AGRA II: Aritmética, grupos y análisis
An ICTP-CIMPA Research School

Introducción a la teoría de las curvas elípticas

Marusia Rebolledo
Université Blaise Pascal, Clermont-Ferrand
Laboratoire de mathématiques
marusia.rebolledo@math.univ-bpclermont.fr

Marc Hindry
Université Paris Diderot
Institut de mathématiques de Jussieu – Paris rive gauche
marc.hindry@imj-prg.fr

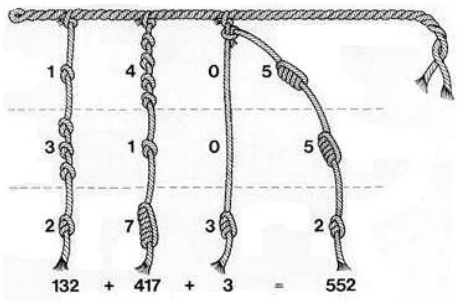
UNIVERSIDAD S. ANTONIO ABAD, CUSCO, PERÚ, del 8 al 22 de Agosto de 2015

Índice general

Prefacio

Este curso es una introducción a la teoría geométrica y aritmética de las curvas elípticas y a las funciones L que les pueden ser asociadas.

Tales curvas aparecen naturalmente en el estudio de ecuaciones diofánticas; son el primer ejemplo donde no se puede aplicar sistemáticamente, como se hace para las cónicas, el principio de Hasse o el método de la cuerda/tangente. Son también las más simples variedades abelianas (dimensión 1). Las estructuras diversas de estas curvas y los lazos, vía las funciones L, con objetos de naturaleza algebraica (representaciones de Galois) o analítica (formas modulares), están en el corazón de numerosos resultados y preguntas actuales en la geometría aritmética. Entre estos resultados, el más conocido es ciertamente el Último Teorema de Fermat. La función L que permite estos lazos es una serie de Dirichlet del mismo tipo que la función zeta de Riemann. Las series de Dirichlet y la función zeta de Riemann fueron introducidas para demostrar los principales teoremas acerca de la distribución de números primos. El éxito de este método ha llevado a introducir análogos llamados funciones L de Hasse-Weil asociados a las curvas elípticas. Presentaremos estas series, sus principales propiedades – algunas apenas conjeturadas como la "hipótesis de Riemann" y sus relaciones con la aritmética de las curvas elípticas.



Completamos este prefacio con dos ejercicios que esconden curvas elípticas. Usted encontrará indicaciones al final destas notas.

Ejercicio 1. (En el estilo de Fermat, número se refiere a número natural)

1. ¿Cuáles cubos pueden escribirse como un cuadrado aumentado de dos unidades?
2. ¿Cuáles números pueden escribirse como un producto de dos números consecutivos y de tres números consecutivos (ejemplo : $6 = 2 \times 3 = 1 \times 2 \times 3$)?

Capítulo 1

Curvas elípticas

En este curso, los pequeños Ejo *siñalan que hay algo que demostrar en la frase anterior que dejamos como ejercicio al lector.*

1.1. Preliminarios

1.1.1. Espacios afines y proyectivos

Sea K un cuerpo y $\bar{K}$ una clausura algebraica de K. En este curso, los más seguido $K = \mathbb{Q}, \mathbb{Q}_p, \mathbb{C}$, o $\mathbb{F}_q$.

- Llamamos *espacio afín de dimension n sobre K* el espacio vectorial : $\mathbb{A}^n = \mathbb{A}^n_K = \mathbb{A}^n(\bar{K}) = \bar{K}^n$. Llamamos *espacio proyectivo de dimensión n sobre K* el conjunto de las lineas vectoriales de $\bar{K}^{n+1}$ o sea el cociente
$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = (\mathbb{A}^{n+1} - \{0\})/\sim$$
por la relación de equivalencia definida por : $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ si y solamente si existe $\lambda \in \bar{K}^*$ tal que $x_i = \lambda y_i$ para todo i.

  Notamos por $(x_0 : \cdots : x_n)$ la clase en $\mathbb{P}^n$ de un elemento $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$.

  Ejercicio 2. Verifica que $\sim$ es una relación de equivalencia.

- El grupo de Galois $G_K = \mathrm{Gal}(\bar{K}/K)$ actúa sobre $\mathbb{A}^n$: para $\sigma \in G_K$, definamos $(x_1, \dots, x_n)^\sigma = (x_1^\sigma, \dots, x_n^\sigma)$. De manera analoga, $G_K = \mathrm{Gal}(\bar{K}/K)$ actúa sobre $\mathbb{P}^n$. Notamos $\mathbb{A}^n(K) = \{(x_1, \dots, x_n) \in \mathbb{A}^n; x_i \in K, i = 1, \dots n\}$ y $\mathbb{P}^n(K) = \{(x_0 : \cdots : x_n) \in \mathbb{A}^n; x_i \in K, i = 0, \dots n\}$ los invariantes por la acción de G_K.

  Cuidado : $P = (y_0, \dots, y_n) \in \mathbb{P}^n(K)$ no significa que $y_i \in K$ para todo i, pero que existe $\lambda \in \bar{K}^*$ tal que $\lambda y_i \in K$ para todo i.

- Consideramos $H = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n; x_0 = 0\}$ y $U = \mathbb{P}^n \setminus H$. La aplicación
$$\phi : U \longrightarrow \mathbb{A}^n; (x_0 : \cdots : x_n) \mapsto \left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$
es bien definida, biyectiva de biyeccion reciproca $(y_1, \dots, y_n) \mapsto (1 : y_1 : \cdots : y_n)$. Ejo

  Así, embebemos una copia de $\mathbb{A}^n$ en $\mathbb{P}^n$, $\mathbb{P}^n$ es la union disjunta de $U \cong \mathbb{A}^n$ y H que llamamos entonces *hiperplano en el infinito*. Haciendo lo analogo con $x_i \neq 0$ al lugar de $x_0 \neq 0$, obtenemos varias immersines de $\mathbb{A}^n$ en $\mathbb{P}^n$ y por cada una, un hiperplano en el infinito.

  Ejemplo 1. linea proyectiva, plano proyectivo.

1.1.2. Curvas planas

- Una *curva algebraica afín plana* es el lugar C en $\mathbb{A}^2$ de los zeros de un polinomio no constante $F \in \bar{K}[x,y]$ o sea $C = V(F) = \{(x,y) \in \mathbb{A}^2; F(x,y) = 0\}$. Una *curva algebraica proyectiva plana* es el lugar $C \subset \mathbb{P}^2$ de los zeros de un polinomio *homogeno* no constante $H \in \bar{K}[X,Y,Z]$.

  Recordamos que $H \in \bar{K}[X,Y,Z]$ de grado total d es *homogeno* si para todo $\lambda \in \bar{K}$, $H(\lambda X, \lambda Y, \lambda Z) = \lambda^d H(X,Y,Z)$. De tal manera que tiene un senso de hablar del lugar de los zeros de H en $\mathbb{P}^2$.

  Ejemplo 2. lineas, conicas, cubicas

- **Puntos racionales** Si un polinomio definendo C tiene sus coeficiente en el cuerpo K, se dice que la curva es *definida sobre* K. En este caso, G_K actúa sobre los puntos de C: si $P = (x_0, y_0) \in C$ y $\sigma \in G_K$, se define $P^\sigma = (x_0^\sigma, y_0^\sigma)$. Es un punto bien definido y que cancela todavía el polinomio. (Ejo) Se puede hacer lo mismo con curvas proyectiva. Notamos $C(K)$ el conjunto de los puntos invariantes sobre esa acción, llamados *puntos K-racionales*.

  Cuidado: C no es determinada por sus puntos racionales sobre K. Ejemplo.

- **Pasar del afín al proyectivo :** el plano proyectivo $\mathbb{P}^2$ puede ser cobrido por tres abiertos afines : $U_i = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2; x_i \neq 0\} \cong \mathbb{A}^2, i = 0,1,2$, como explicado antes. Entonces, una curva proyectiva $C = V(H)$ para $H \in \bar{K}[X,Y,Z]$ homogeno no constante, es la union de tres curvas $C_i = C \cap U_i,\ i = 0,1,2$ que se indentifican con curvas afinas, una vez que hemos identificado U_i con $\mathbb{A}^2$. Mas precisamente, $C_0 \cong \{(y,z) \in \mathbb{A}^2; H(1,y,z) = 0\}$, $C_1 \cong \{(x,z) \in \mathbb{A}^2; H(x,1,z) = 0\}$, $C_2 \cong \{(x,y) \in \mathbb{A}^2; H(x,y,1) = 0\}$. Las curvas afinas C_0, C_1, C_2 son llamadas *cartas afín* de C.

  Reciprocamente, si C' es una curva afín plana dada por un polinomio $F \in \overline{K}[x,y]$ de grado d, hay una curva proyectiva C que contiene C' : la curva dada por el *homogeneizado* de F : $H(X,Y,Z) := Z^d F(X/Z, Y/Z)$. (Ejo) La curva C es llamada *completión proyectiva de* C'. La curva C' es una de las cartas afín de C: la recobrimos haciendo $C \cap U_2$. En esa carta afín C', los puntos de $C \backslash C'$ son llamados *puntos en el infinito*.

- Notamos C_F la curva (afin o proyectiva) definida por un polinomio F sin factor cuadrado.

- **Singularidades, criterio del Jacobiano** – Digamos que un punto P de una curva afín plana C_F es *singular* si el Jacobiano $\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}\right)$ se anula en P. Digamos que es un punto *singular de multiplicidad m* si m es el más grande entero tal que $\left(\frac{\partial^{(m)} F}{\partial x}, \frac{\partial^{(m)} F}{\partial y}\right)(P) = 0$. Para determinar la multiplicidad de un punto singular y las tangentes, se puede usar el desarrollo de Taylor de F en P. Digamos que un punto de una curva proyectiva C es singular si lo es para una carta afin lo conteniendo. También podemos definir la noción de multiplicidad. No depende de la carta elegida como lo muestra el ejercicio siguiente.

  Si todos los puntos de una curva son no singulares, se dice que la curva es *lisa*.

  Ejercicio 3. Sea P un punto de una curva proyectiva C_H. Muestrar que P es singular si y solamente si $H(P) = 0$, $\left(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z}\right)(P) = (0,0,0)$ si y solamente si P singular en todas las cartas afín que lo contienen.

  Ejemplo 3. $C = V(y^2 - x^3) \subset \mathbb{A}^2$ (punta) ; $C = C(y^2 - x^3 - x^2) \subset \mathbb{A}^2$ (nodo)

  Ejemplo 4. $C = V(y^2 - x^3 - ax - b) \subset \mathbb{A}^2$, $a, b \in K, \mathrm{char}(K) \neq 2,3$. Demuestramos que C lisa si y solamente si $x^3 + ax + b$ no tiene raíz doble o sea $4a^3 + 27b^2 \neq 0$. (Ejo)

1.2. Curvas elípticas : propiedades geometricas

En esa sección, de nuevo consideremos K un cuerpo y $\bar{K}$ una clausura algebraica de K.

1.2.1. Curvas definidas por una ecuación de Weierstrass

- Sea C una curva proyectiva plana definida por una *ecuación de Weierstrass*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \overline{K}, i = 1, \dots, 6) \tag{1.1}$$

o sea, más correctamente, por la ecuación homogena asociada $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. Eso significa que la primera ecuación era la ecuación de una carta afín: la carta $C \cap U_2$. En esa carta, los puntos en el infinito son $C \cap \{(X : Y : Z); Z = 0\} = \{(0 : 1 : 0\}$, hay un solo punto en el infinito.

- Si $a_i \in K$ digamos que C es *definida sobre* K.

- Cuando K es de característica $\neq 2$, con el cambio de variables $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, obtenemos una ecuación más simple para C (Ejo) :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \quad \text{donde} \quad b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6.$$

Cuando $\mathrm{char}(K) \neq 2, 3$, podemos también eliminar el termine x^2 con el cambio de variables $(x, y) \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, obteniendo una ecuación de la forma siguiente, dicha *ecuación de Weierstrass reducida*:

$$y^2 = x^3 - 27c_4x - 54c_6 \quad \text{donde} \quad c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Tales cambios de variables respectan la forma de la ecuación y dejan invariable el punto en el infinito si y solamente si son de la forma $(x, y) \mapsto (u^2x+r, u^3y+u^2sx+t)$ donde $u, r, s, t \in \overline{K}, u \neq 0$. Esos cambios son dechos *admisibles*.

- Definamos el *discriminante de la ecuación*(1.1) por

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6 + 9b_2b_4b_6, \tag{1.2}$$

donde $b_i, i = 2, 4, 6$ son como antes y $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

Los cambios admisibles multiplican Δ por u^{12}.

Ejemplo 5. El discriminante de una ecuación de Weierstrass reducida $y^2 = x^3 + Ax + B$ es $\Delta = -16(4A^3 + 27B^2)$.

Se puede ver la singularidades de la curva C sobre Δ y c_4 :

Proposición 1. Sea C dada por una ecuación de Weierstrass (1.1). La curva C es no singular si y solamente si $\Delta \neq 0$. Si no, C tiene solo un punto singular que es un nodo si ($\Delta = 0$ y) $c_4 \neq 0$ y una punta si ($\Delta = 0$ y) $c_4 = 0$.

Demostración. □

1.2.2. Curvas elípticas : definiciones

Definición 1. Una *curva elíptica* (E, O) *sobre* K es el dato de una curva E proyectiva plana no singular, definida sobre K, de *genero* 1, dota de un punto racional $O \in E(K)$. Toda tal curva puede ser definida por una ecuación de Weierstrass (1.1) con discriminante no nulo.

Algunas explicaciones siguen :

- **Genero geometrico**. No vamos a definirlo esactamente pero es un invariante geometrico utíl para clasificar las curvas planas. Por ejemplo, por una curva proyectiva plana no singular de grado d el genero geometrico es igual al genero aritmético, o sea:

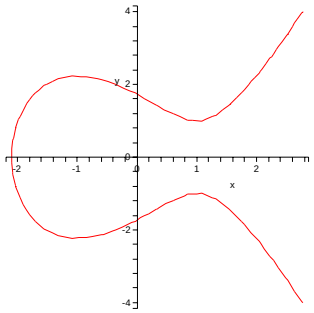
$$g = \frac{(d-1)(d-2)}{2}.$$

(Por una curva singular hay que agregar a eso cuantidades dependente de las singularidades).

- Así se ve que una curva definida por una ecuación de Weierstrass (1.1) con discriminante $\Delta \neq 0$ (entonces lisa) y definida por una ecuación de Weierstrass (1.1) dota de su punto en el infinito $O = (0 : 1 : 0)$, es una curva elíptica definida sobre todo cuerpo conteniendo los coeficientes de la ecuación. Ejo

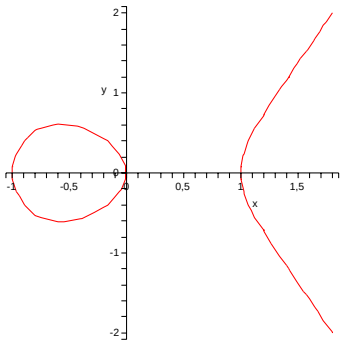
Reciprocamente, se puede demostrar que toda curva elíptica puede ser definida por una ecuación de Weierstrass (con discriminante $\Delta \neq 0$). Eso usa el teorema de Riemann-Roch y lo admitamos.

Ejemplo 6. Los puntos $\mathbb{R}$-racionales de la curva elíptica $E : y^2 = x^3 - 3x + 3$ son dados por el dibujo siguiente



donde hay que pensar a O como un punto en "el infinito".

Los puntos $\mathbb{R}$-racionales de $E : y^2 = x^3 + x$ son dados por



1.2.3. Ley de grupo

- **Multiplicidad de intersección con una recta** : Sea $L : aX + bY + cZ = 0$ una recta de $\mathbb{P}^2$, C_F una curva proyectiva plana y $P \in C_F \cap L \neq \emptyset$. Se puede suponer que $P = (x_0 : y_0 : z_0)$ es en la carta afín U_2 o sea $z_0 \neq 0$ (si no adaptar el discurso). Sea $f(x, y) = F(x, y, 1)$. La recta afín

$L \cap U_2$ se puede parametrizar por $x(t) = bt + x_0, y(t) = -at + y_0$. La multiplicidad del zero $t = 0$ en el polinomio $f(x(t), y(t))$ en t se llama *multiplicidad de intersección de L con C_F en P* con la convención que la multiplicidad es infinita si el polinomio es nulo (i. e. $L \subset C_F$).

El siguiente teorema es un caso particular del teorema de Bézout geometrico :

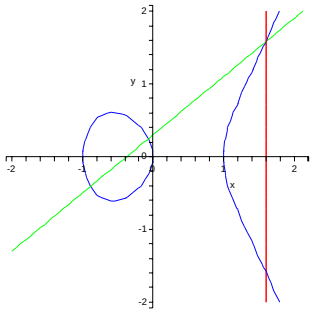
Teorema 1 (Bézout)**.** Una recta proyectiva intersecta una curva proyectiva plana de grado m en m puntos ($\overline{K}$-racionales) contados con multiplicidades. Si la curva proyectiva es de grado 3 y definida sobre K y si dos de los puntos de intersección son K-racionales, entonces el tercero es también K-racional.

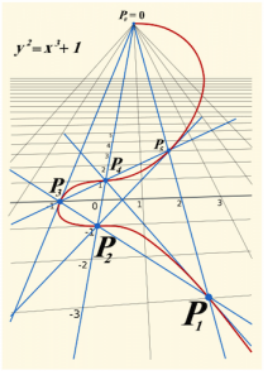
Ejercicio 4. 1. Demostrar que la multiplicidad de intersección de una recta L con una curva C en un punto P es superior a la multiplicidad de P sobre C.

2. Demostrar que una cubica proyectiva plana tiene al maximum un punto singular y que es un punto doble.

3. Demostrar, usando el teorema de Bézout, que toda curva proyectiva plana no singular es irreductible.

- Sea E una curva elíptica sobre un cuerpo K. Definimos sobre E una ley de composición interna de tal modo : sean $P, Q \in E$ y $L \subset \mathbb{P}^2$ la linea pasando por P y Q (la tangente a E si $P = Q$). Como E es una cubica, el teorema de Bézout demuestra que L intersecta E en un tercero punto R (donde contamos las multiplicidades). Sea L' la linea pasando por R y O. Notamos $P + Q$ el tercero punto donde L' corta E.





Proposición 2. La ley de composición precedente pone sobre E una estructura de grupo abeliano de elemento neutro O.

Si elegimos un otro punto base O' la ley $+'$ obtenida verifica $P +' Q = P + Q - O'$ y las estructuras de grupos $E, +'$ y $E, +$ son isomorficas (via $P \mapsto P - O'$). Ejo

Demostración. (Admitimos la asociatividad). □

- Hay formulas explicitas para la ley de grupo (ver [16]). Por ejemplo, si E tiene ecuación (1.1) y si $P = (x : y : 1)$, entonces $-P = (x, -y - a_1 x - a_3)$ y (*formula de duplicación*)

$$x(P + P) = x([2]P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}. \tag{1.3}$$

1.2.4. Morfismos y isogenias

- **Funciones regulares.**– Sea C una curva afín plana. Una aplicación $f : C \longrightarrow \mathbb{A}^1$ es una *función regular* si proviene de un polinomio o sea $f = ((a,b) \in C \mapsto F(a,b))$ por $F \in \overline{K}[X,Y]$. El conjunto de las funciones regulares sobre C es un anillo que notamos $\overline{K}[C]$. Si C es además irreductible, o sea no contiene una curva estricta, entonces $\overline{K}[C]$ es un anillo integral. Notamos $\overline{K}(C) = \mathrm{Frac}(\overline{K}[C])$ el *cuerpo de las funciones racionales de* C. Una función $f \in \overline{K}(C)$ es dicha *regular en un punto* $P \in C$ si existen $g, h \in \overline{K}[C]$ tal que $h(P) \neq 0$ y $f = g/h$. Si $f \in \overline{K}(C)$ es regular en todos los puntos de C entonces $f \in \overline{K}[C]$ (entonces la terminología no causa confusión).

  Para una curva proyectiva plana C, definamos el *cuerpo de las funciones racionales* como el cuerpo de las funciones de una carta afín de C. Eso no depiende de la carta elegida y lo notamos $\overline{K}(C)$. (Ejo) Una función es regular en P si lo es en una carta afín conteniendo P. Se puede mostrar que si C es una curva proyectiva plana irreductible, toda función $f \in \overline{K}(C)$ regular sobre C es constante.

- **Morfismos de curvas proyectivas** Sean C y $C' = C_H$ dos curvas proyectivas planas con C irreductible. Una *aplicación racional desde* C *hacia* C' es el dato de $\phi = (f_0 : f_1 : f_2)$ con $f_i \in \overline{K}(C)$ no todas cero y tal que $H(f_0, f_1, f_2) = 0$. Digamos que es una aplicación *regular en* P si existe $g \in \overline{K}(C)^\times$ tal que gf_i regular en P por $i = 0, 1, 2$ no todas nulas en P. Un *morfismo* es una aplicación racional que es regular en todos puntos. Si C es lisa, toda aplicación racional desde C es un morfismo.

- j**-invariante de una curva elíptica.**– Sea E una curva elíptica sobre K dada por una ecuación de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \overline{K}, i = 1, \ldots, 6)$$

  notamos $j = j(E) = \frac{c_4^3}{\Delta}$ el *j-invariante de* E (con la notación ya introducida para c_4). En particular, si E es dada por una ecuación reducida $y^2 = x^3 + Ax + B$, entonces $j(E) = -1728(4A)^3/\Delta$.

Proposición 3. Dos curvas elípticas sobre K son isomorfas sobre $\bar{K}$ si y solamente si tienen el mismo j-invariante. Para $j_0 \in \bar{K}$ fijado, existe a menos de $\bar{K}$-isomorfismo, una única curva elíptica (definida sobre $K(j_0)$) con j-invariante j_0.

- **Isogenias.**– Un aplicacion $E_1 \longrightarrow E_2$ es una *isogenia* si es un morfismo tal que $\phi(O) = O$. Notamos $\mathrm{Hom}(E_1, E_2)$ al conjunto de las isogenias desde E_1 hacia E_2 y $\mathrm{End}(E)$ el conjunto de los endomorfismos de E o sea de las isogenias $E \longrightarrow E$.

  Una isogenia no constante es suriectiva. Una isogenia $\phi : E_1 \longrightarrow E_2$ induce una inieccion de cuerpos de funciones $\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1)$. Llamamos *grado* de ϕ el grado de la extension $\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$. Digamos que ϕ es *separable* (resp. *inseparable*, resp. *puramente inseparable*) si la extensión correspondiente lo es.

Ejemplo 7 (Endomorfismo de Frobenius)**.** Sea E definida sobre $\mathbb{F}_q$. La aplicación definida por $\phi(O) = O$ y $\varphi : (x, y) \mapsto (x^q, y^q)$ para todo punto $P = (x : y : 1) \neq O$ es un endomorfismo de E llamado *endomorfismo de Frobenius*. Es una isogenia inseparable de grado q. Usando las formulas explicitas por la ley de grupo, se puede ver que es un endomorfismo de grupo. (Ejo) Mas generalmente, tenemos el teorema siguiente.

Teorema 2. Sea $\varphi \in \mathrm{Hom}(E_1, E_2)$ una isogenia de curvas elípticas. Entonces para todos $P, Q \in E_1$, $\varphi(P+Q) = \varphi(P) + \varphi(Q)$. El núcleo de φ es un subgrupo de E_1 de orden el grado separable de φ. Reciprocamente, para todo subgrupo C de E_1 existe una única cuva elíptica E_2 y una isogenía separable $\phi : E_1 \longrightarrow E_2$ de núcleo C. Notamos $E_2 := E_1/C$.

Ejemplo 8 (multiplicación por un entero)**.** Sea E una curva elíptica. Se define de manera natural la *la multiplicación por un entero* $m \in \mathbb{Z}$ denotada $[m] : E \longrightarrow E$. Notamos $E[m]$ el núcleo de $[m]$. Se llama *el conjunto de los puntos de m-torsión* de E. Y notamos E_{tors} *el conjunto de los puntos de torsión* E o sea $E_{tors} = \bigcup_{m\geq 1} E[m]$. Si E es definida sobre K, $E_{tors}(K)$ es el subgrupo de los puntos de orden finito en $E(K)$.

Teorema 3. Sea E una curva elíptica sobre un cuerpo K de característica ℓ.

1. Si $m \neq 0$, $[m]$ es una isognia no constante de grado m^2.
2. Si $\ell = 0$ o $(\ell, m) = 1$, $[m]$ es separable y tenemos $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$;
3. Si $\ell \neq 0$, tenemos $E[\ell^e] = \{O\}$ para todo entero $e \geq 1$, o $E[\ell^e] \cong \mathbb{Z}/\ell^e\mathbb{Z}$ para todo entero $e \geq 1$.

Teorema 4 (isogenia dual)**.** Para toda isogenia no constante $\phi : E_1 \longrightarrow E_2$ de grado m, existe una unica isogenia $\check{\phi} : E_2 \longrightarrow E_1$ dicha *isogenia dual de* ϕ, tal que $\check{\phi} \circ \phi = [m]$.

1.3. Puntos racionales de una curva elíptica - hechos

Sea E una curva elíptica sobre un cuerpo K. La estructura del conjunto de los puntos K-racionales $E(K)$ depende mucho de la natura de K. Nos interesa particularmente el caso donde K es un cuerpo de números (o sea una extensión finita de $\mathbb{Q}$) o un cuerpo finito.

1.3.1. Curvas elípticas sobre $\mathbb{C}$

Cuando $K = \mathbb{C}$, $E(\mathbb{C})$ tiene una estructura de variedad analítica isomorfa a un toro

Teorema 5 (teoréma de uniformisación)**.** Sea E una curva elíptica sobre $\mathbb{C}$. Existe un red $\Lambda \subset \mathbb{C}$ unico a menos de homotetia y un isomorfismo analítico complejo $\alpha : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ de grupos de Lie complejos.

Podemos dar explicitamente el isomorfismo α usando las *funciones de Weierstrass* pero no detallamos este facto (cf [16] VI.5).

1.3.2. Curvas elípticas sobre un cuerpo finito

Sea $K = \mathbb{F}_q$ "el" cuerpo finito con q elementos donde $q = p^k$, p un número primo.

Teorema 6 (Hasse)**.** Para todo $m \geq 1$, el grupo $E(\mathbb{F}_{q^m})$ es un grupo abeliano finito y

$$\sharp E(F_{q^m}) = q^m + 1 - \alpha^m - \beta^m \quad \text{con} \quad |\alpha| = |\beta| = \sqrt{q}.$$

En particular,

$$|\sharp E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Recordamos que $E[p^e]$ es zero para todo $e \geq 1$, o cíclico de orden p^e para todo $e \geq 1$ (cf teorema 3). En el primer caso, digamos que la curva elíptica E es *supersingular* sobre $\mathbb{F}_q$. En el segundo caso, digamos que es *ordinaria*.

Demostración. □

1.3.3. Curvas elípticas sobre un cuerpo local

Si E es una curva elíptica sobre un cuerpo p-adico K (por ejemplo $K = \mathbb{Q}_p$), entonces vedremos que $E(\mathbb{Q}_p)$ tiene una estructura de grupo de Lie p-adico compacto : es una extension de un grupo finito por un pro-p-grupo $E_1(K)$. (cf Seccion 1.4).

1.3.4. Curvas elípticas sobre un cuerpo de números

Teorema 7 (Mordell-Weil)**.** Sea E una curva elíptica sobre un cuerpo de números K. El grupo $E(K)$, dicho *grupo de Mordell-Weil*, es un grupo abeliano de tipo finito, es decir hay un isomorfismo de grupos

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$$

con $r \in \mathbb{Z}_{\geq 0}$ y $E(K)_{tors}$ el grupo formado de los puntos de torsión de $E(K)$. En particular $E(K)_{tors}$ es un grupo finito.

La prueba de este teorema es basada sobre el *método de descenso* de Fermat. Pueden referirse a [2] 1.2 por una breve prueba de este facto o a [16] ch. VIII por una prueba detallada y completa. Ver también la seccion 1.6 de esas notas.

Se puede determinar bastante facilmente el grupo de torsión $E(K)_{tors}$ de una dada curva elíptica. Ver Sección 3. En cambio, el *rang* r es mucho más misterioso y es el objecto de varias conyecturas como por aquella de Birch et Swinnerton-Dyer (3) que lo une al comportamento de una cierta función de una variada compleja asociada a la curva elíptica llamada *función L de Hasse-Weil* (cf clases de Marc Hindry).

1.4. Curvas elípticas sobre un cuerpo local y reducción

En esta sección, K es un cuerpo local completo por una valuación discreta v, por ejemplo $K = \mathbb{Q}_p$ o una extensión finita de $\mathbb{Q}_p$. Notamos R su annillo de valuaciíon discreta, k el cuerpo residual, p su caracteri'stica y $\pi \in \mathcal{O}_K$ una uniformisante. (Por ejemplo, $K = \mathbb{Q}_p, R = \mathbb{Z}_p, k = \mathbb{F}_p, \pi = p$).

1.4.1. Reducción de una curva elíptica

- **Ecuación minimal.**– Sea E una curva elíptica dada por una ecuación de Weierstrass con coeficientes en K:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K, i = 1, \ldots, 6) \tag{1.4}$$

Un cambio de variables admisible $(x', y') = (u^{-2}x, u^{-3}y)$ cambia a_i en $a'_i = u^i a_i$ y Δ en $\Delta' = u^{-12}\Delta$. Si tomamos por u una buena potenza de π que mata los denominadores de los a_i, obtenemos una nueva ecuación con coeficientes $a_i \in R$ para todo i. (Basta elegir $v(u) \geq -\min(v(a_i)/i)$ Ejo). Y en este caso, el nuevo discriminante es también en R, o sea $v(\Delta) \geq 0$. El conjunto de los valuaciones $v(\Delta)$ de discriminante de ecuaciónes de Weiestrass de E con coeficientes en R es un conjunto no vacio de $\mathbb{Z}_{\geq 0}$. Entonces este conjunto admite un minimo : una ecuación es dicha *ecuación de Weierstrass minimal de E en π* si es una ecuación (1.4) con $a_i \in R, i = 2, 4, 6$ y $v(\Delta)$ minimal para todas ecuaciónes con coeficientes en R.

Ejercicio 5. 1. Demostrar que si la ecuación tiene coeficientes en R y $v(\Delta) < 12$ entonces la ecuación ya es minimal. (Lo mismo succede si $v(c_4) < 4$ o si $v(c_6) < 6$.)

2. Demostrar que si $p \neq 2, 3$ y la ecuación es minimal entonces $v(c_4) < 4$ o $v(\Delta) < 12$.

Proposición 4. Una ecuación de Weiestrass minimal para E sobre K es unica a menos de un cambio admisible de la forma $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ con $u \in R^\times$ y $r, s, t \in R$.

Demostración. □

- **Reducción.**– Sea E una curva elíptica sobre K con ecuación minimal

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in R, i = 1, \dots, 6).$$

Reduciendo los coeficientes a_i modulo π, obtenemos una ecuación de Weiestrass sobre k. La curva definida por ese ecuación es una cubica (posiblemente singular) llamada *reducción modulo π de E* y notada $\widetilde{E}$. La proposición 4 muestra que la ecuación obtenida por reducción es unica a menos de un cambio de variables admisible par las ecuaciones de Weierstrass sobre k.

La curva $\bar{E}$ sobre k es de uno de los tipos siguientes :

1. $\widetilde{E}$ es una curva elíptica sobre k : eso cuando $\Delta \in \mathbb{R}^\times$. Digamos que E tiene *buena reducción modulo π*;
2. $\widetilde{E}$ tiene una singularidad que es una punta : digamos que E *tiene mala reducción aditiva* modulo π; Eso cuando $\Delta \equiv \pmod{\pi}$ y $c_4 \in R^\times$.
3. $\widetilde{E}$ tiene una singularidad que es un nodo : digamos que E *tiene mala reducción multiplicativa* modulo π. Eso cuando $\Delta \equiv c_4 \equiv 0 \pmod{\pi}$.

En el caso de reducción multiplicativa, digamos además que la reducción es *desplegada* si las pendientes de las tangentes en el punto singular son en k y *non desplegada* de otra manera.

1.4.2. Aplicación de reducción

Sean E una curva elíptica definida sobre K y $\widetilde{E}$ su reducción modulo π, quizas singular.

- Si $P = (x : y : z) \in \mathbb{P}^2(K)$, existe $\lambda \in K^\times$, tal que $\lambda x, \lambda y, \lambda z$ sean en R y al meno uno de esos sea en $R^\times$. Entonces podemos definir $\widetilde{P} := (\lambda x \pmod{\pi} : \lambda y \pmod{\pi} : \lambda z \pmod{\pi}) \in \mathbb{P}^2(k)$. Eso define una aplicación dicha *aplicación de reducción* $E(K) \longrightarrow \widetilde{E}(k)$.
- La ley de composición cuerdas/tangente dota el sub-conjunto $\widetilde{E}_{ns}$ de los puntos no singular de $\widetilde{E}$ de una ley de grupo abeliano.

Proposición 5. La aplicación de reducción define una secuencia exacta de grupos abelianos

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E}_{ns}(k) \longrightarrow 0$$

donde $E_0(K) = \{P \in E(K); \widetilde{P} \in \widetilde{E}_{ns}(k)\}$ y $E_1(K)$ el núcleo de la aplicación de reducción.

Desde esa proposición y una filtración exhaustiva de $E(K)$ se deduce la proposición siguiente que estará útil a la vez para determinar los puntos de torsion y para demostrar el teorema de Mordell-Weil :

Teorema 8. Sea E una curva elíptica sobre K y m un entero primero a $p = \mathrm{char}(k)$.

1. $E_1(K)[m] = \{O\}$;
2. Si E tiene buena reducción entonces la aplicación de reducción $E(K)[m] \longrightarrow \widetilde{E}(k)$ es iniectiva.

Observación 1. Cuando $K = \mathbb{Q}_p$, las propiedades precedentes son verificadas para todo entero m. Entonces $E_1(\mathbb{Q}_p)_{tors} = \{O\}$ y si E tiene buena reducción entonces $E(\mathbb{Q})_{tors} \hookrightarrow \widetilde{E}(\mathbb{F}_p)$.

1.5. Torsión de las curvas elípticas sobre un cuerpo de números

- Se puede usar la proposición 8 para determinar los puntos de torsion de las curvas elípticas sobre un cuerpo de números. Sea E una curva elíptica sobre un cuerpo de números K. Notamos v una valuacion discreta de K y K_v el cuerpo completo asociado. Entonces $E(K) \subset E(K_v)$. Si encontramos una ecuación minimal de E sobre K_v y reduciamos, podemos aplicar al proposición a E/K_v. Haciendo eso en varios numeros de valuacion permite de determinar la torsion.

  Ejemplo 9. Sea $E/\mathbb{Q} : y^2 + y = x^3 - x + 1$ de discriminante $\Delta = -13{,}47$. Como $v_2(\Delta) = 0 < 12$, la ecuación es minimal en 2 (y en todo número primo) y $\widetilde{E}$ mód 2 es no singular de ecuación $y^2 + y = x^3 + x + 1$. Tenemos $\widetilde{E}(\mathbb{F}_2) = \{0\}$ entonces $E(\mathbb{Q})[m] = \{O\}$ para todo $m \neq 2$. Además $E(\mathbb{Q})[2] = \{O\}$. (ver la formula de duplicacion). Entonces $E(\mathbb{Q})_{tors} = 0$.

- De la proposición 8 se deduce también :

  Teorema 9. Sea E una curva elíptica sobre un cuerpo de números K dada por una ecuación (1.1) con a_i en el anillo de enteros R de K. Sea $P \in E(K)$ de orden exactamente $m \geq 2$.

  1. Si m no es una potenza de un primo, entonces $x(P), y(P)$ son en R.
  2. Si $m = p^r$ es una potenza de un primo p, entonces para todo $v \in M_K$ finita,

  $$ord_v(x(P)) \geq -2r_v \quad \text{y} \quad ord_v(y(P)) \geq -3r_v$$

  donde $r_v = \left[\frac{ord_v(p)}{p^r - p^{r-1}}\right]$. En particular, cuando $ord_v(p) = 0$, $x(P), y(P)$ son v-enteros.

  Cuando especializamos a $K = \mathbb{Q}$ podemos decir un poco mejor :

  Teorema 10 (Lutz-Nagell)**.** Sea $E/\mathbb{Q}$ una curva elíptica con una ecuación de Weierstrass $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$ y sea $P \in E(\mathbb{Q})$ de orden finito, $P \neq O$. Entonces

  1. $x(P), y(P) \in \mathbb{Z}$
  2. $y(P) = 0$ or $y(P)^2 \mid 4A^3 + 27B^2$.

  Cuidado : la reciproca es falsa.

  Demostración. Demostración sobre $\mathbb{Q}_p$. (usa el teorema 8) □

- Eso demuestra en particular que $E(\mathbb{Q})_{tors}$ es un grupo finito y da un algoritmo para determinarlo : hay una lista finita de $y(P)$ verificando a,b, entonces una lista finita $\mathcal{L}$ de puntos posibles para la torsion. Para $P \in \mathcal{L}$, es fácil de ver cuando P no es de torsion : porque en este caso, existe $n \in \mathbb{Z}$ tal que nP no es en $\mathcal{L}$. Entonces, elegimos $P \in \mathcal{L}$, calculamos $P, [2]P, [3]P, \ldots [n]P$ hasta obtener un punto a fuera de $\mathcal{L}$ o obtener $[n]P = O$. En realidad, el teorema de Mazur 11 muestra que $n \leq 12$.

  Teorema 11 (Mazur)**.** Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})_{tors}$ es uno de los grupos siguientes

  $$\mathbb{Z}/N\mathbb{Z},\ 1 \leq N \leq 10, N = 12 \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}\ 1 \leq N \leq 4.$$

  Además, cada de esos grupos es realizado como grupo de torsion de una curva elíptica sobre $\mathbb{Q}$.

Y mejor: hay una infinidad de curvas realizando cada grupo (Kubert) parametrizadas por un parametro.

Cuestión : Que tal cuando $[K : \mathbb{Q}] > 1$? Hay un resultado analogo cuando $[K : \mathbb{Q}] = 2$ (Kamienny, Kenku, Momose). Pero ya cuando $[K : \mathbb{Q}] = 3$ la lista de los grupos posibles no es completa. El teorema de Kamienny cuando K es de grado 2 es uniforme : existe una cota para el tamaño de la torsion de todas las curvas elípticas sobre une cuerpo cuadratico. Eso se generaliza por un cuerpo de números :

Teorema 12 (Merel)**.** Para todo $d \geq 1$ existe $B(d)$ tal que para toda curva elíptica sobre un cuerpo de números K de grado d sobre $\mathbb{Q}$, $|E(K)_{tors}| \leq B(d)$.

1.6. "Demostración" del teorema de Mordell (ideas esenciáles)

Aquí vamos a dar los pasos clave de la demostración del teorema 7 sobre $\mathbb{Q}$ (teorema de Mordell). Hay esencialmente dos pasos : (E una curva elíptica sobre $\mathbb{Q}$)

1. demostrar que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. Vamos a demostrar más : $E(\mathbb{Q})/mE(\mathbb{Q})$ es finito (Teorema débil de Mordell).
2. descenso : approximadamente demostreremos que no se puede "dividir " indefinimente un punto racional por 2, porque, como lo vamos a ver, la division por 2 va diminuyendo la *altura* del punto y porque hay un numéro finito de puntos de pequeña altura.

1.6.1. Teorema débil de Mordell

Teorema 13. Sea E una curva elíptica sobre un cuerpo de números K. Para todo entero $m \geq 2$, $E(K)/mE(K)$ es finito.

Estamos interesados a enunciar ese teorema para todo cuerpo de números porque el primer paso de la demostración es de agrandar el cuerpo hasta que contenga los coordenadas de los puntos de m-torsión :

Paso 1.– El siguiente lema permite de agrandar K hasta que $E[m] \subset E(K)$.

Lema 1. Si L/K es galoisiana finita y si $E(L)/mE(L)$ es finito, entonces $E(K)/mE(K)$ es finito.

Paso 2.– Supongamos ahora que K es tal que $E[m] \subset E(K)$. Se define un acoplamiento dicho *acoplamiento de Kummer* $\lambda : E(K) \times G_K \longrightarrow E[m]$.

Lema 2. Sea $L = K([m]^{-1}E(K))$ el compositum de los cuerpos donde son definidos los puntos Q tal que $mQ \in E(K)$. El acoplamiento de Kummer induce un acoplamiento perfecto

$$\lambda' : E(K)/mE(K) \times \mathrm{Gal}(L/K) \longrightarrow E[m].$$

De este lema, deducimos que $E(K)/mE(K)$ es finito si y solamente si L/K es una extensión finita.

Paso 3.– Demostramos que los cuerpos $K(Q)$ con $Q \in [m]^{-1}E(K)$ son no ramificados afuera de un conjunto finito de plazas de K. Un teorema de Minkowski muestra entonces que hay un número finito de tales extensiones $K(Q)$ de K y deducimos de esto que L/K es finita.

1.6.2. Descenso

- Vamos a definir una noción de altura ingenua que depende de la ecuación de Weierstrass. Eso basta par demostrar el teorema de Mordell. Para demostrar Mordell-Weill se necesita una noción de altura independiente de la ecuación : la altura de Neron-Tate que estará definida por Marc Hindry.

Definición 2 (Altura de un racional)**.** Sea $x = u/v$ con $u, v \in \mathbb{Z}$ primos entre sí, se define $H(x) = \mathrm{Max}(|u|, |v|)$ y $h(x) = \log(H(x)) \geq 0$.

Sea $E/\mathbb{Q}$ una curva elíptica dada por una ecuación reducida

$$y^2 = x^3 + Ax + B \quad \text{con} \quad A, B \in \mathbb{Z}. \tag{1.5}$$

Definición 3 (Altura ingenua)**.** La *altura sobre E relativa a la ecuación* (1.5) es la función

$$\begin{array}{rccc} h: & E(\mathbb{Q}) & \longrightarrow & \mathbb{R} \\ & O \neq P = (x,y) & \mapsto & h(x) \\ & O & \mapsto & 0. \end{array}$$

La altura de una curva elíptica $E/\mathbb{Q}$ tiene las siguientes propiedades :

Proposición 6. 1. Para toda constante C, el conjunto $\{P \in E(\mathbb{Q}); h(P) \leq C\}$ es finito.

2. Sea $P_0 \in E(\mathbb{Q})$. Existe C tal que para todo $P \in E(\mathbb{Q})$, $h(P + P_0) \leq 2h(P) + C$.

3. Existe C' tal que para todo $P \in E(\mathbb{Q})$, $h([2]P) \geq 4h(P) - C'$.

Demostración. □

- **Descenso - Fin de la demostración del Teorema de Mordell.**– Por el teorema 13 $E(\mathbb{Q})/2E(\mathbb{Q})$ es un grupo abeliano finito. Sean $\{Q_1, \ldots, Q_s\}$ un sistemo finito de representantes de $E(\mathbb{Q})/2E(\mathbb{Q})$ en $E(\mathbb{Q})$.

Consideremos $P \in E(\mathbb{Q})$. Existen $i_1 \in \{1, \ldots, s\}$ y $P_1 \in E(\mathbb{Q})$ tal que $P = Q_{i_1} + 2P_1$. Cómo $P_1 \in E(\mathbb{Q})$ podemos repetir el proceso, construyendo por recurrencia dos secuencias $(i_j)_{j\geq 1} \subset \{1, \ldots, s\}^{\mathbb{Z}_{\geq 0}}$ y $(P_j)_{j\geq 1} \subset E(\mathbb{Q})^{\mathbb{Z}_{\geq 0}}$ tal que,

$$P_j = Q_{i_j} + 2P_{j+1} \quad (j \geq 1).$$

Desde la proposición 6, puntos 3. y 2. con $P_0 = -Q_{j+1}$, se deduce que para todo $j \geq 1$, existen constantes C_j y C' tal que

$$\begin{array}{rcl} h(P_{j+1}) & \leq & \frac{1}{4}\left(2h(P_j) + C_j + C'\right) \\ & \leq & \frac{1}{4}\left(2h(P_j) + C + C'\right) \end{array}$$

con $C = \mathrm{Max}(C_j)$.

Deducimos, por recurrencia, que para todo $j \geq 1$,

$$h(P_j) \leq \frac{1}{2^j} h(P) + \frac{C + C'}{2}.$$

Entonces, existen C'' y N tales que para todo $j > N$, $h(P_j) \leq C''$. Ahora

$$P = Q_{i_1} + 2Q_{i_2} + \cdots + 2^N Q_{i_N} + 2^{N+1} P_{N+1}$$

es en el grupo generado por $Q_1, \ldots, Q_s$ y el conjunto $\{Q \in E(\mathbb{Q}); h(Q) \leq C''\}$ que es finito por Proposición 6 1. Así termina la demostración. □

Capítulo 2

Funciones zeta y L clasicas

2.1. Generadores del grupo de Mordell-Weil

Sabemos que el grupo de Mordell-Weil de una curva elíptica $E/\mathbb{Q}$ es de la forma

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}\,P_1 \oplus \cdots \oplus \mathbb{Z}\,P_r.$$

Hemos visto que el subgrupo de los puntos de torsión es fácil de calcular y, además, es bien comprendido del punto de vista teórico. La parte de orden infinito de $E(\mathbb{Q})$ es mucho más misteriosa. Antes de hablar de funciónes zeta y L, queremos motivar la introducción de estas funcionespor la búsqueda de respuestas a las preguntas :

1. ¿Hay un método para calcular el rango $r = \text{rango}\, E(\mathbb{Q})$?
2. ¿Hay una interpretación del rango $r = \text{rango}\, E(\mathbb{Q})$?
3. ¿Hay una cota superior del tamaño de generadores del grupo de Mordell-Weil?

La confesión siguiente hace humilde : nadie sabe responder de manera matemáticamente completa! Es decir, si bien sabemos calcular el grupo de Mordell-Weil para muchos ejemplos, siempre se necesita un poquito de suerte ... Sin embargo existe una vía – todavía conjetural – que necesita la introducción de objetos analíticos y que vamos a desarrollar en esta segunda parte del curso.

Ejercicio 6. Consideramos la curva elíptica de ecuación de Weierstrass

$$y^2 + y = x^3 - x.$$

1. Demostrar que la curva tiene buena reducción en todo p, salvo $p = 37$
2. Demostrar que $E(\mathbb{F}_2) \cong \mathbb{Z}/5\mathbb{Z}$ y $E(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$.
3. Concluir que $E(\mathbb{Q})_{\text{tor}} = \{0_E\}$ y que el punto $P := (0, 0)$ es de orden infinito.

(Nota : en verdad, el rango es igual a 1 y el punto P es un generador del grupo $E(\mathbb{Q})$, es decir $E(\mathbb{Q}) = \mathbb{Z}.P$, pero eso es más difícil de demostrar.)

Ejercicio 7. La cúbica de Fermat, dada en coordenadas proyectivas por $X^3 + Y^3 + Z^3 = 0$ es una curva elíptica, una vez que se escoge el origen, por ejemplo $0_E = (0, 1, -1)$.

1. Mostrar que los tres puntos 0_E, $P = (1, 0, -1)$ y $Q = (1, -1, 0)$ forman un subgrupo de $E(\mathbb{Q})$ isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

2. (Teorema de Fermat por $n = 3$) Mostrar que $E(\mathbb{Q}) = \{0_E, P, Q\}$.
3. Escribir la curva de Fermat en forma minimal de Weierstrass.
   [Indicación : poniendo $X = 3x/y$, con $Y = (y-9)/y$ verificar que $y^2 - 9y = x^3 - 27$.]
4. Verificar en ambos modelos que la curva tiene buena reducción fuera de $p = 3$.

Empezamos por dar una formulación más intrínseca de las preguntas. Recordamos dos propiedades importantes de la altura de puntos racionales (vistas en la subsección 1.6.2)

$$-c_1 \leq h(2P) - 4h(P) \leq c_1 \tag{2.1}$$

$$-c_2 \leq h(P+Q) + h(P-Q) - 2h(P) - 2h(Q) \leq c_2 \tag{2.2}$$

Ejercicio 8. Demostrar las formulas precedentes utilizando las formulas geométricas para la curva elíptica de ecuación $y^2 = x^3 + ax + b$ (ver en el capítulo 1, 1.3) que se podra demostrar:

$$x([2]P) = \frac{x(P)^4 - 2ax(P)^2 - 8bx(P) + a^2}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

$$x(P+Q) + x(P-Q) = \frac{2(x(P) + x(Q)(a + x(P)x(Q) + 4b)}{(x(P) - x(Q)))^2}$$

$$x(P+Q)x(P-Q) = \frac{(x(P)x(Q) - a)^2 - 4b(x(P) + x(Q))}{(x(P) - x(Q)))^2}$$

y las disigualdades aritméticas, para$\alpha, \beta \in \mathbb{Q}$:

$$\frac{1}{2}H(\alpha)H(\beta) \leq H(1, \alpha+\beta, \alpha\beta) \leq 2H(\alpha)H(\beta)$$

[Para $r, s \in \mathbb{Q}$, se escribe $(1, r, s) \sim (a, b, c)$ en $\mathbb{P}^2$ con a, b, c enteros coprimos y se define $H(1, r, s) = \text{máx}(|a|, |b|, |c|)$.]

Utilizaremos el lema elemental siguiente:

Lema 3. (Tate) Sea S un conjunto, $\alpha > 1$ y dos mapas $h : S \to \mathbb{R}$ y $\phi : S \to S$ tales que $|h(\phi(x)) - \alpha h(x)| \leq c_1$ entonces la succesión $\alpha^{-n}h(\phi^n(x))$ es convergente y la función

$$\hat{h}(x) := \lim_{n\to\infty} \frac{h(\phi^n(x))}{\alpha^n},$$

cumple las dos propiedades

1. $|\hat{h}(x) - h(x)| \leq c_1/(\alpha - 1)$;
2. $\hat{h}(\phi(x)) = \alpha\hat{h}(x)$.

Demostración. Empezamos por verificar que $u_n := \alpha^{-n}h(\phi^n(x))$ es una succesión de Cauchy. De hecho, como $-c_1 \leq h(\phi^n(x)) - \alpha h(\phi^{n-1}(x)) \leq c_1$, multiplicando por α^{-n} y sumando las disigualdades, obtenemos

$$-c_1\left(\frac{1}{\alpha^n} + \ldots \frac{1}{\alpha^{m+1}}\right) \leq u_n - u_m \leq c_1\left(\frac{1}{\alpha^n} + \ldots \frac{1}{\alpha^{m+1}}\right)$$

Esto comprueba que u_n es una succesión de Cauchy. Tomando n infinito obtenemos

$$-\frac{c_1}{\alpha^m(\alpha-1)} \leq \hat{h}(x) - \alpha^{-m}h(\phi^m(x)) \leq \frac{c_1}{\alpha^m(\alpha-1)}$$

y en particular que $|\hat{h}(x) - h(x)|$ es acotada por $c_1/(\alpha - 1)$. Finalmente

$$\hat{h}(\phi(x)) = \lim_{n\to\infty} \frac{h(\phi^n(\phi(x)))}{\alpha^n} = \alpha \lim_{n\to\infty} \frac{h(\phi^{n+1}(x))}{\alpha^{n+1}} = \alpha\hat{h}(x).$$

□

Juntando las formulas (2.1) y (2.2) podemos introducir la altura de Néron-Tate y el regulador

Definición 4. La altura de Néron-Tate (o altura canónica) de un punto $P \in E(\mathbb{Q})$ es la cantidad

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h([2^n](P))}{4^n}.$$

Teorema 14. La función "altura de Néron-Tate" $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ es una forma cuadrática definida positiva; la diferencia entre la altura de Néron-Tate y la altura "ingenua" es una función acotada.

Demostración. Aplicando el lema de Tate a la función altura $h : E(\mathbb{Q}) \to \mathbb{R}$ y la aplicación $\phi = [2]$, escogiendo $\alpha = 4$ obtenemos que $\hat{h} - h$ es acotada y que $\hat{h}(2P) = 4\hat{h}(P)$ y más generalmente $\hat{h}(2^m P) = 4^m \hat{h}(P)$. Aplicando la formula (2.2) a los puntos $2^m P$ y $2^m Q$ obtenemos

$$-\frac{c_2}{4^m} \leq \frac{h(2^m(P+Q)) + h(2^m(P-Q)) - 2h(2^m P) - 2h(2^m Q)}{4^m} \leq \frac{c_2}{4^m}$$

Tomando el límite se obtiene la ley del paralelogramo

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

que caracteriza una forma cuadrática. Decir que $\hat{h}$ es definida positiva significa que, tensorizando por $\mathbb{R}$, la forma cuadrática $\hat{h}_{\mathbb{R}} : E(\mathbb{Q}) \otimes \mathbb{R} \to \mathbb{R}$ es definida positiva en el sentido clasico. Eso es verdad porque $\hat{h}_{\mathbb{R}}$ es positiva y verifica que el conjunto de los puntos $P \in E(\mathbb{Q})$ tales que $\hat{h}(P) \leq X$ es finito. Ejo □

Ejercicio 9. Estudiamos algunas propiedades de las alturas.

1. Demostrar que un punto $P \in E(\mathbb{Q})$ verífica $\hat{h}(P) = 0$ si y solamente si P es de torsión.
2. Demostrar la versión siguiente del descenso: sea $Q_1, \ldots, Q_s$ representantes de $E(\mathbb{Q})/2E(\mathbb{Q})$ y $c_E := \max \hat{h}(Q_i)$ entonces el conjunto finito

   $$\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq c_E\}$$

   es un conjunto de generadores del grupo de Mordell-Weil $E(\mathbb{Q})$.
3. Observando que $\hat{h}(P + P_0) \leq 2\hat{h}(P) + 2\hat{h}(P_0)$ concluir que existe una constante c_0 (independiente de P y P_0) tal que

   $$h(P + P_0) \leq 2h(P) + 2h(P_0) + c_0.$$

Notaremos $< P, Q >:= \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$ el producto escalar asociado.

Definición 5. Sea $P_1, \ldots, P_r$ una base sobre $\mathbb{Z}$ de $E(\mathbb{Q})$ modulo la torsión, el regulador de $E/\mathbb{Q}$ es definido por

$$\mathrm{Reg}\,(E/\mathbb{Q}) := \det\left(< P_i, Q_j >\right)_{1\leq i,j\leq r}.$$

El interés viene del teorema siguiente debido a Minkowski y Hermite.

Teorema 15. Sea $F \cong \mathbb{R}^n$ un espacio euclidiano con norma $||\cdot||$ y $\Lambda \cong \mathbb{Z}^n$ una retícula en F. Sea $P_1, \ldots, P_n$ una base de Λ y $\mathrm{Reg}\,(\Lambda) := \det(< P_i, P_j >)$, entonces existe $Q_1, \ldots, Q_n$ una base de Λ tal que

$$||Q_1|| \ldots ||Q_n|| \leq c_n \left(\mathrm{Reg}\,(\Lambda)\right)^{1/2} \tag{2.3}$$

Aplicando el teorema de Hermite-Minkowski a la retícula $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$ en el espacio euclidiano $F = E(\mathbb{Q}) \otimes \mathbb{R}$ provisto de la forma cuadrática $\hat{h}$, obtenemos el corolario siguiente.

Corolario 1. Sea $E/\mathbb{Q}$ una curva elíptica, existe una base $Q_1, \ldots, Q_r$ (la parte infinita) del grupo de Mordell-Weil tal que

$$\hat{h}(Q_1) \ldots \hat{h}(Q_r) \leq c'_r \mathrm{Reg}\,(E/\mathbb{Q}). \tag{2.4}$$

Observamos que, para obtener una cota para las alturas de generadores (minimales), necesitamos una cota *superior* para el regulador, y también una cota *inferior* para la altura minimal de un punto de orden infinito. O sea, si notamos

$$m_E := \min_{Q \notin E(\mathbb{Q})_{\mathrm{tor}}} \hat{h}(Q),$$

y ordenamos en la orden creciente $\hat{h}(Q_1) \leq \cdots \leq \hat{h}(Q_r)$ obtenemos una cota

$$\hat{h}(Q_i) \leq \left(\frac{c'_r \mathrm{Reg}\,(E/\mathbb{Q})}{m_E^{i-1}} \right)^{\frac{1}{r-i+1}}$$

Es útil observar que existen resultados teóricos sobre m_E (por ejemplo [6]) pero también que, para un ejemplo dado, es muy fácil escribir una cota inferior para m_E. El problema fundamental es encontrar una cota superior para $\mathrm{Reg}\,(E/\mathbb{Q})$.

Terminamos esta sección con una breve discusión sobre los parámetros con respeto a los cuales se quiere acotar $\mathrm{Reg}\,(E/\mathbb{Q})$. Escogimos la noción "ingenua" de altura siguiente.

Definición 6. Sea $E/\mathbb{Q}$ una curva elíptica, dada por una ecuación minimal de Weierstrass $y^2 = x^3 + Ax + B$ (es decir $A, B \in \mathbb{Z}$ y para cada primo p, ya sea p^4 no divide A o bien p^6 no divide B). Definimos la altura de E como

$$H(E/\mathbb{Q}) := \max\left\{ |A|^{1/4}, |B|^{1/6} \right\} \tag{2.5}$$

Notamos también $h(E/\mathbb{Q}) := \log H(E/\mathbb{Q})$. Por ejemplo tenemos la disigualdad $\Delta_E \leq c_1 H(E)^{12}$. Ejo

Existe una noción más sofisticada e intrínseca de altura llamada altura de Faltings, pero las dos son comparables en el sentido que hay una desigualdad de la forma $|h_{\mathrm{Faltings}}(E) - h(E)| \leq c_1 \log^+ h(E) + c_2$.

Vamos a ver que varias conjeturas de naturaleza analítica implican una cota del tipo siguiente (ver [7, 12]), que sera repetida al final.

Conjetura 1. Para todo $\epsilon > 0$, existe una constante C_ϵ tal que por toda curva elíptica $E/\mathbb{Q}$ tenemos

$$\mathrm{Reg}\,(E/\mathbb{Q}) \leq C_\epsilon H(E/\mathbb{Q})^{1+\epsilon} \tag{2.6}$$

2.2. La función zeta de Riemann

La función zeta de Riemann, que talvez debería llamarse función zeta de Euler-Riemann[1] es definida por una serie (del tipo serie de Dirichlet) y producto (del tipo producto de Euler), ambos

[1] Los valores reales de $\zeta(s)$ fueran estudiados por Euler (1707–1783), luego Dirichlet (1805–1859) empezó el uso de variable en este contexto para demostrar el teorema de la progresión aritmética y Riemann (1826–1866) publicó en 1859 su famoso artículo sobre la repartición de números primos.

convergentes para $\Re(s) > 1$:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{2.7}$$

La formula (debida a Euler) es una versión analítica de la unicidad de la decomposición en factores primos de los enteros.

Continuación analítica y ecuación funcional.

No es difícil extender la función al semiplano $\Re(s) > 0$, por ejemplo vía la formula Ejo

$$\zeta(s) = s \int_0^{\infty} [t] t^{-s-1} dt = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{s-1} + 1 + s \int_1^{\infty} ([t] - t) t^{-s-1} dt, \tag{2.8}$$

que muestra también que la función zeta tiene un polo simple en $s = 1$ con residuo 1.

Pero hay mucho más. Recordamos que la función Gamma de Euler es definida para $\Re(s) > 0$ por la integral

$$\Gamma(s) := \int_0^{\infty} e^{-t} t^{s-1} dt,$$

y luego extendida al plano complejo (con polos simples en los enteros negativos) gracias a la ecuación $\Gamma(s+1) = s\Gamma(s)$. Ejo

Teorema 16. (Ecuación funciónal) La función $\zeta(s)$ puede ser extendida en una función sobre todo el plano complejo, holomorfa salvo un polo simple en $s = 1$ con residuo 1. Además satisface la ecuación funciónal siguiente. Sea $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ entonces, fuera de 0 y 1, la función $\xi(s)$ es acotada en toda banda vertical y verifica :

$$\xi(s) = \xi(1-s). \tag{2.9}$$

Corolario 2. La función $\zeta(s)$ no se anula en el semiplano $\Re s > 1$; en el semiplano $\Re s < 0$ solamente se anula en los enteros negativos pares no nulos $-2, -4, -6, \ldots$. Todos los otros ceros estan en la banda crítica (critical strip) $0 \leq \Re s \leq 1$.

Demostración. (Esbozo) La prueba utiliza análisis armonico o análisis de Fourier. Sea $\hat{f}(x) := \int_{\mathbb{R}} f(x) \exp(2\pi i x y) dx$, la transformada de Fourier de una función integrable f. Tenemos la formula de Poisson:

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n). \tag{2.10}$$

Definimos $\theta(u) := \sum_{n \in \mathbb{Z}} \exp\left(-\pi u n^2\right)$. Después, aplicando la formula de Poisson a $f(x) = \exp(-\pi u x^2)$ cuya tranformada de Fourier es $\hat{f}(y) = \exp(-\pi y^2/u)/\sqrt{u}$ Ejo , obtenemos una ecuación funciónal para la función theta (cuando veremos la noción de formas modulares, podremos traducirlo como el hecho que θ es modular de peso $1/2$).

$$\theta(1/u) = \sqrt{u}\, \theta(u). \tag{2.11}$$

Podemos hacer el cálculo siguiente, cambiando la variable u por $t = \pi n^2 u$ (el cálculo es válido, inicialmente, para $\Re(s) > 1$).

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \sum_{n \geq 1} \int_0^{\infty} e^{-t} t^{s/2} \pi^{-s/2} n^{-s} \frac{dt}{t}$$

$$= \int_0^{\infty} \left\{ \sum_{n \geq 1} \exp(-\pi u n^2) \right\} u^{s/2} \frac{du}{u} = \int_0^{\infty} \tilde{\theta}(u) \frac{u^{s/2} du}{u}$$

donde

$$\tilde{\theta}(u) := \sum_{n\geq 1} \exp\left(-\pi u n^2\right) = \frac{\theta(u)-1}{2}.$$

Observamos que $\tilde{\theta}(u) = O(\exp(-\pi u)$, cuando u cresce al infinito; insertando (2.11) se obtiene que

$$\tilde{\theta}\left(\frac{1}{u}\right) = \sqrt{u}\,\tilde{\theta}(u) + \frac{1}{2}\left(\sqrt{u}-1\right). \tag{2.12}$$

Como $\int_1^\infty t^{-s} = 1/(s-1)$ y utilizando (2.12), se obtiene

$$\begin{aligned}
\xi(s) &= \int_0^1 \tilde{\theta}(u)\frac{u^{s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u} \\
&= \int_1^\infty \tilde{\theta}(1/u)\frac{u^{-s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u} \\
&= \int_1^\infty \left\{\sqrt{u}\tilde{\theta}(u) + \frac{1}{2}\left(\sqrt{u}-1\right)\right\}\frac{u^{-s/2}du}{u} + \int_1^\infty \tilde{\theta}(u)\frac{u^{s/2}du}{u} \\
&= \int_1^\infty \tilde{\theta}(u)\left\{u^{\frac{s}{2}} + u^{\frac{1-s}{2}}\right\}\frac{du}{u} + \frac{1}{s-1} - \frac{1}{s}.
\end{aligned} \tag{2.13}$$

La última expresión es, a priori, valida para $\Re(s) > 1$, pero es fácil ver que, como $\tilde{\theta}(u) = O(\exp(-\pi u)$, la función definida por la integral es holomorfa sobre $\mathbb{C}$, además es claramente simétrica con respeto a la transformación $s \mapsto 1-s$. Finalmente la función definida por la integral es acotada en cada banda vertical. □

Los ceros en la banda crítica tienien dos simetrías $s \mapsto \bar{s}$ y $s \mapsto 1-s$, esto talvez sugiere la conjetura siguiente.

Conjetura 2. (Hipótesis de Riemann) Los ceros en la banda crítica de la funcion $\zeta(s)$ verifican $\Re(s) = \frac{1}{2}$.

De manera equivalente, la conjetura afirma que la función $\zeta(s)$ no se anula para $\Re(s) > \frac{1}{2}$.

Esencialmente, solamente conocemos la versión más débil – pero suficiente para demostrar el teorema de los números primos – demostrado por Hadamard yde la Vallée Poussin:

Teorema 17. (Hadamard – de la Vallée Poussin) La función $\zeta(s)$ no se anula en la linea $\Re(s) = 1$.

2.3. Generalizaciones de la función de Riemann

2.3.1. La función zeta de de Dedekind

La función zeta de de Dedekind de un cuerpo de números K es definida también por una serie y un producto, ambos convergentes por $\Re(s) > 1$:

$$\zeta_K(s) := \sum_{\mathcal{I}}^{\infty} \frac{1}{N(I)^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \tag{2.14}$$

donde esta vez, I recorre los *ideales* no nulos del anillo de los enteros algebraicos $\mathcal{O}_K$, mientras $\mathfrak{p}$ recorre los ideales *primos* no nulos; la formula es una expresión analítica del teorema sobre la unicidad de la decomposición de un ideal en producto de ideales primos en un anillo de Dedekind.

Para enunciar la ecuación funciónal, recordamos que un cuerpo de números tiene un *discriminante*, notamos Δ_K el valor absoluto de este, y tiene r_1 inmersiones reales $K \hookrightarrow \mathbb{R}$ y r_2 pares de inmersiones complejas conjugadas $K \hookrightarrow \mathbb{C}$, de manera que $r_1 + 2r_2 = [K : \mathbb{Q}]$.

Definición 7. Definimos los factores Gamma real y complejo como:

$$\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2) \qquad \text{y} \qquad \Gamma_{\mathbb{C}}(s) := (2\pi)^{-s}\Gamma(s).$$

Teorema 18. (Ecuación funciónal) La función $\zeta_K(s)$ puede ser extendida en una función sobre todo el plano complejo, holomorfa salvo un pole simple en $s = 1$ con residuo $\lambda(K)$. Además satisface la ecuación funciónal siguiente. Sea

$$\xi_K(s) := \Delta_K^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s)$$

entonces, fuera de 0 y 1, la función $\xi(s)$ es acotada en toda banda vertical y verifica :

$$\xi_K(s) = \xi_K(1-s). \tag{2.15}$$

El residuo $\lambda(K)$ es dado por una formula magnífica que contiene los invariantes más importantes del cuerpo K.

1. El número de clases h_K ;
2. El regulador de las unidades R_K (ver por ejemplo el libro de Lang [11]);
3. El número de raices de la unidad w_K.

El número h_K de ideales modulo los ideales principales de $\mathcal{O}_K$ o sea $h_K = |\mathrm{Pic}\,(\mathcal{O}_K|$. Las unidades, es decir el grupo de los elementos invertibles $\mathcal{O}_K^\times$ es isomorfo a $\mathbb{Z}/w_K\mathbb{Z} \times \mathbb{Z}^r$ con $r = r_1 + r_2 - 1$;

Formula para el residuo de $\zeta_K(s)$ en $s = 1$.

$$\lambda(K) = \frac{h_K R_K}{\sqrt{\Delta_K}} \cdot \frac{2^{r_1}(2\pi)^{r_2}}{w_K} \tag{2.16}$$

Interpretando un ideal primo no nulo como un ideal maximal, es fácil generalizar esta definición para la función zeta de un anillo R de tipo finito sobre $\mathbb{Z}$ (esta condición es para que por todo ideal maximal $\mathfrak{m}$, el cociente $R/\mathfrak{m}$ sea finito de cardinal que notamos $\kappa(\mathfrak{m})$):

$$\zeta_R(s) := \prod_{\mathfrak{m}} \left(1 - \frac{1}{\kappa(\mathfrak{m})^s}\right)^{-1} \tag{2.17}$$

El producto sobre todos los ideales maximales es convergente para $\Re(s) \gg 1$:

2.3.2. La función zeta de un esquema de tipo finito sobre $\mathbb{Z}$

Sea $\mathcal{X}$ un esquema sobre $\mathbb{Z}$ (ver el "appendice" al fin de este texto para una breve introducción al lenguaje de esquemas y, por ejemplo, el libro de Hartshorne [5], para un curso completo). Notamos $|\mathcal{X}|$ el conjunto de los puntos cerrados de $\mathcal{X}$. Por cada punto *cerrado* x de $\mathcal{X}$, tenemos un anillo local $\mathcal{O}_{x,\mathcal{X}}$ con ideal maximal $\mathfrak{M}_{x,\mathcal{X}}$ y cuerpo residual $\kappa(x) := \mathcal{O}_{x,\mathcal{X}}/\mathfrak{M}_{x,\mathcal{X}}$. Notamos $N(x)$ el cardinal de $\kappa(x)$. La función zeta de $\mathcal{X}$ es dada por el producto:

$$\zeta_{\mathcal{X}}(s) := \prod_{x \in |\mathcal{X}|} \left(1 - N(x)^{-s}\right)^{-1} \tag{2.18}$$

Si R es un anillo de tipo finito sobre $\mathbb{Z}$ y $\mathcal{X}$ es el *espectro* de R entonces $\zeta_R(s) = \zeta_{\mathcal{X}}(s)$

Formalmente $\zeta(\mathcal{X}_1 \sqcup \mathcal{X}_2, s) = \zeta(\mathcal{X}_1, s)\zeta(\mathcal{X}_2, s)$. Entonces, si se descompone el conjunto de puntos cerrados segun la característica residual, se obtiene el producto de Euler siguiente, donde se nota $\mathcal{X}_p$ la fibra en p:

$$\zeta(\mathcal{X}, s) = \prod_p \zeta(\mathcal{X}_p, s). \tag{2.19}$$

Observamos que $\mathcal{X}_p$ es una variedad (no necesariamente irreductible) sobre el cuerpo finito $\mathbb{F}_p$. Es claro que tenemos que estudiar la función zeta de tales variedades. Sera el contenido del proximo párrafo.

Ejemplo 10. i) Si $\mathcal{X} = \mathrm{spec}\,(\mathbb{Z})$ (resp. $\mathcal{X} = \mathrm{spec}\,(\mathcal{O}_K)$), entonces $\zeta(\mathcal{X}, s)$ es simplemente la función zeta de Riemann (resp. la función zeta de Dedekind para el cuerpo K).

ii) Si $\mathcal{X} = \mathbb{A}^1_{\mathbb{Z}} = \mathrm{spec}\,(\mathbb{Z}[T])$, podemos identificar los puntos cerrados (ideales maximales de $\mathbb{Z}[T]$) de característica p con los polinomios unitarios irreductibles $\mathbb{F}_p[T]$, cuyo conjunto notamos Irr_p; escribimos también M_p para el conjunto de polinomios unitarios con coeficientes en $\mathbb{F}_p$. El cálculo siguiente es bastante simple :

$$\begin{aligned}
\zeta(\mathbb{A}^1_{\mathbb{Z}}, s) &= \prod_p \prod_{Q \in Irr_p} (1 - p^{-s \deg Q})^{-1} \\
&= \prod_p \prod_{Q \in Irr_p} \sum_{m=0}^{\infty} p^{-sm \deg Q} \\
&= \prod_p \sum_{P \in M_p} p^{-s \deg P} \\
&= \prod_p \sum_{d=0}^{\infty} p^{d-ds} \\
&= \prod_p (1 - p^{1-s})^{-1} \\
&= \zeta(s-1).
\end{aligned}$$

iii) Dividiendo (en partición) los puntos cerrados de $\mathbb{P}^1_{\mathbb{Z}}$ en $\mathbb{A}^1_{\mathbb{Z}} \sqcup \mathbb{A}^0_{\mathbb{Z}}$ se obtiene la formula

$$\zeta(\mathbb{P}^1_{\mathbb{Z}}, s) = \zeta(s)\zeta(s-1).$$

Ejercicio 10. Utilizando la ecuación funcional de la función zeta de Rieman demostrar una relación de la forma (con $G(s)$ un producto de valores de la función Gamma):

$$\zeta(\mathbb{P}^1_{\mathbb{Z}}, 2-s) = G(s)\zeta(\mathbb{P}^1_{\mathbb{Z}}, s).$$

2.3.3. La función zeta de Weil de una variedad sobre un cuerpo finito

Sea X una variedad sobre $\mathbb{F}_p$, luego, para tener propiedades más bonitas, vamos a suponer que X es lisa y proyectiva, pero no es necesario enseguida. Para un punto cerrado x escribimos $d_x = [\mathbb{F}_p(x) : \mathbb{F}_p]$. Se puede calcular

$$\log \zeta_X(s) = \sum_{x,m} \frac{N(x)^{-ms}}{m} = \sum_{x,m} \frac{p^{-d_x ms}}{m} = \sum_{n \geq 1} p^{-ns} \left(\sum_{m d_x = n} \frac{1}{m} \right).$$

Escribimos $\sum_{n \geq 1} u_n p^{-ns}$ la última suma. Continuamos el cálculo observando que, para un punto cerrado $x \in |X|$, tener grado residual d_x que divide n es equivalente a corresponder a una clase de conjugación de puntos en $X(\mathbb{F}_{p^n})$, así :

$$u_n = \sum_{x \in |X|,\, d_x = \frac{n}{m}} \frac{1}{m} = \frac{1}{n} \sum_{x \in |X|,\, d_x | n} d_x = \frac{1}{n} \# X(\mathbb{F}_{p^n}).$$

Eso sugiere la definición siguiente:

Definición 8. Sea $X/\mathbb{F}_p$ una variedad sobre un cuerpo finito, la *función zeta de Weil* es la serie formal

$$Z(X/F_p, T) = \exp\left(\sum_{m=1}^{\infty} \frac{|X(\mathbb{F}_{p^m})|}{m} T^m \right). \tag{2.20}$$

El vínculo con las funciones zeta precedentes es el siguiente: Ejo

Teorema 19. Sea $X/\mathbb{F}_p$ una variedad sobre un cuerpo finito

$$\zeta(X/\mathbb{F}_p, s) = Z(X/F_p, p^{-s}) \tag{2.21}$$

Ejemplo 11. Calculamos el ejemplo simple de $X = \mathbb{P}^n$. En este caso

$$\#X(\mathbb{F}_{p^m}) = \frac{p^{m(n+1)} - 1}{p^m - 1} = p^{mn} + p^{m(n-1)} + \cdots + p^m + 1,$$

entonces

$$\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} T^m = \sum_{j=0}^{n} \sum_{m=1}^{\infty} \frac{p^{mj}}{m} T^m = -\sum_{j=0}^{n} \log(1 - p^j T),$$

entonces:

$$Z(\mathbb{P}^n, T) = \frac{1}{(1-T)(1-pT)\dots(1-p^{n-1}T)(1-p^nT)}. \tag{2.22}$$

Una verificación simple muestra que Z cumple la ecuación funcional :

$$Z(\mathbb{P}^n, T) = (-1)^{n+1} p^{\frac{n(n+1)}{2}} T^{n+1} Z\left(\mathbb{P}^n, \frac{1}{p^n T}\right).$$

Las propiedades provenientes del ejemplo se generalizan ampliamente. Las propiedades de la función zeta de Weil han sido conjeturadas en general por Weil y demostradas por Grothendieck y Deligne.

Teorema 20. (Conjeturas de Weil) Sea X una variedad lisa proyectiva $\mathbb{F}_p$ de dimensión n.

1. (Racionalidad) Existen polinomios $P_j(X,T) = \prod_{i=1}^{b_j}(1 - \alpha_{j,i}T) \in \mathbb{Z}[T]$ para $j = 0, \dots, 2n$ tales que
$$Z(X,T) = \frac{P_1(X,T)\dots P_{2n-1}(X,T)}{P_0(X,T)\dots P_{2n}(X,T)} = \prod_{j=0}^{2n} P_j(X,T)^{(-1)^{j+1}}. \tag{2.23}$$
Además $b_0 = b_{2n} = 1$ y, $P_0(X,T) = 1 - T$ y $P_{2n}(X,T) = 1 - p^nT$.
2. (Ecuación funcional) Sea $\chi(X) = \sum_{j=0}^{2n}(-1)^j b_j$ la característica de Euler-Poincaré entonces
$$Z(X,T) = \pm p^{\frac{n\chi(X)}{2}} T^{\chi(X)} Z\left(X, \frac{1}{p^nT}\right). \tag{2.24}$$
3. (Hipótesis de Riemann) Los enteros algebraicos $\alpha_{j,i}$ satisfacen $|\alpha_{j,i}| = p^{j/2}$.
4. Los números $b_j = b_j(X)$ satisfacen una propiedad de continuidad en familias lisas; en particular si X es la reducción modulo un ideal primo de una variedad Y definida sobre un cuerpo de número K, entonces $b_j(X)$ es igual al número de Betti de la variedad compleja $Y \otimes_K \mathbb{C}$.

El ejemplo siguiente es el ejemplo clave para este curso.

Ejemplo 12. Sea E una curva elíptica sobre $\mathbb{F}_p$. tenemos $b_0 = b_2 = 1$, $b_1 = 2$; los polinomios se escriben $P_0(T) = 1 - T$, $P_2(T) = 1 - pT$ y $P_1(T) = 1 - aT + pT^2$. Entonces hay un entero algebraico α con $\alpha\bar{\alpha} = p$ tal que

$$Z(E,T) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}.$$

Esto es equivalente al teorema de Hasse que dice que

$$\#E(\mathbb{F}_{p^m}) = p + 1 - \alpha^m - \bar{\alpha}^m.$$

Las consideraciones precedentes permiten definir la función ζ (y después L) asociada a una curva elíptica $E/\mathbb{Q}$ como un producto de Euler, donde el factor para p de buena reducción sera:

$$\zeta(E_p, s) = Z(E_p, p^{-s}) = \frac{(1-\alpha_p p^{-s})(1-\bar{\alpha} p^{-s})}{(1-p^{-s})(1-p^{1-s})} = \frac{(1-a_p p^{-s}+p^{1-2s})}{(1-p^{-s})(1-p^{1-s})}.$$

Observamos que el teorema de Hasse nos proporciona que los ceros de $\zeta(E_p, s)$ verifican $\Re(s) = \frac{1}{2}$. Esa es la razón por la cual se llama este resultado (y las generalizaciones por Weil y Deligne) *hipótesis de Riemann*para curvas elípticas (resp. para variedades lisas y proyectivas).

Pero no es claro lo que deben ser los factores para p con mala reducción. siguiendo Serre [15], vamos a introducir las representaciones de Galois, para esclarecer este punto. De hecho, las representaciones de Galois son una herramienta fundamental en la aritmética moderna; por ejemplo juegan un papel fundamental en el trabajo de Wiles.

2.4. La función L asociada a una representación de Galois

Uno de los objetos centrales de la géometria aritmética es el grupo de Galois absoluto :

$$G_{\mathbb{Q}} := \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}). \tag{2.25}$$

Es natural estudiar este enorme grupo profinito a través de sus representaciones. Vamos a considerar dos tipos de representación, primero las de coeficientes complejos (representaciones de Artin) y después las representaciones asociadas a curvas elipiticas, con coeficientes en $\mathbb{Q}_\ell$, que son el prototipo de representaciones asociadas a la cohomologia ℓ-adica de variedades algebraicas.

Definición 9. Sea V un espacio vectorial de dimensión n sobre un cuerpo K, una representación de Galois es un homomorfismo continuo (en estas notas $K = \mathbb{C}$ o $\mathbb{Q}_\ell$ y la topología es natural) de grupos:

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(K) = \mathrm{GL}\,(V).$$

2.4.1. Representaciones de Artin y elementos de Frobenius

Sea $K/\mathbb{Q}$ una extensión finita, cada primo racional p se descompone en K como un producto de ideales primos $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$; el primo p es ramificado en $K/\mathbb{Q}$ si algun $e_i \geq 2$; si notamos $f_i = [\mathcal{O}_K/\mathfrak{P}_i : \mathbb{F}_p]$ entonces $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$. Supongamos ahora que $K/\mathbb{Q}$ es una extensión de Galois con grupo de Galois G.

Definición 10. El *grupo de decomposición* de $\mathfrak{P}/p$ es el subgrupo

$$D(\mathfrak{P}/p) := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Cuando σ está en el grupo de decomposición, se puede definir $\tilde{\sigma} : \mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\mathfrak{P}$ con el diagrama

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\sigma} & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathcal{O}_K/\mathfrak{P} & \xrightarrow{\tilde{\sigma}} & \mathcal{O}_K/\mathfrak{P}. \end{array}$$

Definición 11. El núcleo del mapa $\sigma \to \tilde{\sigma}$ del grupo de decomposición $D(\mathfrak{P}/p)$ hacia Gal $((\mathcal{O}_K/\mathfrak{P})/\mathbb{F}_p)$ es el *grupo de inertia* de $\mathfrak{P}/p$; se le nota $I(\mathfrak{P}/p)$.

Observamos que, si $\#D(\mathfrak{P}/p) = f$ y $\#I(\mathfrak{P}/p) = e$ entonces $\#G = [K : \mathbb{Q}] = efg$. El grupo de inertia $I(\mathfrak{P}/p)$ es trivial cuando $\mathfrak{P}/p$ no es ramificado. La aplicación $\sigma \to \tilde{\sigma}$ de$D(\mathfrak{P}/p)$ hacia Gal $((\mathcal{O}_K/\mathfrak{P})/\mathbb{F}_p)$ es sobreyectiva y se sabe que el grupo imagen es cíclico con un generador canónico dado por $x \mapsto x^p$.

Definición 12. El Frobenius en $\mathfrak{P}$ es el elemento $\mathrm{Frob}_{\mathfrak{P}}$ tal que para todo $x \in \mathcal{O}_K$ tenemos

$$\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^p \mod \mathfrak{P}.$$

Observamos que, en el caso ramificado, el Frobenius es de verdad un *coset* modulo el grupo de inertia. Además, si escogemos un otro primo ensima de p, digamos $\mathfrak{P}' = \sigma(\mathfrak{P})$ entonces $\mathrm{Frob}_{\mathfrak{P}'} = \sigma\mathrm{Frob}_{\mathfrak{P}}\sigma^{-1}$; así $\mathrm{Frob}_{\mathfrak{P}}$ depende solamente de p salvo conjugación; notaremos Frob_p esta clase de conjugación.

Observación 2. Las observaciones siguientes son simples pero importantes y pueden aplicarse a los elementos de Frobenius y el subgrupo de inertia. Sea $\rho : G \to \mathrm{GL}(V)$ una representación. Si $f = hgh^{-1} \in G$ entonces los polinomios característicos de $\rho(f)$ y $\rho(g)$ actuando sobre V son iguales. Si H es un subgrupo de G, notamos

$$V^H := \{v \in V \mid \forall h \in H,\ \rho(h)(v) = v\},$$

el subespacio de los vectores fijos. Si $f \in gH$ y g centraliza H (i.e. para cada $h \in H$, tenemos $gh = hg$) entonces g y f stabilizan V^H y los polinomios característicos de $\rho(f)$ y $\rho(g)$ actuando sobre V^H son iguales.

Esto permite por ejemplo la definición de la función L asociada a una representación de Artin ρ como :

$$L(\rho, s) = \prod_p \det\left(1 - \rho(\mathrm{Frob}_p)p^{-s} \mid V^{I_p}\right)^{-1}. \tag{2.26}$$

No tenemos espacio ni tiempo para desarrollar la teoría de estas funciones L (para una iniciación, ver [11]), solamente indicaremos que son uno de los objetos clave para el programa de Langlands y entender los vínculos entre objetos geométricos – como variedades algebraicas – y analíticos – como formas modulares y automorfas.

2.4.2. Representaciones de Galois asociada a una curva elíptica

Observamos que, por razones topologicas, una representación (que siempre se supone es continua) $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ se factoriza a través de un grupo finito $G = \mathrm{Gal}(K/\mathbb{Q})$; esta propiedad no es verdadera para las representaciones ℓ-adicas asociadas a una curva elíptica que vamos a considerar ahora.

Recordamos que el cuerpo de los números ℓ-adicos $\mathbb{Q}_\ell$ puede ser construido como la completación del cuerpo $\mathbb{Q}$ con respeto al valor absoluto $|x|_\ell := \ell^{-\mathrm{ord}\,_\ell x}$. El anillo de los enteros $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ es entonces la completación de $\mathbb{Z}$. Alternativamente se puede definir $\mathbb{Z}_\ell$ como el límite inverso de los grupos finitos $\mathbb{Z}/\ell^n\mathbb{Z}$ (con los homomorfismos evidentes):

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}.$$

El cuerpo $\mathbb{Q}_\ell$ es el cuerpo de fracciones de $\mathbb{Z}_\ell$.

Definición 13. Sea E una curva elíptica sobre un cuerpo K de característica 0 o p diferente de ℓ. El núcleo de la multiplicación por ℓ^n es denotado por

$$E[\ell^n] := \mathrm{Ker}\left\{[\ell^n] : E(\bar{K}) \to E(\bar{K})\right\},$$

y es isomorfo (como grupo) a $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. El *modulo de Tate* es el límite inverso

$$T_\ell(E) := \varprojlim E[\ell^n] \cong \left(\varprojlim \mathbb{Z}/\ell^n\mathbb{Z}\right)^2 \cong \mathbb{Z}_\ell^2.$$

El grupo de Galois $G_K := \mathrm{Gal}(\bar{K}/K)$ actúa en cada $E[\ell^n]$ y entonces sobre $T_\ell(X)$, definiendo una representación:

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Sea ahora $E/\mathbb{Q}$ una curva elíptica. Tenemos para todo ℓ una representación ρ_ℓ con coeficientes en $\mathbb{Q}_\ell$. A priori el polinomio característico de Frob_p es un polinomio con coefficientes en $\mathbb{Z}_\ell$ pero se sabe (es esencialmente la prueba del teorema de Hasse) que en verdad los coeficientes son enteros y además independientes de ℓ; de hecho $\det \rho_{X,\ell}(\mathrm{Frob}_p) = p$ y $\mathrm{Tr}\, \rho_{X,\ell}(\mathrm{Frob}_p) = a_p = p+1-\#X(\mathbb{F}_p)$. Es decir que el polinomio característico es $1 - a_pT + pT^2$. Ese nos permite la definición siguiente donde notamos V el $\mathbb{Q}_\ell$-espacio vectorial $T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Definición 14. La función L asociada con las representaciones $\rho_{X,\ell}$ es[2]:

$$L(\rho_E, s) = \prod_{\mathfrak{p}} \det\left(1 - \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})N(\mathfrak{p})^{-s} \,|\, V^{I_{\mathfrak{p}}}\right)^{-1}. \tag{2.27}$$

Cuando p divide el discriminante, la curva E modulo p tiene una punta (i.e. en este caso $\dim V^I = 0$) y ponemos $a_p = 0$ o un nodo (i.e. en este caso $\dim V^I = 1$); cuando tenemos un nodo, los dos tangentes pueden ser racionales sobre $\mathbb{F}_p$ y definamos $a_p = 1$, o los dos tangentes no son racionales sobre $\mathbb{F}_p$ y definamos $a_p = -1$. Tenemos la expresión explícita:

$$L(\rho_E, s) = \prod_{p \,|\, \Delta} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}. \tag{2.28}$$

2.5. La función L de Hasse-Weil de una curva elíptica

2.5.1. Definición como producto de Euler

Podemos dar la definición más concreta posible de la función $L(E, s)$, obtenida a través de la consideración de representaciones de Galois, así:

Definición 15. Sea $E/\mathbb{Q}$ una curva elíptica con discriminante minimal Δ_E. Para p que no divide Δ, notamos $a_p = a_p(E) = p + 1 - |E(\mathbb{F}_p)|$; para p que divide Δ_E ponemos

$$a_p = \begin{cases} +1 & \text{si la reducción es multiplicativa y } \textit{split} \\ -1 & \text{si la reducción es multiplicativa y } \textit{non split} \\ 0 & \text{si la reducción es aditiva} \end{cases}$$

Entonces definimos

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \,|\, \Delta_E} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \tag{2.29}$$

La serie de Dirichlet y el producto de Euler son ambos convergentes para $\Re(s) > 3/2$. Esto se demuestra utilisando el teorema de Hasse que proporciona $|a_p| \leq 2\sqrt{p}$ y más generalmente $|a_n| \leq \sigma(n)\sqrt{n}$, donde $\sigma(n)$ es el número de divisores de n. (Ejo)

La función $L(E, s)$ tiene propiedades similares a las otros funciones ζ y L pero son mucho más difíciles de establecer. De hecho el método de demostración consiste en establecer un vínculo con otro objeto analítico : las formas modulares.

2.5.2. Función L asociada a una forma modular

Esta parte es breve y mandamos al curso de Harris-Miatello-Moreno-Pacetti-Tornaria para más detalles.

[2] Serre habla de *sistema de representaciones compatibles*.

Las formas modulares son funciones holomorfas sobre el semiplano de Poincaré $\mathcal{H} := \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$. La condición principal es que, para un número k llamado el *peso* y un subgrupo Γ de

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a,b,c,d \in \mathbb{Z},\ ad - bc = 1\right\}$$

tenemos, para $\gamma \in \Gamma$ y $\tau \in \mathcal{H}$

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \tag{2.30}$$

La segunda condición es una condición de "holomorfía al infinito", vamos a explicitarla para el unico subgrupo que vamos a considérar:

Definición 16. El grupo de congruencia de nivel N es el subgrupo:

$$\Gamma_0(N) := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid N \text{ divide } c\right\} \tag{2.31}$$

Observamos que la matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ pertenece a $\Gamma_0(N)$, así una función holomorfa $f : \mathcal{H} \to \mathbb{C}$ que cumple (2.30) es periódica $f(\tau + 1) = f(\tau)$, entonces se puede escribir como una serie de Fourier:

$$f = \sum_{n \in \mathbb{Z}} a_n q^n \quad (\text{donde } q = \exp(2\pi i \tau))$$

Definición 17. Una función holomorfa de la forma $f = \sum_{n\in\mathbb{Z}} a_n q^n$ es holomorfa en el infinito si $a_n = 0$ para $n < 0$, es holomorfa y se anula en el infinito si $a_n = 0$ para $n \leq 0$.

Definición 18. Una forma modular de peso k, con respeto al grupo $\Gamma_0(N)$ es una función holomorfa $f : \mathcal{H} \to \mathbb{C}$ que cumple (2.30) y además, para cada $\gamma \in \Gamma_0(N)$, la function $(c\tau+d)^{-k} f(\gamma(\tau))$ es holomorfa en el infinito; La forma es dicha parabólica si además se anula en el infinito. Se nota $M_k(\Gamma_0(N))$ el espacio vectorial de las formas modulares de peso k, con respeto al grupo $\Gamma_0(N)$ (resp. $S_k(\Gamma_0(N))$ el espacio vectorial de tales formas modulares parabólicas).

Luego vamos a considerar solamente formas de peso 2.

Definimos la función L asociada a una forma modular parabólica por la formula

$$L(f,s) := \sum_{n \geq 1} a_n n^s \tag{2.32}$$

Notamos la relación : (Ejo)

$$\Gamma_{\mathbb{C}}(s) L(f,s) = (2\pi)^{-s}\Gamma(s) L(f,s) = \int_0^\infty f(it) t^{s-1} dt. \tag{2.33}$$

Definición 19. Sea $f = \sum_n a_n(f) q^n \in M_2(\Gamma_0(N))$. Los *operadores de Hecke* son definidos por las formulas siguientes.

1. Si p no divide N, el operador $f \mapsto T_p f$ es definido por :

$$a_n(T_p f) := a_{np}(f) + p a_{n/p}(f),$$

donde, por convención, $a_{n/p} = 0$ si p no divide n.

2. Si p divide N, el operator $f \mapsto U_p f$ es definido por :

$$a_n(U_p f) := a_{np}(f).$$

Teorema 21. (Hecke, ver [3]) Los operadores de Hecke comutan. Si $f = \sum_n a_n(f)q^n \in S_k(\Gamma_0(N))$ es un vector proprio simultánamente para cada operador, i.e $T_p f = \lambda_p f$, $U_p f = \lambda_p f$, entonces $a_p(f) = \lambda_p a_1(f)$. Si f es normalizada de manera que $a_1(f) = 1$, la función $L(s, f)$ se descompone en producto de Euler así :

$$L(s,f) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_{p \mid N} (1 - a_p(f)p^{-s})^{-1} \prod_{p \nmid N} (1 - a_p(f)p^{-s} + p^{1-2s})^{-1}. \tag{2.34}$$

□

Esta función L se parece mucho a una función L de una curva elíptica. Veamos que, con una condición suplementaria, esta satisface la ecuación funcional esperada por una curva elíptica.

Observamos que la matriz $W_N := \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$, que no pertenece a $\mathrm{SL}(2,\mathbb{Z})$, sin embargo normaliza el subgrupo $\Gamma_0(N)$, porque

$$W_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} W_N^{-1} = \begin{pmatrix} d & -c/N \\ -bN & a \end{pmatrix}.$$

Entonces W_N actúa sobre $M_2(\Gamma_0(N))$ (resp. $S_2(\Gamma_0(N))$), y notando que $W_N^2 = -NId$, actúa como una involución. Así los espacios $M_2(\Gamma_0(N))$ (resp. $S_2(\Gamma_0(N))$) se descomponen en la suma de dos subespacios proprios tales que :

$$f\left(-\frac{1}{Nz}\right) = f(W_N \cdot z) = \pm N z^2 f(z) \tag{2.35}$$

Teorema 22. (Hecke) Sea $\epsilon = \pm 1$ y $f(\tau) = \sum_{n\geq 1} a_n \exp(2\pi i n\tau)$ una forma modular parabolica para $\Gamma_0(N)$ (de peso 2) tal que

$$f\left(-\frac{1}{N\tau}\right) = \epsilon N \tau f(\tau). \tag{2.36}$$

Definimos $\Lambda(s,f) := N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,f)$, donde $L(s,f) := \sum_{n=1}^{\infty} a_n n^{-s}$. La función $\Lambda(s,f)$ tiene continuación analítica a todo el plano $\mathbb{C}$ y satisface la ecuación funcional:

$$\Lambda(s,f) = -\epsilon \Lambda(2-s,f). \tag{2.37}$$

Además, $\Lambda(s,f)$ es acotada en toda banda vertical.

Demostración. Observamos que para $\tau = it$ (con $t \in \mathbb{R}_+$) la ecuación (2.36) nos proporciona:

$$f\left(\frac{i}{Nt}\right) = -\epsilon N t^2 f(it).$$

La analogia con la ecuación (2.11) usada para probar la ecuación funcional de la función zeta de Riemann es clara. Podemos calcular, utilizando (2.33) y el cambio de variables $t \mapsto 1/Nt$:

$$\begin{aligned}
\Lambda(s,f) &= N^{s/2} \int_0^{\infty} f(it) t^{s-1} dt \\
&= N^{s/2} \int_0^{\frac{1}{\sqrt{N}}} f(it) t^{s-1} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) t^{s-1} dt \\
&= N^{-s/2} \int_{\frac{1}{\sqrt{N}}}^{\infty} f(i/Nt) t^{-s-1} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) t^{s-1} dt \\
&= -\epsilon N^{\frac{1}{2}(2-s)} \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) t^{1-s} dt + N^{s/2} \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) t^{s-1} dt \\
&= \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) \left[-\epsilon N^{\frac{1}{2}(2-s)} t^{2-s} dt + N^{s/2} t^s \right] \frac{dt}{t}.
\end{aligned} \tag{2.38}$$

La última expresión define una función entera (utilizando una cota del tipo $|a_n| = O(n^c)$, y la consecuencia $|f(it)| = O(\exp(-2\pi t))$ cuando t cresce hasta el infinito). La $(-\epsilon)$-simetría cuando s es remplazado por $2-s$ es clara ahora, como la propiedad de ser acotada en toda banda vertical. □

2.5.3. Continuación analítica y ecuación funcional de $L(E, s)$

En el capítulo primero, se ha definido el *discriminante* minimal Δ_E de una curva elíptica $E/\mathbb{Q}$, existe un invariante parecido – pero distinto – llamado el *conductor* N_E; vamos a dar la definición solamente menos una potencia de 2 y 3.

Definición 20. El conductor N_E de $E/\mathbb{Q}$ es definido por su decomposición en factores primos:

$$N_E := \prod_{p \mid \Delta_E} p^{n(E,p)}$$

donde $n(E,p)$ vale $+1$ en el caso de reducción multiplicativa, vale $+2$ en el caso de reducción aditiva con $p > 3$, y además $2 \leq n(E,2) \leq 8$ y $2 \leq n(E,3) \leq 5$ en el caso de reducción aditiva.

El teorema siguiente muestra que la función $L(E, s)$ tiene propiedades similares a su antepasado $\zeta(s)$.

Teorema 23. La función $L(E, s)$ se extiende en una función analítica en todo el plano complejo y satisface la ecuación funcional siguiente. Notamos $\Lambda(E, s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$ entonces

$$\Lambda(E, 2-s) = \pm\Lambda(E, s) \tag{2.39}$$

Esto es esencialmente equivalente al Teorema de Wiles! Lo que demuestra Wiles es la conjetura de Shimura-Taniyama que afirma que los coeficientes a_n (obtenidos a partir de los a_p) de la curva elíptica son los coeficientes de una forma modular de peso 2 con respeto al grupo $\Gamma_0(N_E)$. La ecuación funcional es entonces consecuencia de la ecuación funcional de la función L de una forma modular.

Comentario. El teorema de Wiles no utiliza explicitamente funciones L pero unifica tres objetos a priori de origen muy distintos : une curva elíptica $E/\mathbb{Q}$, las representaciones de Galois asociadas y las formas modulares (de peso 2, con respeto a un subgrupo $\Gamma_0(N)$ y que son vectores proprios para operadores de Hecke y W_N). Sin embargo el hilo conductor entre estos tres objetos son las funciones L asociadas. El teorema de Wiles puede ser visto como un pedazo (muy importante) del vasto programa de Langlands.

2.5.4. El signo de la ecuación funcional

Definición 21. Notamos $W(E)$ el signo ± 1 que aparece en la ecuación funcional (2.39).

La importancia del signo $W(E)$ ("*root number*" en inglés) viene del hecho que el determina la paridad del orden de anulación de $L(E, s)$. O sea si notamos $r_{\text{an}} = r_{\text{an}}(E/\mathbb{Q})$ el *rango analítico*, es decir el orden de anulación de $L(E, s)$ en $s = 1$, tenemos

$$W(E) = (-1)^{r_{\text{an}}(E/\mathbb{Q})} \tag{2.40}$$

Además el signo se puede calcular como producto de signos locales.

Teorema 24. Sea E curva elíptica definida sobre $\mathbb{Q}_p$, existen signos locales $W_p(E)$ que se pueden calcular por formulas explícitas (dadas debajo) y cuyo producto es igual al signo global[3]. Es decir que si $E/\mathbb{Q}$ entonces:

$$W(E/\mathbb{Q}) = \prod_p W_p(E/\mathbb{Q}_p)$$

[3]Para que la formula sea exacta, hay que incluir el "primo arquimediano" ∞, cuyo signo es $W_\infty(E) = -1$.

Las reglas de cálculo son las siguientes

1. $W_\infty(E) = -1$;
2. Cuando E tiene buena reducción $W_p(E) = +1$;
3. Cuando E tiene reducción multiplicativa entonces $W_p(E) = -1$ (resp. $W_p(E) = +1$) si los dos tangentes son racionales sobre F_p, caso "*split, déployé* " (resp. si no lo son, caso "*nonsplit, non déployé* ").
4. (para $p > 2$) Cuando la reducción es aditiva y potencialmente multiplicativa $W_p(E) = \left(\frac{-1}{p}\right)$ (simbolo de Legendre);
5. (para $p > 3$) Cuando la reducción es aditiva y potencialmente buena, notamos $e := \frac{12}{\text{mcd}\,(\text{ord}\,(\Delta_E),12)}$, entonces
$$W_p(E) = \begin{cases} \left(\frac{-1}{p}\right) & \text{si } e = 2, 6 \\ \left(\frac{2}{p}\right) & \text{si } e = 4 \\ \left(\frac{3}{p}\right) & \text{si } e = 3 \end{cases}$$

Hay también formulas en el caso de buena reducción potencial y $p = 2$ o 3, pero son más complicadas (ver por ejemplo [14]).

Ejercicio 11. Reconsideramos la curva elíptica E del ejercicio 6 dada por $y^2 + y = x^3 - x$.

1. Mostrar que $W(E) = W_\infty(E)W_{37}(E) = -W_{37}(E)$.
2. Mostrar que E tiene reducción multiplicativa en $p = 37$ y que la reducción es *non split*.
3. Concluir que $W(E) = -1$ y $L(E, 1) = 0$.
   [En efecto $L'(E, 1) \neq 0$ y entonces $r_{\text{an}}(E/\mathbb{Q}) = r(E/\mathbb{Q}) = 1$.]

Ejercicio 12. Reconsideramos la curva elíptica E del ejercicio 7 dada por $y^2 + 9y = x^3 - 27$ (cúbica de Fermat).

1. Mostrar que $W(E) = W_\infty(E)W_3(E) = -W_3(E)$.
2. Admitiendo (o verificando con la ayuda de [14]) que $W_3(E) = -1$, concluir que $W(E) = +1$.
   [En efecto $L(E, 1) \neq 0$ y entonces $r_{\text{an}}(E/\mathbb{Q}) = r(E/\mathbb{Q}) = 0$.]

2.6. Valor en $s = 1$

La primera parte de la conjetura de Birch & Swinnerton-Dyer dice que, para toda curva elíptica $E/\mathbb{Q}$ tenemos:
$$r_{\text{an}}(E/\mathbb{Q}) = r(E/\mathbb{Q}).$$
Sea : el orden de anulación de la función $L(E, s)$ en $s = 1$ es igual al rango del grupo de Mordell-Weil.

Pero la conjetura de Birch & Swinnerton-Dyer da muchas más precisiones que vamos ahora a desarrollar. Como la formula describiendo el residuo de la función $\zeta_K(s)$ en $s = 1$ contiene muchas informaciónes aritméticas, el valor de la función $L(E, s)$ en $s = 1$ contiene bastante de la aritmética de la curva $E/\mathbb{Q}$, o deberia contener.

2.6.1. El grupo de Shafarevich-Tate (esbozo)

El grupo de *Shafarevich-Tate*[4] es una medida de las obstrucciones cohomologicas al principio de Hasse para cúbicas, tecnicamente su definición es:

$$Ш(E/\mathbb{Q}) := \ker\left\{H^1(\mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}), E) \to \prod_p H^1(\mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), E_{\mathbb{Q}_p})\right\}.$$

No tenemos tiempo de desarrollar las herramientas (cohomologia de Galois) para entender mejor este grupo, solamente explicaremos como el grupo Ш interviene naturalmente en el cálculo del grupo de Mordell-Weil. El proceso de la demostración del teorema de Mordell-Weil débil conduce naturalmente a establecer una succesión exacta de grupos finitos o también de módulos de Galois (ver [16])

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0.$$

Donde el grupo en el medio (llamado n-grupo de Selmer es finito y calculable.

La parte anulada por $[n]$ del grupo $Ш(E/\mathbb{Q})$ es finita pero no se sabe, en general, calcular este grupo. Es parte de la conjeture de Birch & Swinnerton-Dyer que el grupo total es finito, pero esto solamente se le ha demostrado en casos particulares. En cambio el grupo de Selmer es mejor conocido, por ejemplo resultados excelentes de Bhargava (con Shankar) han permitido demostrar resultados muy precisos en promedio.

Teorema 25. (Bhargavar–Shankar) Sea $n \in \{2,3,4,5\}$ entonces

$$\lim_{T\to\infty} \frac{\sum_{H(E)\leq T} |S^{(n)}(E/\mathbb{Q})|}{\sum_{H(E)\leq T} 1} = \sigma(n)$$

Como corolario se obtiene por ejemplo

$$\limsup_{T\to\infty} \frac{\sum_{H(E)\leq T} 5^{r(E/\mathbb{Q})}}{\sum_{H(E)\leq T} 1} \leq 6.$$

2.6.2. Conjetura de Birch & Swinnerton-Dyer

Hemos definido el regulador $\mathrm{Reg}\,(E/\mathbb{Q})$ y (brevemente) el grupo de Shafarevich, las otras cantidades incluidas en la formula de Birch & Swinnerton-Dyer son las siguientes.

Definición 22. Sea $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ un modelo de Weierstass minimal de una curva elíptica $E/\mathbb{Q}$. La forma diferencial de Néron es dada por

$$\omega_E := \frac{dx}{2y + a_1x + a_3}.$$

El período real de E es el número real positivo:

$$\Omega_E := \int_{E(\mathbb{R})} |\omega_E|.$$

Se puede comparar el tamaño de Ω_E así (ver [7]) con constantes que se podrian explicitar:

$$c_1 H(E) \leq \Omega_E^{-1} \leq c_2 H(E)\log H(E) \tag{2.41}$$

[4] La notación clásica con la letra rusa o cirílica Ш es un homenaje a Igor Shafarevich (ШАФАРЕВИЧ).

Definición 23. Sea $E/\mathbb{Q}$ una curva elíptica. El subgrupo $E^0(\mathbb{Q}_p)$ es el subgrupo de puntos que se reducen modulo p en un punto no singular. El número de Tamagawa local es definido como el indicio $c_p = (E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)$, el número de Tamagawa global es defindo como el producto $\prod_p c_p$.

Las informaciones simples sobre c_p son las siguientes : $c_p = 1$ en el caso de buena reducción, $c_p = \text{ord}_p(\Delta_E)$ en el caso de reducción multiplicativa *split* y $c_p \leq 4$ en los otros casos.

Podemos ahora expresar la conjetura completa:

Conjetura 3. (Conjetura de Birch & Swinnerton-Dyer) Sea $E/\mathbb{Q}$ una curva elíptica y $L(E,s)$ su función asociada.

1. $r_{\text{an}}(E/\mathbb{Q}) = r(E/\mathbb{Q})$.
2. El grupo $Ш(E/\mathbb{Q})$ es finito.
3. El coeficiente principal de $L(E,s)$ en $s=1$ es dado por:

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = |Ш(E/\mathbb{Q})|\text{Reg}\,(E/\mathbb{Q})\Omega_E \frac{\prod_p c_p}{|E(\mathbb{Q})_{\text{tor}}|^2} \tag{2.42}$$

Notaremos $L^*(E,1)$ el último valor. Damos ahora la aplicación prometida al control de $\text{Reg}\,(E/\mathbb{Q})$. Aceptando la formula conjetural (2.42), recordando que $Ш(E/\mathbb{Q})|\prod_p c_p|$ es un entero y que $|E(\mathbb{Q})_{\text{tor}}| \leq 16$ obtenemos:

$$\text{Reg}\,(E/\mathbb{Q}) \leq 16^2 L^*(E,1)\Omega_E^{-1} \leq cH(E)\log H(E) L^*(E,1).$$

Las técnicas de teoría analítica de números nos proporcionan (ver [9, 8]):

Lema 4. Sea $L(E,s)$ la función asociada a una curva elíptica $E/\mathbb{Q}$ de conductor N_E. Tenemos las estimaciones:

1. $L^*(E,1) \leq 2^r N_E^{1/4}(\log N_E)^2$.
2. Supongamos que la función $L(E,s)$ verifica la hipótesis de Riemann (es decir $L(E,s) \neq 0$ cuando $\Re(s) > 1$), entonces:

$$L^*(E,1) \leq C_\epsilon N_E^\epsilon \leq C'_\epsilon H(E)^\epsilon.$$

Juntando todo eso llegamos naturalmente a la conjetura siguiente, que es implicada por las conjeturas de Birch & Swinnerton-Dyer y de Riemann (aplicada a $L(E,s)$). Observamos que la conjetura es puramente diofántica y no hace referencia a funciones L.

Conjetura 4. Existe, para cada $\epsilon > 0$, una constante C_ϵ, tal que para toda curva elíptica $E/\mathbb{Q}$ tenemos:

$$\text{Reg}\,(E/\mathbb{Q}) \leq C_\epsilon H(E)^{1+\epsilon}. \tag{2.43}$$

Observación 3. Si no queremos utilizar la conjetura de Riemann, obtenemos una cota más débil de la forma $\text{Reg}\,(E/\mathbb{Q}) \leq c_1 H(E)^{c_2}$.

Es el momento de aclarar las respuestas (parciales) a las preguntas iniciales (sección 2.1) que las consideraciones de funciones L y ζ nos proporcionan, *condicionalmente* a la conjetura de Birch & Swinnerton-Dyer.

1. La demostración del teorema de Mordell-Weil proporciona solamente una cota superior para el rango $r = r(E/\mathbb{Q})$,

2. El rango analitico es en general fácil de calcular, la paridad se calcula todavía más rapidamente, calculando $W(E)$: calculamos $L(E,1)$, $L'(E,1)$ etc. hasta encontrar un valor no nulo [5].

3. Existen generadores P_i tales que, si se ordena en orden creciente $\hat{h}(P_1) \leq \hat{h}(P_2) \leq \ldots$, entonces

$$\hat{h}(P_i) \leq C_\epsilon H(E)^{\frac{1}{r-i+1}+\epsilon}$$

Una vez que se tiene una cota, hay un algoritmo obvio para buscar de manera exhaustiva puntos racionales (N.B: el algoritmo es pesimo del punto de vista de complexidad computacional!).

Indicaciones. (para el ejercicio 1).
1) La unica solución es $3^3 = 5^2 + 2$. Se trata de encontrar los puntos enteros sobre $y^2 = x^3 - 2$. Mostrar que x, y son impares; considerar el anillo, que se demostrara ser principal, $A = \mathbb{Z}[i\sqrt{2}]$ y mostrar que $y + i\sqrt{2}$ es un cubo en A, y concluir.
2) Las soluciones son $6 = 2\times 3 = 1\times 2\times 3$ y $210 = 14\times 15 = 5\times 6\times 7$. Es esencialmente equivalente a determinar los puntos enteros de la curva $y^2 + y = x^3 - x$ considerada en los ejercicios 6 y 11. Sea $Q \in E(\mathbb{Q})$, mostrar que si mQ es un punto entero, entonces Q también. Mostrar que $E(\mathbb{R})$ tiene dos componentes : C_0 conteniendo el punto al infinto y C_1; determinar los puntos enteros en el componente C_1 (que es compacto en el plano afín). Una vez que se ha demostrado que el rango es igual a 1 (es la parte mas difícil, admitirlo o ver [16], *exercise* 10.9), mostrar que $E(\mathbb{Q})$ es generado por $P = (0,0)$, que $\pm P$, $\pm 2P$, $\pm 3P$, $\pm 4P$, $\pm 6P$ son puntos enteros, pero que $8P$ y $12P$ no son puntos enteros (notar que $6P = (6,14)$). Concluir argumentando que si mP es un punto entero, escribiendo $m = 2^u m_1$ (con m_1 impar), entonces $m_1 P$ es entero y pertenece a C_1.

[5] La unica dificultad algoritmica es de comprobar que una derivada es nula cuando su valor aproximado es digamos 10^{-100}.

APPENDICE : "esquemas explicados para niños"

Ver por ejemplo [5] para mas detalles sobre la noción de esquema.

Se puede describir una variedad proyectiva sobre un cuerpo K como $\mathbb{P}^n$, por ejemplouna curva elíptica, como recubierta por abiertos afines y pegados.

Ejemplo 13. 1) La línea proyectiva $\mathbb{P}^1$ se puede describir como $U_0 \cup U_1$ donde el abierto afín $U_0 = \{(x_0, x_1) \in \mathbb{P}^n \mid x_0 \neq 0\}$ es isomorfo a la línea $\mathbb{A}^1$ por el mapa $x \mapsto (1, x)$ y el abierto afín $U_1 = \{(x_0, x_1) \in \mathbb{P}^n \mid x_1 \neq 0\}$ es isomorfo a la línea $\mathbb{A}^1$ por el mapa $t \mapsto (t, 1)$ y se pegan los dos identificando $t = x^{-1}$.
2) Una curva elíptica E puede ser descrita como la unión de dos abiertos afines $V_1 \cup V_2$ donde $V_1 = \{(x, y) \in \mathbb{A}^2 \mid y^2 = x^3 + ax + b\}$, $V_2 = \{(u, v) \in \mathbb{A}^2 \mid v^2 = u(bu^3 + au^2 + 1)\}$ pegados a través de $(u, v) = (1/x, y/x^2)$.

Variedades afines pueden ser identificadas con su anillo de funciones, es decir: si V es una variedad afín en $\mathbb{A}^n$, se puede describir como el conjunto de ceros de un ideal $I \subset K[X_1, \ldots, X_n]$; el anillo de funciones de V es $\mathcal{O}(V) = K[X_1, \ldots, X_n]/I$; un punto $a = (a_1, \ldots, a_n)$ en V corresponde al ideal generado por (las imagenes de) los $X_i - a_i$. Hay una correspondencia entre aplicaciónes $\phi : V \to W$ de variedades afines y homomorfismos de anillos $\phi^* : \mathcal{O}(W) \to \mathcal{O}(V)$ (donde $\phi^*(f) = f \circ \phi$).

Los puntos de $\mathbb{A}^1$ (o U_0 o U_1) se identifican con los ideales maximales de $K[X]$ y los mapas de $\mathbb{A}^1$ hacia $\mathbb{A}^1$ corresponden a endomorfismos de anillo de $K[X]$. Así V_1 se identifica con el anillo $B := K[x, y]/(-y^2 + x^3 + ax + b)$ etc., y una aplicación de V_1 hacia $\mathbb{A}^1$ corresponde a un homomorfismo de anillos $K[X] \to B$.

Grothendieck a afinado este concepto introduciendo el espectro de un anillo A (un anillo unitario cualquier!) cuyos puntos son los ideales primos de A. El spectro de un anillo A, denotado spec (A), es el conjunto de sus ideales primos con la topologia de Zariski; se define esta topologia con la propiedad $P \subset Q$ (inclusion de ideales primos) significa que Q esta en el cerradura de $\{P\}$ (como punto de spec (A)).

Un esquema afín es simplemente el espectro de un anillo. Los morfismos de spec $(A) \to$ spec (B) corresponden a homomorfismos de anillos $f : B \to A$ y son definidos por $P \to f^{-1}(P)$. Un esquema general es definido de manera similar, pegando esquemas afines.

Ejemplo 14. 1) Cuando K es un cuerpo, el esquema spec (K) es reducido a un punto; en cambio el esquema spec $(\mathbb{Z})$ tiene una infinidad de puntos cerrados (en correspondencia con números primos o ideales $p\mathbb{Z}$) y un punto denso en spec $(\mathbb{Z})$ (que corresponde al ideal nulo o al imagen de spec $(\mathbb{Q}) \to$ spec $(\mathbb{Z})$ que corresponde a la inclusión de anillos $\mathbb{Z} \hookrightarrow \mathbb{Q}$).
2) El esquema spec $(\mathbb{Z}[X])$ tiene varios tipos de puntos : los punto cerrados, que corresponden a ideales $I = (p, P)$ generados por un número primo p y un polinomio P irreductible modulo p Ejo los puntos de dimensión (o codimensión) uno, correponden a ideales principales generados por un número primo p o un polinimio irreductible P, y finalmente el punto genérico, que corresponde al ideal nulo.
3) El esquema $\mathbb{P}^1_{\mathbb{Z}}$ es recubierto por dos copias de spec $(\mathbb{Z}[X])$ de manera análoga a $\mathbb{P}^1$ sobre K.
4) Se puede definir un esquema $E/\mathbb{Z}$ pegando dos esquemas afines definidos así:

V_1 es el espectro de $\mathbb{Z}[x, y]/(-y^2 + x^3 + ax + b)$

V_2 el espectro de $\mathbb{Z}[u, v]/(-v^2 + u(bu^3 + au^2 + 1))$

En este lenguaje una variedad afín "usual" sobre un cuerpo es el espectro de una K-algebra integral (un dominio) de tipo finito. Pero el lenguaje de esquemas es mucho mas rico, por ejemplo podemos hablar de una línea triple (con multiplicidad tres) $X + Y = 0$ como el esquema $L^{(3)} =$ spec $(K[X, Y]/(X + Y)^3)$ o de una variedad sobre $\mathbb{Z}$, que es un esquema $f : \mathcal{X} \to$ spec $(\mathbb{Z})$. Para el punto genérico η de spec $(\mathbb{Z})$, es decir el punto que corresponde al ideal nulo, se obtiene la fibra genérica $X = f^{-1}(\eta)$ que es una variedad sobre $\mathbb{Q}$ Para cada ideal maximal p la fibra nos proporciona una variedad $\mathcal{X}_p = f^{-1}(P)$ que es la reducción de X modulo p.

Bibliografía

[1] M. Artin, *Néron models.* In Arithmetic geometry, Conf., Storrs/Conn. 1984, 213–230 (1986).

[2] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[3] F. Diamond, J. Shurman, *Introduction to modular forms*, Springer 2008.

[4] D. Goldfeld, L. Szpiro, *Bounds for the order of the Tate-Shafarevich group.* Compositio Math. **97** (1995), 71–87.

[5] R. Hartshone, *Algebraic geometry*, Springer-Verlag, 1983.

[6] M. Hindry, J. H. Silverman, *The canonical height and integral points on elliptic curves.* Invent. Math. 93, 419–450 (1988).

[7] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?*, In Diophantine Geometry Proceedings (éd. Zannier), Scuola Norm. Pisa 2007, 197–219.

[8] M. Hindry, *Introduction to zeta and L-functions from arithmetic geometry and some applications*, Notas de un curso en XXI *scola de álgebra*, Brasilia, 2010. Accesible : http://webusers.imj-prg.fr/∼marc.hindry/Notes_rev_Brasilia.pdf

[9] H. Iwaniec, E. Kowalski, *Analytic number theory.* Colloquium Publications. American Mathematical Society 53, 2004.

[10] A. W. Knapp, *Elliptic curves*, Mathematical Notes 40, 1992, Princeton University Press.

[11] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[12] S. Lang, *Conjectured diophantine estimates on elliptic curves.* In Arithmetic and geometry, Pap. dedic. I. R. Shafarevich, Vol. I: Arithmetic, Prog. Math. 35, 155–171 (1983).

[13] J. S. Milne, *Elliptic Curves*, 2006.

[14] O. G. Rizzo, *Average root numbers for a nonconstant family of elliptic curves.* Compositio Math. 136 (2003), 1–23.

[15] J-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou 1969/70, exposé 19.

[16] J. H. Silverman, *Arithmetic of Elliptic Curves*, Springer Verlag, Graduate Texts in Mathematics, vol. 106, 1986.

[17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Verlag, Graduate Texts in Mathematics, vol.151, 1994.

[18] J. H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, 1992, Springer-Verlag.

[19] J. Tate, Séminaire Bourbaki, exposé 306, 1966, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, [volume 9, pages 415-440, Soc. Math. France, 1995].

[20] D. Ulmer, *Elliptic curves with high rank over function fields*, Annals of Math. **155** (2002), 295–315.