7

Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

Comitè editorial
P. Bayer E. Nart J. Quer

UNA BREU INTRODUCCIÓ A LA COHOMOLOGIA CRISTAL·LINA

Edició a cura de

F. Holgado
Facultad de Ciencias
Universidad Autónoma de Madrid

Comitè editorial

P. Bayer
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de
les Corts Catalanes, 585
08007 Barcelona
Espanya

E. Nart
Facultat de Ciències
Universitat Autònoma de
Barcelona
Dep. de Matemàtiques
08193 Bellaterra
Espanya

J. Quer
Facultat de Matemàtiques
i Estadística
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028 Barcelona
Espanya

Barcelona, 2000

Amb suport parcial de DGES PB 96-0166 i PB 96-0970-C02

ISBN: 84-923250- 8-9

Índice General

Introducción 1

1 Polígonos de Newton y Hodge 7
- 1.1 Polígono de Newton de un polinomio 7
- 1.2 F-cristales y sus polígonos 9
- 1.3 F-cristales geométricos 14

2 Polígonos abstractos 17
- 2.1 Propiedades y ejemplos 17
- 2.2 Caso 1: Pendientes de Newton constantes 20
- 2.3 Caso 2: Pendientes de Newton no constantes 21

3 Polígonos geométricos 25
- 3.1 Definiciones y propiedades 25
- 3.2 Género 1 26
- 3.3 Género 2 28
- 3.4 Género 3 33
  - 3.4.1 Las curvas $y^3 = x^4 - ax$ 35
  - 3.4.2 Las curvas $y^3 = x^4 - a$ 39

Bibliografía 41

Introducción

Para estudiar un esquema de tipo finito X, (un ejemplo son las variedades algebraicas), definido sobre un cuerpo finito $k = \mathbb{F}_q$ con $q = p^a$, necesitamos estudiar $N_s = \#(X(\mathbb{F}_{q^s}))$, el número de puntos de X definidos sobre $\mathbb{F}_{q^s}$ para todo $s \geq 1$. La función Zeta de X/k nos da esta información, ya que se tiene que:

$$Z(t; X/k) = \exp\left(\sum_{s=1}^{\infty}\left(\frac{N_s t^s}{s}\right)\right)$$

y de aquí podemos obtener los N_s tomando derivadas logarítmicas.

Acerca de la función Zeta, Weil propuso las siguientes conjeturas. Sea X/k un esquema de tipo finito de dimensión n. Entonces:

i) *Racionalidad.* $Z(t)$ es una función racional de t, es decir, un cociente de polinomios en t.

ii) *Ecuación funcional.* Sea E el número de autointerseccion de la diagonal Δ de $X \times X$. Entonces $Z(t)$ satisface la siguiente ecuación funcional

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(t).$$

iii) *"Hipótesis de Riemann".* Es posible escribir

$$Z(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

donde $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$ y para cada $1 \leq i \leq 2n-1$, $P_i(t)$ es un polinomio con coeficientes enteros de la forma

$$P_i(t) = \prod_j (1 - \alpha_{ij} t),$$

donde los α_{ij} son enteros algebraicos con $|\alpha_{ij}| = q^{i/2}$.

iv) *Números de Betti.* Si definimos el i-èsimo número de Betti $B_i = B_i(X)$ como el grado del polinomio $P_i(t)$, se tiene que $E = \sum(-1)^i B_i$

Para intentar demostrar estas conjeturas, se buscó una teoría cohomológica para variedades definidas sobre cuerpos de característica $p > 0$ que tuviera buenas propiedades. En particular, la teoría cohomológica buscada debería tener sus coeficientes en un cuerpo de característica cero, K, para poder contar los puntos fijos de un morfismo como una suma alternada de trazas en los grupos de cohomología. A una tal cohomología se le llama cohomología de Weil. Las principales propiedades que debe tener son:

1. $H^i(X, K)$ es un funtor contravariante en X.

2. Los grupos $H^i(X, K)$ son espacios vectoriales sobre K de dimensión finita. Además, son cero excepto en el intervalo $0 \leq i \leq 2n$, donde n es la dimensión de X.

3. Hay una estructura de producto

$$H^i(X, K) \times H^j(X, K) \to H^{i+j}(X, K)$$

definida para todo i, j.

4. *Dualidad de Poincaré.* Si X es liso y propio sobre k, entonces $H^{2n}(X, K)$ es 1-dimensional y el producto cup

$$H^i(X, K) \times H^{2n-i}(X, K) \to H^{2n}(X, K)$$

es perfecto para cada $1 \leq i \leq 2n$.

5. *Fórmula de puntos fijos de Lefschetz.* Sea X liso y propio sobre k. Sea $f : X \to X$ un morfismo. Sea $L(f, X)$ el número de puntos fijos de f contados con multiplicidad. Entonces

$$L(f, X) = \sum (-1)^i \mathrm{Tr}(f^*; H^i(X, K))$$

donde f^* es la función inducida en la cohomología de X.

Dos ejemplos importantes de cohomologías de Weil son:

i) *La cohomología ℓ-ádica.* Sea X un esquema de tipo finito sobre un cuerpo algebraicamente cerrado, k, de característica $p \geq 0$. Sea ℓ un número primo $\ell \neq p$. Sea $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^r\mathbb{Z}$ el anillo de enteros ℓ-ádicos, y $\mathbb{Q}_\ell$ su cuerpo de fracciones. Consideramos la topología étale en X, y definimos la cohomología ℓ-ádica de X como:

$$H^i(X, \mathbb{Q}_\ell) = (\varprojlim H^i_{ét}(X, \mathbb{Z}/\ell^r\mathbb{Z})) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

ii) *La cohomología cristalina.* Sea X un esquema sobre un cuerpo perfecto, k, de característica $p > 0$. Sea $W = W(k)$ el anillo de vectores de Witt y W_n el anillo $W_n(k) = W/p^n$. La cohomología cristalina es por definición el límite inverso de las cohomologías de los haces estructurales sobre los sitios cristalinos $(X/W_n)_{\text{cris}}$, es decir:

$$H^i(X/W) = \varprojlim_n H^i(X/W_n) \text{ donde } H^i(X/W_n) = H^i((X/W_n)_{\text{cris}}, \mathcal{O}_{X/W_n}).$$

La relación entre la función Zeta y una cohomología de Weil es la siguiente, sea X una variedad proyectiva definida sobre el cuerpo finito $k = \mathbb{F}_q$, y sea $\bar{X} = X \times_k \bar{k}$ la correspondiente variedad sobre el cierre algebraico $\bar{k}$ de k. Definimos el *morfismo de Frobenius* $f : \bar{X} \to \bar{X}$ enviando el punto P con coordenadas (a_i), $a_i \in \bar{k}$ al punto con coordenadas (a_i^q). Como $\bar{X}$ está definido por ecuaciones con coeficientes en k, $f(P)$ es también un punto de $\bar{X}$. Además, P es un punto fijo de f si y sólo si sus coordenadas están en k. De forma general, P es un punto fijo de la iterada f^r si y sólo si tiene coordenadas en el cuerpo $k_r = \mathbb{F}_{q^r}$. Entonces tenemos que:

$$N_r = \#\{\text{puntos fijos de} f^r\} = L(f^r, \bar{X}).$$

Si X es lisa, dada cualquier cohomología de Weil, podemos calcular este número por la fórmula de puntos fijos de Lefschetz, obteniendo:

$$N_r = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}\,(f^{r*}; H^i(\bar{X}, K)).$$

Esta igualdad la podemos relacionar con el polinomio característico de f^* mediante el siguiente lema:

Lema 0.1 *Sea φ un endomorfismo de un espacio vectorial finito dimensional, V, sobre un cuerpo K. Entonces tenemos la siguiente igualdad entre series formales:*

$$\exp(\sum_{r=1}^{\infty} Tr\,(\varphi^r; V)\frac{t^r}{r}) = \det(1 - \varphi t; V)^{-1}.$$

Entonces, aplicando el anterior lema , sustituyendo en la función Zeta y realizando algunas manipulaciones algebraicas, obtenemos que la función Zeta se puede expresar como un producto alternado de polinomios característicos,

$$Z(t; X/k) = \prod_i \det(1 - f^* t; H^i(\bar{X}, K))^{(-1)^{i+1}} = \prod_i P_i(t)^{(-1)^{i+1}}$$

La anterior descomposición expresa la función Zeta como un producto alternado de polinomios cuyos coeficientes están en el cuerpo de coeficientes de la cohomología de Weil particular que estemos usando, sin embargo Weil conjeturó

y más tarde fue demostrado por Deligne que los polinomios de la descomposición tienen coeficientes enteros, y que son independientes de la cohomología que estemos usando.

Entonces si α es una raíz recíproca de uno de los P_i, se tiene que α es un entero algebraico. Además, gracias a la ecuación funcional, también lo es q^d/α. Por lo tanto, podemos concluir que α es una unidad ℓ-ádica para todo primo $\ell \neq p$, quedándonos por resolver dos cuestiones concernientes a los distintos valores absolutos de α:

1. "La Hipótesis de Riemann": ¿Cuál es el valor absoluto de α y sus conjugados?

2. ¿Cuál es el valor absoluto p-ádico de α y sus conjugados?

La pregunta 1 fue contestada por Deligne y gracias a ella se consigue estimar el número de puntos racionales de X/k.

La respuesta a la pregunta 2 tiene como consecuencia la obtención de información, módulo potencias de p, sobre el número de puntos racionales de X sobre k y sus extensiones.

En este trabajo nos centraremos en esta segunda pregunta, y más concretamente en una conjetura de Katz que relaciona los valores de $\mathrm{ord}(\alpha)$, mediante una serie de desigualdades, con los números de Hodge de X. Esta conjetura se visualiza mejor geométricamente mediante los llamados polígonos de Newton y Hodge.

Estos resultados se generalizan en el libro de Ogus [14], donde se estudia como varía la relación entre la filtración de Hodge y la acción de Frobenius en una familia de F-cristales parametrizada por un esquema liso, X/k, dándonos una filtración de un F-cristal global formado por la unión de todos ellos. Como aplicaciones, demuestra una versión de la conjetura de Katz válida para el F-cristal global y resultados acerca de la degeneración de la sucesión espectral de Hodge y de la sucesión espectral conjugada.

En el capítulo 1, introduciremos los conceptos básicos que nos permiten definir los polígonos, las principales propiedades de los mismos, así como los resultados más importantes dentro de este campo.

Una vez que tenemos definidos para cada esquema de tipo finito liso unos invariantes geométricos como son los polígonos de Newton y de Hodge, en el resto del trabajo, que es la parte de investigación propiamente dicha, nos preguntaremos por el problema inverso, es decir:

PREGUNTA:Dados un polígono de Newton y un polígono de Hodge que satisfagan las propiedades que necesitan cumplir para poder ser los polígonos asociados a un esquema de tipo finito y liso. ¿Existe un tal esquema, cuyos polígonos sean los dados?

En el capítulo 2, nos centraremos en los llamados polígonos abstractos y veremos que la respuesta a nuestra pregunta es sí cuando el cuerpo de definición es $k = \mathbb{F}_p$ con p un número primo. Además la demostración es constructiva, es decir daremos un algoritmo para decidir quién es el objeto abstracto que tiene como invariantes asociados los polígonos dados.

El capítulo 3 trata de los polígonos geométricos, y motivados por una pregunta que hace B. Mazur en [12], donde deja abierta la cuestión de si todos los posibles polígonos para curvas de género 3 lisas (que son un ejemplo de esquemas de tipo finito y liso) ocurren en la realidad, daremos ejemplos de curvas para cada polígono estudiando dos familias de curvas distintas. Además también daremos ejemplos para género 1 (curvas elípticas) y género 2.

En la actualidad, la respuesta a que posibles polígonos de Newton ocurren como polígonos de Newton de una curva de género g sigue estando abieta. Es bien sabido que la curva genérica es ordinaria, pero en general, ni siquiera se sabe si para cada género existen curvas supersingulares definidas sobre un cuerpo de característica $p > 0$. Los resultados más generales que se conocen se refieren a característica 2. Para $p = 2$, se sabe que existen curvas supersingulares para cualquier género definidas sobre $\mathbb{F}_2$ (véase [6]), mientras que para $p > 2$ sólo se conocen cuvas supersingulares para aquellos géneros tales que su desarrollo p-ádico sólo tiene coeficientes 0 y $(p-1)/2$. Para más detalles acerca de que casos son conocidos o no, nos referimos a [4].

Capítulo 1

Polígonos de Newton y Hodge

1.1 Polígono de Newton de un polinomio

Para reunir la información de los ceros de un polinomio con coeficientes en un cuerpo p-ádico completo K, es decir, cualquier subcuerpo cerrado de $\mathbb{C}_p$ (el cierre algebraico y cerrado de $\mathbb{Q}_p$), se introduce el polígono de Newton de un polinomio de la siguiente forma.

Sea $f(X) \in K[X]$ un polinomio. Como estamos interesados en entender los ceros de $f(X)$, podemos extraer cualquier potencia de X que divida a $f(X)$ y suponer que $f(0) \neq 0$. También, dividiendo entre $f(0)$, podemos suponer que $f(0) = 1$. Por lo tanto, tenemos:

$$f(X) = 1 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

con los $a_i \in K$. En unos ejes coordenados, consideramos los puntos $(0,0)$ y, para cada i entre 1 y n, $(i, v_p(a_i))$, donde v_p es la valoración p-ádica normalizada de modo que $v_p(p) = 1$. (Si algunos de los a_i es nulo, lo ignoramos, ya que entonces $v_p(a_i) = +\infty$, y el punto estaría "infinitamente alto"). El *polígono de Newton* de $f(X)$ es la envolvente convexa de los puntos considerados, empezando en $(0,0)$ y terminando en $(n, v_p(a_n))$. El algoritmo para construirlo consiste en empezar con la semirrecta negativa del eje y, fijarla en el $(0,0)$, y rotarla en el sentido contrario a las aguas del reloj hasta que "chocamos"con uno de los puntos considerados, en ese momento, fijamos la semirrecta en ese punto y seguimos rotando el resto hasta el próximo punto. Reiteramos este proceso hasta que alcanzamos el punto $(n, v_p(a_n))$. Por último, nos olvidamos de la parte de la semirrecta no usada.

Observación 1.1 El polígono de Newton depende sólo de los $v_p(a_i)$, que no dependen de a que cuerpo pertenezcan los a_i. Es decir, el polígono depende del polinomio como elemento de $\mathbb{C}_p[X]$, y no del cuerpo K donde estén definidos sus coeficientes.

Ejemplo 1.2 Sea $p = 3$ y consideremos el polinomio

$$f(X) = 1 + 6X + \frac{2}{3}X^2 + 18X^4 + 18X^5 + 162X^6$$

Los puntos que tenemos que considerar son $(0,0), (1,1), (2,-1), (4,2), (5,2)$ y $(6,4)$, y el polígono viene descrito en la figura 1.1

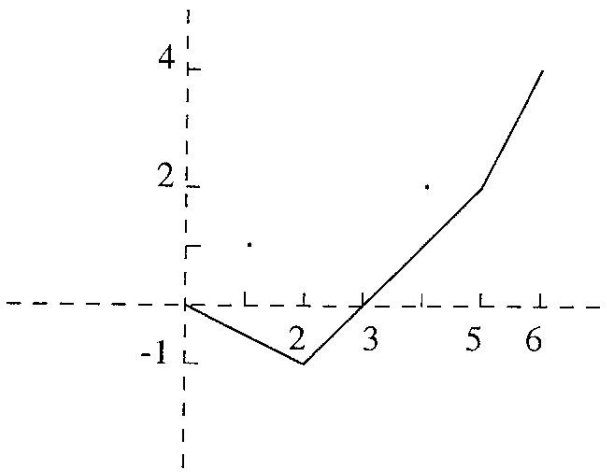


Figura 1.1: Polígono de Newton de $f(X)$

Dentro del polígono, la información que nos interesa viene dada por los siguientes elementos:

Definición 1.3 i) Las *pendientes de Newton* de $f(X)$ son las pendientes de los segmentos que aparecen en el polígono.

ii) La *longitud* de cada pendiente es la longitud de la proyección del segmento sobre el eje de abscisas.

iii) Los *puntos de corte* son los valores de i tales que el punto $(i, v_p(a_i))$ es un vértice del polígono.

Ejemplo 1.4 En el ejemplo anterior, las pendientes son $-1/2$, 1 y 2, con longitudes 2, 3 y 1 respectivamente, y los puntos de corte son 0, 2, 5 y 6.

Observación 1.5 La suma de las longitudes es igual al grado del polinomio, y por la construcción del polígono, también es evidente que las pendientes forman una sucesión creciente.

Una vez definido el polígono de Newton, nos interesamos en la información que dicho polígono nos da acerca de los ceros del polinomio.

Teorema 1.6 *Sea $f(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ un polinomio, y sea $f(X) = (1 - X/\alpha_1)(1 - X/\alpha_2)\cdots(1 - X/\alpha_n)$ su factorización en términos de sus raíces $\alpha_i \in \mathbb{C}_p$. Sea $\lambda_i = v_p(1/\alpha_i)$. Entonces, si λ es una pendiente del polígono de Newton con longitud l, se tiene que exactamente l de los λ_i son iguales a λ. Es decir, las pendientes del polígono de Newton de $f(X)$ son (contando multiplicidades) las valoraciones p-ádicas de las raíces recíprocas de $f(X)$.*

Demostración: Ordenamos los $1/\alpha_i$ de manera que $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Supongamos que $\lambda_1 = \lambda_2 = \cdots = \lambda_r < \lambda_{r+1}$. Veamos que el primer segmento del polígono de Newton une los puntos $(0,0)$ y $(r, r\lambda_1)$. Se tiene que cada a_i se expresa en términos de $1/\alpha_1, 1/\alpha_2, \ldots 1/\alpha_n$ como $(-1)^i$ veces el i-ésimo polinomio simétrico, es decir, la suma de todos los posibles productos de i de los $1/\alpha_i$. Como el valor p-ádico de cada uno de esos productos es al menos $i\lambda_1$, lo mismo le sucede a a_i. Entonces, el punto $(i, v_p(a_i))$ está en o sobre la recta que une $(0,0)$ con $(r, r\lambda_1)$. Consideremos ahora a_r. De los distintos productos de r de los $1/\alpha_i$, exactamente uno tiene tiene valoración p-ádica $r\lambda_1$, el producto $1/(\alpha_1\alpha_2\cdots\alpha_r)$, todos los demás tienen valoración p-ádica mayor, ya que debe incluir a uno de los $1/\alpha_{r+1}, 1/\alpha_{r+2}, \ldots, 1/\alpha_n$. Entonces, a_r es la suma de algo de valor $r\lambda_1$ y algo de valor mayor que $r\lambda_1$, por lo tanto, por el "principio del triángulo isósceles", $v_p(a_r) = r\lambda_1$. Nos falta ver que $(r, r\lambda_1)$ es un vértice, para ello veremos que los puntos $(i, v_p(a_i)), i > r$ están por encima de la recta considerada. Supongamos $i > r$, por lo tanto, por las mismas razones que antes, el producto de i de los $1/\alpha_i$ tiene valoración $> i\lambda_1$, y entonces $v_p(a_i) > i\lambda_1$. Para completar la demostración, sólo hace falta realizar está misma prueba con cada grupo de valoraciones iguales, es decir si $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \cdots \lambda_{s+t} < \lambda_{s+t+1}$, entonces el segmento que une $(s, \lambda_1 + \lambda_2 + \cdots + \lambda_s)$ con $(s+t, \lambda_1 + \lambda_2 + \cdots + \lambda_s + t\lambda_{s+1})$ es un segmento del polígono de Newton.

■

1.2 F-cristales y sus polígonos

En esta sección definiremos los polígonos de Newton y Hodge asociados a un F-cristal así como la relación existente entre ellos.

Sea k un cuerpo perfecto de característica $p > 0$, $W = W(k)$ su anillo de vectores de Witt y $K = FracW$ el cuerpo de fracciones de W. También denotaremos por σ al automorfismo de Frobenius de W.

Definición 1.7 Sea A un anillo y $f : A \to A$ un homomorfismo de anillos. Dado un A-módulo M y una aplicación $\phi : M \to M$, se dice que ϕ es f-lineal si:

$$\phi(m + n) = \phi(m) + \phi(n), \qquad \forall m, n \in M$$

ii) $\phi(am) = f(a)\phi(m), \quad \forall a \in A \qquad \forall m \in M$

Definición 1.8 i) Un *F-cristal* sobre k es un W-módulo libre finitamente generado, M, junto con una aplicación $\varphi : M \to M$ σ-lineal inyectiva.

ii) Un *morfismo* entre el F-cristal M y el F-cristal N es una aplicación W-lineal $u : M \to N$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ \varphi\downarrow & \circlearrowleft & \downarrow\varphi \\ M & \xrightarrow{u} & N \end{array}$$

iii) Una *isogenia* es un morfismo de F-cristales que induce un isomorfismo de K-espacios vectoriales $M \otimes_W K \to N \otimes_W K$.

Ejemplo 1.9 Sea X/k un esquema propio y liso de dimensión n y sea el módulo libre $M = H^m(X/W)/$torsión, i.e., el m-ésimo módulo de cohomología cristalina. En el módulo M se tiene una acción de Frobenius φ, inducida por el morfismo de Frobenius de X. Para probar que es inyectiva, usamos la aplicación bilineal $H^m(X/W) \times H^{2n-m}(X/W) \longrightarrow H^{2n}(X/W) \xrightarrow{Tr} W$ que cumple la siguiente relación $<\varphi x, \varphi y>= p^d\sigma(<x, y>)$ y además, gracias a la dualidad de Poincaré, no tiene núcleo, por lo que si $x \neq 0$, se tiene que $\varphi x \neq 0$.

Ejemplo 1.10 Sea $W_\sigma[T]$ el anillo no conmutativo de polinomios en T con la relación $T\omega = \sigma(\omega)T$ si $\omega \in W$. Sea $\alpha = r/s \in \mathbb{Q}_+$ un racional positivo con $r \in \mathbb{N}$ y $s \in \mathbb{N}^*$ primos entre sí. Definimos $M_\alpha = W_\sigma[T]/(T^s - p^r)$ y si $m \in M_\alpha$, definimos $\varphi(m) = Tm$. Se tiene que φ es σ-lineal por la definición de la operación en $W_\sigma[T]$ y además es inyectiva, ya que si $\varphi(m) = 0$, entonces $T^s m = p^r m = 0$, con lo que $m = 0$. Diremos que M_α tiene pendiente α.

El interés que tiene el primer ejemplo se debe a que nos servirá cuando tratemos con F-cristales geométricos (sección 1.3), ya que se tiene que la cohomología cristalina es una cohomología de Weil y por tanto aparece en la función Zeta de manera natural.

El interés del segundo ejemplo se debe al siguiente resultado:

Teorema 1.11 (Dieudonné-Manin) *i) Supongamos que k es un cuerpo algebraicamente cerrado. Entonces, la categoría de F-cristales salvo isogenia es semisimple y sus objetos simples son los M_α para $\alpha \in \mathbb{Q}_+$ definidos antes. Es decir, todo F-cristal, M, es isogeno a una suma directa $\bigoplus_{\alpha\in\mathbb{Q}_+} M_\alpha^{n_\alpha}$ de F-cristales de pendiente α. Los racionales α para los que $n_\alpha \neq 0$ son por definición las* pendientes *de M, y el entero $n_\alpha \dim_W(M_\alpha)$ es la* multiplicidad *de la pendiente α. Si k no es algebraicamente cerrado, las pendientes de M son por definición las pendientes de $M \otimes_W W(\bar{k})$*

ii) Si $k = \mathbb{F}_q$ es un cuerpo finito, con $q = p^a$, las pendientes *de M son las valoraciones p-ádicas (normalizadas por $v(q) = 1$) de los valores propios del automorfismo W-lineal φ^a; la* multiplicidad *de la pendiente α es el número de valores propios de valoración α.*

Demostración: Para una demostración de este teorema, véase [11]

■

Observación 1.12 Aunque no damos la demostración del teorema, es fácil ver que la parte *ii)* es sólo un caso particular de la parte *i)*, ya que si consideramos el automorfismo W-lineal, φ^a, asociado a φ, tenemos que, en el factor M_α, $\varphi^a(m) = T^a(m) = (p^{r/s})^a m$, es decir, $(p^a)^{r/s}$ es un autovalor y tiene valoración normalizada r/s, por lo que coincide con la definición de pendiente en *i)*. Además es un autovalor para cada $m \in \{1, T, \ldots, T^{s-1}\}$, base de M_α, por lo que las multiplicidades también coinciden.

Observación 1.13 La descomposición de un F-cristal como una suma directa de F-cristales de la forma M_α es única, ya que M_α no es isogeno a M_β si $\alpha \neq \beta$. En efecto, supongamos que M_α fuese isogeno a M_β con $\alpha = r/s$ y $\beta = r'/s'$; entonces, existe una aplicación $u : M_\alpha \to M_\beta$ W-lineal tal que el diagrama de la definición 1.8 conmuta, es decir, $u \circ \varphi_\alpha = \varphi_\beta \circ u$. Si componemos los dos lados de la igualdad con φ_α^{s-1}, y usamos la conmutatividad del diagrama, obtenemos que $u \circ \varphi_\alpha^s = \varphi_\beta^s \circ u$. Evaluando está igualdad en $m_\alpha \in M_\alpha$, obtenemos $u(T^s(m_\alpha)) = T^s u(m_\alpha)$, es decir, $p^r u(m_\alpha) = T^s u(m_\alpha)$. Si tomamos $m_\alpha = 1$, entonces $p^r = T^s$ en M_β, con lo que $T^{s'} - p^{r'} | T^s - p^r$. Intercambiando el papel de M_α y M_β, obtenemos $T^s - p^r | T^{s'} - p^{r'}$, con lo que $s = s'$ y $r = r'$.

Una vez que tenemos definidos los F-cristales y las pendientes, podemos definir el polígono de Newton de un F-cristal. Aunque la definición parece no ser la misma que para el caso de un polinomio, en el último capítulo veremos que para el caso de $\mathbb{F}_p$, el polígono de Newton de un F-cristal geométrico es el polígono de Newton de cierto polinomio asociado al F-cristal.

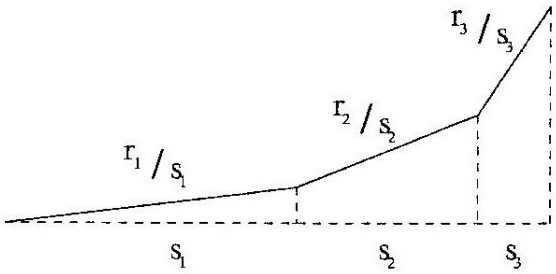


Figura 1.2: Polígono de Newton

Definición 1.14 El *polígono de Newton* de un F-cristal, $M \simeq \bigoplus_{i=1}^{t} M_{r_i/s_i}$ con $r_i/s_i \leq r_{i+1}/s_{i+1}$, es el polígono convexo en el plano cuyo punto más a la izquierda está en el origen y que tiene pendiente r_i/s_i en el tramo horizontal $[s_1 + s_2 + \cdots + s_{i-1},\ s_1 + s_2 + \cdots + s_i]$.

Para definir el polígono de Hodge, necesitamos "linealizar"el morfismo del F-cristal, para ello definimos un nuevo módulo $M^{(\sigma)} = M \otimes_W W^{(\sigma)}$, donde $W^{(\sigma)}$ es el anillo W, pero con la estructura de W-módulo que le da $\sigma : W \to W$. Por lo tanto,el morfismo de un F-cristal es equivalente a un morfismo W-lineal $\varphi : M^{(\sigma)} \hookrightarrow M$. Entonces, gracias al teorema del factor invariante, podemos elegir W-bases de $M^{(\sigma)}$ y de M tal que φ es representable por una matriz diagonal con coeficientes:

$$1, \ldots, 1, p, \ldots, p^2, \ldots, p^2, \ldots, p^m, \ldots, p^m.$$

Sea $h_j := \#\ p^j$ en la diagonal, entonces:

Definición 1.15 El *polígono de Hodge*, se define como el polígono convexo en el plano cuyo punto más a la izquierda es el $(0,0)$ y que tiene pendiente *i en el intervalo horizontal* $[h_0 + \cdots + h_{i-1}, h_0 + \cdots + h_i]$

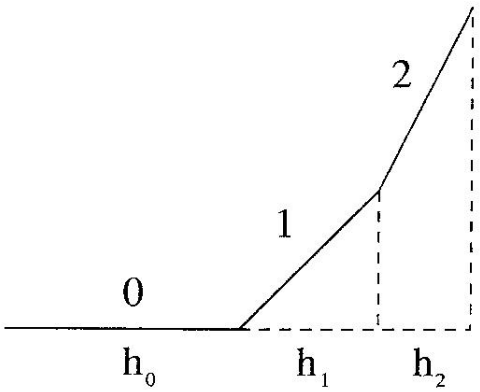


Figura 1.3: Polígono de Hodge

Los polígonos de Newton y de Hodge de un F-cristal están relacionados mediante una serie de desigualdes que relacionan sus pendientes y que se enuncian de una forma mucho más clara si la visualizamos geométricamente. De esta forma geométrica, el enunciado es el siguiente:

Teorema 1.16 *Dado un F-cristal,(M, φ), su polígono de Newton está por encima de su polígono de Hodge. Además, ambos polígonos tienen el mismo punto inicial, $(0,0)$, y también tienen el mismo punto final.*

Antes de dar la demostración del teorema vamos a definir las potencias exteriores de un F-cristal, que jugarán un papel importante en la demostración.

Definición 1.17 La *i-ésima potencia exterior* de un F-cristal, (M, φ), es el F-cris- tal $\left(\bigwedge^i M, \bigwedge^i(\varphi)\right)$, donde el módulo subyacente es $\bigwedge^i_W(M)$, y donde $\bigwedge^i(\varphi)$ viene definido por:

$$\bigwedge^i(\varphi)(m_1 \wedge \ldots \wedge m_i) = \varphi(m_1) \wedge \ldots \wedge \varphi(m_i).$$

Si $i = 0$, pero $(M, \varphi) \neq 0$, definimos $\left(\bigwedge^0 M, \bigwedge^0(\varphi)\right) = (W, \sigma)$.

La utilidad de las potencias exteriores estriba en que sus pendientes de Newton y Hodge están relacionadas con las de M, ya que si $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_r$ son las pendientes de Newton (resp. de Hodge) de M, entonces las pendientes de Newton (resp. de Hodge) de la i-ésima potencia exterior son las $\binom{r}{i}$ pendientes $\lambda_{j_i} + \cdots + \lambda_{j_i} \quad 1 \leq j_1 < \cdots < j_i \leq r$, con lo que, por ejemplo, la suma de las i primeras pendientes de M es la primera pendiente de $\bigwedge^i M$.

Demostración (del teorema 1.16): Para probar el teorema basta con demostrar que en cada punto con coordenada x entera, el polígono de Newton está por encima de el polígono de Hodge, ya que las pendientes de cada polígono forman una sucesión creciente. Para cualquier F-cristal de rango 1, la pendiente de Hodge y la pendiente de Newton coinciden de manera obvia, por lo tanto aplicando está observación a $\left(\bigwedge^0 M, \bigwedge^0(\varphi)\right) = (W, \sigma)$ y a $\left(\bigwedge^r M, \bigwedge^r(\varphi)\right)$ con $r = \mathrm{rg}(M)$, obtenemos que los dos polígonos empiezan y acaban igual. Para ver que:

$$Newton(i) \geq Hodge(i) \quad para \quad 1 \leq i \leq r$$

donde $Newton(i)$ = altura del polígono en el punto i (resp. $Hodge(i)$), basta con probar que para las potencias exteriores de (M, φ) se tiene que:

$$menor\ pendiente\ de\ Newton \geq menor\ pendiente\ de\ Hodge,$$

es decir, queremos probar $Newton(1) \geq Hodge(1)$ de manera universal.

Para ello, cálculamos la forma canónoca de Jordan de la matriz en un anillo donde estén definidos todos sus autovalores (será una extensión finita de W), quedándonos una matriz triangular superior, J, con los autovalores en la diagonal. Para terminar, sólo hace falta observar que la menor pendiente de Hodge es el mayor exponente entero, A, tal que $\varphi \equiv 0 \pmod{p^A}$, por lo que la menor pendiente de Hodge es la parte entera de la menor de las valoraciones de los coeficientes de J, que es menor que la menor de las valoraciones de los coeficientes de la diagonal.

■

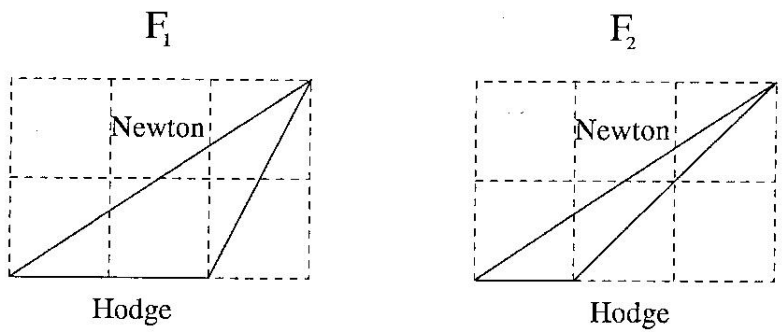
Ejemplo 1.18 Sean $(\mathbb{Z}_p^3, F_1)$, $(\mathbb{Z}_p^3, F_2)$, dos F-cristales dados por las aplicaciones $F_i : \mathbb{Z}_p^3 \to \mathbb{Z}_p^3$, $i = 1, 2$ con matrices,

$$F_1 = \begin{bmatrix} 0 & 0 & p^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad F_2 = \begin{bmatrix} 0 & 0 & p \\ 1 & 0 & 0 \\ 0 & p & 0 \end{bmatrix}$$

Para calcular las pendientes de Newton, tenemos que calcular los autovalores de las aplicaciones (ya que $\mathbb{Z}_p = W(\mathbb{F}_p)$, por lo que $a = 1$ y nuestras aplicaciones son lineales). En ambos casos se tiene que el único autovalor es $p^{2/3}$ con multiplicidad 3, es decir, la única pendiente de Newton es $2/3$ con multiplicidad 3. Para calcular las pendientes de Hodge, hay que calcular bases tal que las matrices sean diagonales. En ambos casos es evidente el cambio de base y también los elementos de la diagonal: para F_1 son 1, 1 y p^2, con lo que sus pendientes de Hodge son 0 con multiplicidad 2 y 2 con multiplicidad 1; para F_2 son 1, p y p, con lo que sus pendientes de Hodge son 0 con multiplicidad 1, y 1 con multiplicidad 2. Como tienen el mismo polígono de Newton, su descomposición en una suma directa de M_α's es la misma, por lo que son isogenos, y una isogenia viene dada por $u : F_2 \to F_1$ definida por la matriz

$$u = \begin{bmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Al tener distinto polígono de Hodge, se tiene que los dos F-cristales no son isomorfos (el determinante de la isogenia es p^2, que no es invertible en $\mathbb{Z}_p$).



1.3 F-cristales geométricos

En el resto del capítulo, trataremos el caso geométrico.

Sea X/k un esquema propio y liso de dimensión n (puede pensarse en una variedad algebraica proyectiva y lisa).

Definición 1.19 Por el *polígono m-dimensional de Newton* de X/k nos referiremos al polígono de Newton del F-cristal $H^m(X/W)/torsión$

Definición 1.20 Por el *polígono m-dimensional de Hodge abstracto* de X/k nos referiremos al polígono de Hodge del F-cristal $H^m(X/W)/torsión$

Definición 1.21 Por el *polígono m-dimensional de Hodge geométrico* nos referiremos al polígono convexo en el plano cuyo punto más a la izquierda es el $(0,0)$ y que tiene pendiente j en el intervalo $[h^{0,m}+h^{1,m-1}+\cdots+h^{j-1,m-j+1}, h^{0,m}+h^{1,m-1}+\cdots+h^{j,m-j}]$, donde $h^{i,m-i} := \dim_K H^{m-i}(X_K, \Omega^i_{X/K})$

En el caso geométrico, los dos polígonos también están relacionados mediante la llamada "Conjetura de Katz".

Teorema 1.22 (Conjetura de Katz) *El polígono m-dimensional de Newton de X/k está por encima del polígono m-dimensional de Hodge geométrico de X/k.*

El resultado anterior fue probado por Mazur en [13] bajo ciertas hipótesis, y más tarde, Ogus lo probó de manera general en [2]. Además, en numerosos casos se tiene que las pendientes de Hodge abstractas coinciden con las pendientes de Hodge geométricas y por tanto los puntos finales de los polígonos también coinciden gracias al teorema 1.16. Los casos más importantes donde se da esta igualdad de pendientes son:

i) *Existencia de Levantamiento.* Supongamos que existe un levantamiento de X/k a característica cero, i.e., existe un esquema propio y liso $\mathfrak{X}/W$ tal que $X = \mathfrak{X} \times_W k$, y que los grupos de cohomología $H^q(\mathfrak{X}, \Omega^p_{\mathfrak{X}/W})$ no tienen torsión. Entonces los números de Hodge abstractos coinciden con los geométricos. Más explicitamente, se tiene que $h^j = h^{j,m-j}$.

ii) *Degeneración de la Sucesión Espectral.* Si los grupos $H^m(X/W)$ no tienen torsión, y si la sucesión espectral Hodge-de Rham

$$E_1^{ij} = H^j(X, \Omega^i_{X/k}) \Rightarrow H^{i+j}_{dR}(X/k)$$

degenera en E_1, entonces los polígonos de Hode abstracto y geométrico son iguales.

Observación 1.23 En el caso geométrico, también tenemos una serie de restricciones acerca de los posibles valores de las pendientes de Newton y Hodge. Estas restricciones son:

1. *Con respecto a las pendientes de Newton.*

i) La aplicación φ del F-cristal geométrico satisface, mediante la *dualidad de Poincaré*, la siguiente relación:

$$\varphi \circ \varphi^{\vee} = p^n,$$

por lo tanto, las pendientes de $H^m(X/W)/torsión$ están en el intervalo $[0, n]$.

ii) Usando también la *dualidad de Poincaré*, se tiene que si α es una pendiente de H^m, entonces $n - \alpha$ es una pendiente de H^{2n-m} con la misma multiplicidad.

iii) Por el *Teorema fuerte de Lefschetz*, el cuál demuestra que $H^{n-k} \simeq H^{n+k}$, se tiene que si α es una pendiente H^m, entonces $n - m + \alpha$ es una pendiente de H^{2n-m} con la misma multiplicidad y por tanto, aplicando la *dualidad de Poincaré* a esta pendiente obtenemos que $m - \alpha$ es una pendiente de H^m.

iv) Combinando los anteriores hechos, es evidente que el punto final del polígono de Newton es $(\beta, m\beta/2)$, donde $\beta = \dim(H^m(X/W))$ es el m-ésimo número de Betti de X.

v) Si $0 \leq m \leq n$, las pendientes de Newton están en $[0, m]$, ya que todas las pendientes son positivas y $\alpha, m - \alpha$ son pendientes de H^m. Si $n \leq m \leq 2n$, las pendientes de Newton están entre $[m - n, n]$, ya que si $\alpha < m - n$, entonces $n - m + \alpha < 0$ y tendría que ser una pendiente de Newton de H^{2n-m}.

2. *Con respecto a las pendientes geométricas de Hodge.*

Como $H^{m-i}(X_K, \Omega^i_{X/K})$ es el dual de $H^i(X_K, \Omega^{m-i}_{X/K})$, sus dimensiones coinciden y por tanto $h^{i,m-i} = h^{m-i,i}$, donde $h^{j,m-j} := \dim_K H^{m-j}(X_K, \Omega^j_{X/K})$.

Capítulo 2

Polígonos abstractos

En este capítulo nos centraremos en la busqueda de F-cristales con polígonos de Newton y Hodge dados. Es decir, dados un polígono de Newton y un polígono de Hodge, trataremos de encontrar un F-cristal que los tenga como polígonos asociados. Durante todo el capítulo trataremos, salvo mención explícita, el problema anterior cuando $k = \mathbb{F}_p$ con p un número primo, por lo tanto $W = W(k) = \mathbb{Z}_p$, el anillo de enteros p-ádicos, además, las aplicaciones que definen los F-cristales son lineales, ya que $\sigma(a) = a \quad \forall a \in \mathbb{Z}_p$.

2.1 Propiedades y ejemplos

El algoritmo que vamos a utilizar para construir los F-cristales consiste en fijar las pendientes de Newton y entonces, construir todos los polígonos de Hodge posibles para esas pendientes de Newton, teniendo en cuenta que los polígonos de Hodge tienen pendientes enteras, van por debajo del polígono de Newton y empiezan y acaban en el mismo punto. Una vez construidas todas las parejas Newton-Hodge (todas con el mismo polígono de Newton), construiremos F-cristales con esas parejas como polígonos asociados.

Definición 2.1 Una *pareja de polígonos de Katz* son un polígono con pendientes racionales de longitud uno, admitiendo repeticiones, $\{n_1, \ldots, n_r\}$, y puntos de corte con coordenadas enteras, y un polígono con pendientes enteras de longitud uno, admitiendo repeticiones, $\{h_1, \ldots, h_r\}$, empezando ambos en el punto $(0,0)$ y tales que:

i) $\sum_{a=1}^{r} h_a = \sum_{a=1}^{r} n_a$

ii) $\sum_{a=1}^{b} h_a \leq \sum_{a=1}^{b} n_a, \quad \forall b < r \quad b \in \mathbb{N}^*$

Observación 2.2 Dado que estamos en el caso $k = \mathbb{F}_p$, y los F-cristales son W-módulos libres de dimensión finita, todos nuestros F-cristales tendrán como

módulo asociado $\mathbb{Z}_p^r$, donde r es el rango del F-cristal, por lo tanto, para definir un F-cristal nos limitaremos a dar su aplicación W-lineal en forma de matriz (con respecto a la base canónica salvo mención explícita).

Empezamos con un resultado que simplifica mucho, a la hora de realizar los cálculos explícitos, la construcción de F-cristales.

Teorema 2.3 *Sea (M, φ) un F-cristal de rango r. Sea $(A, b) \in \mathbb{Z} \times \mathbb{Z}$ un punto del polígono de Newton de (M, φ) que también sea un punto del polígono de Hodge de (M, φ). Entonces existe una única descomposición de (M, φ) como una suma directa:*

$$(M, \varphi) \simeq (M_1, \varphi_1) \oplus (M_2, \varphi_2)$$

de dos F-cristales (M_1, φ_1), (M_2, φ_2) tales que:

i) M_1 tiene rango A, sus pendientes de Newton son las A primeras pendientes de Newton de (M, φ) y sus pendientes de Hodge son las A primeras pendientes de Hodge de (M, φ).

ii) M_2 tiene rango $r - A$, sus pendientes de Newton son las $r - A$ últimas pendientes de Newton de (M, φ) y sus pendientes de Hodge son las $r - A$ últimas pendientes de Hodge de (M, φ).

Demostración: Para una demostración, véase [8].

■

En términos de los polígonos, quiere decir que el polígono de Hodge (resp. Newton) de (M, φ) se construye uniendo el final del polígono de Hodge (resp. Newton) de (M_1, φ_1) con el principio del polígono de Hodge (resp. Newton) de (M_2, φ_2) traladado al punto (A, b), como en la figura 2.1

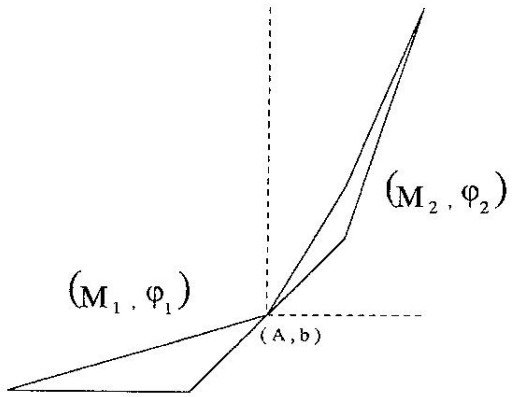


Figura 2.1: Descomposición de un F-cristal

El siguiente ejemplo ilustra una de las piezas claves de la construcción de los F-cristales con polígonos dados. El aspecto importante es el cambio de dos pendientes de Hodge por otras dos distintas sin alterar las pendientes de Newton.

Ejemplo 2.4 Sean (M, φ) y (M', φ') los F-cristales definidos por $M = M' = \mathbb{Z}_p^2$ y con aplicaciones

$$\varphi = \begin{bmatrix} p & 0 \\ 0 & p^2 \end{bmatrix} \qquad \varphi' = \begin{bmatrix} p & 1 \\ 0 & p^2 \end{bmatrix}$$

Los dos F-cristales tienen como pendientes de Newton 1 y 2, ambas con multiplicidad 1 (son las valoraciones p-ádicas de los autovalores de las aplicaciones); en cambio, las pendientes de Hodge de M son 1 y 2, ambas con multiplicidad 1 (la matriz ya es diagonal), mientras que las de M' son 0 y 3, ambas con multiplicidad 1. Para ver esto último, necesitamos encontrar dos bases de $\mathbb{Z}_p^2$, tales que la matriz sea diagonal con respecto a esas bases. Considerando que la matriz viene dada con respecto a la base canónica $\{e_1, e_2\}$, las nuevas bases son $\{v_1, v_2\}$ y $\{w_1, w_2\}$, y el cambio de bases es:

$$\begin{aligned} v_1 &= e_2 & \qquad w_1 &= e_1 + p^2 e_2 \\ v_2 &= -e_1 + pe_2 & \qquad w_2 &= e_2 \end{aligned}$$

Entonces:

$$\varphi'(v_1) = \varphi'(e_2) = e_1 + p^2 e_2 = w_1$$

$$\varphi'(v_2) = \varphi'(-e_1 + pe_2) = -pe_1 + p(e_1 + p^2 e_2) = p^3 e_2 = p^3 w_2$$

y la matriz queda diagonal:

$$\varphi' = \begin{bmatrix} 1 & 0 \\ 0 & p^3 \end{bmatrix}$$

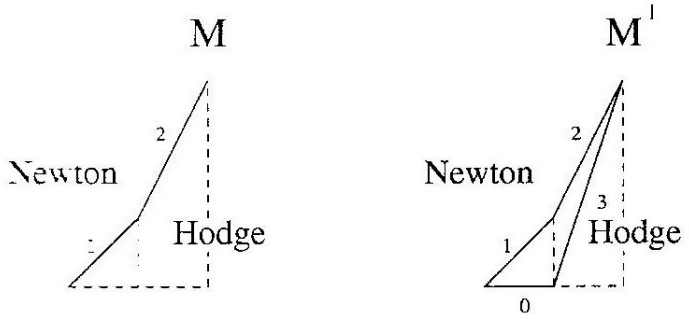


Figura 2.2: Ejemplo de cambio de pendientes

Observación 2.5 El anterior ejemplo prueba la existencia de todos los F-cristales que tienen como pendientes de Newton 1 y 2 ambas con multiplicidad 1, ya que entonces los dos únicos polígonos de Hodge posibles son los obtenidos. En las siguientes secciones generalizaremos este ejemplo construyendo todos los F-cristales con polígono de Newton fijo de la misma forma que en el ejemplo, es decir, perturbando los coeficientes de la matriz para obtener distintos polígonos de Hodge sin cambiar los autovalores de la aplicación.

2.2 Caso 1: Pendientes de Newton constantes

Empezamos por el caso más simple posible, que es cuando todas las pendientes de Newton son iguales. En este caso, la solución a nuestro problema es fácil.

Lema 2.6 *Sea n la pendiente de Newton con multiplicidad m, y sean $i_1, \cdots, i_m$ las pendientes de Hodge pedidas (admitiendo repeticiones) tales que forman una pareja de polígonos de Katz. Entonces, el F-cristal definido por*

$$\varphi = \begin{bmatrix} 0 & 0 & \cdots & 0 & p^{i_m} \\ p^{i_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{i_2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & p^{i_{m-1}} & 0 \end{bmatrix}$$

tiene como pendiente de Newton n con multiplicidad m y como pendientes de Hodge las dadas.

Demostración: i). Para calcular las pendientes de Newton, calculamos los autovalores de la matriz de la aplicación. El polinomio característico viene dado por $\lambda^m - p^{\sum i_a} = 0$, es decir, $\lambda = p^{nm/m}$ salvo unidades p-ádicas, por lo que la valoracion de los autovalores es siempre n, y hay m autovalores.

ii). Para calcular las pendientes de Hodge, necesitamos encontrar dos bases de $\mathbb{Z}_p^m$ tal que la matriz sea diagonal. Las bases que necesitamos son las permutaciónes de los elementos de la base canónica que hacen que los coeficientes p^{i_a} estén en la diagonal, por lo que es evidente que las pendientes de Hodge son las pedidas.

■

Observación 2.7 Por lo tanto, existen todos los F-cristales con pendiente de Newton constante, además, si sabemos que el polígono de Newton tiene pendiente constante n con multiplicidad m, cualquier conjunto de enteros $\{i_1, \cdots, i_m\}$ tal que $\sum i_a = nm$ son un conjunto de pendientes de Hodge de una pareja de polígonos de Katz, ya que el polígono de Hodge es convexo y por tanto siempre va por debajo de la línea que une su punto inicial y final.

2.3 Caso 2: Pendientes de Newton no constantes

A continuación vamos a generalizar el ejemplo 2.4, demostrando un lema que nos permitirá cambiar dos pendientes de Hodge por otras dos tales que una de ellas sea mayor que las primeras y que la suma de las dos pendientes se mantenga constante. Además, las pendientes de Newton no cambiarán.

Lema 2.8 *Sea un F-cristal de rango 2, con pendientes de Hodge y Newton k, ℓ, es decir, tiene una matriz diagonal con coeficientes p^k, p^ℓ con $k \leq \ell$. Entonces, el F-cristal cuya matriz tiene en la diagonal los mismos coeficientes y el coeficiente $a_{12} = p^i$, $i \leq k$, tiene las mismas pendientes de Newton y las pendientes de Hodge son i, j donde $i \leq k \leq \ell \leq j$ con $i + j = k + \ell$*

Demostración: Las pendientes de Newton son claramente las mismas, ya que la nueva matriz tiene los mismos autovalores. Para calcular las pendientes de Hodge, diagonalizamos la matriz. Para ello, calculamos la matriz de la aplicación con respecto a las siguientes bases:

$$\begin{array}{rcl} v_1 & = & e_2 \\ v_2 & = & -e_1 + p^{k-i}e_2 \end{array} \qquad \begin{array}{rcl} w_1 & = & e_1 + p^{\ell-i}e_2 \\ w_2 & = & e_2 \end{array}$$

En estas bases (el hecho de ser $i \leq k$ asegura que los coeficientes de los cambios de base están en $\mathbb{Z}_p$), la aplicación queda:

$$\varphi(v_1) = \varphi(e_2) = p^i e_1 + p^\ell e_2 = p^i(e_1 + p^{\ell-i}e_2) = p^i w_1$$

$$\varphi(v_2) = \varphi(-e_1 + p^{k-i}e_2) = -p^k e_1 + p^{k-i}(p^i e_1 + p^\ell e_2) = p^{k+\ell-i}e_2 = p^{k+\ell-i}w_2 = p^j w_2$$

Es decir, la aplicación es diagonal y los coeficientes de la diagonal son p^i y p^j, con $j = k + \ell - i$

■

Una vez que sabemos cambiar dos pendientes de Hodge por otras dos, pasamos a enunciar y demostrar el resultado más importante de este capítulo.

Proposición 2.9 *Dados los racionales $\underbrace{n_1 = \cdots = n_1}_{m_1} < \underbrace{n_2 = \cdots = n_2}_{m_2} < \cdots < \underbrace{n_s, \cdots, n_s}_{m_s}$ con $N_i = n_i m_i \in \mathbb{Z}$ y dados los números enteros $h_1 \leq h_2 \leq \cdots \leq h_{\sum m_i}$ formando una pareja de polígonos de Katz, se tiene que existe un F-cristal tal que los n_i son sus pendientes de Newton y los h_j son sus pendientes de Hodge.*

Demostración: Sin perdida de generalidad, podemos suponer que no existe ningún punto distinto del inicial y final donde el polígono de Newton y Hodge se toquen, ya que si existe un punto así, aplicando el teorema 2.3, construimos cada uno de los sumandos directos y el F-cristal pedido es la suma directa de los dos construidos. Para costruir un F-cristal tal que el polígono de Newton y el de Hodge sólo se toquen en los extremos hacemos inducción en el numero de pendientes de Newton distintas. Si todas las pendientes de Newton son iguales, el resultado está demostrado en la sección 2.1. Supongamos que sabemos construir todos los F-cristales con $s-1$ pendientes de Newton distintas, y tenemos que construir el F-cristal pedido en el enunciado. Para ello realizamos los siguientes pasos:

i) Como el polígono de Newton va por encima del polígono de Hodge y además acaban en el mismo punto, tenemos que

$$\sum_{i=1}^{m_1} h_a < N_1 \qquad \sum_{j=1+\sum_{i\neq 1} m_i}^{\sum m_i} h_j > N_1$$

(ya que por convexidad las últimas m_1 pendientes de Hodge suman más que las últimas m_1 pendientes de Newton, y estas suman más que las m_1 primeras). Por lo tanto, existe un i_0 tal que $h_{i_0+1}, \ldots, h_{i_0+m_1}$ verifican:

$$\sum_{j=0}^{m_1-1} h_{i_0+j} < N_1 \leq \sum_{j=1}^{m_1} h_{i_0+j}$$

Definimos:

$$h := N_1 - \sum_{j=1}^{m_1-1} h_{i_0+j} \qquad h' := h_{i_0+m_1} + h_{i_0} - h$$

ii) Costruimos los F-cristales siguientes (conocidos por hipótesis de inducción): *F-cristal* M_1. Es el F-cristal que tiene como pendiente de Newton n_1 con multiplicidad m_1, y como pendientes de Hodge (admitiendo repeticiones) $h_{i_0+1}, \cdots, h_{i_0+m_1-1}, h$. Este F-cristal se construye usando el Lema 2.6, ya que $\sum_{j=1}^{m_1-1} h_{i_0+j} + h = N_1 = m_1 n_1$, por lo que se trata de una pareja de polígonos de Katz.

F-cristal M_2. Es el F-cristal que tiene como pendientes de Newton n_2 con multiplicidad $m_2, \ldots, n_s$ con multiplicidad m_s, y como pendientes de Hodge $h_1, \ldots, h_{i_0-1}, h', h_{i_0+m_1+1}, \ldots, h_{\sum m_i}$ (admitiendo repeticiones).

Falta por ver que el segundo F-cristal es un verdadero F-cristal, i.e., las pendientes descritas forman de verdad una pareja de polígonos de Katz. La primera observación es que hay tantas pendientes de Newton como de Hodge: hay $\sum m_i - m_1$. El

comienzo del polígono, desde la pendiente h_1 hasta la pendiente h_{i_0-1}, está por debajo del polígono de Newton, ya que son las mismas que las del F-cristal inicial, mientras que las pendientes de Newton de este segundo F-cristal son mayores que las del primero (empieza con pendientes de tamaño n_2). El final del polígono, desde la pendiente $h_{i_0+m_1+1}$ hasta $h_{\sum m_i}$, está por debajo del polígono de Newton, ya que se tratá de las mismas pendientes de Newton y Hodge que las del F-cristal inicial. Por tanto, si unimos los dos trazos de polígono con una recta de longitud 1 y pendiente h', obtenemos un polígono que va por debajo de el de Newton. Lo último que falta para ver que es un polígono de Hodge es ver que h' es una pendiente positiva y que está bien colocada, es decir, es mayor que la anterior y menor que la siguiente. Pero, por la definición de i_0, h, h', se tiene que $h_{i_0} < h \leq h_{i_0+m_1}$ y que $h + h' = h_{i_0} + h_{i_0+m_1}$, por lo que $h_{i_0-1} \leq h_{i_0} \leq h' \leq h_{i_0+m_1} \leq h_{i_0+m_1+1}$.

iii) Una vez construidos los F-cristales de los puntos i) y ii), los "unimos" para formar el F-cristal pedido. Para ello utilizaremos el Lema 2.8. Si realizamos los cambios de base necesarios para diagonalizar las aplicaciones de los dos F-cristales construidos, denotando por V_1 y por W_1 las bases del F-cristal M_1, y por V_2 y W_2 las del F-cristal M_2, la aplicación del F-cristal pedido es, en las bases $V = \{V_1, V_2\}$ y $W = \{W_1, W_2\}$,

$$\varphi = \left[\begin{array}{cccc|ccccc}
p^{h_{i_0+1}} & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & 0 & \vdots \\
\vdots & \ddots & p^{h_{i_0+m_1-1}} & 0 & \vdots & 0 & 0 & \ddots & 0 \\
0 & \cdots & 0 & p^{h} & 0 & 0 & p^{h_{i_0}} & 0 & 0 \\
\hline
0 & \cdots & \cdots & 0 & p^{h_1} & 0 & \cdots & \cdots & 0 \\
0 & \ddots & 0 & \vdots & 0 & \ddots & \ddots & 0 & \vdots \\
\vdots & \ddots & \ddots & 0 & \vdots & \ddots & p^{h'} & \ddots & \vdots \\
\vdots & 0 & \ddots & 0 & \vdots & 0 & \ddots & \ddots & 0 \\
0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & 0 & p^{h_{\sum m_i}}
\end{array}\right]$$

ya que si realizamos el cambio de bases del Lema 2.8 sobre los vectores $\{v, v'\}$ y $\{w, w'\}$,tales que

$$\varphi(v) = p^h w \qquad \varphi(v') = p^{h_{i_0}} w + p^{h'} w'$$

obtenemos una matriz diagonal con coeficientes las pendientes de Hodge pedidas (ya que el cambio último que hemos hecho transforma las pendientes h, h' en $h_{i_0}, h_{i_0-m_1}$ y a las demás no las afecta). Más explicitamente, el cambio es:

$$\begin{array}{rcl} \widetilde{v} & = & v' \\ \widetilde{v'} & = & -v + p^{h-h_{i_0}} v' \end{array} \qquad \begin{array}{rcl} \widetilde{w} & = & w + p^{h'-h_{i_0}} w' \\ \widetilde{w'} & = & w' \end{array}$$

Por último, deshacemos el cambio que diagonalizaba los F-cristales M_1 y M_2 en la matriz φ (que no afecta al término p^{i0}, salvo quizás cambiándolo de sitio, ya que por el Lema 2.6, el cambio que hay que hacer para diagonalizar un F-cristal con pendientes de Newton constantes es sólo una permutación de la base), y obtenemos la matriz del F-cristal pedido. Para acabar, observamos que el término que hemos añadido, i.e., el coeficiente p^{i0}, no afecta al polinomio característico, por lo que las pendientes de Newton de nuestro F-cristal son la unión de las pendientes de los F-cristales M_1 y M_2, que eran las pedidas.

■

Capítulo 3

Polígonos geométricos

En este capítulo encontraremos ejemplos de curvas proyectivas y lisas de géneros 1, 2 y 3, para cada pareja de polígonos geométricos de Katz, centrándonos principalmente en el género 3, por ser este el género más pequeño donde el p-rango (el cardinal de pendientes de Newton nulas) no determina totalmente el polígono de Newton.

3.1 Definiciones y propiedades

Definición 3.1 Una *pareja de polígonos geométricos de Katz* es una pareja de polígonos de Katz, tales que satisfacen además las condiciones de la observación 1.23.

Dado un esquema propio y liso de dimensión 1, X/k, el F-cristal más importante es $H^1(X/W)$, ya que tanto $H^0(X/W)$ como $H^2(X/W)$ están completamente determinados en la función Zeta del esquema (curva). Por lo tanto, calcularemos el polígono de Newton del F-cristal $H^1(X/W)$.

Observación 3.2 Dada una curva de género g, su polígono geométrico de Hodge está determinado, ya que por dualidad se tiene que $h^{0,1} = h^{1,0}$, y además $h^{0,1} + h^{1,0} = \dim H^1(C) = 2g$. Por lo tanto, para encontrar parejas de polígonos geométricos de Katz, una vez fijado el género, sólo necesitamos fijarnos en el polígono de Newton, ya que el polígono de Hodge geométrico es el mismo para todas las curvas proyectivas y lisas de género dado, tiene pendientes 0 y 1 ambas con multiplicidad g. Además, por la observación 1.23, sabemos que las pendientes de Newton están en el intervalo $[0,1]$ y que si α es una pendiente de Newton, entonces $1-\alpha$ es pendiente y con la misms multiplicidad.

Para calcular el polígono de Newton de una curva proyectiva y lisa definida sobre $k = \mathbb{F}_p$, C/k, usaremos la función Zeta de la curva (véase la introducción):

$$Z(C/k,t) = \frac{P(t)}{(1-t)(1-pt)},$$

donde $P(t) = 1+\sum_{i=1}^{2g} a_i t^i = \prod_{i=1}^{2g}(1-\alpha_i t) \in \mathbb{Z}[t]$. Además, la ecuación funcional de la función Zeta es equivalente a:

$$P(t) = p^g t^{2g} P(1/pt)$$

con lo que $a_{2g} = p^g$ y $a_i = p^{i-g} a_{2g-i}$ $i = 1, \ldots, 2g-1$, es decir, los números $a_1, \ldots, a_g$ determinan la función Zeta.

Por otro lado, ya que la cohomología cristalina es una cohomología de Weil, se tiene también que:

$$Z(C/k, t) = \prod_{i=0}^{2} \det(1 - f^* t | H^i(X/W))^{(-1)^{i+1}},$$

es decir, el polinomio $P(t)$ es el polinomio recíproco del polinomio característico del F-cristal $H^1(X/W)$, por lo tanto, sus raíces recíprocas son los autovalores del F-cristal y por el teorema 1.6 el polígono de Newton de $H^1(X/W)$ coincide con el polígono de Newton del polinomio $P(t)$, mucho más fácil de calcular, ya que tiene coeficientes enteros.

3.2 Género 1

Los posibles polígonos de Newton para curvas de género 1 son los siguientes:

1. Una pendiente 0 y una pendiente 1. Este es el caso ordinario y lo denotaremos por *ord.*

2. Dos pendientes 1/2. Este es el caso supersingular y lo denotaremos *ss*

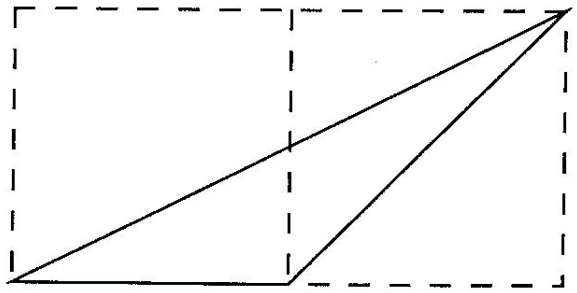


Figura 3.1: Polígonos de Newton de las curvas de género 1

Tabla 3.3 El polígono de Newton viene determinado por las valoraciones p-ádicas del coeficient a_1 del numerador de la función Zeta, por lo que los posibles casos se relacionan con este valor de la siguiente manera:

1. $a_1 \equiv 0 \pmod p$. Este es el caso *ss*.

2. $a_1 \not\equiv 0 \pmod p$. Este es el caso *ord*.

Tomando derivadas logarítmicas en la función Zeta y evaluando en cero, podemos relacionar el coeficiente a_1 con el número N_1, obteniendo que:

$$N_1 = a_1 + 1 + p$$

Por lo tanto, podemos escribir la tabla 3.3 en función de N_1, quedándonos la siguiente tabla:

Tabla 3.4 N_1 determina los distintos polígonos de Newton de la siguiente manera:

1. $N_1 \equiv 1 \pmod p$. Este es el caso *ss*.

2. $N_1 \not\equiv 1 \pmod p$. Este es el caso *ord*.

Las curvas de género 1 lisas (curvas elípticas), están ampliamente estudiadas y se conocen numerosos ejemplos tanto de curvas ordinarias como supersingulares. Una referencia clásica es el libro de Silverman ([15]).

El siguiente teorema nos da un criterio para determinar si una curva elíptica es supersingular o no.

Teorema 3.5 *Sea K un cuerpo finito de característica $p > 2$. Sea E/K una curva elíptica con ecuación de Weierstrass $E : y^2 = f(x)$, donde $f(x)$ es un polinomio de grado tres con raíces distintas. Entonces E es supersingular sii el coeficiente de x^{p-1} en $f(x)^{(p-1)/2}$ es cero.*

Demostración: Para una demostración, véase [15].

■

Ejemplo 3.6 Sea $p \geq 5$. Sea la curva elíptica $E : y^2 = x^3 + 1$ definida sobre $\mathbb{F}_p$. Para ver si esta curva es supersingular o no, tenemos que calcular el coeficiente de x^{p-1} en $(x^3 - 1)^{(p-1)/2}$. Si $p \equiv 2 \pmod 3$, entonces no hay término x^{p-1}, por lo que la curva es supersingular; mientras que si $p \equiv 1 \pmod 3$, el coeficiente es $\binom{(p-1)/2}{(p-1)/3}$, que es distinto de cero modulo p, por lo que en este caso la curva es ordinaria.

Ejemplo 3.7 Sea $p \geq 3$. Sea la curva elíptica $E : y^2 = x^3 + x$ definida sobre $\mathbb{F}_p$. Para ver si esta curva es supersingular o no, tenemos que calcular el coeficiente de x^{p-1} en $(x^3 - x)^{(p-1)/2}$. Si $p \equiv 3 \pmod 4$, entonces no hay término x^{p-1}, por lo que la curva es supersingular; mientras que si $p \equiv 1 \pmod 4$, el coeficiente es $\binom{(p-1)/2}{(p-1)/4}$, que es distinto de cero modulo p, por lo que en este caso la curva es ordinaria.

3.3 Género 2

Los posibles polígonos de Newton para curvas de género 2 son los siguientes:

1. Dos pendientes de Newton 0 y dos pendientes 1. Este es el caso ordinario y lo denotaremos por *ord.*

2. Una pendiente 0, dos pendientes 1/2 y una pendiente 1. A este caso lo denotaremos *0.*

3. Cuatro pendientes 1/2. Este es el caso supersingular y lo denotaremos *ss*

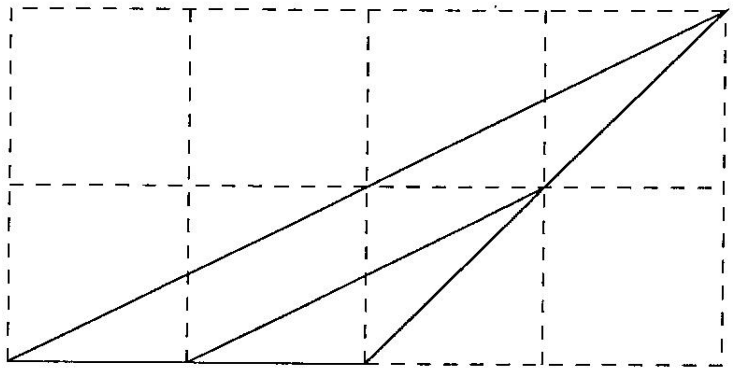


Figura 3.2: Polígonos de Newton de las curvas de género 2

Tabla 3.8 El polígono de Newton viene determinado por las valoraciones p-ádicas de los coeficientes a_1 y a_2 del numerador de la función Zeta, por lo que los posibles casos se relacionan con estos valores de la siguiente manera:

1. $a_1 \equiv 0 \pmod{p}$. Tenemos dos casos:

   i) $a_2 \equiv 0 \pmod{p}$. Caso *ss.*

   ii) $a_2 \not\equiv 0 \pmod{p}$. Caso *ord.*

2. $a_1 \not\equiv 0 \pmod{p}$. Tenemos dos casos:

   i) $a_2 \equiv 0 \pmod{p}$. Caso *0.*

   ii) $a_2 \not\equiv 0 \pmod{p}$. Caso *ord.*

Tomando sucesivas derivadas logarítmicas en la función Zeta y evaluando en cero, podemos relacionar los coeficientes $\{a_i, 1 \leq i \leq 2\}$ con los números $\{N_j, 1 \leq j \leq 2\}$, obteniendo que:

$$\begin{aligned} N_1 &= a_1 + 1 + p \\ N_2 &= 2a_2 - a_1^2 + 1 + p^2 \end{aligned}$$

Por lo tanto, podemos escribir la tabla 3.8 en función de los N_i, quedándonos la siguiente tabla:

Tabla 3.9 Los N_i determinan los distintos polígonos de Newton de la siguiente manera:

1. $N_1 \equiv 1 \pmod p$. Tenemos dos casos:
   i) $N_2 \equiv 1 \pmod p$ (mod 4 si $p = 2$). Caso *ss*.
   ii) $N_2 \not\equiv 1 \pmod p$ (mod 4 si $p = 2$). Caso *ord*.
2. $N_1 \not\equiv 1 \pmod p$. Tenemos dos casos:
   i) $N_2 + N_1^2 - 2N_1 \equiv 0 \pmod p$ (mod 4 si $p = 2$). Caso *0*.
   ii) $N_2 + N_1^2 - 2N_1 \not\equiv 0 \pmod p$ (mod 4 si $p = 2$). Caso *ord*.

Para terminar está sección, deremos algunos ejemplos de curvas de género dos sobre $\mathbb{F}_2$ y $\mathbb{F}_3$ que cubren todos los posibles polígonos de Newton.

Observación 3.10 El género de una curva proyectiva plana y lisa, C, viene dado por la fórmula:

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

donde d es el grado de la ecuación que define la curva proyectiva. Está formula implica que no existen curvas planas y lisas de género dos, por lo tanto, buscaremos curvas con puntos singulares y relacionaremos sus puntos con los puntos del modelo liso que resulta tras explotar los puntos singulares.

Los ejemplos que vamos a dar son curvas de grado cuatro con un nodo de orden 2, i. e., un punto de multiplicidad dos con dos rectas tangentes distintas. Este tipo de punto singular afecta al género de la curva disminuyendo en uno el género esperado si consideramos que la curva es lisa. Más explicitamente, el género de una curva plana, C, con r nodos de orden $m_1, \ldots, m_r$, i. e., puntos de multiplicidad $m_1, \ldots, m_r$ con tantas rectas tangentes distintas como indica su multiplicidad, es :

$$g(C) = \frac{(d-1)(d-2)}{2} - \sum_{i=1}^{r} \frac{m_i(m_i-1)}{2}$$

Por lo tanto, nuestras curvas tienen género dos.

Observación 3.11 Cuando explotamos un nodo de orden r, obtenemos r puntos distintos en una recta proyectiva, correspondiendo a los puntos de la recta proyectiva cuyos valores son las pendientes de las rectas tangentes del punto singular. Por lo tanto, al explotar nuestros nodos de orden dos, obtendremos dos puntos si las pendientes de las tangentes están definidas en el cuerpo o ninguno si no están definidas. Al explotar, los puntos lisos corresponden a un único punto liso que está definido en el cuerpo si el primero lo estaba, por lo que el número de puntos no cambia.

1. ***Curvas definidas sobre*** $\mathbb{F}_2$.

Observación 3.12 Para calcular los puntos del infinito de una curva, calculamos los puntos de intersección de C y $\{z = 0\}$. Una vez calculados estos, nos podemos restringir a la curva afín $C \cap \{z = 1\}$.

Ejemplo 3.13 Sea $C_1 \equiv x^4 + xyz^2 + y^3z = 0$.

i) Los puntos del infinito. Se tiene que $z = 0 \Rightarrow x^4 = 0 \Rightarrow x = 0 \Rightarrow y = 1$, por lo que sólo hay un punto en el infinito, $P = [0, 1, 0]$. Como $\frac{\partial C_1}{\partial z}\Big|_P = 1$, el punto es no singular.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_1}{\partial x} \equiv y = 0 \Leftrightarrow y = 0 \qquad \frac{\partial C_1}{\partial y} \equiv x + y^2 = 0 \Leftrightarrow x = 0 \quad (y = 0).$$

Por lo tanto, el único punto singular es el $(0, 0)$, que es un nodo de orden dos con rectas tangentes $x = 0$ y $y = 0$. Las dos pendientes de las rectas están definidas en cualquier cuerpo.

iii) Número de puntos. Sobre $\mathbb{F}_2$, está curva tiene, después de explotar, 3 puntos. Sobre $\mathbb{F}_4$ tiene 5 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *ss*.

Ejemplo 3.14 Sea $C_2 \equiv x^4 + xy^2z + y^3z + y^2z^2 + xyz^2 = 0$.

i) Los puntos del infinito. Se tiene que $z = 0 \Rightarrow x^4 = 0 \Rightarrow x = 0 \Rightarrow y = 1$, por lo que sólo hay un punto en el infinito, $P = [0, 1, 0]$. Como $\frac{\partial C_2}{\partial z}\Big|_P = 1$, el punto es no singular.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_2}{\partial x} \equiv y^2 + y = 0 \Leftrightarrow y = 0, 1 \qquad \frac{\partial C_2}{\partial y} \equiv x + y^2 = 0 \Leftrightarrow x = y^2.$$

El punto $(1,1)$ no pertenece a la curva, por lo tanto, el único punto singular es el $(0,0)$, que es un nodo de orden dos con rectas tangentes $y=0$ y $x+y=0$. Las dos pendientes de las rectas están definidas en cualquier cuerpo.

iii) Número de puntos. Sobre $\mathbb{F}_2$, está curva tiene, después de explotar, 4 puntos. Sobre $\mathbb{F}_4$ tiene 4 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *0*.

Ejemplo 3.15 Sea $C_3 \equiv yx^3 + x^3z + y^3z + xyz^2 = 0$.

i) Los puntos del infinito. Se tiene que $z=0 \Rightarrow yx^3=0$, por lo que hay dos puntos en el infinito, $P_1=[0,1,0]$ y $P_2=[1,0,0]$. Como $\frac{\partial C_3}{\partial z} = x^3+y^3$, se tiene que $\frac{\partial C_3}{\partial z}\Big|_{P_1} \neq 0$ y $\frac{\partial C_3}{\partial z}\Big|_{P_2} \neq 0$, por lo que los puntos son no singulares.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_3}{\partial x} \equiv yx^2 + x^2 + y \qquad\qquad \frac{\partial C_3}{\partial y} \equiv x^3 + y^2 + x.$$

Se tiene que $C_3 = x(\frac{\partial C_3}{\partial x}) + y^3 = y(\frac{\partial C_3}{\partial y}) + x^3$, por lo tanto $C_3=0, \frac{\partial C_3}{\partial x} = 0 \Rightarrow y=0$ y $C_3=0, \frac{\partial C_3}{\partial y}=0 \Rightarrow x=0$, i.e., el único punto singular es el $(0,0)$ que es un nodo de orden dos con rectas tangentes $y=0$ y $x=0$. Las dos pendientes de las rectas están definidas en cualquier cuerpo.

iii) Número de puntos. Sobre $\mathbb{F}_2$, está curva tiene, después de explotar, 5 puntos. Sobre $\mathbb{F}_4$ tiene 7 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *ord*.

2 ***Curvas definidas sobre*** $\mathbb{F}_3$.

Ejemplo 3.16 Sea $C_4 \equiv x^3y + y^3z - y^2z^2 + x^2z^2 = 0$.

i) Los puntos del infinito. Se tiene que $z=0 \Rightarrow x^3y=0 \Rightarrow x=0$ *ó* $y=0$, por lo que hay dos puntos en el infinito, $P_1=[0,1,0]$ y $P_2=[1,0,0]$. Como $\frac{\partial C_4}{\partial z}\Big|_{P_1} = 1$ y $\frac{\partial C_4}{\partial y}\Big|_{P_2} = 1$, los punto son no singulares.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_4}{\partial x} \equiv 2x = 0 \Leftrightarrow x=0 \qquad\qquad \frac{\partial C_4}{\partial y} \equiv x^3 - 2y = 0 \Leftrightarrow y=0 \ (x=0).$$

Por lo tanto, el único punto singular es el $(0,0)$, que es un nodo de orden dos con rectas tangentes $x+y=0$ y $x-y=0$. Las dos pendientes de las rectas están definidas en cualquier cuerpo.

iii) Número de puntos. Sobre $\mathbb{F}_3$, está curva tiene, después de explotar, 7 puntos. Sobre $\mathbb{F}_9$ tiene 13 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *ss*.

Ejemplo 3.17 Sea $C_5 \equiv x^4 + y^3z + y^2z^2 + x^2z^2 = 0$.

i) Los puntos del infinito. Se tiene que $z = 0 \Rightarrow x^4 = 0 \Rightarrow x = 0 \Rightarrow y = 1$, por lo que sólo hay un punto en el infinito, $P = [0, 1, 0]$. Como $\frac{\partial C_5}{\partial z}\Big|_P = 1$, el punto es no singular.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_5}{\partial x} \equiv x^3 - x = 0 \Leftrightarrow x = 0, \pm 1 \qquad \frac{\partial C_5}{\partial y} \equiv 2y = 0 \Leftrightarrow y = 0.$$

Como los puntos $(\pm 1, 0)$ no pertenecen a la curva, el único punto singular es el $(0, 0)$. Además, es un nodo de orden dos con rectas tangentes $x+iy = 0$ y $x - iy = 0$*. Las dos pendientes de las rectas están definidas en cualquier extensión de grado par de $\mathbb{F}_3$.

iii) Número de puntos. Sobre $\mathbb{F}_3$, está curva tiene, después de explotar, 2 puntos. Sobre $\mathbb{F}_9$ tiene 12 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *0*.

Ejemplo 3.18 Sea $C_6 \equiv x^4 + y^4 + y^2z^2 - x^2z^2$.

i) Los puntos del infinito. Se tiene que $z = 0 \Rightarrow x^4 + y^4 = 0$, por lo que no hay puntos en el infinito definidos sobre $\mathbb{F}_3$, ya que $x^4 = 1$ para cualquier $x \in \mathbb{F}_3$, y hay cuatro puntos definidos sobre $\mathbb{F}_9$, ya que $x^4 = -1$ tiene como soluciones los cuatro generadores del grupo multiplicativo. Como además $\frac{\partial C_6}{\partial x}\Big|_{z=0} = x^3 \neq 0$ en los puntos del infinito, los puntos son no singulares.

ii) Singularidades. Para calcular los puntos singulares afines, miramos que puntos de la curva afín anulan las derivadas parciales con respecto a x e y.

$$\frac{\partial C_6}{\partial x} \equiv x^3 - 2x = 0 \Leftrightarrow x = 0, \pm i \qquad \frac{\partial C_6}{\partial y} \equiv y^3 + 2y = 0 \Leftrightarrow y = 0, \pm 1.$$

Como los puntos $(\pm i, 0)$, $(0, \pm 1)$ y $(\pm i. \pm 1)$ no pertenecen a la curva, el único punto singular es el $(0, 0)$, que es un nodo de orden dos con rectas tangentes $x + y = 0$ y $x - y = 0$. Las dos pendientes de las rectas están definidas en cualquier cuerpo.

iii) Número de puntos. Sobre $\mathbb{F}_3$, está curva tiene, después de explotar, 4 puntos. Sobre $\mathbb{F}_9$ tiene 14 puntos

Por lo tanto, según la tabla 3.9, está curva es del tipo *ord*.

*El elemento i es cualquier elemento tal que $i^2 = -1$

3.4 Género 3

Los posibles polígonos de Newton para curvas de género 3 son los siguientes:

1. Tres pendientes de Newton 0 y tres pendientes 1. Este es el caso ordinario y lo denotaremos por *ord.*

2. Dos pendientes 0, dos pendientes 1/2 y dos pendientes 1. A este caso lo denotaremos *0-0*

3. Una pendiente 0, cuatro pendientes 1/2 y una pendiente 1. A este caso lo denotaremos *0.*

4. Tres pendientes 1/3 y tres pendientes 2/3. A este caso lo denotaremos *1/3*

5. Seis pendientes 1/2. Este es el caso supersingular y lo denotaremos *ss*

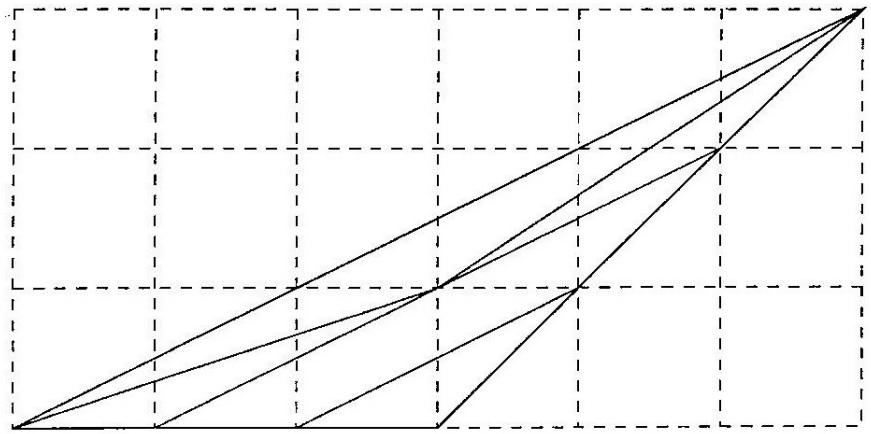


Figura 3.3: Polígonos de Newton de las curvas de género 3

Tabla 3.19 El polígono de Newton viene determinado por las valoraciones p-ádicas de los coeficientes a_1, a_2 y a_3 del numerador de la función Zeta, por lo que los posibles casos se relacionan con estos valores de la siguiente manera:

1. $a_1 \equiv 0 \pmod{p}$. Tenemos los casos:

   i) $a_2 \equiv 0 \pmod{p}$. Tenemos tres casos:

      a) $a_3 \equiv 0 \pmod{p^2}$. Caso *ss.*

      b) $a_3 \equiv\equiv 0 \pmod{p}$ †. Caso *1/3.*

      c) $a_3 \equiv 0 \pmod{p}$. Caso *ord.*

† La notación $a \equiv\equiv b \pmod{p^r}$ quiere decir que $a \equiv b \pmod{p^r}$, pero $a \not\equiv b \pmod{p^{r+1}}$

ii) $a_2 \not\equiv 0 \pmod p$. Tenemos dos casos:

a) $a_3 \equiv 0 \pmod p$. Caso *0-0*.

b) $a_3 \not\equiv 0 \pmod p$. Caso *ord*.

2. $a_1 \not\equiv 0 \pmod p$. Tenemos los casos:

i) $a_2 \equiv 0 \pmod p$. Tenemos dos casos:

a) $a_3 \equiv 0 \pmod p$. Caso *0*.

b) $a_3 \not\equiv 0 \pmod p$. Caso *ord*.

ii) $a_2 \not\equiv 0 \pmod p$. Tenemos dos casos:

a) $a_3 \equiv 0 \pmod p$. Caso *0-0*.

b) $a_3 \not\equiv 0 \pmod p$. Caso *ord*.

Tomando sucesivas derivadas logarítmicas en la función Zeta y evaluando en cero, podemos relacionar los coeficientes $\{a_i, 1 \leq i \leq 3\}$ con los números $\{N_j, 1 \leq j \leq 3\}$, obteniendo que:

$$\begin{aligned} N_1 &= a_1 + 1 + p \\ N_2 &= 2a_2 - a_1^2 + 1 + p^2 \\ N_3 &= 3a_3 - 3a_2a_1 + a_1^3 + 1 + p^3 \end{aligned}$$

Por lo tanto, podemos escribir la tabla 3.19 en función de los N_i, quedándonos la siguiente tabla ($p \neq 2, 3$):

Tabla 3.20 Los N_i determinan los distintos polígonos de Newton de la siguiente manera:

1. $N_1 \equiv 1 \pmod p$. Tenemos los casos:

i) $N_2 \equiv 1 \pmod p$. Tenemos tres casos:

a) $N_3 \equiv 1 \pmod{p^2}$. Caso *ss*.

b) $N_3 \equiv\equiv 1 \pmod p$. Caso *1/3*.

c) $N_3 \not\equiv 1 \pmod p$. Caso *ord*.

ii) $N_2 \not\equiv 1 \pmod p$. Tenemos dos casos:

a) $N_3 \equiv 1 \pmod p$. Caso *0-0*.

b) $N_3 \not\equiv 1 \pmod p$. Caso *ord*.

2. $N_1 \not\equiv 1 \pmod p$. Tenemos los casos:

i) $N_2 + N_1^2 - 2N_1 \equiv 0 \pmod p$. Tenemos dos casos:

a) $N_3 + N_2N_1 - N_2 - N_1 \equiv 0 \pmod p$. Caso *0*.

b) $N_3 + N_2N_1 - N_2 - N_1 \not\equiv 0 \pmod p$. Caso *ord.*

ii) $N_2 + N_1^2 - 2N_1 \not\equiv 0 \pmod p$. Tenemos dos casos:

a) $2N_3 + N_1^3 + 3N_2N_1 - 3N_1^2 - 3N_2 \equiv 0 \pmod p$. Caso *0-0.*

b) $2N_3 + N_1^3 + 3N_2N_1 - 3N_1^2 - 3N_2 \not\equiv 0 \pmod p$. Caso *ord.*

3.4.1 Las curvas $y^3 = x^4 - ax$

En está sección estudiremos las reducciones modulo p de las curvas de la familia $y^3 = x^4 - ax$, con $a \in \{1, \ldots, p-1\}$.

Observación 3.21 En realidad, las curvas que consideramos son las proyectivizadas de esa familia, es decir, las curvas de la forma $zy^3 = x^4 - az^3x$. Todas estas curvas tienen un único punto en el infinito, ya que si $z = 0$, entonces la ecuación queda $x^4 = 0$ y el único punto proyectivo que está en la curva es el $[0, 1, 0]$. Además se tiene que la derivada con respecto a z evaluada en el punto del infinito vale 1, por lo que el punto del infinito de todas las curvas es no singular. Por lo tanto, sólo consideraremos las ecuaciones afines teniendo siempre en cuenta que hay un punto más en el infinito.

Proposición 3.22 Sea $p \neq 3$, entonces las curvas afines $C \equiv y^3 = x^4 - ax$ con $a \in \{1, \ldots, p-1\}$ son lisas y por tanto de género tres (por ser un polinomio de grado cuatro).

Demostración: Se tiene que:

$$\frac{\partial C}{\partial y} \equiv 3y^2 = 0 \Leftrightarrow y = 0 \ (p \neq 3)$$

y, por tanto, la coordenada x de un punto singular es un cero de $x^4 - ax$ y de su derivada, es decir, un cero doble. Como el polinomio $x^4 - ax$ no tiene ceros dobles, no existen puntos singulares y la curva es lisa.

■

Observación 3.23 Para conocer el polígono de Newton de las reducciones modulo p de estas curvas, nos basta con conocer los números N_1, N_2 y N_3 y comparar con la Tabla 3.20. Para calcular esos números, dividiremos los primos p en dos grandes familias dependiendo de su clase de congruencia modulo 3.

1. *Caso* $p \equiv 2 \pmod 3$.

Lema 3.24 Sea $p \equiv 2 \pmod 3$. Entonces la aplicación $x \mapsto x^3$ es biyectiva en $\mathbb{F}_p$ y en cualquier extensión de grado impar de $\mathbb{F}_p$

Demostración: Como la aplicación $x \mapsto x^3$ está definida en un conjunto finito, se tiene que es biyectiva sii es inyectiva. Si $x^3 = 0$ la única antimagen posible es $x = 0$ porque la aplicación esta definida en un cuerpo, por lo tanto, podemos suponer que $x \neq 0$. Entonces, $x^3 = y^3 \Leftrightarrow (x/y)^3 = 1$, es decir, la aplicación es inyectiva sii no existen elementos de orden tres en el grupo multiplicativo de $\mathbb{F}_{p^r}, r \equiv 1 \pmod 2$. Por teoría elemental de cuerpos, se tiene que el grupo multiplicativo $\mathbb{F}_{p^r}^*$ es cíclico de orden $p^r - 1$, y por tanto, existe un elemento de orden 3 sii $3|(p^r - 1)$, es decir, sii $p \equiv 1 \pmod 3$.

■

Corolario 3.25 Sea $C \equiv y^3 = P_4(x)$, con $P_4(x)$ un polinomio de grado 4 una curva proyectiva y lisa definida sobre $\mathbb{F}_p$ con $p \equiv 2 \pmod 3$. Entonces, por el lema anterior se tiene que:

$$N_1 = p + 1 \qquad\qquad N_3 = p^3 + 1$$

con lo que según la tabla 3.20

$$C \text{ es ss si } N_2 \equiv 1 \pmod p \qquad ó \qquad C \text{ es 0-0 si } N_2 \not\equiv 1 \pmod p.$$

Proposición 3.26 Sea $p \equiv 2, 5 \pmod 9$. Sea $C \equiv y^3 = x^4 - ax$. Entonces $N_2 = p^2 + 1$, con $N_2 = 1 + \#\{(x_0, y_0) \in (\mathbb{F}_{p^2})^2 \,|(x_0, y_0) \in C\}$

Demostración: Si $y_0 = 0$, entonces $x_0 = 0$, ó $x_0^3 = a$, que tiene tres o ninguna solución en $\mathbb{F}_{p^2}^*$ y por lo tanto tenemos uno o cuatro puntos. Supongamos que $y_0 \neq 0$. Sea $\omega \in \mathbb{F}_{p^2}^*$ tal que $\omega^3 = 1, \omega \neq 1$ (ω está en $\mathbb{F}_{p^2}^*$, por ser una extensión de grado par, y además no es un cubo porque $p^2 \equiv\equiv 1 \pmod 9$ y no existen elementos de orden 9). Dados $\{x_0, \omega x_0, \omega^2 x_0\}$, cuyas imágenes son $\{x_0^4 - ax_0, \omega(x_0^4 - ax_0), \omega^2(x_0^4 - ax_0)\}$, se tiene que una y sólo una de las imágenes es un cubo en $\mathbb{F}_{p^2}$, ya que cada uno de ellos pertenece a una clase distinta de $\mathbb{F}_{p^2}^*/(\mathbb{F}_{p^2}^*)^3 = \{1, \omega, \omega^2\}$, y por lo tanto nos da tres valores distintos de y_0. En resumen, si $p^2 = 3s + 1$, tenemos s grupos de tres elementos, y de cada una obtenemos tres puntos. Si añadimos el punto $(0, 0)$ y el punto del infinito, obtenemos los $p^2 + 1$ puntos.

■

Corolario 3.27 Sea $p \equiv 2, 5 \pmod 9$. Entonces por el Corolario 3.25, por la Proposición 3.26 y según la tabla 3.20, se tiene que todas las curvas de la forma $y^3 = x^4 - ax$ son supersingulares y además

$$N_1 = p + 1 \qquad N_2 = p^2 + 1 \qquad N_3 = p^3 + 1.$$

2 ***Caso*** $p \equiv 1 \pmod 3$.

Proposición 3.28 Sea $p \equiv 1 \pmod 3$. Si $p \not\equiv 1 \pmod 9$, las curvas $y^3 = x^4 - ax$ tienen $N_1 = p+1$ y $N_2 = p^2+1$

Demostración: La demostración es análoga a la de la Proposición 3.26 , ya que no existen elementos de orden 9 en $\mathbb{F}_p^*$ ni en $\mathbb{F}_{p^2}^*$, por lo que de cada grupo de tres valores de x como antes, obtenemos tres puntos, a los que hay que añadirle el punto $(0,0)$ y el punto del infinito. La única observación es que por ser $p \equiv 1 \pmod 3$, se tiene que ahora $\omega \in \mathbb{F}_p^*$, y por tanto la cuenta vale en $\mathbb{F}_p$.

■

Corolario 3.29 Según la Proposición 3.28 y la Tabla 3.20, las curvas $y^3 = x^4 - ax$ definidas sobre $p \equiv 4, 7 \pmod 9$ son de los tipos *ss,1/3* o *ord.*

Tabla 3.30 La siguiente tabla muestra los resultados obtenidos hasta ahora:

$p \equiv 1$	(mod 9)	$N_1 = ?$	$N_2 = ?$	$N_3 = ?$	*Tipo* : ?
$p \equiv 2$	(mod 9)	$N_1 = p+1$	$N_2 = p^2+1$	$N_3 = p^3+1$	*Tipo* : *ss*
$p \equiv 4$	(mod 9)	$N_1 = p+1$	$N_2 = p^2+1$	$N_3 = ?$	*Tipo* : *ss, 1/3, ord*
$p \equiv 5$	(mod 9)	$N_1 = p+1$	$N_2 = p^2+1$	$N_3 = p^3+1$	*Tipo* : *ss*
$p \equiv 7$	(mod 9)	$N_1 = p+1$	$N_2 = p^2+1$	$N_3 = ?$	*Tipo* : *ss, 1/3, ord*
$p \equiv 8$	(mod 9)	$N_1 = p+1$	$N_2 = ?$	$N_3 = p^3+1$	*Tipo* : *ss, 0-0*

Los valores tales que $N_i = ?$ son lugares donde no hay un resultado teórico que nos diga el número de puntos de las curvas, y por tanto, el tipo de la curva no está totalmente determinado sino que depende de los valores particulares de los N_i desconocidos.

Para determinar los tipos exactos de las curvas, calcularemos numéricamente los valores que nos faltan para los primos $p < 100$.

Empezamos reduciendo nuestra familia de curvas viendo que curvas son isomorfas entre sí.

Proposición 3.31 La curva $C \equiv y^3 = x^4 - ax$ es isomorfa sobre $\mathbb{F}_p$ a la curva $C' \equiv y^3 = x^4 - bx$ si $b = a\ell^9, \ell \in \mathbb{F}_p$.

Demostración: El isomorfismo viene dado por:

$$x \mapsto \ell^3 x \qquad\qquad y \mapsto \ell^4 y$$

El morfismo anterior es claramente biyectivo y sólo hay que ver que está bien definido. Pero si $(x_0, y_0) \in C$, entonces $\ell^{12} y_0^3 = \ell^{12} x_0^4 - \ell^{12} a x_0 \Rightarrow (\ell^4 y_0)^3 = (\ell^3 x_0)^4 - b\,\ell^3 x_0$, por lo que $(\ell^3 x_0, \ell^4 y_0) \in C'$

■

Corolario 3.32 Sobre $\mathbb{F}_p$ sólo existen 9 curvas, como mucho, no isomorfas de la forma $y^3 = x^4 - ax$. Las curvas vienen dadas eligiendo cada a como un representante de cada una de las clases de $\mathbb{F}_p^*/(\mathbb{F}_p^*)^9$.

Proposición 3.33 Sea $p \equiv 2 \pmod 3$. Entonces todas las curvas de la forma $C \equiv y^3 = x^4 - ax$ son isomorfas sobre $\mathbb{F}_p$.

Demostración: Por la proposición anterior, es suficiente con encontrar, dados $b, a \in \mathbb{F}_p$ un $\ell \in \mathbb{F}_p$ tal que $b = a\ell^9$, pero la ecuación $b = ax^9$ siempre tiene solución en $\mathbb{F}_p$ con $p \equiv 2 \pmod 3$, ya que en estos cuerpos no existen elementos de orden 3 (y por tanto tampoco de orden 9), por lo que la aplicación $x \mapsto x^9$ de $\mathbb{F}_p \to \mathbb{F}_p$ es inyectiva y por ser el cuerpo finito biyectiva.

■

Para estudiar cuantas curvas hay en el caso $p \equiv 1 \pmod 3$, dividimos este caso en dos:

Lema 3.34 Sea $p \equiv\equiv 1 \pmod 3$, entonces sólo existen tres curvas, como mucho, no isomorfas de la forma $y^3 = x^4 - ax$.

Demostración: Sabemos por la Proposición 3.31 que dos curvas son isomorfas si $b = a\ell^9$, pero por ser $p \equiv\equiv 1 \pmod 3$, se tiene que la aplicación $x^3 \mapsto x^9$ es inyectiva en $(\mathbb{F}_p^*)^3$ (ya que $x^9 = y^9 \Leftrightarrow \mathrm{ord}(x/y) \big| 9 \Leftrightarrow \mathrm{ord}(x/y) \in \{1, 3\} \Leftrightarrow x^3 = y^3$), y por tanto sobre. Es decir, dos curvas son isomorfas si b y a están en la misma clase del grupo $\mathbb{F}_p^*/(\mathbb{F}_p^*)^3$, que tiene cardinal tres por ser $p \equiv 1 \pmod 3$. Las curvas son $y^3 = x^4 - ax$, con a recorriendo un representante de cada clase de $\mathbb{F}_p^*/(\mathbb{F}_p^*)^3 = \{1, \eta, \eta^2\}$ con $\eta \notin (\mathbb{F}_p^*)^3$.

■

Observación 3.35 Sea $p \equiv 1 \pmod 9$. Para calcular el número de puntos de las curvas sobre $\mathbb{F}_{p^3}$, aunque en principio tenemos 9 curvas no isomorfas sobre $\mathbb{F}_p$, sobre $\mathbb{F}_{p^3}$ sólo tenemos tres, ya que si $b/a = x^3$ tiene solución en $\mathbb{F}_p$, entonces existe un $\ell \in \mathbb{F}_{p^3}$ tal que $\ell^3 = x$ y las curvas son isomorfas sobre $\mathbb{F}_{p^3}$. Por lo tanto, sobre $\mathbb{F}_{p^3}$, las curvas dependen de la clase a la que pertenezca a en $\mathbb{F}_p^*/(\mathbb{F}_p^*)^3$.

El cálculo, hecho con MAPLE, se basa en los siguientes Lemas:

Lema 3.36 Sea m un divisor positivo de $q - 1$, $f \in \mathbb{F}_q[x]$ y $g = f^{(q-1)/m}$. Entonces, el número, N, de soluciones de $y^m = f(x)$ en $\mathbb{F}_q \times \mathbb{F}_q$ viene dado por $N = |T_0| + m|T_1|$, donde $T_0 = \{c \in \mathbb{F}_q | f(c) = 0\}$ y $T_1 = \{c \in \mathbb{F}_q | g(c) = 1\}$.

Demostración: Sea (x_0, y_0) una solución de $y^m = f(x)$. Si $y_0 = 0$, entonces $x_0 \in T_0$ y por tanto el número de soluciones de la forma $(x_0, 0)$ es $|T_0|$. Si $y_0 \neq 0$, entonces $f(x_0) \neq 0$ y, como $\mathbb{F}_q^*$ es cíclico, $f(x_0)$ es una m-ésima potencia si y sólo si $g(x_0) = f(x_0)^{(q-1)/m} = 1$. Si $g(x_0) = 1$, entonces hay m elementos $y_0 \in \mathbb{F}_q$ tales que $y_0 = f(x_0)$. Por lo tanto $N = |T_0| + m|T_1|$.

■

Lema 3.37 *El número de raíces en $\mathbb{F}_q$ de un polinomio $f \in \mathbb{F}_q[x]$ viene dado por el grado del polinomio $g(x) = \gcd(f(x), x^q - x)$.*

Demostración: El polinomio $x^q - x$ factoriza en $\mathbb{F}_q[x]$ en todos los factores lineales distintos de la forma $x - a$, $a \in \mathbb{F}_q$, por lo tanto el máximo común divisor de f y $x^q - x$ está formado por aquellos factores $x - a$ tales que $x - a \mid f$, es decir, sus raíces en $\mathbb{F}_q$.

■

El algoritmo usado para calcular el número de puntos de las curvas se basa en calcular el máximo común divisor de $x^q - x$ y $(x^4 - ax)^{(q-1)/3}$, ya que en todos los casos en los que no conocemos el número de puntos se tiene que el cardinal del cuerpo es congruente con 1 modulo 3, y por tanto estamos en las hipótesis del Lema 3.36.

Los resultados obtenidos son:

$p \equiv 1 \pmod 9$. El tipo de todas las curvas es *ord.*
$p \equiv 4 \pmod 9$. El tipo de todas las curvas es *1/3.*
$p \equiv 7 \pmod 9$. El tipo de todas las curvas es *1/3.*
$p \equiv 8 \pmod 9$. El tipo de todas las curvas es *ss.*

3.4.2 Las curvas $y^3 = x^4 - a$

El objeto de estudiar está nueva familia de curvas, i.e., las curvas de la forma $y^3 = x^4 - a$, $a \in \{1, \ldots, p-1\}$, se basa en tratar de encontrar ejemplos de los tipos *0* y *0-0*, ya que en la anterior familia no se encontraban estos tipos. Para ello empezamos calculando unos ejemplos sobre primos pequeños, con la suerte de encontrar los dos casos que nos faltan en los primeros primos considerados: $p = 5, 7$.

Observación 3.38 En realidad, igual que antes, las curvas que consideramos son las proyectivizadas de esa familia, es decir, las curvas de la forma $zy^3 = x^4 - az^4$. Todas estas curvas tienen un único punto en el infinito, ya que si $z = 0$, entonces la ecuación queda $x^4 = 0$ y el único punto proyectivo que está en la curva es el $[0, 1, 0]$. Además se tiene que la derivada con respecto a z evaluada en el punto del infinito vale 1, por lo que el punto del infinito de todas las curvas es no singular. Por lo tanto, sólo consideraremos las ecuaciones afines teniendo siempre en cuenta que hay un punto más en el infinito.

Proposición 3.39 Sea $p \neq 2, 3$, entonces las curvas $C \equiv y^3 = x^4 - a$ son lisas y por tanto de género tres(por ser un polinomio de grado cuatro).

Demostración: Se tiene que:

$$\frac{\partial C}{\partial y} = 3y^2 = 0 \Leftrightarrow y = 0 \ (p \neq 3)$$

y, por tanto, la coordenada x de un punto singular es un cero de $x^4 - a$ y de su derivada, es decir, un cero doble. Como el polinomio $x^4 - a$ no tiene ceros dobles $(p \neq 2)$, no existen puntos singulares y la curva es lisa.

■

1. ***Caso*** $p = 5$.

Observación 3.40 Como $5 \equiv 2 \pmod 3$, podemos usar el corolario 3.25, y obtener que:

$$N_1 = p + 1 \qquad\qquad N_3 = p^3 + 1$$

con lo que según la tabla 3.20

$$C \text{ es ss si } N_2 \equiv 1 \pmod p \qquad ó \qquad C \text{ es 0-0 si } N_2 \not\equiv 1 \pmod p.$$

Observación 3.41 Para $p = 5$ se tiene que $y^3 = x^4 - a \simeq y^3 = x^4 + a$ sobre $\mathbb{F}_{p^2}$, donde el isomrfimo viene dado por:

$$x \mapsto i^{1/2}x \qquad\qquad y \mapsto -y$$

ya que $i \in \mathbb{F}_p$ y por tanto $i^{1/2} \in \mathbb{F}_{p^2}$. Por lo tanto sólo tenemos dos curvas no isomrfas como mucho, las que tienen $a = 1$ ó $a = 2$.

Con el mismo algoritmo usado para la otra familia, ya que $5^2 \equiv 1 \pmod 3$, se obtiene que las dos curvas son de tipo *0-0*.

2 ***Caso*** $p = 7$.

En este caso, aplicando el algoritmo de la sección anterior, ya que $7 \equiv 1 \pmod 3$, a las tres extensiones que tenemos que calcular y a las seis curvas, obtenemos que todas ellas pertenecen al tipo *0*.

Bibliografía

[1] P. Berthelot: *Slopes of Frobenius in cristalline cohomology*, Proceedings of Symposia in Pure Maths. Volume **29** (1975), p. 315-328.

[2] P. Berthelot & A. Ogus: *Notes on cristalline cohomology*, Mathematical notes. Princeton University Press. 1978.

[3] A. Chambert-Lior: *Cohomologie Cristalline: un Survol*, Expositiones Mathematicae **16** (1998), p. 333-382.

[4] G. van der Geer: *Curves over Finite Fields and Codes*, Proceedings 3rd European Congress of Math., Barcelona 2000 (to appear Birkhäuser).

[5] P. Griffiths & J. Harris: *Principles of algebraic geometry*, Pure & Applied mathematics. A Wiley-Interscience publication. 1978.

[6] G. van der Geer & M. van der Vlugt: *On the existance of supersingular curves of given genus*, Journal für die Reine und angewandte Math. **458** (1995), p. 53-61.

[7] R. Hartshorne: *Algebraic geometry*, GTM **52**, Springer, 1977.

[8] N. Katz: *Slope filtration of F-crystals*, Journées de Géométrie algébrique de Rennes, Asterisque **63**, Soc. Math. France (1979), p. 113-164.

[9] N. Koblitz: *p-adic Numbers, p-adic Analysis, and Zeta-Functions. Second Edition*, GTM **58**, Springer-Verlag, 1984

[10] R. Lidl & H.Ñiederreiter: *Finite Fields*, Encyclopedia of mathematics and its applications, volume **20**, Cambridge University Press, 1997.

[11] Yu. I. Manin: *The theory of commutative formal groups over fields of finite characteristic*, Russian Math. Surveys **18** (1963), p. 1-80.

[12] B. Mazur: *Frobenius and the Hodge filtration*, Bull. Amer. Math. Soc. **78** (1972), p. 653-667.

[13] B. Mazur: *Frobenius and the Hodge filtration (estimates)*,Ann. Math. Volume **98** (1973), p. 58-95.

[14] A. Ogus: *F-Crystals, Griffiths transversality, and the Hodge decomposition*, Astérisque **221**, Société Mathématique de France, 1994.

[15] J. Silverman: *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, 1986.