esta construcción de forma $\mathbb{Z}$-lineal para obtener homomorfismos inducidos para cualquier correspondencia.

Definición 7.6. Si $Z = \sum_i n_i Z_i$ es una correspondencia en $C_1 \times C_2$ con cada Z_i prima, entonces el homomorfismo inducido por Z entre J_1 y J_2 es

$$\phi_Z := \sum n_i ({\pi_2}_*^{Z_i}) \circ ({\pi_1}^{*Z_i}).$$

✎ **Ejercicio 7.7.** Con la notación del Ejercicio 7.5, encuentre ϕ_{Γ_f} en términos de f.

Definición 7.8. Sea C una curva hiperelíptica buena. Una correspondencia no-trivial $Z \subseteq C \times C$ es buena si

1. existen $c_1, c_2 \in \mathrm{Pic}(C)$ tales que el pushforward de $[Z] \in \mathrm{Pic}(C \times C)$ bajo $(x, y) \to (y, x)$ es $[Z] + \pi_1^* 1 c_1 + \pi_2^* c_2$; y
2. La clase ξ_Z, vista como un endomorfismo de $\mathrm{H}^1(C, \mathbb{Q}_p)$ tiene traza cero.

7.1.2. Alturas p-ádicas

El ingrediente fundamental del método es el emparejamiento de alturas

$$h : J(\mathbb{Q}) \times J(\mathbb{Q}) \longrightarrow \mathbb{Q}_p,$$

el cual constituye un análogo p-ádico de la altura de Néron–Tate. Gracias a la hipótesis sobre el logaritmo p-ádico, este emparejamiento puede describirse mediante formas bilineales sobre el espacio de diferenciales holomorfas y extenderse de manera localmente analítica a puntos p-ádicos del jacobiano.

Para relacionar estas alturas con la curva, se fija un punto base $b \in X(\mathbb{Q})$ y una clase no trivial

$$Z \in \ker(\mathrm{NS}(J) \to \mathrm{NS}(C)) .$$

A partir de estos datos se construye una función $h_Z : C(\mathbb{Q}) \longrightarrow \mathbb{Q}_p$, definida por

$$h_Z(P) := h([P - b], E_Z([P - b]) + c_Z),$$

la cual admite una extensión localmente analítica $h_Z : C(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$.

Esta función constituye el objeto central del método.

7.1.3. Descomposición local

Una propiedad fundamental de las alturas p-ádicas es que admiten una descomposición en contribuciones locales

$$h_Z(P) = \sum_q h_{Z,q}(P),$$

donde la suma recorre todos los primos racionales y tenemos que $h_{Z,q}(P) \colon C(\mathbb{Q}_q) \to \mathbb{Q}_p$. Cada término depende únicamente de la geometría local de la curva en el primo correspondiente. En particular,

1. $h_{Z,p} \colon C(\mathbb{Q}_p) \to \mathbb{Q}_p$ es una función localmente analítica;
2. si C tiene potencialmente buena reducción en $\ell \neq p$, entonces $h_{Z,\ell} \equiv 0$.
3. para todo primo $q \neq p$, el conjunto $h_{Z,q}(C(\mathbb{Q}))$ es finito;

Estas propiedades permiten definir la función $F = h_Z - h_{Z,p}$, la cual desempeña un papel análogo al de la integral de Coleman en el método clásico. En efecto, si todas las contribuciones locales fuera de p son nulas, entonces para todo punto racional $P \in C(\mathbb{Q})$ se tiene $F(P) = 0$.

En consecuencia, el problema de determinar los puntos racionales de la curva se reduce a encontrar los ceros de una función localmente analítica definida sobre $C(\mathbb{Q}_p)$.

7.1.4. Aspectos computacionales

Desde un punto de vista algorítmico, la implementación de *Skimmed Quadratic Chabauty* requiere cuatro ingredientes fundamentales:

1. encontrar una clase Z tal que las contribuciones locales fuera de p sean nulas o, al menos, explícitamente computables;
2. calcular el desarrollo local de la función $h_{Z,p}$ sobre $C(\mathbb{Q}_p)$;
3. extender computacionalmente la función global h_Z a puntos p-ádicos;
4. determinar con precisión certificada los ceros de la función

$$F = h_Z - h_{Z,p}.$$

Estos pasos constituyen el núcleo de las implementaciones actuales del método.

Con un ejemplo describiremos el terminos generales las herramientas que se usan para encontrar una aproximación de la función F.

7.2. Una fuente de ejemplos: curvas modulares

El método de *skimmed quadratic Chabauty* ha sido usado para encontrar los puntos racionales de varias curvas interesantes, casi todas curvas modulares. En esta sección presentaremos nuestra motivación para estudiar puntos racionales en formas modulares.

Mazur's Program B ([Maz77]). Dado un campo de números K y un subgrupo H del grupo $\mathrm{GL}_2\,\hat{\mathbb{Z}} = \prod_p \mathrm{GL}_2\,\mathbb{Z}_p$, clasificar todas las curvas elípticas E/K cuya representación de Galois en puntos de torsión transforma $\mathrm{Gal}(\bar{K}/K)$ en $H \subseteq \mathrm{GL}_2\,\hat{\mathbb{Z}}$.

En vez de estudiar la imagen de representaciones de Galois en todo $\mathrm{GL}_2(\hat{\mathbb{Z}})$, podemos hacerlo paso a paso para cada conjunto de torsión $E[N]$:

$$\rho_{E,N}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

para todo $N \geq 1$.

Ejemplo 7.9. Supongamos que E es una curva elíptica con una base $\{P, Q\}$ de puntos en $E(K)[N]$ para la N-torsión de E. Entonces, para todo $\sigma \in \mathrm{Gal}(\bar{K}/K)$ tenemos que $\sigma(P) = P$ y $\sigma(Q) = Q$. Entonces la imagen de la representación de Galois, módulo N es la matriz

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

De esta forma, definimos $\Gamma(N)$ como el subgrupo de $\mathrm{GL}_2\,\hat{\mathbb{Z}}$, con matrices que módulo N son la identidad.

Ejemplo 7.10. Ahora suponemos que existe un punto de torsión $P \in E(K)[N]$ para algún entero positivo N. Por el mismo argumento del Ejemplo 7.9, tenemos que $\sigma P = P$. Podemos extender $\{P\}$ a una base $\{P, Q\}$ para $E[N]$. Por consiguiente, la representación de Galois módulo N tiene imagen en el subgrupo dado por matrices de la forma

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

Ejemplo 7.11. Si en cambio la curva elíptica E tiene una isogenia cíclica de orden N definida sobre K, tenemos que $\langle P\rangle$ está estabilizado por elementos del grupo de Galois para algún $P \in E[N]$. Por ello tenemos que $\sigma P = a_\sigma P$ para todo $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Extendiendo $\{P\}$, a una $\bar{K}$-base de $E[N]$, tenemos que la imagen de la representación de Galois módulo N está contenida en el subgrupo de matrices de la forma

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Definición 7.12. Sea $N \geq 1$. La curva modular $X(N)$ es la curva definida sobre $\mathbb{Q}$ tal que para todo campo de números K

$$X(N)(K) = \{(E/K, P, Q) \,:\, E[N] = E(K)[N] = \langle P, Q\rangle\} \cup \{\text{cúspides}\}.$$

Es decir, $(E/K, P, Q) \in X(N)(K)$ si y solo si $\rho_{E,N}(\mathrm{Gal}\,\bar{K}/K) = \{I\}$.
Sea $\Gamma(N) \subseteq H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. El N minimal se denomina el nivel de H.
Para $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, tenemos que

$$X_H := X(N)/H(N),$$

donde $H(N)$ es la imagen de H en $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Es decir, $(E/K, \iota) \in X_H(K)$ si y solo si $\rho_{E,N}(\mathrm{Gal}\,\bar{K}/K) \subseteq H(N)$.
La curva correspondiente al grupo maximal en Ejemplo 7.10 se denota como $X_1(N)$ y la curva correspondiente al Ejemplo 7.11 es $X_0(N)$.

De esta forma, el programa B de Mazur nos pide determinar $X_{H(N)}(K)$ para todo $H(N)$.
La idea ahora es estudiar las representaciones $X_{H(\ell^s)}$ para todos los primos ℓ y potencias s.

Conjetura 7.13 (Conjetura de uniformidad de Serre)**.** *Sea $E/\mathbb{Q}$ una curva elíptica sin multiplicación compleja. Entonces, para todo primo $\ell > 37$, la representación residual*

$$\rho_{E,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

es sobreyectiva.

El teorema de imagen abierta de Serre establece que, para cada curva elíptica $E/\mathbb{Q}$ sin multiplicación compleja, $\rho_{E,\ell}$ es sobreyectiva para todo ℓ suficientemente grande; la cota a priori depende de E [Ser72]. La conjetura afirma que se puede tomar uniformemente la cota 37.

El problema se traduce en la determinación de puntos racionales sobre curvas modulares asociadas a posibles imágenes excepcionales. El marco sistemático para la clasificación de imágenes ℓ-ádicas y de las curvas X_H correspondientes fue desarrollado por Rouse–Sutherland–Zureick-Brown [RSZB22]; para las imágenes residuales, véase también [Zyw15]. En el caso en que la imagen esté contenida en el normalizador de un Cartan split, los resultados de Bilu–Parent y Bilu–Parent–Rebolledo reducen la clasificación al nivel 13 [BP11, BPR13]. Balakrishnan–Dogra–Müller–Tuitman–Vonk determinaron $X_{\mathrm{s}}(13)(\mathbb{Q})$ mediante skimmed Chabauty cuadrático, y con ello completaron este caso [BDM+19]. Por otra parte, Lemos probó la conjetura para la familia de curvas elípticas sin CM sobre $\mathbb{Q}$ que admiten una isogenia cíclica racional no trivial [Lem19].

Entre los avances recientes, Balakrishnan–Betts–Hast–Jha–Müller determinaron $X^+_{\mathrm{ns}}(27)(\mathbb{Q})$ y completaron la clasificación de las imágenes 3-ádicas [BBH+25]. Furio y Lombardo demostraron

que $X_{\text{ns}}^+(49)$ no tiene puntos racionales no-CM [FL26]. Este último resultado es un paso importante hacia la clasificación de las imágenes 7-ádicas, pero no la completa: aún es necesario encontrar puntos racionales en dos curvas de nivel 49. Trabajo anunciado de Zureick-Brown–Arango-Piñeros termina esta clasificación.

✎ **Ejercicio 7.14.** Consideremos la curva $X_1(11)$, que tiene un modelo dado por

$$C\colon y^2 = x^3 - 432x + 8208.$$

Las cúspides en este modelo resultan ser

$$[-12 : 108 : 1], [24 : 108 : 1], [0 : 1 : 0], [24 : -108 : 1], [-12 : -108 : 1].$$

1. Demonstrar que el rango de E es 0.

2. Usar el Teorema 3.25 (Teorema de Nagell–Lutz) para concluir que

$$C(\mathbb{Q}) = \{\text{cúspides}\}.$$

3. Concluir que no existen curvas elípticas sobre $\mathbb{Q}$ con un punto de torsión (sobre $\mathbb{Q}$) de orden 11. Este es un caso particular de la descripción completa de las posibilidades para $E(\mathbb{Q})_{\text{tor}}$ dada por Mazur [Maz77].

7.3. Ejemplo: La curva modular $X_0^+(167)$

Ilustraremos ahora el método anterior mediante el ejemplo de la curva modular $X_0^+(167)$, estudiado por Balakrishnan y Müller, ver [BM20, § 5.5].

Resulta que $X_0^+(167)$ es isomorfa a la curva hiperelíptica C dada por la ecuación

$$y^2 = 1881x^6 - 3328x^5 + 2418x^4 - 926x^3 + 197x^2 - 22x + 1. \tag{7.15}$$

Esta curva tiene género 2 por el Ejercicio 2.29.

Primero, definamos la curva en Magma y encontremos algunos puntos de coordenadas pequeñas.

```
> _<x> := PolynomialRing(Rationals());
> f := 1881*x^6 -3328*x^5 + 2418*x^4 -926*x^3 + 197*x^2-22*x+ 1;
> C := HyperellipticCurve(f);
> Points(C : Bound := 1000);
{@ (0 : -1 : 1), (0 : 1 : 1), (1 : -1 : 2), (1 : 1 : 2) @}
```

Nuestro objetivo es demostrar $C(\mathbb{Q})$ coincide con

$$C(\mathbb{Q})_{\text{known}} = \{[0 : -1 : 1], [0 : 1 : 1], [1 : -1 : 2], [1 : 1 : 2]\} \subseteq C(\mathbb{Q})$$

usando el método de Chabauty cuadrático.

7.3.1. Hipótesis

Recordemos que el método de Chabauty cuadrático aplica para curvas con rango igual a su género, entonces debemos comprobar que el rango del Jacobiano J de C es 2. Aquí está el cálculo en Magma.

```
> J := Jacobian(C);
> M, phi := MordellWeilGroup(J);
```

Que nos dice que el grupo de Mordell Weil de J es isomorfo a $\mathbb{Z}^2$, con generadores (en representación de Mumford)

```
(x^2 - 7/13*x + 1/13, 17/169*x - 8/169, 2),
(x^2 - 3/5*x + 1/10, -13/50*x + 3/50, 2).
```

Estas representaciones corresponden a los divisores para los cuales (la homogenización hasta grado 2 de) el primer polinomio es cero y el segundo es igual a y.

Lo último que debemos asegurar es que el rango de Nerón–Severi es mayor a 1. Para ello, basta con encontrar un endomorfismo no-trivial del Jacobiano de C. Para esto, podemos usar el código para encontrar endomorfismos en este repositorio de GitHub.

```
> prec := 300;
> F := RationalsExtra(prec);
> R<x> := PolynomialRing(F);
>
> f := 1881*x^6 -3328*x^5 + 2418*x^4 -926*x^3 + 197*x^2-22*x+ 1;
> C := HyperellipticCurve(f);
>
> P := PeriodMatrix(C);
> GeoEndoRep := GeometricEndomorphismRepresentation(P, F);
>
> GeoEndoRep;
[ [*
    [1 0]
    [0 1],

    [1 0 0 0]
    [0 1 0 0]
    [0 0 1 0]
    [0 0 0 1]
*], [*
    [-3 11]
    [-1  4],

    [ 1  0  0  1]
    [ 0  0 -1  0]
    [ 0 -1  1  0]
    [ 1  0  0  0]
*] ]
```

Esto es, existe una correspondencia que actúa sobre las 1-formas holomorfas de la curva con base $\{\mathrm{d}x/y,\, x\mathrm{d}x/y\}$.

7.3.2. Alturas

De acuerdo con el algoritmo descrito en la sección anterior, el primer paso consiste en escoger una correspondencia Z adecuada. En este ejemplo, una propiedad geométrica de $X_0^+(167)$ implica que todas las contribuciones locales fuera de p son nulas. En consecuencia, la función

$$F = h_Z - h_{Z,p}$$

satisface $F(P) = 0$ para todo punto racional $P \in C(\mathbb{Q})$.

Remark 7.16. La condición que las alturas locales sean cero lejos de p no es necesaria, pero si ayuda mucho en los cálculos. Cuando esto no pasa, uno puede mostrar que dichas alturas sólo toman finitos valores cuando se fija un modelo regular propio. Hay toda una teoría para calcular estas alturas fuera de p, ver por ejemplo [DRHS23].

Consecuentemente, lo que necesitamos es qué sobre cada disco residual podamos encontrar una expansión de las funciones h_Z y $h_{Z,p}$ y mediante el método de Newton p-ádico, determinar todos sus ceros. Daremos una idea general de como calcularlas:

- Dada la condición que asumimos sobre log, y del hecho que la altura global h_Z es un emparejamiento bilineal simétrico, podemos encontrar $\alpha_{ij} \in \mathbb{Q}_p$ tales que para todo $P \in C(\mathbb{Q})$ tenemos que:

  $$h_Z((P) - (\infty), (P) - (\infty)) = \sum \alpha_{ij} \int_\infty^P \omega_i \int_\infty^P \omega_i,$$

  donde la suma corre sobre diferenciales de una base de $H^0(C, \Omega^1)$. El lado derecho puede extenderse a todo $C(\mathbb{Q}_p)$, del hecho que h_Z es una función analítica nos permite asegurar que las extensiones a izquierda y derecha son iguales. Por ejemplo, en el disco residual de $b := [0 : -1 : 1] \in C(\mathbb{F}_7)$ tenemos que:

  $$(-10t + 5 \cdot 7^{-1}t^2 - 12t^3) + O(t^4, 7^2).$$

- El siguiente paso consiste en calcular la expansión local de $h_{Z,p}$ en cada disco residual de $C(\mathbb{Q}_p)$. Este paso es mucho mas complicado y se necesitan entre otros descomposición de Hodge p-ádica, teoría de Arakelov, teoría de Adeles e Ideles. Vale la pena resaltar que para curva hiperelípticas, existe un algoritmo explícito que incluye usar el Algoritmo de Tuitman, calcular el operador de Frobenius en $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_7)$ y calcular integrales de Coleman. Por ejemplo, en el disco residual de b tenemos que:

  $$h_{Z,7}(x) = t - 5t^2 - 24t^3 + O(t^4, 7^2)$$

En conclusión, en el disco residual de b tenemos que:

$$F(x) = 17t + 9 \cdot 7^{-1}t^2 - 12t^3 + O(t^4, 7^2),$$

la cuál es una función que solo tiene un cero en $p\mathbb{Z}_p$ por lo que concluimos en este disco residual hay a lo más un punto de $C(\mathbb{Q}_p)_U$. Es decir, el único punto racional que reduce a b es el $[0 : -1 : 1]$.

7.3.3. Conclusión

Al finalizar este proceso se obtiene un conjunto finito

$$C(\mathbb{Q}_p)_U,$$

que contiene todos los puntos racionales de la curva,

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_U.$$

Sin embargo, como ocurre frecuentemente en Chabauty cuadrático, algunos de estos puntos corresponden únicamente a soluciones p-ádicas y no a puntos racionales.

Para eliminar estos candidatos se utiliza el *Mordell–Weil Sieve*. La idea consiste en estudiar la imagen de cada punto candidato bajo la inmersión de Abel–Jacobi

$$P \longmapsto [(P) - (b)] \in J(\mathbb{Q}_p).$$

Si un punto de $C(\mathbb{Q}_p)_U$ proviniera de un punto racional, entonces su clase debería pertenecer al grupo de Mordell–Weil del jacobiano. Combinando información módulo varios primos es posible descartar los candidatos que no satisfacen esta condición.

Finalmente, después del sieve, los únicos puntos que permanecen son precisamente los puntos de $C(\mathbb{Q})_{\text{known}}$. De esta manera se concluye que

$$C(\mathbb{Q}) = C(\mathbb{Q})_{\text{known}}.$$

Remark 7.17. Este ejemplo ilustra la filosofía general del método. Chabauty cuadrático no determina directamente los puntos racionales de la curva; en cambio, construye un conjunto finito de puntos p-ádicos que los contiene. El paso final consiste en eliminar los candidatos sobrantes mediante información aritmética adicional, típicamente el Mordell–Weil sieve.

7.4. Comentarios adicionales

Terminaremos esta sección con algunos ejercicios adicionales y generalizaciones del método de Chabauty cuadrático.

✎ **Ejercicio 7.18.** La curva $X_0(67)^+$ es la curva modular que obtenemos al tomar el cociente de $X_0(67)$ por la involución de Atkin-Lehner w_{67}. Como en [BBB+21] se puede probar que esta curva está definida por la ecuación

$$y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1.$$

En este ejercicio, calcularemos algunos de los pasos de Chabauty cuadrático para esta curva en el primo $p = 11$.

1. Encuentre al menos 10 puntos racionales de esta curva.
2. Calcule el género y rango de Mordell–Weil de esta curva. *Sugerencia:* Usando Magma, compruebe que el rango de Mordell-Weil es ≤ 2. Compruebe que los elementos del Jacobiano

   $$D_1 = 2 \cdot [0 : -1 : 1] - [1 : -1 : 0] - [1 : 0 : 0] \qquad \text{y} \qquad D_2 = [0 : 0 : 1] - [1 : -1 : 0]$$

   tienen orden infinito. Reduciendo módulo dos primos, pruebe que D_1 y D_2 son linealmente independientes.

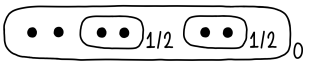
3. Sea p un primo de buena reducción y Z una correspondencia no trivial. En esta parte, probaremos que todas las alturas locales en primos $\ell \neq p$ son triviales.

   a) Justificar por qué el único primo de mala reducción es 67. Concluir que todas las alturas $h_{Z,\ell}$ son triviales para $\ell \neq p, 67$

   b) Para el primo $\ell = 67$, comprobar que el *cluster picture* del polinomio

   $$x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$$

   es:

   Una buena referencia para este proceso es [BBB+22].

   c) Usar [BDHS25, Proposition 5] para concluir que $h_{Z,67} \equiv 0$ en puntos racionales.

4. La siguiente matriz (proveniente de un operador de Hecke) representa la acción de un endomorfismo no trivial en la cohomología de de Rham de la curva

   $$\begin{pmatrix} 0 & -8 & 12 & 8 \\ 8 & 0 & -8 & -12 \\ -12 & 8 & 0 & 0 \\ -8 & 12 & 0 & 0 \end{pmatrix}$$

   Existen dos formas de calcular esta matriz. Una que usa directamente el operador de Hecke en formas modulares (ver [BM20, Algorithm 1.53]) y otra usando el método general para calcular endomorfismos de jacobianos en [CMSV19].

5. Para terminar el cálculo de Chabauty, podemos modificar uno de los ejemplos de [BDM+] con la información que hemos obtenido. Al final, se necesitará aplicar el Mordell-Weil Sieve en 31 para demonstrar que los 10 puntos racionales que encontramos son todos los que existen.

7.4.1. Otras versiones de Chabauty cuadrático

Además de la formulación cohomológica presentada anteriormente, existe una formulación geométrica de Chabauty cuadrático, propuesta por Edixhoven y Lido [EL23]. El objeto central es la biextensión de Poincaré, vista como un torsor bajo $\mathbb{G}_m$ sobre $J \times J^\vee$. A partir de una correspondencia en $C \times C$, esta biextensión produce un torsor sobre J y un levantamiento de la aplicación de Abel–Jacobi de C. El método compara, dentro de este torsor, el levantamiento de $C(\mathbb{Q}_p)$ con la clausura p-ádica de los puntos integrales. Así se obtiene, bajo la condición

$$\operatorname{rank} J(\mathbb{Q}) < g + \rho(J) - 1,$$

un conjunto finito de puntos p-ádicos que contiene $C(\mathbb{Q})$.

Duque-Rosero–Hashimoto–Spelier hicieron efectiva esta construcción al expresarla mediante alturas p-ádicas e integrales de Coleman [DRHS23]. Además, comparan el conjunto producido por el método geométrico con el de Chabauty cuadrático cohomológico: el primero está contenido en el segundo. Su § 9 presenta, disco residual por disco residual, un cálculo para la curva $X_0(67)^+$ del Ejercicio 7.18.

Desde otra perspectiva, Besser–Müller–Srinivasan desarrollan una teoría de Arakelov p-ádica para variedades sobre campos de números [BMS25]. En este marco, las alturas p-ádicas se construyen

a partir de métricas adélicas p-ádicas en fibrados en rectas. Al aplicar esta teoría a un fibrado adecuado sobre el jacobiano, obtienen una formulación simplificada de Chabauty cuadrático que recupera, para jacobianos, las alturas de Coleman–Gross y que también admite primos de mala reducción.

Clase 8: Geometría de superficies

Dos preguntas naturales respecto al método de Chabauty y Coleman son: ¿Qué se sabe en dimensión superior? ¿Hay métodos tan efectivos como para el caso de curvas?

El primer acercamiento fue presentado por S. Siksek [Sik09] para potencias simétricas de una curva. Más adelante veremos una definición formal de este objeto. Sin embargo, este proceso no permite dar una cota superior para el número de puntos racionales.

El objetivo de esta clase es mostrar algunos ejemplos en donde aparecen superficies. Además mostraremos algunos resultados y conjeturas acerca de los puntos racionales en estas variedades.

Ejemplo 8.1. Suma de tres cubos iguales al número 3. En 1953 Mordell dijo: *"I do not know anything about the integer solutions of $x^3 + y^3 + z^3 = 3$ beyond the existence of the four triples $(1, 1, 1)$, $(4, 4, -5)$, $(4, -5, 4)$, $(-5, 4, 4)$; and it must be very difficult indeed to find out anything about any other solutions."* Fue hasta Septiembre de 2019 que Andrew Booker y Andrew Sutherland descubrieron la quinta solución a la ecuación $x^3 + y^3 + z^3 = 3$.

Ejemplo 8.2. Problema de Büchi Dada una lista de cuadrados consecutivos, las segundas diferencias siempre son $2, 2, 2, \ldots$, por ejemplo

4		1		0		1		4		9
	-3		-1		1		3		5	
		2		2		2		2		

A estas secuencias (de cuadrados consecutivos) le llamaremos trivial. **Hay ejemplos con secuencias no triviales, a saber**

0		49		100
	49		51	
		2		

6^2		23^2		32^2		39^2
	493		495		497	
		2		2		

Problema: Existe una constante M tal que cada secuencia de enteros cuadrados $x_1^2, \ldots, x_M^2$ teniendo segunda diferencia $2, 2, \ldots, 2$, es necesariamente trivial.

Note que secuencias de longitud de cuadrados con segundas diferencias $2, 2, \ldots, 2$ pueden ser interpretadas como puntos enteros de cierta superficie. Para ver esto, podemos reinterpretar las condiciones por el siguiente sistema:

$$\begin{array}{ccccc} x_3^2 & - & 2x_2^2 & + & x_1^2 = 2 \\ \vdots & & \vdots & & \vdots \quad \vdots \\ x_n^2 & - & 2x_{n-1}^2 & + & x_{n-2}^2 = 2 \end{array}$$

Estas ecuaciones definen una superficie que para $n \geq 6$ es una superficie de tipo general.

Ejemplo 8.3. El **problema del cuboide perfecto** pregunta si existe un paralelepípedo rectangular cuyas *tres aristas*, las *tres diagonales de las caras* y la *diagonal espacial* sean todas *enteras*. Si las aristas son a, b, c, las condiciones se escriben como

$$a^2 + b^2 = d_{ab}^2, \qquad a^2 + c^2 = d_{ac}^2, \qquad b^2 + c^2 = d_{bc}^2, \qquad a^2 + b^2 + c^2 = D^2.$$

Se conocen ejemplos donde las tres diagonales de las caras son enteras (los llamados *Euler bricks*), pero *no se conoce ningún cuboide perfecto* donde también la diagonal espacial sea entera.

Desde el punto de vista de la *geometría algebraica*, el problema puede reformularse como el estudio de los *puntos racionales* de una variedad algebraica definida por estas ecuaciones cuadráticas. Esta superficie es una variedad es una superficie y gracias a que es una intersección completa es muy fácil ver que es de tipo general.

8.1. Puntos racionales en subvariedades en variedades abelianas

En 1994, sorprendentemente Faltings [Fal91b, Fal94], quién ya había probado la conjetura de Mordell (que las curvas de tipo general tienen finitos puntos), probó la siguiente conjetura de Mordell-Lang sobre subvariedades de variedades abelianas.

Teorema 8.4 (Conjetura de Mordell–Lang)**.** *Sea X una subvariedad cerrada de una variedad abeliana A ambos definidos sobre un campo de números K. Entonces existen un subconjunto finito $S \subset X(K)$, finitos puntos $x_1, \ldots, x_n \in X(K)$ y subvariedades abelianas propias $B_1, \ldots, B_n \subseteq A$ de rango positivo tales que para cada i, $x_i + B_i(K) \subseteq X(K)$ y además*

$$X(K) = \bigcup_{i=1}^{n} (x_i + B_i(K)) \coprod S. \tag{8.5}$$

✎ **Ejercicio 8.6.** Sean E_1, E_2, E_3 3 curvas elípticas que no son isogeneas, cada una de ellas con coordenadas x_i, y_i. Considere el hiperplano X en $A := E_1 \times E_2 \times E_3$ dado por la ecuación $x_1 + x_2 + x_3 = 0$.

(i) Pruebe que si $E \subset A$ es una curva elíptica, entonces es isogenea a E_i para algún $i \in \{1, 2, 3\}$.

(ii) Pruebe que si $B \subset A$ es una superficie abeliana, entonces es isogenea a $E_i \times E_j$ para $i, j \in \{1, 2, 3\}$, con $i \neq j$.

(iii) Use el teorema grande de Faltings para demostrar que $X(\mathbb{Q})$ es finito.

Este teorema nos dice, en el caso de superficies, que una superficie contenida en una variedad abeliana A, que no contiene trasladados de curvas elípticas de rango positivo, tiene a lo más finitos puntos.

8.2. Puntos racionales en superficies de tipo general

Empezaremos con la definición de superficies de tipo general y luego expondremos una conjetura importante sobre sus puntos racionales.'

Definición 8.7. Sea X una superficie suave proyectiva e irreducible y sea K_X un divisor canónico de X. Para cada $m \geq 1$ tal que $h^0(X, \mathcal{O}(mK_X)) \neq 0$, sea

$$\Phi_{mK_X} : X \to \mathbb{P}^{N_m}$$

el mapa racional inducido por el sistema lineal $|mK_X|$. La dimensión de Kodaira de X es definida por:

$$\kappa(X) = \begin{cases} -\infty & \text{si } h^0(X, \mathcal{O}(mK_X)) = 0, \text{ para todo } m \geq 0 \\ \max \dim \Phi_{mK_X} & \text{de otro modo.} \end{cases}$$

Definición 8.8 (Superficie de tipo general)**.** Sea X una superficie suave, proyectiva e irreducible. Si $\kappa(X) = 2$ entonces X se llama superficie de tipo general.

Remark 8.9. Si una superficie suave X se define por r ecuaciones homogéneas en $\mathbb{P}^{r+2}$, diremos que la superficie es una intersección completa. Si $d_1, \ldots, d_r$ son los grados de las ecuaciones que definen a X, se puede probar que

$$\kappa(X) = \begin{cases} 2 & \text{si } \sum d_i > r + 3 \\ 0 & \text{si } \sum d_i = r + 3 \\ -\infty & \text{de otro modo.} \end{cases}$$

En particular, en el caso de la superficie del problema de Büchi X_n es de tipo general para $n \geq 6$ y la superficie del cuboide perfecto es de tipo general.

✎ **Ejercicio 8.10.** Probar que la superficie que definimos en el Ejemplo 8.3 es una intersección completa de tipo general.

Hay una conjetura importante sobre puntos racionales en superficies de tipo general.

Conjetura 8.11 (Bombieri–Lang)**.** *Sea X una superficie suave de tipo general definida sobre un campo de números K. Entonces el conjunto $X(K)$ no es Zariski denso en $X(\overline{K})$.*

No se sabe mucho sobre esta conjetura, pero gracias al Teorema 8.4 se sabe esta conjetura para superficies de tipo general contenidas en variedades abelianas.

Remark 8.12. Asumiendo esta la conjetura de Bombieri-Lang, Vojta probó en 1999 que el problema de Büchi tiene solución afirmativa.

8.3. Una cota tipo Chabauty–Coleman para superficies

En 2023, Caro y Pastén [CP23] dieron una cota superior para el orden de este conjunto, asumiendo ciertas condiciones geométrico-algebraicas.

Teorema 8.13. *[CP23, Teorema 1.5] Sea X una superficie de tipo general suave, proyectiva y geométricamente irreducible contenida en un variedad abeliana A de dimensión 3, ambas definidas sobre $\mathbb{Q}$. Sea $p > (128/9) \cdot c_1^2(X)^2$ un primo de buena reducción para X y A. Si* $\operatorname{rank}(A(\mathbb{Q})) \leq 1$ *y X_p no contiene curvas elípticas sobre $\mathbb{F}_p^{alg}$, entonces*

$$\#X(\mathbb{Q}) \leq \#X_p(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 5\right) \cdot c_1^2(X).$$

Recordamos que $c_1^2(X)$ denota la autointersección del divisor canónico K_X de X.

Remark 8.14. Es importante resaltar que el Teorema 8.13 también tiene una versión para campos de números y para variedades abelianas de mayor dimensión. En este último caso, es necesario ciertas condicione en la reducción de A y la existencia de un divisor amplio que satisfaga ciertas condiciones numéricas.

Clase 9: Método de Chabauty para superficies

Dos preguntas naturales respecto al método de Chabauty y Coleman son: ¿Qué se sabe en dimensión superior? ¿Hay métodos tan efectivos como para el caso de curvas?

El primer acercamiento fue presentado por S. Siksek [Sik09] para potencias simétricas de una curva. Más adelante veremos una definición formal de este objeto. Sin embargo, este proceso no permite dar una cota superior para el número de puntos racionales.

En 2023, Caro y Pastén [CP23] obtuvieron la primera cota explícita para el número de puntos racionales en el caso de superficies. El objetivo de esta clase es explicar este resultado y un par de aplicaciones de este método.

9.1. Continuación: Una cota tipo Chabauty–Coleman para superficies

Como vimos en la clase anterior, tenemos el siguiente teorema probado por Caro y Pastén.

Teorema 9.1. *[CP23, Teorema 1.5] Sea X una superficie de tipo general suave, proyectiva y geométricamente irreducible contenida en un variedad abeliana A de dimensión 3, ambas definidas sobre $\mathbb{Q}$. Sea $p > (128/9) \cdot c_1^2(X)^2$ un primo de buena reducción para X y A. Si $\operatorname{rank}(A(\mathbb{Q})) \leq 1$ y X_p no contiene curvas elípticas sobre $\mathbb{F}_p^{alg}$, entonces*

$$\#X(\mathbb{Q}) \leq \#X_p(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 5\right) \cdot c_1^2(X).$$

Podemos resumir el Teorema 9.1 como sigue: Sea X una superficie de tipo general suave, proyectiva e irreducible contenida en una variedad abeliana A de dimensión 3 ambas definidas sobre $\mathbb{Q}$, y sea p un primo de buena reducción para X y A.

Asumimos que:

- $p > (\frac{128}{9}) \cdot (c_1^2(X))^2$,
- $\operatorname{rank} A(\mathbb{Q}) \leq 1$,
- X' no contiene curvas elípticas sobre $\mathbb{F}_p^{alg}$: "*finitud*".

Entonces

$$\#X(\mathbb{Q}) < \#X'(\mathbb{F}_p) + 4p \cdot c_1^2(X).$$

Antes de mostrar la idea de la prueba del Teorema 9.1, necesitamos definir un objeto y enunciar un lema importantes en la demostración.

Definición 9.2 (ω-integralidad)**.** Sea k un campo. Sean Z, Y dos k-esquemas y $\omega \in H^0(Y, \Omega_Y^1)$. Un k-morfismo $\phi : Z \to Y$ se llama *ω-integral* si la composición

$$\phi^\bullet : H^0(Y, \Omega_Y^1) \to H^0(Y, \phi_*\phi^*\Omega_Y^1) = H^0(Z, \phi^*\Omega_Y^1) \to H^0(Z, \Omega_Z^1)$$

satisface $\phi^\bullet(\omega) = 0$.

A lo largo de esta sección fijaremos la siguiente notación: denotamos por k a $\mathbb{F}_p^{alg}$ por V_m a $\operatorname{Spec} k[z]/(z^{m+1})$. Sea S una superficie suave definida sobre k, sea $x \in S$, sean $w_1, w_2 \in H^0(S, \Omega^1_{S/k})$ diferenciales independientes sobre $\mathcal{O}_S$, y sea $D := \operatorname{div}(w_1 \wedge w_2) = \sum_{j=1}^q a_j D_j$ el divisor de Weil asociado a la dos formar $w_1 \wedge w_2$ con las D_j curvas irreducibles. Sean $\nu_j : \widetilde{D_j} \to D_j \subseteq S$ los morfismos de normalización.

Lema 9.3. *Sea $\phi : V_m \to S$ una inmersión cerrada soportada en x. Si ϕ es w_i-integral para ambos $i = 1, 2$ entonces*

$$m \leq \sum_{j=1}^{q} \sum_{y \in \nu_j^{-1}(x)} a_j (\operatorname{ord}_y(\nu_j^\bullet w_i) + 1).$$

Idea de la prueba del Teorema 8.13. Denotamos por Γ la clausura p-ádica de $A(\mathbb{Q})$ en $A(\mathbb{Q}_p)$. Γ es un subgrupo p-ádico a un parámetro de $A(\mathbb{Q}_p)$. Notamos que:

$$X(\mathbb{Q}) = X(\mathbb{Q}_p) \cap A(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \Gamma.$$

Consideremos el morfismo reducción $\operatorname{red}\colon A(\mathbb{Q}_p) \to A'(\mathbb{F}_p)$. Para cada disco residual $U_x = \operatorname{red}^{-1}(x)$ con $x \in X'(\mathbb{F}_p)$ queremos acotar $\#X(\mathbb{Q}_p) \cap \Gamma \cap U_x$. Para acotar $\#X(\mathbb{Q}_p) \cap \Gamma \cap U_x$ consideramos el subgrupo analítico a un parámetro $\gamma : p\mathbb{Z}_p \to \Gamma \cap U_x$. Sea f una ecuación local de X sobre U_x. Entonces $f \circ \gamma(z)$ es una serie de potencias p-ádica y

$$\#X(\mathbb{Q}_p) \cap \Gamma \cap U_x \leq n_0(f \circ \gamma(z), 1/p),$$

donde $n_0(f \circ \gamma(z), 1/p)$ representa el número de ceros de $f \circ \gamma(z)$ con radio $1/p$. Escribimos entonces

$$f \circ \gamma(z) = \sum_n a_n z^n \in \mathbb{Q}_p[[z]].$$

Para acotar $n_0(f \circ \gamma(z), 1/p)$ necesitamos encontramos un entero N tal que $|a_N| \geq 1$.

Suponga que para algún $m < p$, se satisface que $|a_i| < 1$ para cada $i \leq m$ (esta es la situación que queremos acotar). En este caso, uno puede probar que existe una inmersión cerrada

$$\phi_m : V_m \to X_k,$$

soportada en x la cuál es w_i-integral para algunos $w_1, w_2 \in H^0(X_k, \Omega^1_{X_k/k})$ independientes. Lo que necesitamos es acotar los m que satisfagan la siguiente condición:

> Existe una inmersión cerrada
> $$\phi : V_m \to X_k,$$
> en x que es w_i-integral para algunos $w_1, w_2 \in H^0(X_k, \Omega^1_{X_k/k})$ independientes.

Denotemos por $m(x)$ el mayor m para el que exista una inmersión como antes. Consecuentemente, $m(x)$ puede ser acotado usando el Lema 9.3.

Usando análisis p-ádico obtenemos que:

$$\#X(\mathbb{Q}_p) \cap \Gamma \cap U_x \leq n_0(f \circ \gamma(z), 1/p) \leq 1 + \frac{p-1}{p-2} \cdot m(x).$$

En cuánto a $m(x)$ tenemos los siguientes casos:

- Si $x \notin \text{supp}(D)$ Tenemos que $m(x) = 0$. Por tanto

$$\#X(\mathbb{Q}_p) \cap \Gamma \cap U_x \leq 1 + \frac{p-1}{p-2} \cdot m(x) = 1.$$

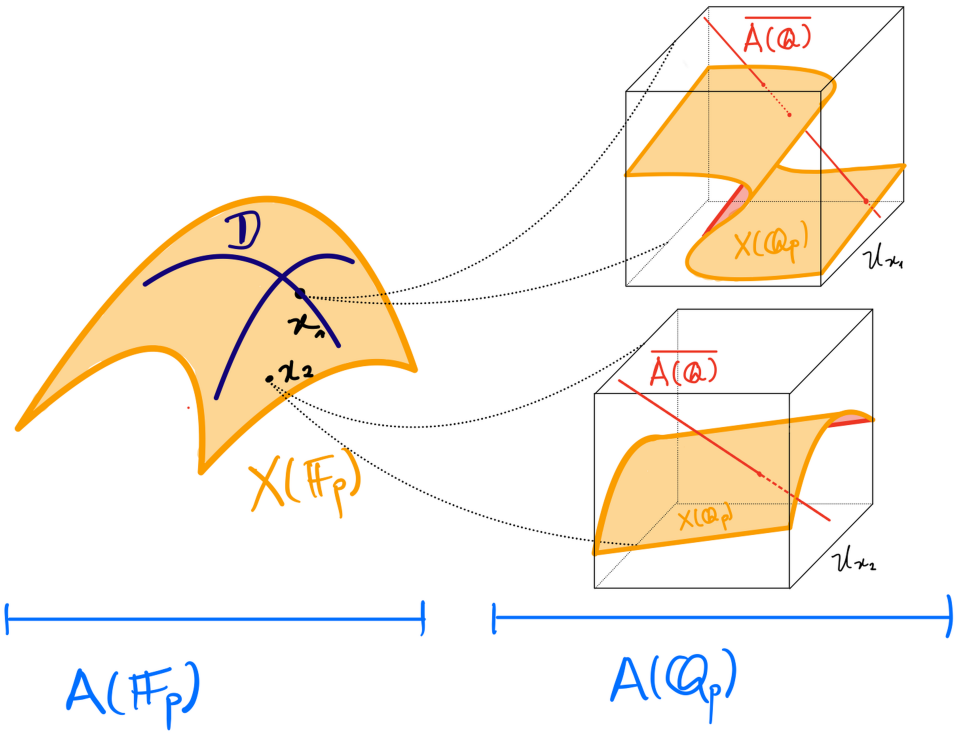
- Si $x \in \text{supp}(D)$. Usamos la hipótesis de Riemann para curvas singulares, cálculos de teorías de intersección, control de singularidades D, etc. Cuando sumamos sobre todos los puntos en el soporte de D, obtenemos un cota en términos del primo p y $c_1^2(X) = (D.D)$.

Pegando todo junto tenemos

$$\begin{aligned}\#X(\mathbb{Q}_p) \cap \Gamma = \sum_{x \in X'(\mathbb{F}_p)} \#X(\mathbb{Q}_p) \cap \Gamma \cap U_x &\leq \sum_{x \in X'(\mathbb{F}_p)} \left(1 + \frac{p-1}{p-2} \cdot m(x)\right) \\ &< \#X'(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \underbrace{(p + 4p^{1/2} + 5) \cdot c_1^2(X)}_{\text{términos } m(x) \text{ para } x \in D(\mathbb{F}_p)}.\end{aligned}$$

□

La siguiente gráfica resume un poco la prueba:



En los discos residuales de puntos que no están en el soporte de D (como en el caso de x_2) hay a lo más un punto racional. Sin embargo, en los discos residuales asociados a los puntos que están en el soporte de D (como en el caso de x_1) puede haber mas de un punto racional (pero este conjunto de puntos está acotado gracias al Lema 9.3).

9.2. Potencias simétricas de una curva

Sea C una curva suave, proyectiva y geométricamente irreducible definida sobre un campo de números K. Para un entero $d \geq 1$, la d-ésima potencia simétrica de C, denotada por $\mathrm{Sym}^d(C)$, se define como el cociente

$$\mathrm{Sym}^d(C) = C^d/S_d,$$

donde S_d (el grupo de simétrico de $d!$ elementos) actúa sobre el producto cartesiano C^d permutando las coordenadas.

Las potencias simétricas desempeñan un papel central en la geometría aritmética de curvas. En particular, los puntos racionales de $\mathrm{Sym}^d(C)$ parametrizan divisores efectivos de grado d definidos sobre el campo base. Equivalente y más geométricamente, estos puntos codifican órbitas de Galois de puntos de grado d sobre la curva. Por esta razón, el estudio de $\mathrm{Sym}^d(C)(K)$ está estrechamente relacionado con la comprensión de los puntos algebraicos de grado d de C.

Además, la inclusión de Abel–Jacobi

$$\iota_d : \mathrm{Sym}^d(C) \longrightarrow J(C), \tag{9.4}$$

que envía un divisor efectivo D a su clase lineal respecto de un divisor base fijo, conecta el estudio de las potencias simétricas con la teoría de las variedades abelianas. Esta relación ha permitido extender diversas técnicas clásicas para curvas, incluyendo métodos de Chabauty–Coleman, al contexto de puntos de grado superior. En consecuencia, la determinación de los puntos racionales de $\mathrm{Sym}^d(C)$ constituye un problema fundamental para el estudio efectivo de puntos algebraicos de grado acotado sobre curvas.

En 2025, Balakrishnan y Caro refinaron las cotas dadas por Caro y Pastén en el caso particular en el que las superficies son la imagen de cuadrados simétricos de curva hiperelípticas vía (9.4).

Teorema 9.5. *[BC25, Teorema 1.1] Sea C un curva hiperelíptica definida sobre $\mathbb{Q}$ de género 3 cuyo Jacobiano tiene rango ≤ 1. Sea $p \geq 11$ un primo de buena reducción para C. Suponga que la reducción de $C + C$ no contiene curvas elípticas sobre $\mathbb{F}_p^{\mathrm{alg}}$. Entonces:*

$$\#(C + C)(\mathbb{Q}) \leq \#(C + C)(\mathbb{F}_p) + 2p + 12\sqrt{p} + 7.$$

Además, ellos implementaron un algoritmo basado en el método de Chabauty–Coleman–Caro–Pastén.

Input: Curva hiperelíptica C.

Output: Una cota superior para el número de puntos racionales de la superficie $C + C$.

Con este algoritmo produjimos ejemplos de superficies en donde nuestro método permite calcular sus puntos racionales.

Ejemplo 9.6. Sea C una curva hiperelíptica de género 3 definida por la ecuación:

$$y^2 = x(x^2 + 4)(x^2 - 4x - 3)(x^2 + 4x + 2).$$

Probamos que $(C+C)(\mathbb{Q}) = \{0_J\} \cup \{P_i : i = 1, \ldots, 6\}$, donde

$$\begin{aligned}
P_1 &= (0,0) + 0_J, \\
P_2 &= (Q) + (Q^\sigma), \\
P_3 &= \left(2\sqrt{-1}, 0\right) + \left(-2\sqrt{-1}, 0\right), \\
P_4 &= \left(-2 + 2\sqrt{2}, 0\right) + \left(-2 - 2\sqrt{2}, 0\right), \\
P_5 &= \left(2 + \sqrt{7}, 0\right) + \left(2 - \sqrt{7}, 0\right), \\
P_6 &= \iota P_2,
\end{aligned}$$

con $Q = \left(\dfrac{-13 + 2\sqrt{-14}}{9}, \dfrac{12560 - 7045\sqrt{-14}}{2187}\right)$ y Q^σ el conjugado de Q.

En aras de la claridad, mostraremos como se encuentran cotas superiores al número de puntos racionales en un disco residual.

Para $p = 5$ y $z = \overline{(0,0)} + \overline{(1,0)} \in W_2(\mathbb{F}_5)$, tenemos que

$$\{P_2, P_6, (2\sqrt{-1}, 0) + (0,0)\} \subset W_2(\mathbb{Q}_5) \cap \overline{J(\mathbb{Q})} \cap U_z.$$

El aniquilador de $J(\mathbb{Q})$ respecto al pairing de integración esta generado por los diferenciales:

$$\begin{aligned}
\omega_1 &= (4 + 5 + 4 \cdot 5^3 + O(5^4))\frac{dx}{y} + (3 + 2 \cdot 5 + O(5^4))\frac{x dx}{y}, \\
\omega_2 &= (4 + 4 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + O(5^4))\frac{dx}{y} + (3 + 2 \cdot 5 + O(5^4))\frac{x^2 dx}{y}.
\end{aligned}$$

Entonces tenemos que nuestra 2-forma es:

$$(w_1 \wedge w_2) = (4x_1x_2 + 2(x_1 + x_2) + 3)\frac{d(x_1x_2) \wedge d(x_1 + x_2)}{y_1 y_2}.$$

Su divisor asociado es

$$D = Z_{W_2}(4x_1x_2 + 2(x_1 + x_2) + 3),$$

el cuál es fácil ver que es una curva irreducible. Note que $z \in D$. Uno puede probar fácilmente los siguientes hechos:

- z es un punto singular de D.
- z tiene dos preimagenes z_1 y z_2 vía el morfismo normalización $\nu : \widetilde{D} \to D$.
- Para $i = 1, 2$ tenemos que:
$$\mathrm{ord}_{z_i}(\nu^\bullet w_1) = 0$$

De estos hechos, y de la cota dada por el Lema 9.3

$$m(z) \leq \sum_{j=1}^{q} \sum_{y \in \nu^{-1}(x)} a_j(\mathrm{ord}_y(\nu^\bullet w_1) + 1) = 2.$$

Finalmente, tenemos que

$$3 \leq \#W_2(\mathbb{Q}_5) \cap \overline{J(\mathbb{Q})} \cap U_z \leq 1 + \frac{p-1}{p-2} m(z) = 1 + \frac{4}{3} m(z) = 3.\overline{6},$$

de donde concluimos que $\#W_2(\mathbb{Q}_5) \cap \overline{J(\mathbb{Q})} = 3$.

Bibliografía

[BB12] Jennifer S. Balakrishnan and Amnon Besser. Computing local p-adic height pairings on hyperelliptic curves. *Int. Math. Res. Not. IMRN*, (11):2405–2444, 2012. ↑52.

[BBB+21] Jennifer S Balakrishnan, Alex J Best, Francesca Bianchi, Brian Lawrence, J Steffen Müller, Nicholas Triantafillou, and Jan Vonk. Two recent p-adic approaches towards the (effective) mordell conjecture. In *Arithmetic L-Functions and Differential Geometric Methods: Regulators IV, May 2016, Paris*, pages 31–74. Springer, 2021. ↑64.

[BBB+22] Alex J. Best, L. Alexander Betts, Matthew Bisatt, Raymond van Bommel, Vladimir Dokchitser, Omri Faraggi, Sabrina Kunzweiler, Céline Maistret, Adam Morgan, Simone Muselli, and Sarah Nowell. A user's guide to the local arithmetic of hyperelliptic curves. *Bull. Lond. Math. Soc.*, 54(3):825–867, 2022. ↑65.

[BBH+25] Jennifer S. Balakrishnan, L. Alexander Betts, Daniel Rayor Hast, Aashraya Jha, and J. Steffen Müller. Rational points on the non-split cartan modular curve of level 27 and quadratic chabauty over number fields, 2025. Preprint, arXiv:2501.07833. ↑52, 60.

[BC25] Jennifer S Balakrishnan and Jerson Caro. A refined chabauty–coleman bound for surfaces. *arXiv preprint arXiv:2501.03483*, 2025. ↑74.

[BD18] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller. ↑56.

[BD20] L. Alexander Betts and Netan Dogra. The local theory of unipotent Kummer maps and refined Selmer schemes, 2020. Preprint, arXiv:1909.05734v2. ↑54.

[BD21] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *Int. Math. Res. Not. IMRN*, 2021(15):11923–12008, 2021. ↑56.

[BDHS25] L. Alexander Betts, Juanita Duque-Rosero, Sachi Hashimoto, and Pim Spelier. Local heights on hyperelliptic curves and quadratic Chabauty, 2025. Preprint, 2401.05228v3. ↑54, 65.

[BDM+] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. *Magma code*. https://github.com/steffenmueller/QCMod. ↑65.

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019. ↑60.

[BKM25] Francesca Bianchi, Enis Kaya, and J. Steffen Müller. Algorithms for p-adic heights on hyperelliptic curves of arbitrary reduction. *Res. Number Theory*, 11(1):Paper No. 31, 21, 2025. ↑52.

[BM20] Jennifer Balakrishnan and J Steffen Müller. Computational tools for quadratic Chabauty, 2020. *Unpublished*, https://math.bu.edu/people/jbala/2020BalakrishnanMuellerNotes.pdf. ↑46, 56, 61, 65.

[BMS25] Amnon Besser, J. Steffen Müller, and Padmavathi Srinivasan. p-adic adelic metrics and quadratic Chabauty I. *J. Reine Angew. Math.*, 828:223–305, 2025. ↑65.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011. ↑60.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013. ↑60.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑52.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019. ↑65.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985. ↑40.

[CP23] Jerson Caro and Hector Pasten. A Chabauty-Coleman bound for surfaces. *Invent. Math.*, 234(3):1197–1250, 2023. ↑69, 70, 71.

[DGH21] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger. Uniformity in Mordell-Lang for curves. *Ann. of Math. (2)*, 194(1):237–298, 2021. ↑48.

[DRHS23] Juanita Duque-Rosero, Sachi Hashimoto, and Pim Spelier. Geometric quadratic chabauty and p-adic heights. *Expositiones Mathematicae*, 41(3):631–674, 2023. ↑63, 65.

[EL23] Bas Edixhoven and Guido Lido. Geometric quadratic chabauty. *Journal of the Institute of Mathematics of Jussieu*, 22(1):279–333, 2023. ↑65.

[Fal91a] Gerd Faltings. Diophantine approximation on abelian varieties. *Ann. of Math. (2)*, 133(3):549–576, 1991. ↑39.

[Fal91b] Gerd Faltings. Diophantine approximation on abelian varieties. *Annals of Mathematics*, 133(3):549–576, 1991. ↑68.

[Fal94] Gerd Faltings. The general case of s. lang's conjecture. In *Barsotti Symposium in Algebraic Geometry*, pages 175–182. Elsevier, 1994. ↑68.

[FL26] Lorenzo Furio and Davide Lombardo. On 7-adic galois representations for elliptic curves over $\mathbb{Q}$, 2026. Preprint, arXiv:2507.17967. ↑61.

[GG93] Daniel M. Gordon and David Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus two. *Trans. Amer. Math. Soc.*, 337(2):807–824, 1993. ↑41.

[GM25] Stevan Gajović and J. Steffen Müller. Computing p-adic heights on hyperelliptic curves. *Math. Comp.*, 94(354):2059–2088, 2025. ↑52.

[Har13] Robin Hartshorne. *Algebraic geometry*. Springer Science & Business Media, 2013. ↑16.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry, an introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ↑9.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005. ↑54.

[Kim09] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009. ↑54.

[Lan12] Serge Lang. *Introduction to algebraic and abelian functions*. Springer Science & Business Media, 2012. ↑16.

[Lem19] Pedro Lemos. Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. *Trans. Amer. Math. Soc.*, 371(1):137–146, 2019. ↑60.

[Maz77] B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, volume Vol. 601 of *Lecture Notes in Math.*, pages 107–148. Springer, Berlin-New York, 1977. ↑59, 61.

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995. ↑1, 3, 6, 25, 26, 30.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922. ↑32.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012. ↑36, 40.

[MST06] Barry Mazur, William Stein, and John Tate. Computation of p-adic heights and log convergence. *Doc. Math.*, pages 577–614, 2006. ↑51.

[Nar92] Raghavan Narasimhan. *Compact Riemann surfaces*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1992. ↑31.

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:Paper No. e62, 63, 2022. ↑60.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972. ↑60.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. With a foreword by Brown and Serre. ↑1, 3, 47.

[Sik09] Samir Siksek. Chabauty for symmetric powers of curves. *Algebra & Number Theory*, 3(2):209–236, 2009. ↑67, 71.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. ↑1, 3, 5, 13, 16, 33, 48, 51.

[Smi23] Benjamin Andrew Smith. *Explicit endomorphisms and correspondences*. PhD thesis, The University of Sydney, 2005-12-23. ↑57.

[Voj91] Paul Vojta. Siegel's theorem in the compact case. *Ann. of Math. (2)*, 133(3):509–548, 1991. ↑39.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929. ↑32.

[Zyw15] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$, 2015. ↑60.